

ECN330-switch User Guide

EDA

Ethernet Layer 3 Switch



ECN330-switch User Guide

EDA

Ethernet Layer 3 Switch

Copyright

© Ericsson AB - 2006 All Rights Reserved

Disclaimer

No part of this document may be reproduced in any form without the written permission of the copyright owner.

The contents of this document are subject to revision without notice due to continued progress in methodology, design and manufacturing. Ericsson shall have no liability for any error or damage of any kind resulting from the use of this document.

Abstract

This document describes the ECN330 (Ethernet Controller Node) Layer 3 Switch and provides an overall knowledge about the product.

Trademark list

Windows

Windows is a registered trademark of Microsoft Corporation

Contents

1	Introduction to this Guide	1
1.1	Conventions	2
1.2	Revision History	2
2	Introduction to the ECN330-switch	5
2.1	Overview	5
2.2	Hardware Description	7
2.3	LEDs User Interface	11
2.4	Fan Tray	13
2.5	Features and Benefits	14
3	Maintenance	17
3.1	Replacing a Fuse	17
3.2	Replacing a Fan Tray	18
4	Management Features Overview	21
4.1	Key Features	21
4.2	Description of Features	23
4.3	System Defaults	30
5	Initial Configuration	35
5.1	Managing System Files	35
5.2	Connecting to the ECN330-switch	36
5.3	Basic Configuration	39
6	Configuring the ECN330-switch	51
6.1	Accessing the Management Interface	51
6.2	Navigating the Web Browser Interface	52
6.3	System Management Configuration	69
6.4	Simple Network Management Protocol	106

6.5	User Authentication	126
6.6	Access Control Lists	156
6.7	Port Configuration	184
6.8	Power Over Ethernet Settings	221
6.9	Address Table Settings	227
6.10	Spanning Tree Algorithm Configuration	231
6.11	Ethernet Automatic Protection Switching Configuration	258
6.12	VLAN Configuration	272
6.13	Layer 2 over MPLS Configuration	314
6.14	Class of Service Configuration	324
6.15	Quality of Service	342
6.16	Multicast Filtering	352
6.17	Configuring Domain Name Service	370
6.18	Dynamic Host Configuration Protocol	376
6.19	Configuring Router Redundancy	387
6.20	IP Routing	397
6.21	Multicast Routing	469
7	Command Line Interface	515
7.1	Using the Command Line Interface	515
7.2	Entering Commands	518
7.3	Command Groups	528
7.4	General Commands	531
7.5	System Management Commands	540
7.6	Simple Network Management Protocol Commands	608
7.7	User Authentication Commands	632
7.8	Access Control List Commands	690
7.9	Interface Commands	736
7.10	Link Aggregation Commands	756
7.11	Mirror Port Commands	773
7.12	Rate Limit Commands	776

7.13	Power over Ethernet Commands	778
7.14	Address Table Commands	786
7.15	Spanning Tree Algorithm Commands	794
7.16	Ethernet Automatic Protection Switching Commands	824
7.17	VLAN Commands	841
7.18	Layer 2 over MPLS Commands	890
7.19	Class of Service Commands	897
7.20	Quality of Service Commands	921
7.21	Multicast Filtering Commands	935
7.22	Domain Name Service Commands	963
7.23	Dynamic Host Configuration Protocol Commands	974
7.24	Router Redundancy Commands	998
7.25	IP Interface Commands	1015
7.26	IP Routing Commands	1028
7.27	Multicast Routing Commands	1103
8	Upgrading Firmware	1167
9	Troubleshooting	1171
9.1	Diagnosing ECN330 Indicators	1171
9.2	Power and Cooling Problems	1172
9.3	Installation	1172
9.4	Problems Accessing the Management Interface	1173
10	Specifications	1175
10.1	Physical Characteristics	1175
10.2	Compliances	1176
10.3	Switch Features	1177
10.4	Management Features	1177
10.5	Standards	1179

List of Abbreviations	1183
Glossary	1191
Index	1201

1 Introduction to this Guide

This guide describes the ECN330 Ethernet Layer 3 switch. It describes the hardware, functionality and installation process. Furthermore, it provides an overview of the software features, and detailed information on how to use the Command Line Interface (CLI) to configure the ECN330-switch.

This guide is intended for both installers and system administrators responsible for operating and maintaining network equipment. For reading and using the management and CLI sections, a basic working knowledge of general switch functions, the Internet Protocol (IP), and Simple Network Management Protocol (SNMP) is needed. This guide does not attempt to give a complete explanation of different standards (for example spanning tree), but rather their implementation in the ECN330-switch. For a more comprehensive knowledge and understanding of the standards, please refer to the standards.

This section gives a short introduction to this guide.

Section 2 on page 5 provides an overview of the switch system and its functionality.

Section 3 on page 17 describes maintenance tasks.

Section 4 on page 21 provides an overview of the switch's management features.

Section 5 on page 35 describes initial configuration options and other basic system information.

Section 6 on page 51 describes how to configure the switch's software features and provides details on the web user interface.

Section 7 on page 515 describes how to use the switch's CLI and provides details on all available commands.

Section 8 on page 1167 describes how to download switch software updates.

Section 9 on page 1171 discusses troubleshooting issues.

Section 10 on page 1175 provides the technical specifications of the ECN330-switch.

1.1 Conventions

The following conventions apply for textual instructions (not screen dumps):

Bold monospace letters mark text typed by the user (input) in Command Line Interface (CLI).

Regular monospace letters mark text output in a CLI.

<*ServerIP*> is a parameter (argument) that should be replaced with the actual value (for example, the IP address of a server). The <> symbols are not typed.

[*argument*] the brackets indicate that this argument is optional and can be omitted. If used, the brackets are not typed.

{*argument1*|*argument2*} means that either argument1 or argument 2 can be used as a value for this parameter.

1.2 Revision History

This guide is valid for EDA 2.2 MA2. Other product versions, which include functions not described in this guide, may be available.

1.2.1 This Version

This is the fourth version of this guide. It includes the following changes:

- Added information on RFC3014 Notification Log MIB, section 10.4.

1.2.2 Version C

This is the third version of this guide. It includes the following changes:

- Configuring Interface Connections, section 6.7.2 – Added information to clarify the use of auto-negotiation for Gigabit Ethernet ports.
- Setting IGMP Snooping Status per Interface, section 6.16.2.6.

- Added information to clarify the use of auto-negotiation for Gigabit Ethernet ports in section 7.9.3 - section 7.9.6.
- ip igmp snooping (Interface Configuration), section 7.21.2

1.2.3

Version B

This is the second version of this guide. It includes the following changes:

- Access Control List in section 4.1 and section 6.6.1 – Changed the number of allowed ACL rules.
- Local and remote engine ID in section 6.4.4.1, section 6.4.4.2 and section 7.6.8 – Changed the allowed string length for the engine ID to 10 - 64 characters.
- SNMPv3 group in section 6.4.4.5 and section 7.6.12 – Changed the allowed string length for Read View, Write View and Notify View to 16 characters.
- SNMPv3 view in section 6.4.4.6 and section 7.6.10 – Changed the allowed string length for view name to 16 characters.
- Ethernet Automatic Protection Switching Configuration, section 6.11 – A note was added to the end of the Functional Description.
- Creating VLANs, section 6.12.1.7 – Changed the number of allowed VLANs to 4094.
- MPLS uplink port in section 6.13.2 and section 7.18.1 – Changed the allowed port range to 1-27.
- Configuring a Class Map, section 6.15.1.1 – Changed the maximum string length for Class Name to 16 characters, and the maximum string length for the description of this parameter to 64 characters.
- Creating QoS Policies, section 6.15.1.2 – Changed the maximum string length for Policy Name to 16 characters, and the maximum string length for the description of this parameter to 64 characters.
- Configuring IGMP Snooping and Query Parameters, section 6.16.2.1 – Added a note to Command Usage.
- Displaying Multicast Group Information, section 6.16.3.2 – Add a note to Command Usage.

- class-map, section 7.20.1 – Changed the maximum string length for class-map-name to 16 characters.
- policy-map, section 7.20.3 – Changed the maximum string length for policy-map-name to 16 characters.
- show ip igmp groups, section 7.21.23 – Changed the displayed default value for V1Timer to 260 seconds.

1.2.4 Version A

This is the first version of this guide.

2 Introduction to the ECN330-switch

2.1 Overview

The Ericsson ECN330-switch is an Ethernet Layer 3 switch that contains 24 100BASE-TX ports, and 3 1000BASE-T ports, two of which are combo ports — 1000BASE-T RJ45 ports with associated Small Form Factor Pluggable (SFP) transceiver slots that operate as an alternate media connection.

The ECN330-switch is used as second level aggregation switch in the EDA network.

As well as its Power-over-Ethernet capabilities, the ECN330-switch provides comprehensive network management features, such as Spanning Tree Protocol, multicast switching, virtual LANs, IP routing, and Layer 2/3/4 CoS services that provide reliability and consistent performance for network traffic.

Figure 1 shows the front and rear panels of the ECN330.

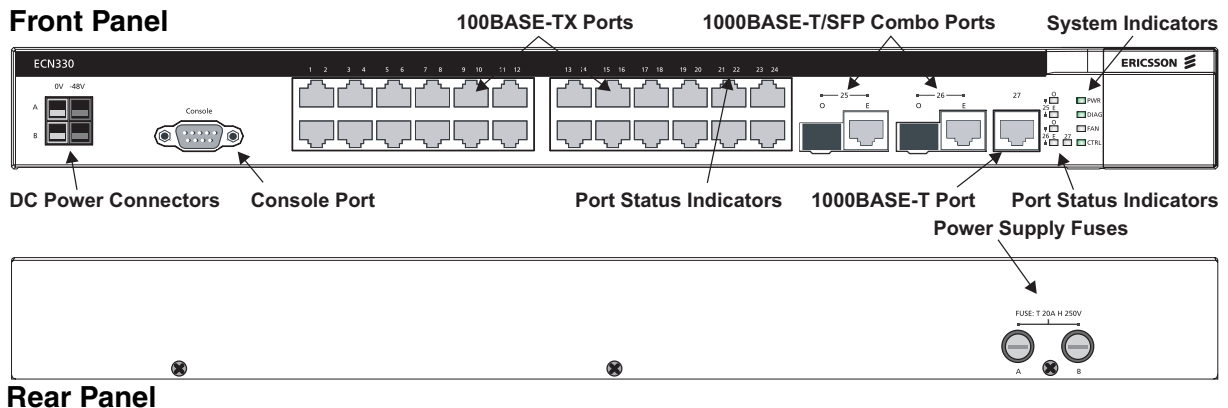


Figure 1 ECN330 Front and Rear Panels

2.1.1 Switch Architecture

The ECN330-switch employs a wire-speed, non-blocking switching fabric. This permits simultaneous wire-speed transport of multiple packets at low latency on all ports. The ECN330-switch also features full-duplex capability on all ports, which effectively doubles the bandwidth of each connection.

For communications within the same VLAN, the ECN330-switch uses store-and-forward switching to ensure maximum data integrity. With this type of switching, the entire packet must be received into a buffer and checked for validity before being forwarded. This prevents errors from being propagated throughout the network. For communications between different VLANs, the ECN330-switch also performs store-and-forward checking on each packet crossing the switch, routing traffic at wire speed using RIP or OSPF for unicast traffic, and DVMRP or PIM for multicast traffic.

2.1.2 Management Options

The ECN330-switch contains a comprehensive array of LEDs for “at-a-glance” monitoring of network and port status. It also includes a management agent that enables configuration and monitoring of the ECN330-switch using its embedded management software or through SNMP applications. The ECN330-switch can be managed by making a direct connection to the RS-232 console port or by connecting to the switch through a network connection using Telnet or network management software.

For a detailed description of the ECN330-switch’s management features, see section 4 on page 21.

2.1.2.1 Management of ECN330 and ECN330-switch

The ECN330 includes a Single Board Computer (SBC) and an ECN330-switch. The SBC is connected to the Gigabit Ethernet port 28 of the ECN330-switch.

When the SBC is enabled (see “Enabling the SBC to Access Advanced Management Tools” on page 74), the SBC provides a management proxy functionality, where management of embedded nodes including the ECN330-switch is done by the SBC which is managed by PEM. Note that when the SBC is enabled, the console interface is set to SBC display mode.

When the SBC is disabled, the ECN330 runs in ECN330-switch mode.

2.2 Hardware Description

2.2.1 Power-over-Ethernet Ports

All of the 24 10BASE-T/100BASE-TX RJ45 ports support PoE capability and can supply up to 23.1 W per port to connected EDA nodes.

The PoE enables DC power to be supplied to the connected nodes through the Ethernet cable. IP DSLAMs attached to a port can directly draw power from the ECN330-switch over the Ethernet cable without requiring a separate power source. The ECN330-switch automatically detects an EDA node by its authenticated PoE signature and senses its required load before turning on DC power to the port. An electrical port of ESN108 (which is also a PoE node) can also be connected to the ECN330-switch. The sense circuit in both nodes (ECN330 and ESN108) will sense that no power is required. This detection mechanism also prevents damage to other network equipment that is not an EDA node.

The ECN330-switch delivers power to the IP DSLAM using the two wire pairs in UTP or STP CAT 5 cable that are not used for 10BASE-T/100BASE-TX connections (for details see the *ECN330 Installation Guide*). Each line is 100% individually controlled with an auto-detect circuit that opens up if a load within the EDA-specified range is detected, and shuts down if the load exceeds the limit of 23.1 W. Each line is filtered for surge currents and has a 4 ms backup reservoir, should short voltage dropouts occur.

The ECN330-switch can provide up to 600 mA continuously on each 10/100 Mbps port, or up to 23.1 W of power. However, taking into account some power loss over the cable run, the amount of power that can be delivered to an EDA node is about 21 W. If a device draws more than 625 mA from a port, an overload condition occurs and the port turns off the power.

These ports also support automatic MDI/MDI-X operation, so straight-through cables can be used for all network connections to PCs or servers, or to other switches or hubs.

The ports also support auto-negotiation, so the optimal transmission mode (half or full duplex), and data rate (10 or 100 Mbps), or flow control method (IEEE 802.3x, Back-Pressure or none) can be selected automatically, if this feature is also supported by the attached device. If a device connected to one of these ports does not support auto-negotiation, the correct speed will be sensed by the port, but the transmission mode will by default be half duplex.

Each port also supports auto-negotiation of flow control, so the ECN330-switch can automatically prevent port buffers from becoming saturated.

The ECN330-switch controls the power and data on a port independently. Power can be requested from a device that already has a data link to the ECN330-switch-switch. In addition, the ECN330-switch can supply power to a device even if the port's data connection has been disabled. The power on a port is continuously monitored by the ECN330-switch and it will be turned off as soon as a device connection is removed.

Note: The 1000BASE-T RJ45 ports do not support PoE capability.

2.2.2 1000BASE-T RJ45 Ports and SFP Slots

The ECN330 contains two combo Gigabit RJ45 ports with shared Small Form Factor Pluggable (SFP) transceiver slots (Ports 25-26). In its default configuration, if an SFP transceiver (purchased separately) is installed in a slot and has a valid link on its port, the associated RJ45 port is disabled and cannot be used. The ECN330-switch can also be configured to force the use of an RJ-45 port or SFP slot, as required.

SFP is a new specification for compact, modular transceivers that are hot swappable. The SFP slots support 100BASE-FX, 1000BASE-SX, 1000BASE-LX, or 1000BASE-LH transceivers for fiber optic connections to remote devices.

The ECN330 also contains one independent 1000BASE-T RJ45 port (Port 27) that operates at 10 Mbps or 100 Mbps, half or full duplex, or at 1000 Mbps, full duplex. Because all of the Gigabit RJ45 ports support automatic MDI/MDI-X operation, straight-through cables can be used for all network connections to PCs or servers, or to other switches or hubs. (For more information, refer to the *ECN330 Installation Guide*.)

The 1000BASE-T RJ45 ports support auto-negotiation, so the optimum optimum transmission mode (half or full duplex), and data rate (10, 100, or 1000 Mbps) can be selected automatically. If a device connected to one of these ports does not support auto-negotiation, the communication mode of that port can be configured manually.

Each port also supports auto-negotiation of flow control, so the ECN330-switch can automatically prevent port buffers from becoming saturated.

Note: The 1000BASE-T RJ45 ports do not support PoE capability.

2.2.3 Power Supply Input Connectors

The dual power supply input connectors are located on the front panel of the ECN330. The standard power supply for the ECN330 is -48 VDC, which includes protection through a disposable fuse on the rear panel. Power redundancy can be established by connecting both power inputs.

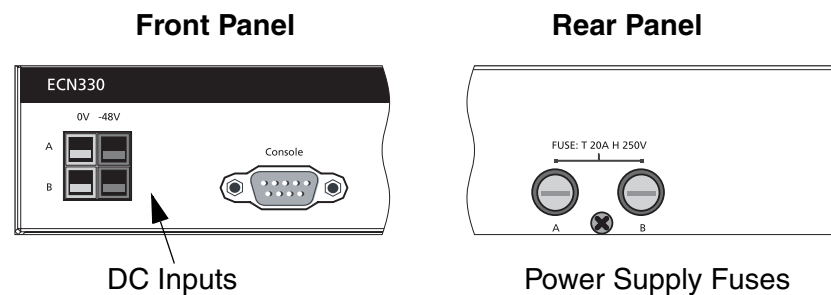


Figure 2 Power Supply Input Connectors and Fuses

2.2.4 Console Port Pin Assignments

The DB-9 serial port on the ECN330's front panel is used to connect to the switch for out-of-band console configuration. The command line configuration program can be accessed from a terminal or a PC running a terminal emulation program. The pin assignments used to connect to the serial port are provided in Tables 1 and 2 on page 10, and Table 3 on page 10.

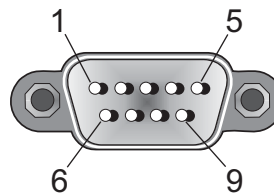


Figure 3 Console Port Pin Assignments

Table 1 DB-9 Port Pin Assignments

EIA Circuit	CCITT Signal	Description	ECN330's DB9 DTE Pin #	PC DB9 DTE Pin #	PC DB25 DTE Pin #
BB	104	RxD (Received Data)	2	2	3
BA	103	TxD (Transmitted Data)	3	3	2
AB	102	SG (Signal Ground)	5	5	7

No other pins are used.

Table 2 Console Port to 9-Pin DTE Port

ECN330's 9-Pin Serial Port	Null Modem	PC's 9-Pin DTE Port
2 RXD	<-----TXD -----	3 TXD
3 TXD	-----RXD ----->	2 RXD
5 SGND	-----SGND -----	5 SGND

No other pins are used.

Table 3 Console Port to 25-Pin DTE Port

ECN330's 9-Pin Serial Port	Null Modem	PC's 25-Pin DTE Port
2 RXD	<-----TXD -----	2 TXD
3 TXD	-----RXD ----->	3 RXD
5 SGND	-----SGND -----	7 SGND

No other pins are used.

2.3 LEDs User Interface

The unit also includes a display panel for key system and port indications that simplify installation and network troubleshooting. The LEDs, which are located on the front panel for easy viewing, are shown in Figure 4 and described in Table 4 on page 11.

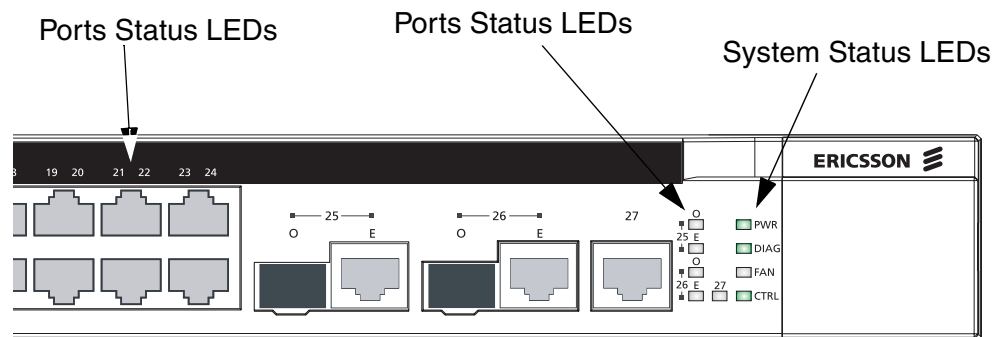


Figure 4 System and Port Status LEDs

Table 4 System and Port Status LEDs

LED	Condition	Status
System Status		
PWR	Steady Green	The unit's internal power supply is operating normally.
	Steady Red	The unit's internal power supply is not operating normally.
	Off	The unit has no power connected.

LED	Condition	Status
DIAG	Steady Green	The system diagnostic test has completed successfully.
	Flashing Green	The system diagnostic test is in progress.
	Steady Red	The system diagnostic test has detected a fault in the ECN330
FAN	Steady Red	One or both cooling fans have failed.
	Off	The unit's cooling fans are operating normally.
CTRL	Flashing Green (fast)	ENC self test and boot in progress (during start)
	Steady Green	ENC in normal operation
	Steady Red	Error in ENC (Fallback state and when booting)
	Off	ENC not present
10/100 Mbps Ports		
Ports 1~24 (Link/Activity)	Steady or Flashing Green	Port has established a valid 10 or 100 Mbps network connection. Flashing indicates activity.
	Flashing Red	Port has detected a power overload or short circuit and shut down the port's power.
	Off	There is no valid link on the port.

LED	Condition	Status
Gigabit Combo Ports		
Ports 25, 26 (E - RJ45), (O - SFP)	Steady or Flashing Green	Port has established a valid 10, 100, or 1000 Mbps network connection. Flashing indicates activity.
	Off	There is no valid link on the port.
10/100/1000 Mbps Ports		
Port 27 (Link/Activity)	Steady or Flashing Green	Port has established a valid 10, 100, or 1000 Mbps network connection. Flashing indicates activity.
	Off	There is no valid link on the port.

2.4 Fan Tray

The ECN330 contains one removable fan tray located behind a front-panel access cover on the right side of the unit, see Figure 5 on page 13. The fan tray includes two fans for cooling the ECN330. A front-panel LED indicates if one or both fans have failed, in which case, the fan tray should be replaced.



Figure 5 Fan Tray

2.5 Features and Benefits

2.5.1 Connectivity

- 24 dual-speed ports for 10 or 100 Mbps Ethernet connections. All 10/100 Mbps RJ45 ports support Power-over-Ethernet (PoE)
- One independent 10/100/1000BASE-T Gigabit Ethernet port.
- Two Gigabit combo ports—use either 10/100/1000BASE-T RJ45 ports or Small Form Factor Pluggable (SFP) transceiver slot (100 Mbps and 1000 Mbps)
- Auto-negotiation enables each RJ45 port to automatically select the optimum communication mode (half or full duplex) and speed (10 Mbps, 100 Mbps, or 1000 Mbps) if this feature is supported by the attached device; otherwise the port can be configured manually.
- All RJ45 ports support auto MDI/MDI-X pinout selection.
- Unshielded (UTP) cable supported on all RJ45 ports: Category 3 or better for 10 Mbps connections, Category 5 or better for 100 Mbps connections, and Category 5, 5e, or 6 for 1000 Mbps connections.
- IEEE Std 802.3-2002 Ethernet, Fast Ethernet, and Gigabit Ethernet compliance ensures compatibility with standards-based hubs, network cards and switches from any vendor.

2.5.2 Expandability

- Supports 1000BASE-SX, 1000BASE-LX, 1000BASE-LH, and other SFP-compatible transceivers.

2.5.3 Performance

- Transparent bridging
- Aggregate bandwidth of up to 10.8 Gbps
- Packet capacity 8.9 Mpps (million packets per second)
- Switching table with a total of 16K MAC address entries and 4K IP address entries

- Wire-speed performance when switching for intra-VLAN traffic at Layer 2 or routing for inter-VLAN traffic at Layer 3
- Supports flow control, using back pressure for half duplex and IEEE 802.3x for full duplex
- Broadcast storm control
- The ECN330-switch supports up to 4094 tagged Service VLANs (VLANs used for End-user traffic) based on the IEEE 802.1Q standard.
- Multicast Switching based on IGMP Snooping
- Link redundancy supported with Multiple Spanning Tree (MSTP)
- Link aggregation by utilizing LACP
- Layer 2 tunneling with QinQ or L2MPLS
- EAPS for increased availability of Ethernet rings
- Layer 2, 3 and 4 port priority settings, plus Differentiated Services

2.5.4 Management

- “At-a-glance” LEDs for easy troubleshooting
- Network management agent:
 - Manages ECN330-switch in-band or out-of-band
 - Supports Telnet, SSH, SNMP/RMON and web-based interface

3 Maintenance

3.1 Replacing a Fuse

Each ECN330 DC power supply is protected by a disposable fuse, which is located on the rear panel (please refer to Figure 1 on page 5). If needed, replace it with a new 20 A, 250 V fuse.

Warning!

First power off the ECN330 before replacing a DC power supply fuse.

To replace a fuse, follow these steps:

1. Remove the -48 VDC power source from the ECN330.
2. Unscrew the fuse holder counter-clockwise from its socket. Pull out the blown fuse and discard it.
3. Insert a new 20 A, 250 V fuse into the fuse holder and then screw the holder clockwise back into the fuse socket.
4. Reconnect the -48 VDC power source to the ECN330.

3.2 Replacing a Fan Tray

The fan tray should be replaced if the FAN status LED turns on red (a cooling fan in the fan tray has failed).

Caution!

To ensure proper cooling of the ECN330, both fans must be operational. If one fan fails the ECN330 will continue to run, but the fan tray should be replaced as soon as possible.

The ECN330's fan tray can be completely removed without powering off the unit. To replace a fan tray, follow these steps:

1. Remove the fan tray plastic access cover on the right side of the ECN330's front panel by pulling the cover's right edge out, until it becomes free.

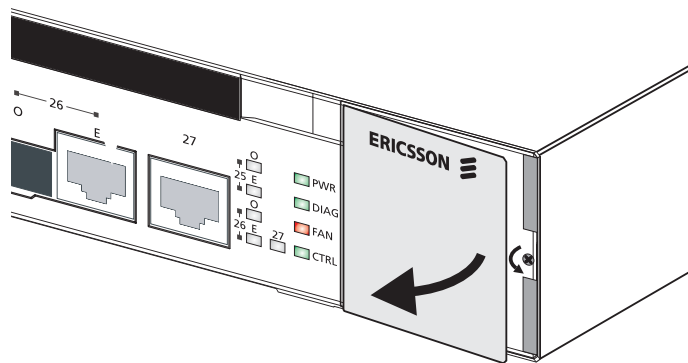


Figure 6 Fan Tray Access

2. Unscrew the fan tray's screw.
3. Grasp the fan-tray's handle and pull it outward to disconnect it from the ECN330. Carefully slide the fan tray out of the ECN330.

Caution!

The new Fan tray must be inserted immediately after the old one is removed.

4. Install a new fan tray in the ECN330 by sliding it back into the empty slot. Push in firmly so that the fan tray's connector is fully engaged with the ECN330.
5. Screw and tighten the fan tray's screw.
6. Check that the FAN status LED on the ECN330 front panel is off and that both new fans are running.
7. Replace the fan tray access cover on the ECN330 front panel by pushing the cover's right edge in until it snaps into place.

4 Management Features Overview

The ECN330-switch provides a broad range of features for Layer 2 switching and Layer 3 routing. It includes a management agent that enables features listed in this guide to be configured. The default configuration can be used for most of the features provided by the ECN330-switch. However, there are many options that can be configured to maximize the ECN330-switch's performance for a particular network environment.

4.1 Key Features

Table 5 Key Features

Feature	Description
Configuration Backup and Restore	Backup to TFTP server
Authentication	Console, Telnet, web – User name / password, RADIUS, TACACS+ Web – HTTPS Telnet – SSH SNMP v1/2c - Community strings SNMP version 3 – MD5 or SHA password Port – IEEE 802.1X, MAC address filtering
Access Control Lists	Supports up to 32 IP, MAC or VLAN ACLs: Fast Ethernet ports – 193 rules, 2 masks shared by 8-port groups Gigabit Ethernet ports – 65 rules, 2 masks VLANs – One IP or MAC ACL per VLAN, 1 mask
DHCP Client, Relay and Server	Supported

Feature	Description
DNS	Client and proxy service
Port Configuration	Speed, duplex mode and flow control
Rate Limiting	Input and output rate limiting per port
Port Mirroring	Single session, one source port to one analysis port
Port Trunking	Supports up to 13 trunks using either static or dynamic trunking (LACP)
Broadcast Storm Control	Supported
Address Table	Up to 16K MAC addresses in the forwarding table, 1024 static MAC addresses; Up to 4K IP address entries in the ARP cache, 1K static IP routes
IEEE 802.1D Bridge	Supports dynamic data switching and addresses learning
Store-and-Forward Switching	Supported to ensure wire-speed switching while eliminating bad frames
Spanning Tree Algorithm	Supports standard STP, Rapid Spanning Tree Protocol (RSTP), and Multiple Spanning Trees (MSTP)
Virtual LANs	Up to 4094 using IEEE 802.1Q, port-based, private VLANs, protocol VLANs, and QinQ tunneling
Traffic Prioritization	Default port priority, traffic class map, queue scheduling, IP Precedence, or Differentiated Services Code Point (DSCP), and TCP/UDP Port
Quality of Service	Supports Differentiated Services (DiffServ)
Router Redundancy	Router backup is provided with the Virtual Router Redundancy Protocol (VRRP)
IP Routing	Routing Information Protocol (RIP), Open Shortest Path First (OSPF), static routes

Feature	Description
ARP	Static and dynamic address configuration, proxy ARP
Multicast Filtering	Supports IGMP snooping and query for Layer 2, and IGMP for Layer 3
Multicast Routing	Supports DVMRP, PIM-DM, and PIM-SM
Tunneling	Supports tunneling with IEEE 802.1Q tunneling (QinQ) or L2MPLS
EAPS	Supports Ethernet Automatic Protection Switching for increased availability of Ethernet rings (RFC3619)
Power over Ethernet	Powers attached devices using Power over Ethernet (PoE)

4.2 Description of Features

The ECN330-switch provides a wide range of advanced performance-enhancing features. Flow control eliminates the loss of packets due to bottlenecks caused by port saturation. Broadcast storm suppression prevents broadcast traffic storms from engulfing the network. Port-based (untagged), tagged and protocol-based VLANs, plus support for automatic registration of VLANs using GARP VLAN Registration Protocol (GVRP), provides traffic security and efficient use of network bandwidth. CoS priority queueing ensures the minimum delay for moving real-time multimedia data across the network. While multicast filtering and routing provides support for real-time network applications. The following is a brief description of some of the key management features.

Configuration Backup and Restore – The current configuration settings can be saved to a file on a TFTP server, and later download this file to restore the ECN330-switch configuration settings.

Authentication – The ECN330-switch authenticates management access through the console port, Telnet or web browser. User names and passwords can be configured locally or can be verified using a remote authentication server (RADIUS or TACACS+). Port-based authentication is also supported through the IEEE 802.1X protocol. This protocol uses Extensible Authentication Protocol

over LANs (EAPOL) to request user credentials from the 802.1X client, and then uses the EAP between the ECN330-switch and the authentication server to verify the client's right to access the network through an authentication server (RADIUS server).

Other authentication options include HTTPS for secure management access using the web, SSH for secure management access over a Telnet-equivalent connection, SNMP Version 3, IP address filtering for SNMP/web/Telnet management access, and MAC address filtering for port access.

Access Control Lists (ACL) – ACLs provide packet filtering for IP frames (based on address, protocol, TCP/UDP port number or TCP control code) or any frames (based on MAC address or Ethernet type). ACLs can be used to improve performance by blocking unnecessary network traffic or to implement security controls by restricting access to specific network resources or protocols.

DHCP Server and DHCP Relay – A DHCP server is provided to assign IP addresses to host devices. Since DHCP uses a broadcast mechanism, a DHCP server and its client must physically reside on the same subnet. Since it is not practical to have a DHCP server on every subnet, DHCP Relay is also supported to allow dynamic configuration of local clients from a DHCP server located in a different network.

Port Configuration – The speed, duplex mode, and flow control can be manually configured for use on specific ports, or auto-negotiation can be used to detect the connection settings used by the attached device. Use the full-duplex mode on ports whenever possible to double the throughput of switch connections. Flow control should also be enabled to control network traffic during periods of congestion and prevent the loss of packets when port buffer thresholds are exceeded. The ECN330-switch supports flow control based on the IEEE 802.3-2002 standard.

Rate Limiting – This feature controls the maximum rate for traffic transmitted or received on an interface. Rate limiting is configured on interfaces at the edge of a network to limit traffic into or out of the network. Traffic that falls within the rate limit is transmitted, while packets that exceed the acceptable amount of traffic are dropped.

Port Mirroring – The ECN330-switch can unobtrusively mirror traffic from any port to a monitor port. A protocol analyzer or RMON probe can be connected to this port to perform traffic analysis and verify connection integrity.

Port Trunking – Ports can be combined into an aggregate connection. Trunks can be manually set up or dynamically configured using IEEE 802.3-2002 (formerly IEEE 802.3ad) Link Aggregation Control Protocol (LACP). The additional ports dramatically increase the throughput across any connection, and provide redundancy by taking over the load if a port in the trunk should fail. The ECN330-switch supports up to 13 trunks.

Broadcast Storm Control – Broadcast suppression prevents broadcast traffic from overwhelming the network. When enabled on a port, the level of broadcast traffic passing through the port is restricted. If broadcast traffic rises above a pre-defined threshold, it will be throttled until the level falls back beneath the threshold.

Static Addresses – A static address can be assigned to a specific interface on the ECN330-switch. Static addresses are bound to the assigned interfaces and will not be moved. When a static address is seen on another interface, the static address will be ignored and will not be written to the address table. Static addresses can be used to provide network security by restricting access for a known host to a specific port.

IEEE 802.1D Bridge – The ECN330-switch supports IEEE 802.1D transparent bridging. The address table facilitates data switching by learning addresses, and then filtering or forwarding traffic based on this information. The address table supports up to 16K addresses.

Store-and-Forward Switching – The ECN330-switch evaluates in its memory each frame before forwarding them to another port. This ensures that all frames are a standard Ethernet size and have been verified for accuracy with the cyclic redundancy check (CRC), thus preventing bad frames from entering the network and wasting bandwidth.

To avoid dropping frames on congested ports, the ECN330-switch provides 1 MByte for frame buffering. This buffer can queue packets awaiting transmission on congested networks.

Spanning Tree Algorithm – The ECN330-switch supports the following spanning tree protocols:

- **Spanning Tree Protocol (STP, IEEE 802.1D)** – This protocol provides loop detection. When there are multiple physical paths between segments, this protocol will choose a single path and disable all others to ensure that only one route exists between any two stations on the

network. This prevents the creation of network loops. However, if the chosen path should fail for any reason, an alternate path will be activated to maintain the connection.

- **Rapid Spanning Tree Protocol (RSTP, IEEE 802.1w)** – This protocol reduces the convergence time for network topology changes to about 3 to 5 seconds, compared to 30 seconds or more for the IEEE 802.1D STP standard. It is intended as a complete replacement for STP, but can still interoperate with switches running the STP protocol, by automatically reconfiguring ports to STP-compliant mode if they detect STP protocol messages from attached devices.
- **Multiple Spanning Tree Protocol (MSTP, IEEE 802.1s)** – This protocol is a direct extension of RSTP. It can provide independent spanning trees for different VLANs. It simplifies network management, provides for even faster convergence than RSTP by limiting the size of each region, and prevents VLAN members from being segmented from the rest of the group.

Virtual LANs – The ECN330-switch supports up to 4094 VLANs. A Virtual LAN is a collection of network nodes that share the same collision domain regardless of their physical location or connection point in the network. The ECN330-switch supports tagged VLANs based on the IEEE 802.1Q standard. Members of VLAN groups can be dynamically learned through GVRP, or ports can be manually assigned to a specific set of VLANs. This enables the ECN330-switch to restrict traffic to the VLAN groups to which a user has been assigned. Segmenting a network into VLANs can:

- Eliminate broadcast storms, which severely degrade performance in a flat network.
- Simplify network management for node changes and moves by remotely configuring VLAN membership for any port, rather than having to manually change the network connection.
- Provide data security by restricting traffic to the originating VLAN, except where a connection is explicitly defined by the ECN330-switch's routing service.
- Use private VLANs to restrict traffic to pass only between data ports and the uplink ports, thereby isolating adjacent ports within the same VLAN, and limiting the total number of VLANs that need to be configured.
- Use protocol VLANs to restrict traffic to specified interfaces based on protocol type.

Traffic Prioritization – The ECN330-switch prioritizes each packet based on the required level of service, using eight priority queues with strict priority, Weighted Round Robin (WRR) or Weighted Fair Queueing (WFQ) scheduling. It uses IEEE 802.1p and 802.1Q tags to prioritize incoming traffic based on input from the end-station application. These functions can be used to provide independent priorities for delay-sensitive data and best-effort data.

The ECN330-switch also supports several common methods of prioritizing Layer 3 and 4 traffic to meet application requirements. Traffic can be prioritized based on the priority bits in the IP frame's Type of Service (ToS) octet or the number of the TCP or UDP port. When these services are enabled, the priorities are mapped to a Class of Service value by the ECN330-switch, and the traffic then sent to the corresponding output queue.

IP Routing – The ECN330-switch provides Layer 3 IP routing. To maintain a high rate of throughput, the ECN330-switch forwards all traffic passing within the same segment, and routes only traffic that passes between different subnetworks. The wire-speed routing provided by the ECN330-switch lets network segments or VLANs be easily linked together without having to deal with the bottlenecks or configuration hassles normally associated with conventional routers.

Routing for unicast traffic is supported with the Routing Information Protocol (RIP) and the Open Shortest Path First (OSPF) protocol.

- **RIP** – This protocol uses a distance-vector approach to routing. Routes are determined on the basis of minimizing the distance vector, or hop count, which serves as a rough estimate of transmission cost.
- **OSPF** – This approach uses a link state routing protocol to generate a shortest-path tree, then builds up its routing table based on this tree. OSPF produces a more stable network because the participating routers act on network changes predictably and simultaneously, converging on the best route more quickly than RIP.

Router Redundancy – Virtual Router Redundancy Protocol (VRRP) uses a virtual IP address to support a primary router and multiple backup routers. The backups can be configured to take over the workload if the master fails or to load share the traffic. The primary goal of this protocol is to allow a host device which has been configured with a fixed gateway to maintain network connectivity in case the primary gateway goes down.

Address Resolution Protocol – The ECN330-switch uses ARP and Proxy ARP to convert between IP addresses and MAC (hardware) addresses. The ECN330-switch supports conventional ARP, which locates the MAC address corresponding to a given IP address. This allows the ECN330-switch to use IP addresses for routing decisions and the corresponding MAC addresses to forward packets from one hop to the next. Either static or dynamic entries can be configured in the ARP cache.

Proxy ARP allows hosts that do not support routing to determine the MAC address of a device on another network or subnet. When a host sends an ARP request for a remote network, the ECN330-switch checks to see if it has the best route. If it does, it sends its own MAC address to the host. The host then sends traffic for the remote destination through the ECN330-switch, which uses its own routing table to reach the destination on the other network.

Quality of Service – Differentiated Services (DiffServ) provides policy-based management mechanisms used for prioritizing network resources to meet the requirements of specific traffic types on a per-hop basis. Each packet is classified upon entry into the network based on access lists, IP Precedence or DSCP values, or VLAN lists. Using access lists allows traffic to be selected based on the Layer 2, Layer 3, or Layer 4 information contained in each packet. Based on network policies, different kinds of traffic can be marked for different kinds of forwarding.

Multicast Filtering – Specific multicast traffic can be assigned to its own VLAN to ensure that it does not interfere with normal network traffic and to guarantee real-time delivery by setting the required priority level for the designated VLAN. The ECN330-switch uses IGMP Snooping and Query at Layer 2 and IGMP at Layer 3 to manage multicast group registration.

Multicast Routing – Routing for multicast packets is supported by the Distance Vector Multicast Routing Protocol (DVMRP) and Protocol-Independent Multicasting - Dense Mode and Sparse Mode (PIM-DM, PIM-SM). These protocols work in conjunction with IGMP to filter and route multicast traffic. DVMRP is a comprehensive Multicast Router method that maintains its own routing table, but is gradually being replaced by most network managers with PIM, Dense Mode and Sparse Mode. PIM is a very simple protocol that uses the routing table of the unicast routing protocol enabled on an interface. Dense Mode is designed for areas where the probability of multicast clients is relatively high, and the overhead of frequent flooding is justified. While Sparse mode is designed for network areas, such as the Wide Area Network, where the probability of multicast clients is low.

Tunneling – Configures tunnels for customer traffic crossing the service provider's network using IEEE 802.1Q or Layer 2 over MPLS.

- **IEEE 802.1Q Tunneling (QinQ)** – This feature is designed for service providers carrying traffic for multiple customers across their networks. QinQ tunneling is used to maintain customer-specific VLAN and Layer 2 protocol configurations even when different customers use the same internal VLAN IDs. This is accomplished by inserting Service Provider VLAN (SPVLAN) tags into the customer's frames when they enter the service provider's network, and then stripping the tags when the frames leave the network.
- **Layer 2 over MPLS (L2MPLS)** – This feature encapsulates Ethernet frames in MPLS packets and uses label stacking to forward them across an MPLS tunnel. Tunnel labels define the path across the MPLS network and virtual channel labels define the entry and exit points to the customer. The edge switches connected to the service provider's network add and remove these labels as appropriate for packet encapsulation.

Ethernet Automatic Protection Switching – EAPS can be used to increase the availability and robustness of Ethernet rings, e.g. used in Metropolitan Area Networks (MAN). EAPS technology converges in less than 500 ms. EAPS does not limit the number of nodes included in the ring structure. The convergence time is independent of the number of nodes in the ring.

Power over Ethernet – The ECN330-switch's 24 Fast Ethernet ports support Power-over-Ethernet (PoE) that enables DC power to be supplied to attached devices over the unused pairs of wires in the connecting Ethernet cable.

4.3 System Defaults

The ECN330-switch's system defaults are provided in the configuration file "Factory_Default_Config.cfg". To reset the ECN330-switch defaults, this file should be set as the startup configuration file. (See section 7.5.18 on page 568.)

Table 6 lists some of the basic system defaults.

Table 6 System Defaults

Function	Parameter	Default
Console Port Connection	Baud Rate	9600
	Data bits	8
	Stop bits	1
	Parity	none
	Local Console Timeout	0 (disabled)

Function	Parameter	Default
Authentication	Privileged Exec Level	Username “admin” Password “admin”
	Normal Exec Level	Username “guest” Password “guest”
	Enable Privileged Exec from Normal Exec Level	Password “super”
	RADIUS Authentication	Disabled
	TACACS Authentication	Disabled
	802.1X Port Authentication	Disabled
	HTTPS	Enabled
	SSH	Disabled
	Port Security	Disabled
	IP Filtering	Disabled
Web Management	HTTP Server	Enabled
	HTTP Port Number	80
	HTTP Secure Server	Enabled
	HTTP Secure Port Number	443
SNMP	Community Strings	“public” (read/write) “private” (read/write)
	Traps	Authentication traps: enabled Link-up-down events: enabled
	SNMP V3	View: defaultview Group: public (read/write), private (read/write)

Function	Parameter	Default
Port Configuration	Admin Status	Enabled
	Auto-negotiation	Enabled
	Flow Control	Disabled
Rate Limiting	Input and output limits	Disabled
Port Trunking	Static Trunks	None
	LACP (all ports)	Disabled
Broadcast Storm Protection	Status	Enabled (all ports)
	Broadcast Limit Rate	500 packets per second
Spanning Tree Algorithm	Status	Disabled
	Fast Forwarding (Edge Port)	Disabled
Address Table	Aging Time	300 seconds
Virtual LANs	Default VLAN	1
	PVID	ECN330 mode: Ports 1-24: 248, Port 25-27: 1, Port 28: 4093 ECN330-switch mode: Ports 1-27: 1, Port 28: disabled
	Acceptable Frame Type	All
	Ingress Filtering	Enabled
	Switchport Mode (Egress Mode)	Hybrid: tagged/untagged frames
	GVRP (global)	Disabled
	GVRP (port interface)	Disabled

Function	Parameter	Default
Traffic Prioritization	Ingress Port Priority	0
	Queue Mode	Strict
	Weighted Round Robin	Queue: 0 1 2 3 4 5 6 7 Weight: 1 2 4 6 8 10 12 14
	IP Precedence Priority	Disabled
	IP DSCP Priority	Disabled
	IP Port Priority	Disabled
IP Settings	Management VLAN	ECN330 mode - VLAN 246-249, ECN330-switch mode - VLAN 246
	IP Address	0.0.0.0
	Subnet Mask	255.0.0.0
	Default Gateway	0.0.0.0
	DHCP	Client: Enabled ECN330 mode - VLAN 247, ECN330-switch mode - VLAN 246 Relay: Disabled Server: Disabled
	DNS	Service: Disabled
	BOOTP	Disabled
	ARP	Enabled Cache Timeout: 20 minutes Proxy: Disabled
Unicast Routing	RIP	Disabled
	OSPF	Disabled

Function	Parameter	Default
Router Redundancy	VRRP	Disabled
Multicast Filtering	IGMP Snooping (Layer 2)	Snooping: Enabled Querier: Disabled
	IGMP (Layer 3)	Disabled
Multicast Routing	DVMRP	Disabled
	PIM-DM	Disabled
	PIM-SM	Disabled
System Log	Status	Enabled
	Messages Logged	Levels 0-7 (all)
	Messages Logged to Flash	Levels 0-3
SMTP Email Alerts	Event Handler	Disabled
SNTP	Clock Synchronization	Disabled

5 Initial Configuration

5.1 Managing System Files

The ECN330-switch's flash memory supports four types of system files. All of these file types can be managed by the Command Line Interface (CLI) or SNMP. Only configuration and operation code file types can be managed by the web interface.

The ECN330-switch allows system files to be uploaded and downloaded, copied, deleted, and set as a start-up file that is loaded when the ECN330-switch boots. See section on page 560 for detailed information on the available CLI commands.

Each file type can be described as follows:

- **Configuration** — Files that store system configuration information and are created when configuration settings are saved. (Configuration commands only modify a "running-configuration" file, which is not saved when the ECN330-switch is rebooted.) Saved configuration files can be selected as a system start-up file or can be uploaded through TFTP to a server for backup. A file named "Factory_Default_Config.cfg" contains all the system default settings and cannot be deleted from the system.
- **Operation Code** — System software that is executed after boot-up, also known as run-time code. This code runs the ECN330-switch operations and provides the CLI, web, and SNMP management interfaces.
- **Diagnostic Code** — Software that is run during system boot-up, also known as POST (Power On Self-Test).
- **Loader Code** — This is the first software module that boots up when the system is powered on. It supports system file download through XModem and a few basic file management options.

Due to the size limit of the flash memory, the ECN330-switch supports only two operation code files, and two diagnostic code files. However, there can be as many configuration files as available flash memory space allows. The ECN330-switch has a total of 32 Mbytes of flash memory for system files.

In the system flash memory, one file of each type must be set as the start-up file. During a system boot, the diagnostic and operation code files set as the start-up file are run, and then the start-up configuration file is loaded.

Note that configuration files should be downloaded using a file name that reflects the contents or usage of the file settings. Downloading a file directly to the running-configuration file (running-config) causes the system to reboot, and the settings then have to be copied from the running-config to a permanent file.

When specifying file names for configuration or code files, take note of the following restrictions:

- File names on the ECN330-switch are case-sensitive.
- The length can be from 1 to 31 characters.
- The name must not contain slashes (\ or /).
- The leading letter of the file name must not be a period (.).
- Valid characters are A-Z, a-z, 0-9, ".", "-", and "_".

5.2 Connecting to the ECN330-switch

5.2.1 Configuration Options

When the ECN330-switch is set to ECN330 mode (see “Enabling the SBC to Access Advanced Management Tools” on page 74), it can be managed by the Ethernet Node Controller (also called Single-board Computer or SBC). When set to either ECN330 mode or ECN330-switch mode, the Ethernet switch functions can be managed by the software described in this manual.

The ECN330-switch includes a built-in network management agent. The agent offers a variety of management options, including SNMP, RMON, and a web-based interface. A PC may also be connected directly to the ECN330-switch for configuration and monitoring through a Command Line Interface (CLI).

Note: The IP address for the ECN330-switch is obtained through DHCP by default. To change this address, see section 5.3.4 on page 42.

The ECN330-switch’s management agent is based on SNMP (Simple Network Management Protocol). This SNMP agent permits the ECN330-switch to be managed from any system in the network using management software.

The ECN330-switch's HTTP web agent allows switch parameters to be configured, port connections monitored, and statistics displayed using a standard web browser such as Netscape Navigator version 6.2 and higher or Microsoft IE version 5.0 and higher. The ECN330-switch's web management interface can be accessed from any computer attached to the network.

The CLI program can be accessed by a direct connection to the RS-232 serial console port on the ECN330-switch, or remotely by a Telnet or Secure Shell (SSH) connection over the network.

The ECN330-switch's CLI configuration program and SNMP agent enable the following management functions to be performed:

- Set user names and passwords
- Set an IP interface for any VLAN
- Configure SNMP parameters
- Enable or disable any port
- Set the speed and duplex mode for any port
- Configure the bandwidth of any port by limiting input or output rates
- Control port access through IEEE 802.1X security or static address filtering
- Filter packets using Access Control Lists (ACLs)
- Configure up to 4094 IEEE 802.1Q VLANs
- Enable GVRP automatic VLAN registration
- Configure IP routing for unicast or multicast traffic
- Configure router redundancy
- Configure IGMP multicast filtering
- Upload and download system firmware through TFTP
- Upload and download ECN330-switch configuration files through TFTP
- Configure Spanning Tree parameters
- Configure Class of Service (CoS) priority queuing
- Configure up to 13 static or LACP trunks

- Enable port mirroring
- Set broadcast storm control on any port
- Display system information and statistics

5.2.2 Required Connections

The ECN330-switch provides an RS-232 serial port that enables a connection to a PC or terminal for monitoring and configuring the switch.

Attach a VT100-compatible terminal, or a PC running a terminal emulation program to the ECN330-switch. Use a null-modem cable that complies with the wiring assignments shown in section 2.2.4 on page 9.

To connect a terminal to the console port, complete the following steps:

1. Connect the console cable to the serial port on a terminal, or a PC running terminal emulation software, and tighten the captive retaining screws on the DB-9 connector.
2. Connect the other end of the cable's to the RS-232 serial port on the ECN330-switch.
3. Make sure the terminal emulation software is set as follows:
 - Select the appropriate serial port (COM port 1 or COM port 2).
 - Set the baud rate to 9600.
 - Set the data format to 8 data bits, 1 stop bit, and no parity.
 - Set flow control to none.
 - Set the emulation mode to VT100.
 - When using HyperTerminal, select Terminal keys, not Windows keys.

Note: When using HyperTerminal with Microsoft Windows 2000, make sure that Windows 2000 Service Pack 2 or later is installed. Windows 2000 Service Pack 2 fixes the problem of arrow keys not functioning in HyperTerminal's VT100 emulation.

Note: Please refer to section on page 569 for a complete description of console configuration options.

Note: Once the terminal is set up correctly, the console login screen is displayed.

For a description of how to use the CLI, see section 7.1 on page 515. For a list of all the CLI commands and detailed information on using the CLI, please see section 7.3 on page 528.

5.2.3 Remote Connections

Prior to accessing the ECN330-switch's onboard agent through a network connection, it must first be configured with a valid IP address, subnet mask, and default gateway using a console connection, DHCP or BOOTP protocol.

The IP address for the ECN330-switch is assigned through DHCP by default. To manually configure this address or enable dynamic address assignment through BOOTP, see section 5.3.4 on page 42.

Note: The ECN330-switch supports four concurrent Telnet sessions.

Note: Each VLAN group can be assigned its own IP interface address (page 42). The ECN330-switch can be managed through any of these addresses if no management VLAN has been defined. To define a management VLAN, see section 5.3.4.3 on page 45.

After configuring the ECN330-switch's IP parameters, the onboard configuration program can be accessed from anywhere within the connected network. The onboard configuration program can be accessed using Telnet from any computer attached to the network. The ECN330-switch can also be managed by any computer using a web browser (Internet Explorer 5.0 or above, or Netscape Navigator 6.2 or above), or from a network computer using SNMP network management software.

Note: The onboard program only provides access to basic configuration functions. To access the full range of SNMP management functions, SNMP-based network management software must be used. For a full description of the MIB parameters, please refer to the *ECN330-switch MIB Description*.

5.3 Basic Configuration

5.3.1 Console Connection

The CLI program provides two different command levels — normal access level (Normal Exec) and privileged access level (Privileged Exec). The commands available at the Normal Exec level are a limited subset of those available at the

Privileged Exec level and allow only basic utilities to be used and information displayed. To fully configure ECN330-switch parameters, the CLI must be accessed at the Privileged Exec level.

Access to both CLI levels are controlled by user names and passwords. The ECN330-switch has a default user name and password for Privileged Exec level. To log into the CLI at the Privileged Exec level using the default user name and password, perform these steps:

1. To initiate a console connection, press <Enter>. The “User Access Verification” procedure starts.
2. At the `Username` prompt, type **admin**.
3. At the `Password` prompt, also type **admin**. (The password characters are not displayed on the console screen.)
4. The session is opened and the CLI displays the `Console#` prompt indicating access at the Privileged Exec level.

5.3.2 Saving Configuration Settings

Configuration commands only modify the running-configuration file and are not saved when the ECN330-switch is rebooted. To save configuration changes, use the **copy running-config startup-config** command to create a configuration file in the ECN330-switch’s nonvolatile flash memory.

New startup configuration files must have a name specified. File names on the ECN330-switch are case-sensitive, can be from 1 to 31 characters, must not contain slashes (\ or /), and the leading letter of the file name must not be a period (.). (Valid characters: A-Z, a-z, 0-9, “.”, “-”, “_”)

There can be more than one user-defined configuration file saved in the ECN330-switch’s flash memory, but only one is designated as the “startup” file that is loaded when the ECN330-switch boots. The **copy running-config startup-config** command always sets the new file as the startup file. To select a previously saved configuration file, use the **boot system config: <filename>** command.

The maximum number of saved configuration files depends on available flash memory, with each configuration file normally requiring less than 20 kbytes. The amount of available flash memory can be checked by using the **dir** command.

To save the current configuration settings, type the following command:

1. At the Privileged Exec mode prompt, type **copy running-config startup-config** and press <Enter>.
2. Type the startup file name when prompted and press <Enter>.

```
Console#copy running-config startup-config
Startup configuration file name []: startup

Console#
```

5.3.3 Setting Passwords

Note: If this is the first time to log into the CLI program, define a new password for the default user name using the **username** command, record it and put it in a safe place.

Passwords can consist of up to 8 alphanumeric characters and are case sensitive. To prevent unauthorized access to the ECN330-switch, set the passwords as follows:

1. Open the console interface with the default user name and password **admin** to access the Privileged Exec level.
2. Type **configure** and press <Enter>.
3. Type **username guest password 0 <password>**, for the Normal Exec level, where **password** is the new password. Press <Enter>.
4. Type **username admin password 0 <password>**, for the Privileged Exec level, where **password** is the new password. Press <Enter>.

```
Username: admin
Password:

CLI session with the Embedded Switching/Routing Unit is opened.
To end the CLI session, enter [Exit].

Console#configure
Console(config)#username guest password 0 [password]
Console(config)#username admin password 0 [password]
Console(config)#
```

5.3.4 Setting an IP Address

To obtain management access through the network, IP address information for the ECN330-switch must be established. The assignment of an IP Address to the ECN330-switch is done by assigning an IP Address to a VLAN interface, this can be done in either of the following ways:

Manual — Input the information, including IP address and subnet mask. If the management station is not in the same IP subnet as the ECN330-switch, the default gateway router also needs to be specified.

Dynamic — The ECN330-switch sends IP configuration requests to BOOTP or DHCP address allocation servers on the network.

Each VLAN interface on the ECN330-switch can be assigned its own IP address. When no management VLAN has been defined, the ECN330-switch can be managed through any of these IP addresses. For more secure management access, a management VLAN should be defined, which restricts management access to only the specified VLAN interface. Any IP address assigned to the management VLAN can be used to manage the ECN330-switch.

By default, the ECN330-switch is configured to operate in ECN330 mode (see “Enabling the SBC to Access Advanced Management Tools” on page 74). The factory defaults designate VLAN 246 for external management and VLAN 247 for internal management. VLAN 247 is already configured to obtain an IP address using DHCP. If the ECN330-switch is configured for ECN330-switch mode, then VLAN 246 is designated for external management and is configured to obtain an IP address using DHCP. All other management VLANs are disabled.

5.3.4.1 Manual Configuration

The IP address, subnet mask and default gateway can be assigned manually to the ECN330-switch. Valid IP addresses consist of four decimal numbers, 0 to 255, separated by periods. Anything not in this format is not accepted by the CLI program.

Note: The IP address for the ECN330-switch is obtained through DHCP by default.

Before the IP Address can be configured, the following must be known:

- IP address for the ECN330-switch
- Default gateway for the network
- Network mask for this network

To assign an IP address to the ECN330-switch, complete the following steps:

1. At the global configuration mode prompt, type **interface vlan** *<vlan-id>* to access the interface-configuration mode. The range for VLAN IDs is 1-4094 for ECN330 mode, and 1 or 246 for ECN330-switch mode. To manually configure an address for VLAN 246, type **interface vlan 246** and press <Enter>.
2. Type **ip address** *<ip-address>* *<netmask>*, where *ip-address* is the ECN330-switch's IP address and *netmask* is the network mask for the network. Press <Enter>.
3. Type **exit** to return to the global configuration mode prompt. Press <Enter>.
4. To set the IP address of the default gateway for the network to which the ECN330-switch belongs, type **ip default-gateway** *<gateway>*, where *gateway* is the IP address of the default gateway. Press <Enter>.

```
Console(config)#interface vlan 246
Console(config-if)#ip address 192.168.1.5 255.255.255.0
Console(config-if)#exit
Console(config)#ip default-gateway 192.168.1.254
Console(config)#
```

5.3.4.2

Dynamic Configuration

If the **bootp** or **dhcp** option is selected, IP is enabled but does not function until a BOOTP or DHCP reply has been received. Therefore, the **ip dhcp restart client** command must be used to start broadcasting service requests. Requests are sent once every minute until IP configuration information is obtained from a BOOTP or DHCP server. (BOOTP and DHCP values can include the IP address, subnet mask, and default gateway.)

If the **bootp** or **dhcp** option is saved to the startup-config file (step 6), then the ECN330-switch will start broadcasting service requests as soon as it is powered on.

To automatically configure the ECN330-switch by communicating with BOOTP or DHCP address allocation servers on the network, complete the following steps:

1. At the global configuration mode prompt, type **interface vlan <vlan-id>** to access the interface-configuration mode. The range for VLAN IDs is 1-4094 for ECN330 mode, and 1 or 246 for ECN330-switch mode. To dynamically configure an address for VLAN 246, type **interface vlan 246** and press <Enter>.
2. At the interface-configuration mode prompt, use one of the following commands:
 - To obtain IP settings through DHCP, type **ip address dhcp** and press <Enter>.
 - To obtain IP settings through BOOTP, type **ip address bootp** and press <Enter>.
3. Type **exit** to return to the global configuration mode. Press <Enter>.
4. Type **ip dhcp restart client** to begin broadcasting service requests. Press <Enter>.
5. Wait a few minutes, and then check the IP configuration settings by typing the **show ip interface** command. Press <Enter>.
6. Save the configuration changes by typing **copy running-config startup-config**. Type the startup file name when prompted and press <Enter>.

```

Console(config)#interface vlan 246
Console(config-if)#ip address dhcp
Console(config-if)#exit
Console#ip dhcp restart client
Console#show ip interface

Vlan 246 is up, addressing mode is DHCP
  Interface address is 192.168.1.54, mask is 255.255.255.0,
  Primary
  MTU is 1500 bytes
  Proxy ARP is disabled
  Split horizon is enabled
Console#copy running-config startup-config
Startup configuration file name []: startup
\Write to FLASH Programming.

\Write to FLASH finish.
Console#

```

5.3.4.3 Specifying a Management VLAN

For secure management access to the ECN330-switch, specify a management VLAN and use IP addresses assigned to this VLAN to manage the switch. The management VLAN applies to management access through the web, Telnet, SSH, and SNMP. When the management VLAN is enabled, IP addresses assigned to other VLAN interfaces cannot be used for management access.

Note: The management VLAN operates as an isolated VLAN and data traffic is not routed to or from other VLANs. Routing protocols cannot be enabled on the management VLAN interface nor is the management IP interface advertised by routing protocols to other routers. The management VLAN also ensures that all management traffic within this VLAN is sent to the SBC, and not to the ECN330-switch's CPU.

Note: If the management VLAN is connected to a management network that includes several IP subnets, a static route must be configured for each subnet.

To specify the management VLAN, complete the following steps:

1. From the Privileged Exec level, type **configure** and press <Enter>.
2. At the Privileged Exec level global configuration mode prompt, type **management vlan internal <vlan-id>**, where **<vlan-id>** is the management VLAN ID, and the range for VLAN IDs is 1-4094. Press <Enter>.

3. Type **exit** to return to the global configuration mode prompt. Press <Enter>.
4. To display the current management VLAN setting, type **show management vlan**. Press <Enter>.

```
Console#configure
Console(config)#management vlan internal 247
Console(config)#exit
Console#show management vlan
Current Internal Management VLAN: 247
Current Dynamic Management VLAN: 0
Current External Management VLAN: 0
Current Native Management VLAN: 0
Current FSA Management VLAN: 0
Console#
```

5.3.5 Enabling SNMP Management Access

The ECN330-switch can be configured to accept management commands from Simple Network Management Protocol (SNMP) applications. The ECN330-switch can be configured to respond to SNMP requests and generate SNMP traps.

When SNMP management stations send requests to the ECN330-switch (either to return information or to set a parameter), it provides the requested data or sets the specified parameter. The ECN330-switch can also be configured to send information to SNMP managers (without being requested by the managers) through trap messages, which inform the manager that certain events have occurred.

The ECN330-switch includes an SNMP agent that supports SNMP version 1, 2c, and 3 clients. To provide management access for version 1 or 2c clients, a community string must be specified. The ECN330-switch provides a default MIB View (that is, an SNMPv3 construct) for the default “public” community string that provides read access to the entire MIB tree, and a default view for the “private” community string that provides read/write access to the entire MIB tree. However, new views may be assigned to version 1 or 2c community strings that suit specific security requirements (see page 123).

5.3.5.1 Community Strings (for SNMP Version 1 and 2c Clients)

Community strings are used to control management access to SNMP version 1 and 2c stations, as well as to authorize SNMP stations to receive trap messages from the ECN330-switch. Therefore, community strings need to be assigned to specified users and their access level set.

The default strings are:

- **public** - Specifies read/write access. Authorized management stations are able to both retrieve and modify MIB objects.
- **private** - Specifies read/write access. Authorized management stations are able to both retrieve and modify MIB objects.

Note: If access from SNMP version 1 and 2c clients is not intended to be utilized, it is recommended that both of the default community strings be deleted. If there are no community strings, then SNMP management access from version 1 and 2c clients is disabled.

To prevent unauthorized access to the ECN330-switch from SNMP version 1 or 2c clients, it is recommended to change the default community strings.

To configure a community string, complete the following steps:

1. At the Privileged Exec level global configuration mode prompt, type **snmp-server community <string> <mode>**, where *string* is the community access string and *mode* is either **rw** (read/write) or **ro** (read only). Press <Enter>.
2. To remove an existing string, type **no snmp-server community <string>**, where *string* is the community access string to remove. Press <Enter>.

```
Console(config)#no snmp-server community private
Console(config)#snmp-server community abc rw
Console(config)#
```

5.3.5.2 Trap Receivers

SNMP stations that are to receive traps from the ECN330-switch can also be specified.

To configure a trap receiver, use the **snmp-server host** command. From the Privileged Exec level global configuration mode prompt, type:

```
snmp-server host <host-address> <community-string>
[version {1 | 2c | 3 {auth | noauth | priv}}]
```

where **host-address** is the IP address for the trap receiver, **community-string** specifies access rights for a version 1/2c host, or is the user name of a version 3 host, **version** indicates the SNMP client version, and **auth** | **noauth** | **priv** means that authentication, no authentication, or authentication and privacy is used for v3 clients. Then press <Enter>.

For a more detailed description of these parameters, see section 7.6.6 on page 615. The following example creates a trap host for each type of SNMP client

```
Console(config)#snmp-server host 10.1.19.23 batman
Console(config)#snmp-server host 10.1.19.98 robin version 2c
Console(config)#snmp-server host 10.1.19.34 barbie version 3 auth
Console(config)#
```

5.3.5.3 Configuring Access for SNMP Version 3 Clients

To configure management access for SNMPv3 clients, first create a view that defines the portions of MIB that the client can read or write, assign the view to a group, and then assign the user to a group.

The following example creates one view called “mib-2” that includes the entire MIB-2 tree branch, and then another view that includes the IEEE 802.1d bridge MIB. It assigns these respective read and read/write views to a group call “r&d” and specifies group authentication through MD5 or SHA. In the last step, it assigns a v3 user to this group, indicating that MD5 will be used for authentication, provides the password “greenpeace” for authentication, and the password “einstien” for encryption.

```
Console(config)#snmp-server view mib-2 1.3.6.1.2.1 included
Console(config)#snmp-server view 802.1d 1.3.6.1.2.1.17 included
Console(config)#snmp-server group r&d v3 auth mib-2 802.1d
Console(config)#snmp-server user steve group r&d v3 auth md5
    greenpeace priv des56 einstien
Console(config)#
```

For a more detailed explanation on how to configure the ECN330-switch for access from SNMP v3 clients, refer to “Simple Network Management Protocol” on page 106, or refer to the specific CLI commands for SNMP starting on page 608.

6 Configuring the ECN330-switch

6.1 Accessing the Management Interface

The ECN330-switch provides an embedded HTTP web agent. A web browser can be used to configure the ECN330-switch and view statistics to monitor network activity. The web agent can be accessed by any computer on the network using a standard web browser (Internet Explorer 5.0 or above, or Netscape Navigator 6.2 or above).

Note: The Command Line Interface (CLI) can also be used to manage the ECN330-switch over a serial connection to the console port or through Telnet. For more information on using the CLI, refer to “Command Line Interface” on page 515.”

Prior to accessing the ECN330-switch from a web browser, be sure to have first performed the following tasks:

1. Configure the ECN330-switch with a valid IP address, subnet mask, and default gateway using an out-of-band serial connection, BOOTP or DHCP protocol. (See “Setting an IP Address” on page 42.)
2. Set user names and passwords using an out-of-band serial connection. Access to the web agent is controlled by the same user names and passwords as the onboard configuration program. (See “Setting Passwords” on page 41.)
3. Enter a user name and password to gain access to the system configuration program.

Note: Three attempts are allowed to enter the correct password; on the third failed attempt the current connection is terminated.

Note: Logging into the web interface as guest (Normal Exec level) allows configuration settings to be viewed and the guest password changed. Logging in as “admin” (Privileged Exec level) allows settings to be changed on any page.

Note: If the path between the management station and the ECN330-switch does not pass through any device that uses the Spanning Tree Algorithm, then the ECN330-switch port attached to the management station can be set to fast

forwarding (that is, enable Admin Edge Port) to improve the ECN330-switch's response time to management commands issued through the web interface. See "Configuring Interface Settings" on page 247.

6.2 Navigating the Web Browser Interface

To access the web-browser interface, first enter a user name and password. The administrator has Read/Write access to all configuration parameters and statistics. The default user name is **admin** with corresponding password of **admin**.

6.2.1 Home Page

When a web browser connects with the ECN330-switch's web agent, the home page is displayed as shown in Figure 7. The home page displays the Main Menu on the left side of the screen and System Information on the right side. The Main Menu links are used to navigate to other menus, and display configuration parameters and statistics.

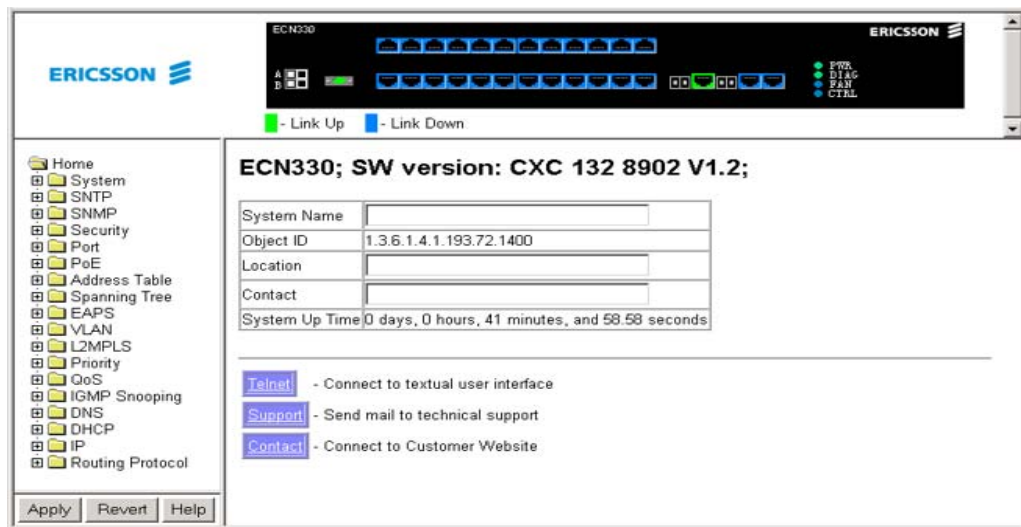


Figure 7 Home Page

6.2.2 Configuration Options

Configurable parameters have a dialog box or a drop-down list. Once a configuration change has been made on a page, be sure to click on the “Apply” button to confirm the new setting. Table 7 summarizes the web page configuration buttons.

Table 7 Web Page Configuration Buttons

Button	Action
Apply	Sets specified values to the system.
Revert	Cancels specified values and restores current values prior to pressing “Apply.”
Help	Links directly to web help.

Note: To ensure proper screen refresh, be sure that Internet Explorer 5.x is configured as follows: Under the menu “Tools / Internet Options / General / Temporary Internet Files / Settings,” the setting for item “Check for newer versions of stored pages” should be “Every visit to the page.”

Note: When using Internet Explorer 5.0, the screen may have to be manually refreshed after making configuration changes by pressing the browser’s refresh button.

6.2.3 Panel Display

The web agent displays an image of the ECN330-switch’s ports. The Mode can be set to display different information for the ports, including Active (that is, up or down), Duplex (that is, half or full duplex), or Flow Control (that is, with or without flow control). Clicking on the image of a port opens the Port Configuration page as described on page 184.



Figure 8 Front Panel Indicators

6.2.4 Main Menu

Using the onboard web agent, system parameters can be defined, the ECN330-switch and all its ports can be managed and controlled, and network conditions monitored. Table 8 briefly describes the selections available from this program.

Table 8 ECN330-switch Main Menu

Menu	Description	Page
System		69
System Information	Provides basic system description, including contact information	69
System Mode	Configure the ECN330-switch to operate in normal mode or one of the tunneling modes (QinQ or L2MPLS)	71
System MTU	Sets the maximum transfer unit for traffic crossing the ECN330-switch	72
System SBC Mode	Enables or disables the Single-Board Computer	74
Switch Information	Shows the number of ports, hardware/firmware version numbers, and power status	75
Bridge Extension	Shows the bridge extension parameters	77
Jumbo Frames	Enables support for jumbo frames	79
File Management		86
Copy Operation	Allows the transfer and copying files	87
Delete	Allows deletion of files from the flash memory	87
Set Startup	Sets the startup file	87

Menu	Description	Page
Line		92
Console	Sets console port connection parameters	92
Telnet	Sets Telnet connection parameters	94
Log		96
Logs	Sends error messages to a logging process	96
System Logs	Stores and displays error messages	100
Remote Logs	Configures the logging of messages to a remote logging process	98
SMTP	Sends an SMTP client message to a participating server	101
Reset	Restarts the ECN330-switch	101
SNTP		104
Configuration	Configures SNTP client settings, including a specified list of servers	104
Clock Time Zone	Sets the local time zone for the system clock	105
SNMP		106
Configuration	Configures community strings and related trap functions	109
Agent Status	Enables or disables SNMP	108
SNMPv3		113
Engine ID	Sets the SNMP v3 engine ID	114
Remote Engine ID	Sets the SNMP v3 engine ID on a remote device	115
Users	Configures SNMP v3 users	116

Menu	Description	Page
Remote Users	Configures SNMP v3 users on a remote device	118
Groups	Configures SNMP v3 groups	121
Views	Configures SNMP v3 views	123
Security		126
User Accounts	Configures user names, passwords, and access levels	126
Authentication Settings	Configures authentication sequence, RADIUS and TACACS	128
HTTPS Settings	Configures secure HTTP settings	132
SSH		135
Settings	Configures Secure Shell server settings	140
Host-Key Settings	Generates the host key pair (public and private)	138
Port Security	Configures per port security, including status, response for security breach, and maximum allowed MAC addresses	142
802.1X	Port authentication	145
Information	Displays global configuration settings	147
Configuration	Configures global configuration parameters	148
Port Configuration	Sets the authentication mode for individual ports	148
Statistics	Displays protocol statistics for the selected port	152
ACL		156
Configuration	Configures packet filtering based on IP or MAC addresses	156
Mask Configuration	Controls the order in which ACL rules are checked	166

Menu	Description	Page
Port Binding	Binds a port to the specified ACL	172
Trunk Binding	Binds a trunk to the specified ACL	172
VLAN ACL		174
Configuration	Configures a VLAN ACL for packet filtering	174
Mask Configuration	Controls the order in which ACL rules are checked	177
VLAN Filtering	Binds a VLAN access map to one or more VLANs	182
IP Filter	Configures IP addresses that are allowed management access	154
Port		184
Port Information	Displays port connection status	184
Trunk Information	Displays trunk connection status	184
Port Configuration	Configures port connection settings	187
Trunk Configuration	Configures trunk connection settings	190
Trunk Membership	Specifies ports to group into static trunks	191
LACP		190
Configuration	Allows ports to dynamically join trunks	193
Aggregation Port	Configures parameters for link aggregation group members	196
Port Counters Information	Displays statistics for LACP protocol messages	200
Port Internal Information	Displays settings and operational state for local side	202
Port Neighbors Information	Displays settings and operational state for remote side	205

Menu	Description	Page
Port Broadcast Control	Sets the broadcast storm threshold for each port	207
Trunk Broadcast Control	Sets the broadcast storm threshold for each trunk	207
Mirror Port Configuration	Sets the source and target ports for mirroring	209
Rate Limit		211
Input Port Configuration	Sets the input rate limit for each port	211
Input Port Configuration per VLAN	Sets the input rate limit for each port for each VLAN	212
Input Trunk Configuration	Sets the input rate limit for each trunk	211
Output Port Configuration	Sets the output rate limit for each port	211
Output Trunk Configuration	Sets the output rate limit for each trunk	211
Port Statistics	Lists Ethernet and RMON port statistics	213
PoE		221
Power Status	Displays the status of global power parameters	221
Power Configuration	Configures the power budget for the ECN330-switch	223
Power Port Status	Displays the status of port power parameters	224
Power Port Configuration	Configures port power parameters	225

Menu	Description	Page
Address Table		227
Static Addresses	Displays entries for interface, address or VLAN	227
Dynamic Addresses	Displays or edits static entries in the Address Table	228
Address Aging	Sets timeout for dynamically learned entries	230
Address Threshold	Sends a trap message when address entries exceed a specified threshold	230
Spanning Tree		231
STA		231
Information	Displays STA values used for the bridge	234
Configuration	Configures global bridge settings for STP, RSTP and MSTP	238
Port Information	Displays individual port settings for STA	243
Trunk Information	Displays individual trunk settings for STA	243
Port Configuration	Configures individual port settings for STA	247
Trunk Configuration	Configures individual trunk settings for STA	247
MSTP		
VLAN Configuration	Configures priority and VLANs for a spanning tree instance	250
Port Information	Displays port settings for a specified MST instance	254
Trunk Information	Displays trunk settings for a specified MST instance	254
Port Configuration	Configures port settings for a specified MST instance	256
Trunk Configuration	Configures trunk settings for a specified MST instance	256

Menu	Description	Page
EAPS		258
Configuration	Activates the configured EAPS domains	264
Domain Configuration	Creates an EAPS domain, configures domain parameters, and protected VLANs	265
VLAN		272
802.1Q VLAN		272
GVRP Status	Enables GVRP VLAN registration protocol	276
Basic Information	Displays information on the VLAN type supported by the ECN330-switch	277
Current Table	Shows the current port members of each VLAN and whether or not the port is tagged or untagged	283
Static List	Used to create or remove VLAN groups	284
Static Table	Modifies the settings for an existing VLAN	287
Static Membership	Configures membership type for interfaces, including tagged, untagged or forbidden	289
Port Configuration	Specifies default PVID and VLAN attributes	290
Trunk Configuration	Specifies default trunk VID and VLAN attributes	290
VLAN MAC Address	Configures the MAC address of a VLAN	294
Private VLAN		303
Information	Shows private VLANs and associated ports	304
Configuration	Configures private VLANs	306
Association	Maps a secondary VLAN to a primary VLAN	307
Port Information	Shows VLAN port type, and associated primary or secondary VLANs	308

Menu	Description	Page
Port Configuration	Configures VLAN port type, and associated primary or secondary VLANs	309
Trunk Information	Shows VLAN trunk type, and associated primary or secondary VLANs	308
Trunk Configuration	Configures VLAN trunk type, and associated primary or secondary VLANs	309
Protocol VLAN		311
Configuration	Creates a protocol group, specifying the supported protocols	312
Port Configuration	Maps a protocol group to a VLAN	313
L2MPLS		314
VLAN Configuration	Configures a VLAN to operate as an L2MPLS tunnel, associates input/output MPLS labels with the VLAN	319
Port Configuration	Sets the MPLS characteristics for an uplink port	320
Trunk Configuration	Sets the MPLS characteristics for an uplink trunk	320
VPN Information	Displays the L2MPLS client VLAN interface and uplink interface information	322
Priority		324
Default Port Priority	Sets the default priority for each port	324
Default Trunk Priority	Sets the default priority for each trunk	324
Traffic Classes	Maps IEEE 802.1p priority tags to output queues	326
Traffic Classes Status	Enables/disables traffic class priorities (not implemented)	NA
Queue Mode	Sets queue mode to strict priority or Weighted Round-Robin	329

Menu	Description	Page
Queue Scheduling	Configures Weighted Round Robin queueing	330
WFQ Queue Minimum Bandwidth	Assigns a minimum bandwidth to each of the priority queues when using Weighted Fair Queueing (WFQ)	332
IP Precedence/ DSCP Priority Status	Globally selects IP Precedence or DSCP Priority, or disables both.	334
IP Precedence Priority	Sets IP Type of Service priority, mapping the precedence tag to a class-of-service value	335
IP DSCP Priority	Sets IP Differentiated Services Code Point priority, mapping a DSCP tag to a class-of-service value	338
IP Port Priority Status	Globally enables or disables IP Port Priority	340
IP Port Priority	Sets TCP/UDP port priority, defining the socket number and associated class-of-service value	340
QoS		342
DiffServ	Configure QoS classification criteria and service policies	342
Class Map	Creates a class map for a type of traffic	343
Policy Map	Creates a policy map for multiple interfaces	346
Service Policy	Applies a policy map defined to an ingress port	350
IGMP Snooping		352
IGMP Configuration	Enables multicast filtering; configures parameters for multicast query	355
Multicast Router Port Information	Displays the ports that are attached to a neighboring multicast router for each VLAN ID	358
Static Multicast Router Port Configuration	Assigns ports that are attached to a neighboring multicast router	359

Menu	Description	Page
IP Multicast Registration Table	Displays all multicast groups active on the ECN330-switch, including multicast IP addresses and VLAN ID	360
IGMP Member Port Table	Indicates multicast addresses associated with the selected VLAN	361
IGMP Snooping Status per VLAN	Enables IGMP snooping per VLAN interface	362
DNS		370
General Configuration	Enables DNS; configures domain name and domain list; and specifies IP address of name servers for dynamic lookup	370
Static Host Table	Configures static entries for domain name to address mapping	372
Cache	Displays cache entries discovered by designated name servers	374
DHCP		376
Relay Configuration	Specifies DHCP relay servers; enables or disables relay service	376
Server	Configures DHCP server parameters	376
General	Enables DHCP server; configures excluded address range	379
Pool Configuration	Configures address pools for network groups or a specific host	380
IP Binding	Displays addresses currently bound to DHCP clients	386

Menu	Description	Page
IP		397
General		401
Global Settings	Enables or disables routing, specifies the default gateway	401
Routing Interface	Configures the IP interface for the specified VLAN	403
ARP		405
General	Sets the protocol timeout, and enables or disables proxy ARP for the specified VLAN	406
Static Addresses	Statically maps a physical address to an IP address	407
Dynamic Addresses	Shows dynamically learned entries in the IP routing table	408
Other Addresses	Shows internal addresses used by the ECN330-switch	410
Statistics	Shows statistics on ARP requests sent and received	412
IGMP		362
Interface Settings	Configures Layer 3 IGMP for specific VLAN interfaces	364
Group Membership	Displays the current multicast groups learned through IGMP	368
Statistics		413
IP	Shows statistics for IP traffic, including the amount of traffic, address errors, routing, fragmentation and reassembly	413
ICMP	Shows statistics for ICMP traffic, including the amount of traffic, protocol errors, and the number of echoes, timestamps, and address masks	416

Menu	Description	Page
UDP	Shows statistics for UDP, including the amount of traffic and errors	418
TCP	Shows statistics for TCP, including the amount of traffic and TCP connection activity	419
Routing		398
Static Routes	Configures and display static routing entries	421
Routing Table	Shows all routing entries, including local, static and dynamic routes	422
Multicast Routing		469
General Settings	Globally enables multicast routing	469
Multicast Routing Table	Shows each multicast route the ECN330-switch has learned	470
VRRP		389
Group Configuration	Configures VRRP groups, including virtual interface address, advertisement interval, preemption, priority, and authentication	389
Global Statistics	Displays global statistics for VRRP protocol packet errors	394
Group Statistics	Displays statistics for VRRP protocol events and errors on the specified VRRP group and interface	395
Routing Protocol		400
RIP		424
General Settings	Enables or disables RIP, sets the global RIP version and timer values	425
Network Addresses	Configures the network interfaces that will use RIP	428

Menu	Description	Page
Interface Settings	Configures RIP parameters for each interface, including send and receive versions, message loopback prevention, and authentication	429
Statistics	Displays general information on update time, route changes and number of queries, as well as a list of statistics for known interfaces and neighbors	433
OSPF		436
General Configuration	Enables or disables OSPF; also configures the Router ID and various other global settings	438
Area Configuration	Specifies rules for importing routes into each area	442
Area Range Configuration	Configures route summaries to advertise at an area boundary	446
Interface Configuration	Shows area ID and designated router; also configures OSPF protocol settings and authentication for each interface	449
Virtual Link Configuration	Configures a virtual link through a transit area to the backbone	453
Network Area Address Configuration	Defines OSPF areas and associated interfaces	456
Summary Address Configuration	Aggregates routes learned from other protocols for advertising into other autonomous systems	458
Redistribute Configuration	Redistributes routes from one routing domain to another	460
NSSA Settings	Configures settings for importing routes into or exporting routes out of not-so-stubby areas	462
Link State Database Information	Shows information about different OSPF Link State Advertisements (LSAs) stored in this router's database	463

Menu	Description	Page
Border Router Information	Displays routing table entries for area border routers and autonomous system boundary routers	466
Neighbor Information	Displays information about neighboring routers on each interface within an OSPF area	467
DVMRP		484
General Settings	Configure global settings for prune and graft messages, and the exchange of routing information	474
Interface Settings	Enables/disables DVMRP per interface and sets the route metric	479
Neighbor Information	Displays neighboring DVMRP routers	481
Routing Table	Displays DVMRP routing information	482
PIM-DM		
General Settings	Enables or disables PIM-DM globally for the ECN330-switch	484
Interface Settings	Enables or disables PIM-DM per interface, configures protocol settings for hello, prune and graft messages	485
Interface Information	Displays summary information for each interface	488
Neighbor Information	Displays neighboring PIM-DM routers	489
PIM-SM		490
General Settings	Enable PIM-SM globally on the ECN330-switch	492
Global Settings	Configures global settings that affect RP selection, timers for join/prune messages, register messages, and register suppression, and use of the SPT	493
Interface Settings	Enables PIM-SM for each interface that will participate in multicast routing	497

Menu	Description	Page
RP Address	Sets a static address for the RP for the specified multicast group	499
BSR Candidate	Configured the ECN330-switch as a BSR candidate	502
RP Candidate	Advertises the ECN330-switch as an RP candidate to the BSR	504
RP Hash	Displays the RP elected for the specified multicast group, the source of this information, and the method of election	506
BSR Router Information	Displays information about the BSR	507
Interface Information	Displays information about interfaces configured for PIM-SM	510
RP Mapping Information	Displays the active RPs and associated multicast routing entries	511
Neighbor Information	Displays all the neighboring PIM-SM routers	513

6.3 System Management Configuration

6.3.1 Displaying System Information

The system can be identified by displaying the device name, location and contact information.

Field Attributes

- **System Name** – Name assigned to the ECN330-switch.
- **Object ID** – MIB II object ID for ECN330-switch's network management subsystem.
- **Location** – Specifies the system location.
- **Contact** – Administrator responsible for the system.
- **System Up Time** – Length of time the management agent has been up.

These additional parameters are displayed for the CLI.

- **MAC Address** – The physical layer address for the ECN330-switch.
- **Web server** – Shows if management access through HTTP is enabled.
- **Web server port** – Shows the TCP port number used by the web interface.
- **Web secure server** – Shows if management access through HTTPS is enabled.
- **Web secure server port** – Shows the TCP port used by the HTTPS interface.
- **Telnet server** – Shows if management access through Telnet is enabled.
- **Telnet server port** – Shows the TCP port used by the Telnet interface.
- **Jumbo Frame** – Shows if jumbo frames are enabled.
- **POST result** – Shows results of the power-on self-test

Web – Click System, System Information. Specify the system name, location, and contact information for the system administrator, then click Apply. (This page also includes a Telnet button that allows access to the Command Line Interface through Telnet.)

ECN330; SW version: CXC 132 8902 V1.2;

System Name	
Object ID	1.3.6.1.4.1.193.72.1400
Location	
Contact	
System Up Time	0 days, 0 hours, 41 minutes, and 58.58 seconds

[Telnet](#) - Connect to textual user interface
[Support](#) - Send mail to technical support
[Contact](#) - Connect to Customer Website

Figure 9 System Information

CLI – Specify the hostname, location and contact information.

```

Console(config)#hostname R&D 5
Console(config)#snmp-server location WC 9
Console(config)#snmp-server contact Ted
Console(config)#exit
Console#show system
System Description: ECN330; SW version: CXC 132 8902 V1.2;
System OID String: 1.3.6.1.4.1.193.72.1400
System information
  System Up Time:          0 days, 1 hours, 11 minutes, and 53.80
                           seconds
  System Name:             R&D 5
  System Location:        WC 9
  System Contact:         Ted
  MAC Address (Unit1):    00-00-12-33-89-76
  Web Server:             Enabled
  Web Server Port:        80
  Web Secure Server:      Enabled
  Web Secure Server Port: 443
  Telnet Server:          Enable
  Telnet Server Port:     23
  Jumbo Frame:            Disabled

  POST Result:
Console#

```

6.3.2**Configuring the ECN330-switch for Normal Operation or Tunneling Mode**

The system can be configured to operate in normal mode or one of the tunneling modes used for passing Layer 2 traffic across a service provider's metropolitan area network, including IEEE 802.1Q tunneling (QinQ) or Layer 2 over MPLS (L2MPLS).

Command Attributes

System Mode – Sets the ECN330-switch to operate in one of the following modes:

- **Normal Mode** – The ECN330-switch functions in normal operating mode. (This is the default operating mode.)

- **QinQ Mode** – Sets the ECN330-switch to QinQ mode, and allows the QinQ tunnel port to be configured. For an explanation of QinQ see “Configuring IEEE 802.1Q Tunneling” on page 296.
- **L2MPLS Mode** – Sets the ECN330-switch to L2MPLS mode, and allows all L2MPLS commands to be configured. For an explanation of L2MPLS see section 6.13 on page 314.

Web – Click System, System Mode. Select the required system mode, and click Apply.

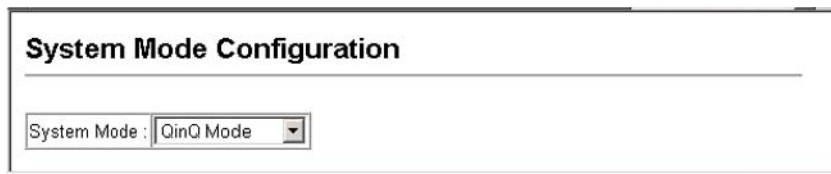


Figure 10 System Mode

CLI – This example sets the ECN330-switch to operate in QinQ mode.

```
Console(config)#system mode qinq
Console(config)#exit
Console#show system mode

System mode is QinQ mode
Console#
```

6.3.3

Configuring the Maximum Frame Size

The maximum transfer unit (or frame size) for traffic crossing the ECN330-switch should be set to minimize unnecessary fragmentation and maximize the transfer of large sequential data streams.

Command Usage

- Fast Ethernet ports are only affected by the System MTU setting.
- Gigabit Ethernet ports are only affected by the Jumbo frame size setting.
- The ECN330-switch provides more efficient throughput for large sequential data transfers by supporting jumbo frames on Gigabit

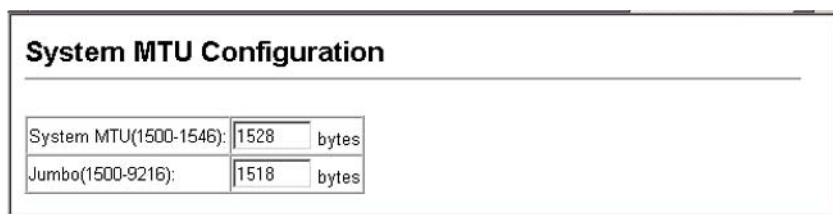
Ethernet ports of up to 9216 bytes. Compared to standard Ethernet frames that run only up to 1.5 KB, using jumbo frames significantly reduces the per-packet overhead required to process protocol encapsulation fields.

- To use jumbo frames, both the source and destination end nodes (such as a computer or server) must support this feature. Also, when the connection is operating at full duplex, all switches in the network between the two end nodes must be able to accept the extended frame size. And for half-duplex connections, all devices in the collision domain would need to support jumbo frames.

Command Attributes

- **System MTU (1500-1546)** – Specifies the MTU size for Fast Ethernet ports. (Range: 1500-1546 bytes)
- **Jumbo (1500-9216)** – Specifies the jumbo frame size (MTU) for Gigabit Ethernet ports. (Range: 1500-9216 bytes)

Web – Click System, System MTU. Set the maximum frame size for Fast Ethernet and Gigabit Ethernet ports, then click Apply.



System MTU Configuration		
System MTU(1500-1546):	1528	bytes
Jumbo(1500-9216):	1518	bytes

Figure 11 System MTU

CLI – This example sets the MTU for Fast Ethernet ports to 1528 bytes

```
Console(config)#system mtu 1528
Console(config)#exit
Console#show system mtu
System MTU size is 1528 Bytes
System Jumbo MTU size is 1518 Bytes
Console#
```

6.3.4 Enabling the SBC to Access Advanced Management Tools

The ECN330-switch includes a Single Board Computer (SBC) and an ECN330-switch. The SBC is connected to the Gigabit Ethernet port 28 of the ECN330-switch.

Command Usage

- When the SBC is enabled, the SBC provides a management proxy functionality, where management of embedded nodes including the ECN330-switch is done by the SBC which is managed by PEM. Note that when the SBC is enabled, the console interface is set to SBC display mode.
- After re-enabling the SBC, the `Factory_Default_Config.cfg` is automatically regenerated to ECN330 mode, the startup configuration is set to use this file, and the system is restarted.
- After the system reboots, the management VLANs (247-249 and 4093) are reserved and configured. The default Internal Management VLAN (VLAN 247) is set to obtain an IP address through DHCP, allowing management access to the ECN330-switch. Information on other default settings for the management VLANs is shown under “Configuring Management VLANs” on page 278.
- When the SBC is disabled, the ECN330 runs in ECN330-switch mode.
 - After disabling the SBC, the `Factory_Default_Config.cfg` is automatically regenerated to ECN330-switch mode, the startup configuration is set to use this file, and the system is restarted.
 - After the system reboots, the management VLANs (247-249 and 4093) are not set nor reserved (as in the ECN330 mode) and can now be configured. Only the default External Management VLAN (VLAN 246) is set to allow management access to the ECN330-switch. VLAN 246 is also changed to obtain an IP address through DHCP. Ports 1-27 are configured as untagged members of VLAN 1 and tagged members of VLAN 246. Interface 28 (that is, the SBC) is shut down.
 - Also, note that if the SBC is unplugged from the system, the operating mode is automatically changed to ECN330-switch mode.

Command Attributes

- **SBC** – Enables or disables the SBC. (Default: ON)

Web – Click System, SBC. Enable or disable the SBC, and click Apply.



Figure 12 System SBC Status

CLI – This example enables the SBC.

```
Console(config)#sbc power
System will switch to ECN330 mode, continue <y/n>? y

FS_STORAGE_Write::Begin writing to the protected area!!
FS_STORAGE_Write::Writing to the protected area completed.
```

6.3.5

Displaying ECN330-switch Hardware/Software Versions

Use the Switch Information page to display hardware/firmware version numbers for the main board and management software, as well as the power status of the system.

Field Attributes

Main Board

- **Serial Number** – The serial number of the ECN330-switch.
- **Number of Ports** – Number of built-in ports.
- **Hardware Version** – Hardware version of the main board.
- **Main Power Status** – Displays the status of the internal power supply.

Management Software

- **EPLD Version** – Version of EEPROM Programmable Logic Device.
- **Loader Version** – Version number of loader code.
- **Boot-ROM Version** – Version of Power-On Self-Test (POST) and boot code.
- **Operation Code Version** – Version number of runtime code.
- **Role** – Shows that the ECN330-switch is operating as Master (that is, operating stand-alone).

These additional parameters are displayed for the CLI.

- **Unit ID** – Unit number in stack.
- **Redundant Power Status** – Displays the status of the redundant power supply.

Web – Click System, Switch Information.

Switch Information	
Main Board:	
Serial Number	A521002155
Number of Ports	28
Hardware Version	ROB
Main Power Status	Active
Management Software:	
EPLD Version	1.02
Loader Version	1.2
Boot-ROM Version	1.1
Operation Code Version	3.15
Role	Master

Figure 13 Switch Information

CLI – Use the following command to display version information.

```

Console#show version
Unit 1
  Serial Number:      A521002166
  Hardware Version:   R0B
  EPLD Version:       1.02
  Number of Ports:    28
  Main Power Status:  Up

Agent (Master)
  Unit ID:            1
  Loader Version:     1.2
  Boot ROM Version:   1.1
  Operation Code Version: 3.15

Console#

```

6.3.6

Displaying Bridge Extension Capabilities

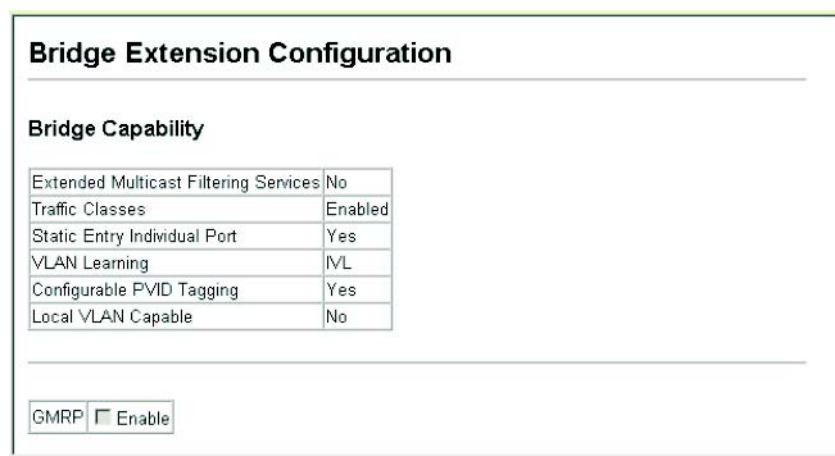
The Bridge MIB includes extensions for managed devices that support Multicast Filtering, Traffic Classes, and Virtual LANs. These extensions can be accessed to display default settings for the key variables.

Field Attributes

- **Extended Multicast Filtering Services** – The ECN330-switch does not support the filtering of individual multicast addresses based on GMRP (GARP Multicast Registration Protocol).
- **Traffic Classes** – The ECN330-switch provides mapping of user priorities to multiple traffic classes. (Refer to “Class of Service Configuration” on page 324.)
- **Static Entry Individual Port** – The ECN330-switch allows static filtering for unicast and multicast addresses. (Refer to 6.9.1 “Setting Static Addresses” 227.)
- **VLAN Learning** – The ECN330-switch uses Independent VLAN Learning (IVL), where each port maintains its own filtering database.
- **Configurable PVID Tagging** – The ECN330-switch allows the default Port VLAN ID (PVID used in frame tags) and egress status (VLAN-Tagged or Untagged) on each port to be overridden. (Refer to “VLAN Configuration” on page 272.)

- **Local VLAN Capable** – The ECN330-switch does not support multiple local bridges outside of the scope of 802.1Q defined VLANs.
- **GMRP** – GARP Multicast Registration Protocol (GMRP) allows network devices to register endstations with multicast groups. The ECN330-switch does not support GMRP; it uses the Internet Group Management Protocol (IGMP) to provide automatic multicast filtering.

Web – Click System, Bridge Extension.



The screenshot shows the 'Bridge Extension Configuration' web page. It features a 'Bridge Capability' section with a table of settings. Below the table is a 'GMRP' section with an 'Enable' checkbox that is currently unchecked.

Bridge Capability	
Extended Multicast Filtering Services	No
Traffic Classes	Enabled
Static Entry Individual Port	Yes
VLAN Learning	IVL
Configurable PVID Tagging	Yes
Local VLAN Capable	No

GMRP ☐ Enable

Figure 14 Bridge Extension Configuration

CLI – Enter the following command.

```
Console#show bridge-ext
Max support vlan numbers: 255
Max support vlan ID: 4094
Extended multicast filtering services: No
Static entry individual port: Yes
VLAN learning: IVL
Configurable PVID tagging: Yes
Local VLAN capable: Yes
Traffic classes: Enabled
Global GVRP status: Disabled
GMRP: Disabled
Console#
```


6.3.7 Configuring Support for Jumbo Frames

The ECN330-switch provides more efficient throughput for large sequential data transfers by supporting jumbo frames of up to 9216 bytes for the Gigabit Ethernet ports. Compared to standard Ethernet frames that run only up to 1.5 KB, using jumbo frames significantly reduces the per-packet overhead required to process protocol encapsulation fields.

Command Usage

To use jumbo frames, both the source and destination end nodes (such as a computer or server) must support this feature. Also, when the connection is operating at full duplex, all switches in the network between the two end nodes must be able to accept the extended frame size. And for half-duplex connections, all devices in the collision domain would need to support jumbo frames.

Command Attributes

- **Jumbo Packet Status** – Configures support for jumbo frames. (Default: Disabled)

Web – Click System, Jumbo Frames. Enable or disable support for jumbo frames, and click Apply.



Figure 15 Configuring Support for Jumbo Frames

CLI – This example enables jumbo frames globally for the switch.

```
Console(config)#jumbo frame
Console(config)#
```

6.3.8 Setting the ECN330-switch's IP Address

This section describes how to configure an initial IP interface for management access over the network. The IP address for the ECN330-switch is unassigned by default. To manually configure an address, the ECN330-switch's default settings need to be changed to values that are compatible with the network. A default gateway may also need to be established between the switch and management stations that exist on another network segment (if routing is not enabled on the switch).

A specific IP address can be manually configured, or the device directed to obtain an address from a BOOTP or DHCP server. Valid IP addresses consist of four decimal numbers, 0 to 255, separated by periods. Anything other than this format is not accepted by the CLI program.

For secure management access to the ECN330-switch, specify a management VLAN and use an IP address assigned to this VLAN interface to manage the ECN330-switch. The management VLAN applies to management access through the web, Telnet, SSH, and SNMP. To specify a management VLAN, see "Configuring Management VLANs" on page 278.

By default, the ECN330-switch is configured to operate in ECN330 mode (see "Enabling the SBC to Access Advanced Management Tools" on page 74). The factory defaults designate VLAN 246 for external management and VLAN 247 for internal management. VLAN 247 is already configured to obtain an IP address using DHCP. If the ECN330-switch is configured for ECN330-switch mode, then VLAN 246 is designated for external management and is configured to obtain an IP address using DHCP. All other management VLANs are disabled.

Note: When a management VLAN is enabled, IP addresses assigned to other VLAN interfaces cannot be used for management access.

Command Usage

- This section describes how to configure a single IP interface for initial access to the ECN330-switch. To configure additional IP interfaces for management access on the ECN330-switch, specify each VLAN to be used for management access (see "Configuring Management VLANs" on page 278), and configure an IP interface for each of these VLANs (see "Basic IP Interface Configuration" on page 401).

- There may be one or more management VLANs on the ECN330-switch, depending on whether the switch is set the ECN330 mode or ECN330-switch mode. Management VLANs operate as isolated VLANs and data traffic is not routed to or from other VLANs, nor is the management IP interface advertised by routing protocols to other routers.
- To enable routing between the different management interfaces on the ECN330-switch, IP routing must be enabled (see “Basic IP Interface Configuration” on page 401).
- To enable routing between the management interfaces defined on the ECN330-switch and external network interfaces, static routes must be configured (see “Configuring Static Routes” on page 421) or dynamic routing enabled; that is, either RIP (see “Configuring the Routing Information Protocol” on page 424) or OSPF (see “Configuring the Open Shortest Path First Protocol” on page 436).
- The ECN330-switch attempts to map outgoing IP traffic to a configured IP interface based on the following order of precedence:
 - IP / General / Routing Interface menu (page 403),
 - Static routes (page 421), and then
 - Dynamic routing using RIP (page 424) or OSPF (page 436).

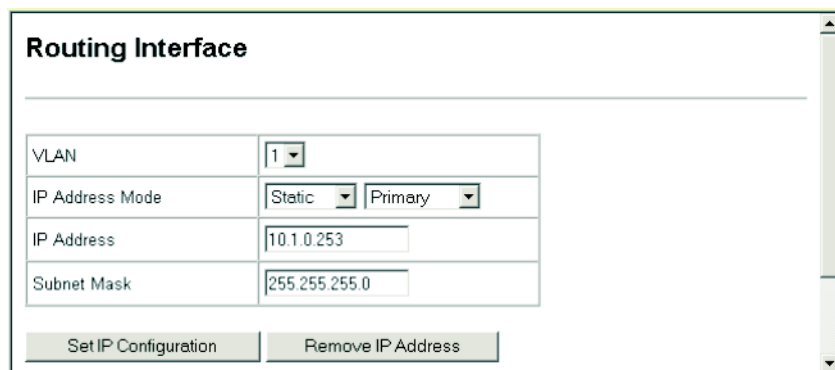
Command Attributes

- **VLAN** – ID of the configured VLAN (1-4094, no leading zeroes). The default configuration for ECN330 mode uses VLAN 246 for external management and VLAN 247 for internal management. VLAN 247 is already configured to obtain an IP address using DHCP. The default configuration for ECN330-switch mode designates all ports as tagged members of VLAN 246 and untagged members of VLAN 1. If the management station is attached directly to the ECN330 and a management VLAN has been enabled, it must be attached to a port belonging to the specified VLAN.
- **IP Address Mode** – Specifies whether IP functionality is enabled through manual configuration (Static), Dynamic Host Configuration Protocol (DHCP), or Boot Protocol (BOOTP). If DHCP/BOOTP is enabled, IP will not function until a reply has been received from the server. Requests will be broadcast periodically by the ECN330-switch for an IP address. (DHCP/BOOTP values can include the IP address, subnet mask, and default gateway.)

- **IP Address** – Address of the VLAN to which the management station is attached. Valid IP addresses consist of four numbers, 0 to 255, separated by periods. (Default: 0.0.0.0)
- **Subnet Mask** – This mask identifies the host address bits used for routing to specific subnets. (Default: 255.0.0.0)
- **Default Gateway** – IP address of the gateway router between this device and management stations that exist on other network segments. (Default: 0.0.0.0)

6.3.8.1 Manual Configuration

Web – Click IP, General, Routing Interface. Select the VLAN through which the management station is attached, set the IP Address Mode to “Static,” and specify a “Primary” interface. Enter the IP address, subnet mask and gateway, then click Apply.



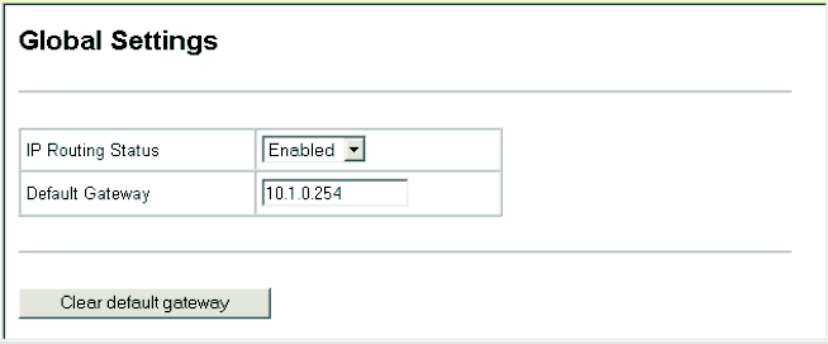
The screenshot shows a web-based configuration interface titled "Routing Interface". It contains a table with the following fields:

VLAN	1
IP Address Mode	Static Primary
IP Address	10.1.0.253
Subnet Mask	255.255.255.0

Below the table are two buttons: "Set IP Configuration" and "Remove IP Address".

Figure 16 IP Interface Configuration - Manual

Click IP, Global Setting. If the ECN330-switch and management stations exist on other network segments, then specify the default gateway, and click Apply.



Global Settings

IP Routing Status	Enabled ▾
Default Gateway	10.1.0.254

Clear default gateway

Figure 17 Default Gateway

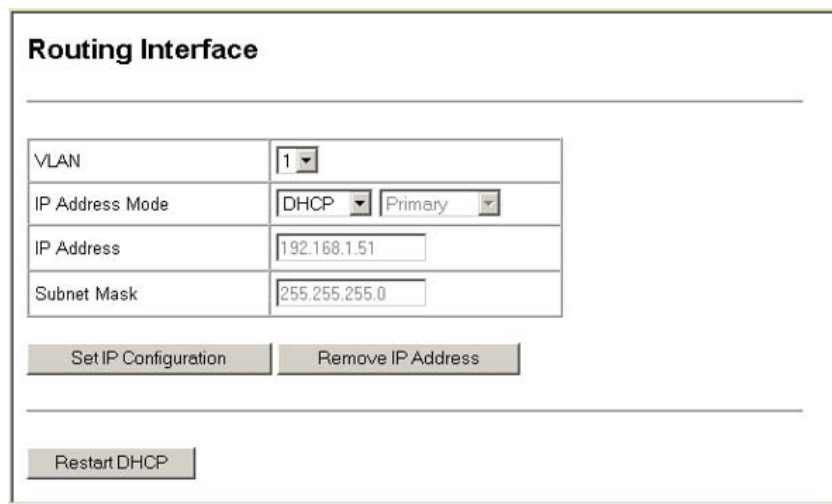
CLI – Specify the management interface, IP address and default gateway.

```
Console#config
Console(config)#interface vlan 1
Console(config-if)#ip address 10.1.0.253 255.255.255.0
Console(config-if)#exit
Console(config)#ip default-gateway 10.1.0.254
Console(config)#
```

6.3.8.2 Using DHCP/BOOTP

If the network provides DHCP/BOOTP services, the ECN330-switch can be configured to be dynamically configured by these services.

Web – Click IP, General, Routing Interface. Specify the VLAN to which the management station is attached, set the IP Address Mode to DHCP or BOOTP. Click Apply to save the changes. Then click Restart DHCP to immediately request a new address. Note that the ECN330-switch will also broadcast a request for IP configuration settings on each power reset.



The screenshot shows a web interface titled "Routing Interface". It contains a table with four rows for configuration: VLAN (set to 1), IP Address Mode (set to DHCP with a Primary dropdown), IP Address (set to 192.168.1.51), and Subnet Mask (set to 255.255.255.0). Below the table are two buttons: "Set IP Configuration" and "Remove IP Address". At the bottom of the form is a "Restart DHCP" button.

Routing Interface	
VLAN	1
IP Address Mode	DHCP Primary
IP Address	192.168.1.51
Subnet Mask	255.255.255.0

Set IP Configuration Remove IP Address

Restart DHCP

Figure 18 IP Interface Configuration - DHCP

Note: If the management connection is lost, use a console connection and enter **show ip interface** to determine the new ECN330-switch address.

CLI – Specify the management interface, and set the IP address mode to DHCP or BOOTP, and then enter the “ip dhcp restart client” command.

```

Console#config
Console(config)#interface vlan 1
Console(config-if)#ip address dhcp
Console(config-if)#end
Console#ip dhcp restart client
Console#show ip interface

Vlan 1 is up, addressing mode is DHCP
  Interface address is 192.168.1.249, mask is 255.255.255.0, Primary
  MTU is 1500 bytes
  Proxy ARP is disabled
  Split horizon is enabled
.
.
.

```

Renewing DHCP – DHCP may lease addresses to clients indefinitely or for a specific period of time. If the address expires or the ECN330-switch is moved to another network segment, management access to the ECN330-switch will be lost. In this case, reboot the ECN330-switch or submit a client request to restart DHCP service through the CLI.

Web – If the address assigned by DHCP is no longer functioning, the IP settings will not be able to be renewed through the web interface. The DHCP service can only be restarted through the web interface if the current address is still available.

CLI – Enter the following command to restart DHCP service.

```

Console#ip dhcp restart client
Console#

```

6.3.9 Managing Firmware

Firmware can be uploaded/downloaded to or from a TFTP server. By saving runtime code to a file on a TFTP server, that file can later be downloaded to the ECN330-switch to restore operation. The ECN330-switch can also be set to use new firmware without overwriting the previous version. Specify the method of file transfer, along with the file type and file names as required.

Command Attributes

- **File Transfer Method** - The firmware copy operation includes these options:
 - file to file - Copies a file within the ECN330-switch directory, assigning it a new name.
 - file to tftp - Copies a file from the ECN330-switch to a TFTP server.
 - tftp to file - Copies a file from a TFTP server to the ECN330-switch.
- **TFTP Server IP Address** – The IP address of a TFTP server.
- **File Type** – Specify opcode (operational code) to copy firmware.
- **File Name** – The file name should not contain slashes (\ or /), the leading letter of the file name should not be a period (.), and the maximum length for file names on the TFTP server is 127 characters or 31 characters for files on the ECN330-switch. (Valid characters: A-Z, a-z, 0-9, “.”, “-”, “_”)

Note: Up to two copies of the system software (that is, the runtime firmware) can be stored in the file directory on the ECN330-switch. The currently designated startup version of this file cannot be deleted.

6.3.9.1 Downloading System Software from a Server

When downloading runtime code, specify the destination file name to replace the current image, or first download the file using a different name from the current runtime code file, and then set the new file as the startup file.

Web – Click System, File Management, Copy Operation. Select “tftp to file” as the file transfer method, enter the IP address of the TFTP server, set the file type to “opcode,” enter the file name of the software to download, select a file on the ECN330-switch to overwrite or specify a new file name, then click Apply. If the current firmware used for startup is replaced, reboot the system through the System/Reset menu to start using the new operation code.

Copy

tftp to file

TFTP Server IP Address: 192.168.0.110

File Type: opcode

Source File Name: 32_8902_V3.15.bix

Destination File Name: ☒ CXC_132_8902_V1.31.bix ☐ 32_8902_V3.15.bix

Figure 19 Copy Firmware

If downloading to a new destination file, go to the File Management, Set Start-Up menu, mark the operation code file used at startup, and click Apply. To start the new firmware, reboot the system using the System/Reset menu.

Set Start-Up

Note: You can only change one file type at a time.

	Name	Type	Startup	Size(bytes)
☐	Factory_Default_Config.cfg	Config_File	N	6286
☒	startup1.cfg	Config_File	Y	6821
☐	CXC_132_8902_V1.31.bix	Operation_Code	N	4567344
☒	CXC_132_8902_V3.15.bix	Operation_Code	Y	5130696

Figure 20 Setting the Startup Code

To delete a file select System, File Management, Delete. Select the file name from the given list by checking the tick box and click Apply. Note that the file currently designated as the startup code cannot be deleted.

Delete

	Name	Type	Startup	Size (bytes)
☐	Factory_Default_Config.cfg	Config_File	N	6286
☐	startup1.cfg	Config_File	Y	6821
☒	CXC_132_8902_V1.31.bix	Operation_Code	N	4567344
☐	CXC_132_8902_V3.15.bix	Operation_Code	Y	5130696

Figure 21 Deleting Files

CLI – To download new firmware form a TFTP server, enter the IP address of the TFTP server, select “config” as the file type, then enter the source and destination file names. When the file has finished downloading, set the new file to start up the system, and then restart the ECN330-switch.

To start the new firmware, enter the “reload” command or reboot the system.

```

Console#copy tftp file
TFTP server ip address: 10.1.0.19
Choose file type:
  1. config:  2. opcode:  3. diag:  4. loader:  2
Source file name: CXC_132_8902_V3.15.BIX
Destination file name: CXC_132_8902_V3.15.BIX
\Write to FLASH Programming.
-Write to FLASH finish.
Success.
Console#config
Console(config)#boot system opcode:CXC_132_8902_V3.15.BIX
Console(config)#exit
Console#reload

```

6.3.10 Saving or Restoring Configuration Settings

Configuration settings can be uploaded/downloaded to/from a TFTP server. The configuration file can be later downloaded to restore the ECN330-switch's settings.

Command Attributes

- **File Transfer Method** – The configuration copy operation includes these options:
 - file to file – Copies a file within the ECN330-switch directory, assigning it a new name.
 - file to running-config – Copies a file in the ECN330-switch to the running configuration.
 - file to startup-config – Copies a file in the ECN330-switch to the startup configuration.
 - file to tftp – Copies a file from the ECN330-switch to a TFTP server.
 - running-config to file – Copies the running configuration to a file.
 - running-config to startup-config – Copies the running config to the startup config.
 - running-config to tftp – Copies the running configuration to a TFTP server.
 - startup-config to file – Copies the startup configuration to a file on the ECN330-switch.
 - startup-config to running-config – Copies the startup config to the running config.
 - startup-config to tftp – Copies the startup configuration to a TFTP server.
 - tftp to file – Copies a file from a TFTP server to the ECN330-switch.
 - tftp to running-config – Copies a file from a TFTP server to the running config.
 - tftp to startup-config – Copies a file from a TFTP server to the startup config.
- **TFTP Server IP Address** – The IP address of a TFTP server.

- **File Type** – Specify config (configuration) to copy configuration settings.
- **File Name** — The configuration file name should not contain slashes (\ or /), the leading letter of the file name should not be a period (.), and the maximum length for file names on the TFTP server is 127 characters or 31 characters for files on the ECN330-switch. (Valid characters: A-Z, a-z, 0-9, “.”, “-”, “_”)

Note: The maximum number of user-defined configuration files is limited only by available flash memory space.

6.3.10.1

Downloading Configuration Settings from a Server

The configuration file can be downloaded under a new file name and then set as the startup file, or the current startup configuration file can be specified as the destination file to directly replace it. Note that the file “Factory_Default_Config.cfg” can be copied to the TFTP server, but cannot be used as the destination on the ECN330-switch.

Web – Click System, File Management, Copy Operation. Choose “tftp to startup-config” or “tftp to file,” and enter the IP address of the TFTP server. Specify the name of the file to download, select a file on the ECN330-switch to overwrite or specify a new file name, and then click Apply.

Copy	
tftp to startup-config	
TFTP Server IP Address	192.168.1.19
Source File Name	config-startup
Startup File Name	☒ Factory_Default_Config.cfg ☐ startup

Figure 22 Downloading Configuration Settings for Start-Up

If downloading to a new file name using “tftp to startup-config” or “tftp to file,” the file is automatically set as the start-up configuration file. To use the new settings, reboot the system using the System/Reset menu. Or select any configuration file as the start-up configuration by using the System/File Management/Set Start-Up page.

Set Start-Up

Note: You can only change one file type at a time.

	Name	Type	Startup	Size(bytes)
☐	Factory_Default_Config.cfg	Config_File	N	6286
☒	startup	Config_File	N	6821
☐	startup1.cfg	Config_File	Y	6821
☒	CXC_132_8902_V3.15.bix	Operation_Code	Y	5130696

Figure 23 Setting the Startup Configuration Settings

CLI – Enter the IP address of the TFTP server, specify the source file on the server, set the startup file name on the ECN330-switch, and then restart the ECN330-switch.

```

Console#copy tftp startup-config
TFTP server ip address: 192.168.1.19
Source configuration file name: config-1
Startup configuration file name [] : startup
\Write to FLASH Programming.
-Write to FLASH finish.
Success.

Console#reload

```

If the startup configuration file is downloaded under a new file name, this file can be set as the startup file at a later time before restarting the ECN330-switch.

```

Console#config
Console(config)#boot system config: startup
Console(config)#exit
Console#reload

```

6.3.11 Console Port Settings

The onboard configuration program can be accessed by attaching a VT100 compatible device to the ECN330's serial console port. Management access through the console port is controlled by various parameters, including a password, timeouts, and basic communication settings. These parameters can be configured using the web or CLI interface.

Command Attributes

- **Login Timeout** – Sets the interval that the system waits for a user to log into the CLI. If a login attempt is not detected within the timeout interval, the connection is terminated for the session. (Range: 0 - 300 seconds; Default: 0)
- **Exec Timeout** – Sets the interval that the system waits until user input is detected. If user input is not detected within the timeout interval, the current session is terminated. (Range: 0 - 65535 seconds; Default: 0 seconds)
- **Password Threshold** – Sets the password intrusion threshold, which limits the number of failed logon attempts. When the logon attempt threshold is reached, the system interface becomes silent for a specified amount of time (set by the Silent Time parameter) before allowing the next logon attempt. (Range: 0-120; Default: 3 attempts)
- **Silent Time** – Sets the amount of time the management console is inaccessible after the number of unsuccessful logon attempts has been exceeded. (Range: 0-65535; Default: 0)
- **Data Bits** – Sets the number of data bits per character that are interpreted and generated by the console port. If parity is being generated, specify 7 data bits per character. If no parity is required, specify 8 data bits per character. (Default: 8 bits)
- **Parity** – Defines the generation of a parity bit. Communication protocols provided by some terminals can require a specific parity bit setting. Specify Even, Odd, or None. (Default: None)
- **Speed** – Sets the terminal line's baud rate for transmit (to terminal) and receive (from terminal). Set the speed to match the baud rate of the device connected to the serial port. (Range: 9600, 19200, 38400, 57600, or 115200 baud; Default: 9600 baud)

- **Stop Bits** – Sets the number of the stop bits transmitted per byte. (Range: 1-2; Default: 1 stop bit)

These parameters can only be configured in the CLI.

- **Password** – Specifies a password for the line connection. When a connection is started on a line with password protection, the system prompts for the password. If the correct password is entered, the system shows a prompt. (Default: No password)
- **Login** – Enables password checking at login. Select authentication by entering a single global password as configured for the Password parameter, or by entering a password set up for a specific user-name account. (Default: Local)

Web – Click System, Line, Console. Specify the console port connection parameters as required, then click Apply.

Console	
Login Timeout (0-300)	0 secs (0 : Disabled)
Exec Timeout (0-65535)	0 secs (0 : Disabled)
Password Threshold (0-120)	3 (0 : Disabled)
Silent Time (0-65535)	0 secs (0 : Disabled)
Data Bits	8
Parity	None
Speed	9600
Stop Bits	1

Figure 24 Configuring the Console Port

CLI – Enter Line Configuration mode for the console, then specify the connection parameters as required. To display the current console port settings, use the **show line** command from the Normal Exec level.

```

Console(config)#line console
Console(config-line)#login local
Console(config-line)#password 0 secret
Console(config-line)#timeout login response 0
Console(config-line)#exec-timeout 0
Console(config-line)#password-thresh 5
Console(config-line)#silent-time 60
Console(config-line)#databits 8
Console(config-line)#parity none
Console(config-line)#speed 9600
Console(config-line)#stopbits 1
Console(config-line)#end
Console#show line console
  Console configuration:
    Password threshold:  5 times
    Interactive timeout:  Disabled
    Login timeout:       Disabled
    Silent time:         60
    Baudrate:            9600
    Databits:            8
    Parity:              none
    Stopbits:            1
Console#

```

6.3.12 Telnet Settings

The onboard configuration program can be accessed over the network using Telnet (that is, a virtual terminal). Management access through Telnet can be enabled/disabled and other various parameters set, including the TCP port number, timeouts, and a password. These parameters can be configured using the web or CLI interface.

Command Attributes

- **Telnet Status** – Enables or disables Telnet access to the ECN330-switch. (Default: Enabled)
- **Telnet Port Number** – Sets the TCP port number for Telnet on the ECN330-switch. (Range: 1-65535; Default: 23)
- **Login Timeout** – Sets the interval that the system waits for a user to log into the CLI. If a login attempt is not detected within the timeout interval,

the connection is terminated for the session. (Range: 0 - 300 seconds; Default: 300 seconds)

- **Exec Timeout** – Sets the interval that the system waits until user input is detected. If user input is not detected within the timeout interval, the current session is terminated. (Range: 0 - 65535 seconds; Default: 600 seconds)
- **Password Threshold** – Sets the password intrusion threshold, which limits the number of failed logon attempts. When the logon attempt threshold is reached, the system interface becomes silent for a specified amount of time (set by the Silent Time parameter) before allowing the next logon attempt. (Range: 0-120; Default: 3 attempts)

These parameters can only be configured in the CLI.

- **Password** – Specifies a password for the line connection. When a connection is started on a line with password protection, the system prompts for the password. If the correct password is entered, the system shows a prompt. (Default: No password)
- **Login** – Enables password checking at login. Select authentication by a entering single global password as configured for the Password parameter, or by entering a password set up for a specific user-name account. (Default: Local)

Web – Click System, Line, Telnet. Specify the connection parameters for Telnet access, then click Apply.

Telnet	
Telnet Status	☒ Enabled
Telnet Port Number	23
Login Timeout (0-300)	300 secs (0 : Disabled)
Exec Timeout (0-65535)	600 secs (0 : Disabled)
Password Threshold (0-120)	8 (0 : Disabled)

Figure 25 Configuring the Telnet Interface

CLI – Enter Line Configuration mode for a virtual terminal, then specify the connection parameters as required. To display the current virtual terminal settings, use the **show line** command from the Normal Exec level.

```
Console(config)#line vty
Console(config-line)#login local
Console(config-line)#password 0 secret
Console(config-line)#timeout login response 300
Console(config-line)#exec-timeout 600
Console(config-line)#password-thresh 3
Console(config-line)#end
Console#show line vty
VTY configuration:
  Password Threshold: 3 times
  Interactive Timeout: 600 sec
  Login Timeout:      300 sec
Console#
```

6.3.13 Configuring Event Logging

The ECN330-switch allows the logging of error messages to be controlled, including the type of events that are recorded in switch memory, logging to a remote System Log (syslog) server, and displays a list of recent event messages.

6.3.13.1 System Log Configuration

The system allows event logging to be enabled or disabled, and which levels are logged to RAM or flash memory to be specified.

Severe error messages that are logged to flash memory are permanently stored in the ECN330-switch to assist in troubleshooting network problems. Up to 4096 log entries can be stored in the flash memory, with the oldest entries being overwritten first when the available log memory (256 kilobytes) has been exceeded.

The System Logs page allows system messages that are logged to flash or RAM memory to be configured and limited. The default is for event levels 0 to 3 to be logged to flash and levels 0 to 7 to be logged to RAM.

Command Attributes

- **System Log Status** – Enables/disables the logging of debug or error messages to the logging process. (Default: Enabled)
- **Flash Level** – Limits log messages saved to the ECN330-switch's permanent flash memory for all levels up to the specified level. For example, if level 3 is specified, all messages from level 0 to level 3 will be logged to flash. (Range: 0-7, Default: 3)

Table 9 Logging Levels

Level	Severity Name	Description
7	Debug	Debugging messages
6	Informational	Informational messages only
5	Notice	Normal but significant condition, such as cold start
4	Warning	Warning conditions (for example, return false, unexpected return)
3	Error	Error conditions (for example, invalid input, default used)
2	Critical	Critical conditions (for example, memory allocation, or free memory error - resource exhausted)
1	Alert	Immediate action needed
0	Emergency	System unusable

* There are only Level 2, 5 and 6 error messages for the current firmware release.

- **RAM Level** – Limits log messages saved to the ECN330-switch's temporary RAM memory for all levels up to the specified level. For example, if level 7 is specified, all messages from level 0 to level 7 will be logged to RAM. (Range: 0-7, Default: 7)

Note: The Flash Level must be equal to or less than the RAM Level.

Web – Click System, Log, System Logs. Specify System Log Status, set the level of event messages to be logged, and click Apply.

System Logs	
System Log Status	☒ Enabled
Flash Level (0-7)	3
Ram Level (0-7)	7

Figure 26 System Logs

CLI – Enable system logging and then specify the level of messages to be logged to RAM and flash memory. Use the **show logging** command to display the current settings.

```
Console(config)#logging on
Console(config)#logging history ram 0
Console(config)#
Console#show logging flash
Syslog logging:           Enabled
History logging in FLASH: level errors
Console#
```

6.3.13.2

Remote Log Configuration

The Remote Logs page allows the logging of messages that are sent to syslog servers or other management stations to be configured. Event messages can also be limited to send only those messages at or above a specified level.

Command Attributes

- **Remote Log Status** – Enables/disables the logging of debug or error messages to the remote logging process. (Default: Disabled)
- **Logging Facility** – Sets the facility type for remote logging of syslog messages. There are eight facility types specified by values of 16 to 23. The facility type is used by the syslog server to dispatch log messages to an appropriate service.

- The attribute specifies the facility type tag sent in syslog messages. (See RFC 3164.) This type has no effect on the kind of messages reported by the ECN330-switch. However, it may be used by the syslog server to process messages, such as sorting or storing messages in the corresponding database. (Range: 16-23, Default: 23)
- **Logging Trap** – Limits log messages that are sent to the remote syslog server for all levels up to the specified level. For example, if level 3 is specified, all messages from level 0 to level 3 will be sent to the remote server. (Range: 0-7, Default: 7)
- **Host IP List** – Displays the list of remote server IP addresses that will receive syslog messages. The maximum number of host IP addresses allowed is five.
- **Host IP Address** – Specifies a new server IP address to add to the Host IP List.

Web – Click System, Log, Remote Logs. To add an IP address to the Host IP List, type the new IP address in the Host IP Address box, and then click Add. To delete an IP address, click the entry in the Host IP List, and then click Remove.

Remote Logs

Remote Log Status	☐ Enabled
Logging Facility (16-23)	23
Logging Trap (0-7)	7

Host IP Address:

Current:

Host IP List

(none)

<< Add

Remove

New:

Host IP Address

Figure 27 Remote Logs

CLI – Enter the syslog server host IP address, choose the facility type and set the logging trap.

```

Console(config)#logging host 10.1.0.9
Console(config)#logging facility 23
Console(config)#logging trap 4
Console(config)#logging trap
Console(config)#
Console#show logging trap
Syslog logging:           Enabled
REMOTELOG status:        Disabled
REMOTELOG facility type:  local use 7
REMOTELOG level type:     Warning conditions
REMOTELOG server ip address: 10.1.0.9
REMOTELOG server ip address: 0.0.0.0
REMOTELOG server ip address: 0.0.0.0
REMOTELOG server ip address: 0.0.0.0
REMOTELOG server ip address: 0.0.0.0
Console#

```

6.3.13.3

Displaying Log Messages

Use the Logs page to scroll through the logged system and event messages. The ECN330-switch can store up to 2048 log entries in temporary random access memory (RAM; that is, memory flushed on power reset) and up to 4096 entries in permanent flash memory.

Web – Click System, Log, Logs.

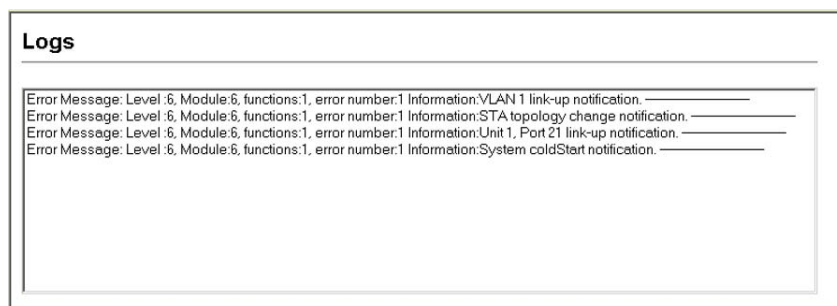


Figure 28 Displaying Logs

CLI – This example shows the event message stored in RAM.

```

Console#show log ram
[1] 00:01:30 2001-01-01
    "VLAN 1 link-up notification."
    level: 6, module: 5, function: 1, and event no.: 1
[0] 00:01:30 2001-01-01
    "Unit 1, Port 1 link-up notification."
    level: 6, module: 5, function: 1, and event no.: 1
Console#

```

6.3.13.4

Sending Simple Mail Transfer Protocol Alerts

To alert system administrators of problems, the ECN330-switch can use SMTP (Simple Mail Transfer Protocol) to send email messages when triggered by logging events of a specified level. The messages are sent to specified SMTP servers on the network and can be retrieved using POP or IMAP clients.

Command Attributes

- **Admin Status** – Enables/disables the SMTP function.
(Default: Enabled)
- **Email Source Address** – Sets the email address used for the “From” field in alert messages. Use a symbolic email address that identifies the ECN330-switch, or the address of an administrator responsible for the ECN330.
- **Severity** – Sets the syslog severity threshold level (see the table on page 97) used to trigger alert messages. All events at this level or higher will be sent to the configured email recipients. For example, using Level 7 will report all events from level 7 to level 0. (Default: Level 7)
- **SMTP Server List** – Specifies a list of up to three recipient SMTP servers. The ECN330-switch attempts to connect to the other listed servers if the first fails. Use the New SMTP Server text field and the Add/Remove buttons to configure the list.
- **Email Destination Address List** – Specifies the email recipients of alert messages. Specify up to five recipients. Use the New Email Destination Address text field and the Add/Remove buttons to configure the list.

Web – Click System, Log, SMTP. Enable SMTP, specify a source email address, and select the minimum severity level. To add an IP address to the SMTP Server List, type the new IP address in the SMTP Server field and click Add. To delete an IP address, click the entry in the SMTP Server List and click Remove. Specify up to five email addresses to receive the alert messages, and click Apply.

SMTP

Admin Status	☒ Enabled
Email Source Address	pig-wheels@matel.com
Severity	4 - Warning

SMTP Server List:

192.168.1.4
192.168.1.5

<< Add
Remove

New:

SMTP Server

Email Destination Address List:

chris@matel.com

<< Add
Remove

New:

Email Destination Address

Figure 29 Enabling and Configuring SMTP Alerts

CLI – Enter the IP address of at least one SMTP server, set the syslog severity level to trigger an email message, and specify the ECN330-switch (source) and up to five recipient (destination) email addresses. Enable SMTP with the **logging sendmail** command to complete the configuration. Use the **show logging sendmail** command to display the current SMTP configuration.

```

Console(config)#logging sendmail host 192.168.1.4
Console(config)#logging sendmail level 3
Console(config)#logging sendmail source-email
    big-wheels@matel.com
Console(config)#logging sendmail destination-email
    chris@matel.com
Console(config)#logging sendmail
Console(config)#exit
Console#show logging sendmail
SMTP servers
-----
    1. 192.168.1.4

SMTP minimum severity level: 4

SMTP destination email addresses
-----
    1. chris@matel.com

SMTP source email address: big-wheels@matel.com

SMTP status:                      Enabled
Console#

```

6.3.14 Resetting the System

Web – Click System, Reset. Click the Reset button to restart the ECN330-switch. When prompted, confirm to reset the ECN330-switch.



Figure 30 Resetting the System

CLI – Use the reload command to restart the ECN330-switch.

```
Console#reload
System will be restarted, continue <y/n>?
```

Note: When restarting the system, it will always run the Power-On Self-Test.

6.3.15 Setting the System Clock

Simple Network Time Protocol (SNTP) allows the ECN330-switch to set its internal clock based on periodic updates from a time server (SNTP or NTP). Maintaining an accurate time on the ECN330-switch enables the system log to record meaningful dates and times for event entries. The clock can also be set manually using the CLI. (See “calendar set” on page 606.) If the clock is not set, the ECN330-switch will only record the time from the factory default set at the last bootup.

When the SNTP client is enabled, the ECN330-switch periodically sends a request for a time update to a configured time server. Up to three time server IP addresses can be configured. The ECN330-switch will attempt to poll each server in the configured sequence.

6.3.15.1 Configuring SNTP

The ECN330-switch can be configured to send time synchronization requests to time servers.

Command Attributes

- **SNTP Client** – Configures the ECN330-switch to operate as an SNTP client. This requires at least one time server to be specified in the SNTP Server field. (Default: Disabled)
- **SNTP Poll Interval** – Sets the interval between sending requests for a time update from a time server. (Range: 16-16284 seconds; Default: 16 seconds)
- **SNTP Server** – Sets the IP address for up to three time servers. The ECN330-switch attempts to update the time from the first server, if this fails it attempts an update from the next server in the sequence.

Web – Select SNTP, Configuration. Modify any of the required parameters, and click Apply.

SNTP Configuration			
SNTP Client	☒ Enabled		
SNTP Polling Interval (16-16384)	16		
SNTP Server	10.1.0.19	137.82.140.80	128.250.36.2

Figure 31 SNTP Configuration

CLI – This example configures the ECN330-switch to operate as an SNTP client and then displays the current time and settings.

```

Console(config)#sntp client
Console(config)#sntp poll 16
Console(config)#sntp server 10.1.0.19 137.82.140.80 128.250.36.2
Console(config)#exit
Console#show sntp
Current Time: Jan 6 14:56:05 2004
Poll Interval: 60
Current Mode: unicast
SNTP Status: Enabled
SNTP Server: 10.1.0.19 137.82.140.80 128.250.36.2
Current Server: 128.250.36.2
Console#

```

6.3.15.2 Setting the Time Zone

SNTP uses Coordinated Universal Time (or UTC, formerly Greenwich Mean Time, or GMT) based on the time at the Earth's prime meridian, zero degrees longitude. To display a time corresponding to the local time, indicate the number of hours and minutes the time zone is east (before) or west (after) of UTC.

Command Attributes

- **Current Time** – Displays the current time.
- **Name** – Assigns a name to the time zone. (Range: 1-29 characters)
- **Hours (0-13)** – The number of hours before/after UTC.

- **Minutes (0-59)** – The number of minutes before/after UTC.
- **Direction** – Configures the time zone to be before (east) or after (west) UTC.

Web – Select SNTP, Clock Time Zone. Set the offset for the time zone relative to the UTC, and click Apply.

Clock Time Zone	
Note: The maximum value is 13:00	
Current Time	Jan 1 01:31:02 2001
Name	
Hours (0-13)	0
Minutes (0-59)	0
Direction	☐ Before-UTC ☒ After-UTC

Figure 32 Clock Time Zone

CLI - This example shows how to set the time zone for the system clock.

```
Console(config)#clock timezone Dhaka hours 6 minute 0 after-UTC
Console#
```

6.4 Simple Network Management Protocol

Simple Network Management Protocol (SNMP) is a communication protocol designed specifically for managing devices on a network. Equipment commonly managed with SNMP includes switches, routers and host computers. SNMP is typically used to configure these devices for proper operation in a network environment, as well as to monitor them to evaluate performance or detect potential problems.

Managed devices supporting SNMP contain software, which runs locally on the device and is referred to as an agent. A defined set of variables, known as managed objects, is maintained by the SNMP agent and used to manage the device. These objects are defined in a Management Information Base (MIB) that provides a standard presentation of the information controlled by the agent.

SNMP defines both the format of the MIB specifications and the protocol used to access this information over the network.

The ECN330-switch includes an onboard agent that supports SNMP versions 1, 2c, and 3. This agent continuously monitors the status of the ECN330-switch hardware, as well as the traffic passing through its ports. A network management station can access this information using SNMP-based management software. Access to the onboard agent from clients using SNMP v1 and v2c is controlled by community strings. To communicate with the ECN330-switch, the management station must first submit a valid community string for authentication.

Access to the ECN330-switch using from clients using SNMPv3 provides additional security features that cover message integrity, authentication, and encryption; as well as controlling user access to specific areas of the MIB tree.

The SNMPv3 security structure consists of security models, with each model having it's own security levels. There are three security models defined, SNMPv1, SNMPv2c, and SNMPv3. Users are assigned to "groups" that are defined by a security model and specified security levels. Each group also has a defined security access to set of MIB objects for reading and writing, which are known as "views." The ECN330-switch has a default view (all MIB objects) and default groups defined for security models v1 and v2c. Table 10 shows the security models and levels available and the system default settings.

Table 10 SNMPv3 Security Models and Levels

Model	Level	Group	Read View	Write View	Notify View	Security
v1	noAuthNoPriv	public	default view	none	none	Community string only
v1	noAuthNoPriv	private	default view	default view	none	Community string only
v1	noAuthNoPriv	user defined	user defined	user defined	user defined	Community string only
v2c	noAuthNoPriv	public	default view	none	none	Community string only

Model	Level	Group	Read View	Write View	Notify View	Security
v2c	noAuthNoPriv	private	default view	default view	none	Community string only
v2c	noAuthNoPriv	user defined	user defined	user defined	user defined	Community string only
v3	noAuthNoPriv	user defined	user defined	user defined	user defined	A user name match only
v3	AuthNoPriv	user defined	user defined	user defined	user defined	Provides user authentication through MD5 or SHA algorithms
v3	AuthPriv	user defined	user defined	user defined	user defined	Provides user authentication through MD5 or SHA algorithms and data privacy using DES 56-bit encryption

Note: The predefined default groups and view can be deleted from the system. Customized groups and views can then be defined for the SNMP clients that require access.

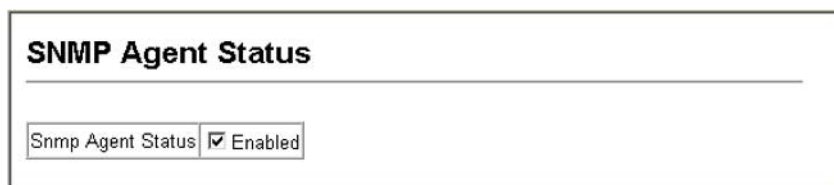
6.4.1 Enabling the SNMP Agent

Enables SNMPv3 service for all management clients (that is, versions 1, 2c, 3).

Command Attributes

SNMP Agent Status – Enables SNMP on the ECN330-switch.

Web – Click SNMP, Agent Status. Enable the SNMP Agent by marking the Enabled checkbox, and click Apply.



The image shows a web-based configuration window titled "SNMP Agent Status". Inside the window, there is a label "Snmp Agent Status" followed by a checkbox that is checked and labeled "Enabled".

Figure 33 Enabling the SNMP Agent

CLI – The following example enables SNMP on the ECN330-switch.

```
Console(config)#snmp-server
Console(config)#
```

6.4.2

Setting Community Access Strings

Up to five community strings can be configured, which authorize management access by clients using SNMP v1 and v2c. All community strings used for IP Trap Managers should be listed in this table. For security reasons, consider removing the default strings.

Command Attributes

- **SNMP Community Capability** – The ECN330-switch supports up to five community strings.
- **Current** – Displays a list of the community strings currently configured.
- **Community String** – A community string that acts like a password and permits access to the SNMP protocol.
Default strings: “public” (read/write access), “private” (read/write access)
Range: 1-32 characters, case sensitive
- **Access Mode** – Specifies the access rights for the community string:
 - **Read-Only** – Authorized management stations are only able to retrieve MIB objects.
 - **Read/Write** – Authorized management stations are able to both retrieve and modify MIB objects.

Web – Click SNMP, Configuration. Add new community strings as required, select the access rights from the Access Mode drop-down list, then click Add.

The image shows a web-based configuration window titled "SNMP Configuration". Inside, there is a section for "SNMP Community:" with a sub-label "SNMP Community Capability: 5". Below this, there are two columns: "Current:" and "New:". The "Current:" column contains a list box with two items: "public RW" and "private RW". To the right of this list box are two buttons: "<< Add" and "Remove". The "New:" column contains two input fields: "Community String" and "Access Mode". The "Access Mode" field is a dropdown menu currently set to "Read-Only".

Figure 34 Configuring SNMP Community Strings

CLI – The following example adds the string “spiderman” with read/write access.

```
Console(config)#snmp-server community spiderman rw
Console(config)#
```

6.4.3 Specifying Trap Managers and Trap Types

Traps indicating status changes are issued by the ECN330-switch to specified trap managers. Trap managers must be specified so that key events are reported by the ECN330-switch to the management station (using SNMP network management software). Up to five management stations can be specified to receive authentication failure messages and other trap messages from the ECN330-switch.

Command Usage

- When specifying an SNMP Version 3 host, the “Trap Manager Community String” is interpreted as an SNMP user name. If V3 authentication or encryption options (authNoPriv or authPriv) are used, the user name must first be defined in the SNMPv3 Users page (page 116). Otherwise, the authentication password and privacy password or both will not exist, and the ECN330-switch will not authorize SNMP access for the host. However, if a V3 host is specified with the no authentication (noAuth) option, an SNMP user account will

be automatically generated, and the ECN330-switch will authorize SNMP access for the host.

- Notifications are issued by the ECN330-switch as trap messages by default. The recipient of a trap message does not send a response to the ECN330-switch. Traps are therefore not as reliable as inform messages, which include a request for acknowledgement of receipt. Informs can be used to ensure that critical information is received by the host. However, note that informs consume more system resources because they must be kept in memory until a response is received. Informs also add to network traffic. These effects should be considered when deciding whether to issue notifications as traps or informs.

To send an inform to a SNMPv2c host, complete these steps:

1. Enable the SNMP agent (page 108).
2. Enable trap informs as described in the following pages.
3. Create a view with the required notification messages (page 123).
4. Create a group that includes the required notify view (page 121).

To send an inform to a SNMPv3 host, complete these steps:

1. Enable the SNMP agent (page 108).
2. Enable trap informs as described in the following pages.
3. Create a view with the required notification messages (page 123).
4. Create a group that includes the required notify view (page 121).
5. Specify a remote engine ID where the user resides (page 115).
6. Then configure a remote user (page 118).

Command Attributes

- **Trap Manager Capability** – The ECN330-switch supports up to five trap managers.
- **Current** – Displays a list of the trap managers currently configured.
- **Trap Manager IP Address** – IP address of a new management station to receive trap messages.

- **Trap Manager Community String** – Specifies a valid community string for the new trap manager entry. Though this string can be set in the Trap Managers table, it is recommended that this string be defined in the SNMP Configuration page (for Version 1 or 2c clients), or define a corresponding “User Name” in the SNMPv3 Users page (for Version 3 clients). (Range: 1-32 characters, case sensitive)
- **Trap UDP Port** – Specifies the UDP port number used by the trap manager.
- **Trap Version** – Indicates if the user is running SNMP v1, v2c, or v3. (Default: v1)
- **Trap Security Level** – When trap version 3 is selected, specify one of the following security levels. (Default: noAuthNoPriv)
 - **noAuthNoPriv** – There is no authentication or encryption used in SNMP communications.
 - **AuthNoPriv** – SNMP communications use authentication, but the data is not encrypted (only available for the SNMPv3 security model).
 - **AuthPriv** – SNMP communications use both authentication and encryption (only available for the SNMPv3 security model).
- **Trap Inform** – Notifications are sent as inform messages. Note that this option is only available for version 2c and 3 hosts. (Default: traps are used)
 - **Timeout** – The number of seconds to wait for an acknowledgment before resending an inform message. (Range: 0-2147483647 centiseconds; Default: 1500 centiseconds)
 - **Retry times** – The maximum number of times to resend an inform message if the recipient does not acknowledge receipt. (Range: 0-255; Default: 3)
- **Enable Authentication Traps** – Issues a trap message to specified IP trap managers whenever authentication of an SNMP request fails. (Default: Enabled)
- **Enable Link-up and Link-down Traps** – Issues a trap message whenever a port link is established or broken. (Default: Enabled)

Note: **Enable Authentication Traps** and **Enable Link-up and Link-down Traps** are legacy notifications and therefore when used for SNMP Version 3

hosts, they must be enabled in conjunction with the corresponding entries in the Notification View (page 3-48).

Web – Click SNMP, Configuration. Enter the IP address and community string for each management station that will receive trap messages, specify the UDP port, SNMP trap version, trap security level (for v3 clients), trap inform settings (for v2c/v3 clients), and then click Add. Select the trap types required using the check boxes for Authentication and Link-up/down traps, and then click Apply.

Trap Managers:

Trap Manager Capability: 5

Current: (none) << Add Remove

New:

Trap Manager IP Address	10.1.19.23
Trap Manager Community String	private
Trap UDP Port	160
Trap Version	2c
Trap Security Level	noAuthNoPriv
☒ Trap Inform	Timeout (0-2147483647) (1/100 secs)
	Retry times (0-255)

Enable Authentication Traps: ☒

Enable Link-up and Link-down Traps: ☐

Figure 35 Configuring SNMP Trap Managers

CLI – This example adds a trap manager and enables authentication traps.

```
Console(config)#snmp-server host 10.1.19.23 batman private
version 2c udp-port 162
Console(config)#snmp-server enable traps authentication
Console(config)#
```

6.4.4

Configuring SNMPv3 Management Access

To configure SNMPv3 management access to the ECN330-switch, follow these steps:

1. Configure an SNMP engine ID.
2. Specify read and write access views for the ECN330-switch MIB tree.
3. Configure SNMP user groups with the required security model (that is, SNMP v1, v2c or v3) and security level (that is, authentication and privacy).

4. Assign SNMP users to groups, along with their specific authentication and privacy passwords.

6.4.4.1 Setting a Local Engine ID

An SNMPv3 engine is an independent SNMP agent that resides on the ECN330-switch. This engine protects against message replay, delay, and redirection. The engine ID is also used in combination with user passwords to generate the security keys for authenticating and encrypting SNMPv3 packets.

A local engine ID is automatically generated that is unique to the ECN330-switch. This is referred to as the default engine ID. If the local engineID is deleted or changed, all SNMP users will be cleared. All existing users will need to be reconfigured.

A new engine ID can be specified by entering 10 to 64 hexadecimal characters.

Web – Click SNMP, SNMPv3, Engine ID. Enter an ID of up to 64 hexadecimal characters and then click Save.

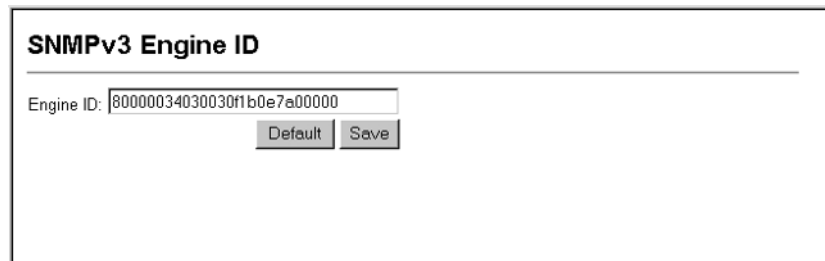


Figure 36 Setting the SNMPv3 Engine ID

CLI – This example sets an SNMPv3 engine ID.

```
Console(config)#snmp-server engine-id local 12345abcdef
Console(config)#exit
Console#show snmp engine-id
Local SNMP engineID: 12345abcdef0000000000000000
Local SNMP engineBoots: 1
Console#
```

6.4.4.2 Specifying a Remote Engine ID

To send inform messages to an SNMPv3 user on a remote device, first specify the engine identifier for the SNMP agent on the remote device where the user resides. The remote engine ID is used to compute the security digest for authenticating and encrypting packets sent to a user on the remote host.

SNMP passwords are localized using the engine ID of the authoritative agent. For informs, the authoritative SNMP agent is the remote agent. Therefore the remote agent's SNMP engine ID needs to be configured before sending proxy requests or informs to it. (See "Specifying Trap Managers and Trap Types" on page 110 and "Configuring Remote SNMPv3 Users" on page 118.)

The engine ID can be specified by entering 10 to 64 hexadecimal characters.

Web – Click SNMP, SNMPv3, Remote Engine ID. Enter an ID of up to 64 hexadecimal characters and then click Save.

Remote Engine ID	Remote IP Host	Action
8000000030004e2b316c54321	192.168.1.19	Remove
		Add

Figure 37 Setting an Engine ID

CLI – This example specifies a remote SNMPv3 engine ID.

```

Console(config)#snmp-server engineID remote 54321 192.168.1.19
Console(config)#exit
Console#show snmp engine-id
Local SNMP engineID: 8000002a8000000000e8666672
Local SNMP engineBoots: 1

Remote SNMP engineID                               IP address
80000000030004e2b316c54321                         192.168.1.19
Console#

```

6.4.4.3 Configuring SNMPv3 Users

Each SNMPv3 user is defined by a unique name. Users must be configured with a specific security level and assigned to a group. The SNMPv3 group restricts users to a specific read, write, or notify view.

Command Attributes

- **User Name** – The name of user connecting to the SNMP agent.
(Range: 1-32 characters)
- **Group Name** – The name of the SNMP group to which the user is assigned. (Range: 1-32 characters)
- **Security Model** – The user security model; SNMP v1, v2c or v3.
- **Security Level** – The security level used for the user:
 - noAuthNoPriv – There is no authentication or encryption used in SNMP communications. (This is the default for SNMPv3.)
 - AuthNoPriv – SNMP communications use authentication, but the data is not encrypted (only available for the SNMPv3 security model).
 - AuthPriv – SNMP communications use both authentication and encryption (only available for the SNMPv3 security model).
- **Authentication Protocol** – The method used for user authentication.
(Options: MD5, SHA; Default: MD5)
- **Authentication Password** – A minimum of eight plain text characters is required.
- **Privacy Protocol** – The encryption algorithm use for data privacy; only 56-bit DES is currently available
- **Privacy Password** – A minimum of eight plain text characters is required.
- **Actions** – Enables the user to be assigned to another SNMPv3 group.

Web – Click SNMP, SNMPv3, Users. Click New to configure a user name. In the New User page, define a name and assign it to a group, then click Add to save the configuration and return to the User Name list. To delete a user, check the box next to the user name, then click Delete. To change the assigned group of a user, click Change Group in the Actions column of the users table and select the new group.

SNMPv3 Users

New... Delete

	User Name	Group Name	Model	Level	Authentication	Privacy	Actions
☐	david	DefaultROGroup	V1	noAuthNoPriv	None	None	Change Group...
☐	chris	snmpv3users	V3	authPriv	MD5	DES56	Change Group...
☐	steve	snmpv3users	V3	authNoPriv	MD5	None	Change Group...

SNMPv3 Users -- New

SNMPV3 User:

User Name:

Group Name: ☐ ☐ snmpv3users

Security Model:

Security Level:

User Authentication:

Authentication Protocol:

Authentication Password:

Data Privacy:

Privacy Protocol:

Privacy Password:

Back Add

SNMPv3 Users -- Edit

User Name:

Group Name: ☐ ☐ DefaultROGroup

Back Change

Figure 38 Configuring SNMPv3 Users

CLI – Use the **snmp-server user** command to configure a new user name and assign it to a group.

```

Console(config)#snmp-server user chris group r&d v3 auth md5
    greenpeace priv des56 einstien
Console(config)#exit
Console#show snmp user
EngineId: 80000034030001f488f5200000
User Name: chris
Authentication Protocol: md5
Privacy Protocol: des56
Storage Type: nonvolatile
Row Status: active

Console#

```

6.4.4.4 Configuring Remote SNMPv3 Users

Each SNMPv3 user is defined by a unique name. Users must be configured with a specific security level and assigned to a group. The SNMPv3 group restricts users to a specific read and a write view.

To send inform messages to an SNMPv3 user on a remote device, first specify the engine identifier for the SNMP agent on the remote device where the user resides. The remote engine ID is used to compute the security digest for authenticating and encrypting packets sent to a user on the remote host. (See “Specifying Trap Managers and Trap Types” on page 110 and “Specifying a Remote Engine ID” on page 115.)

Command Attributes

- **User Name** – The name of user connecting to the SNMP agent. (Range: 1-32 characters)
- **Group Name** – The name of the SNMP group to which the user is assigned. (Range: 1-32 characters)
- **Engine ID** – The engine identifier for the SNMP agent on the remote device where the remote user resides. Note that the remote engine identifier must be specified before a remote user can be configured. (See 6.4.4.2 "Specifying a Remote Engine ID" 115.)
- **Remote IP** – The Internet address of the remote device where the user resides.

- **Security Model** – The user security model; SNMP v1, v2c or v3.
(Default: v1)
- **Security Level** – The security level used for the user:
 - noAuthNoPriv – There is no authentication or encryption used in SNMP communications. (This is the default for SNMPv3.)
 - AuthNoPriv – SNMP communications use authentication, but the data is not encrypted (only available for the SNMPv3 security model).
 - AuthPriv – SNMP communications use both authentication and encryption (only available for the SNMPv3 security model).
- **Authentication Protocol** – The method used for user authentication.
(Options: MD5, SHA; Default: MD5)
- **Authentication Password** – A minimum of eight plain text characters is required.
- **Privacy Protocol** – The encryption algorithm use for data privacy; only 56-bit DES is currently available.
- **Privacy Password** – A minimum of eight plain text characters is required.

Web – Click SNMP, SNMPv3, Remote Users. Click New to configure a user name. In the New User page, define a name and assign it to a group, then click Add to save the configuration and return to the User Name list. To delete a user, check the box next to the user name, then click Delete.

SNMPv3 Remote Users

New Delete

	User Name	Group Name	Engine ID	Model	Level	Authentication	Privacy
☐	mark	r&d	80000000030004e2b316c54321	V3	noAuthNoPriv	None	None

SNMPv3 Remote Users -- New

SNMPv3 User:

User Name:

Group Name: ☐ ☐ public

Remote IP:

Security Model:

Security Level:

User Authentication:

Authentication Protocol:

Authentication Password:

Data Privacy:

Privacy Protocol:

Privacy Password:

Back Add

Figure 39 Configuring Remote SNMPv3 Users

CLI – Use the **snmp-server user** command to configure a new user name and assign it to a group.

```

Console(config)#snmp-server user mark group r&d remote 192.168.1.19
v3 auth md5 greenpeace priv des56 einstien
Console(config)#exit
Console#show snmp user
No user exist.

SNMP remote user
EngineId: 80000000030004e2b316c54321
User Name: mark
Authentication Protocol: none
Privacy Protocol: none
Storage Type: nonvolatile
Row Status: active

Console#

```

6.4.4.5

Configuring SNMPv3 Groups

An SNMPv3 group sets the access policy for its assigned users, restricting them to specific read and write views. Use the pre-defined default groups or create new groups to map a set of SNMP users to SNMP views.

Command Attributes

- **Group Name** – The name of the SNMP group. (Range: 1-32 characters)
- **Model** – The group security model; SNMP v1, v2c or v3.
- **Level** – The security level used for the group:
 - noAuthNoPriv – There is no authentication or encryption used in SNMP communications.
 - AuthNoPriv – SNMP communications use authentication, but the data is not encrypted (only available for the SNMPv3 security model).
 - AuthPriv – SNMP communications use both authentication and encryption (only available for the SNMPv3 security model).
- **Read View** – The configured view for read access. (Range: 1-32 characters)

- **Write View** – The configured view for write access. (Range: 1-32 characters)
- **Notify View** – The configured view for notifications. (Range: 1-32 characters)

Note: Refer to the Alarm Description manual for a list of supported notification messages.

Web – Click SNMP, SNMPv3, Groups. Click New to configure a new group. In the New Group page, define a name, assign a security model and level, and then select read and write views. Click Add to save the new group and return to the Groups list. To delete a group, check the box next to the group name, then click Delete.

SNMPv3 Groups

New... Delete

	Group Name	Model	Level	Read View	Write View
☐	public	V1	noAuthNoPriv	defaultview	none
☐	public	V2C	noAuthNoPriv	defaultview	none
☐	private	V1			
☐	private	V2C			

SNMPv3 Groups -- New

Group Properties:

Group Name:

Security Model:

Security Level:

SNMPv3 Views:

Read View: ☒ ☐ defaultview

Write View: ☒ ☐ defaultview

Notify View: ☒ ☐ defaultview

Back Add

Figure 40 Configuring SNMPv3 Groups

CLI – Use the **snmp-server group** command to configure a new group, specifying the security model and level, and restricting MIB access to defined read and write views.

```

Console(config)#snmp-server group v3secure v3 priv read
                defaultview write defaultview
Console(config)#exit
Console#show snmp group
.
.
Group Name: secure-users
Security Model: v3
Read View: defaultview
Write View: defaultview
Notify View: defaultview
Storage Type: nonvolatile
Row Status: active

Console#

```

6.4.4.6

Setting SNMPv3 Views

SNMPv3 views are used to restrict user access to specified portions of the MIB tree. The predefined view “defaultview” includes access to the entire MIB tree.

Command Attributes

- **View Name** – The name of the SNMP view. (Range: 1-32 characters)
- **View OID Subtrees** – Shows the currently configured object identifiers of branches within the MIB tree that define the SNMP view.
- **Edit OID Subtrees** – Allows the object identifiers of branches within the MIB tree to be configured. Wild cards can be used to mask a specific portion of the OID string.
- **Type** – Indicates if the object identifier of a branch within the MIB tree is included or excluded from the SNMP view.

Web – Click SNMP, SNMPv3, Views. Click New to configure a new view. In the New View page, define a name and specify OID subtrees in the ECN330-switch MIB to be included or excluded in the view. Click Back to save the new view and return to the SNMPv3 Views list. For a specific view, click on View OID Subtrees to display the current configuration, or click on Edit OID Subtrees to make changes to the view settings. To delete a view, check the box next to the view name, then click Delete.

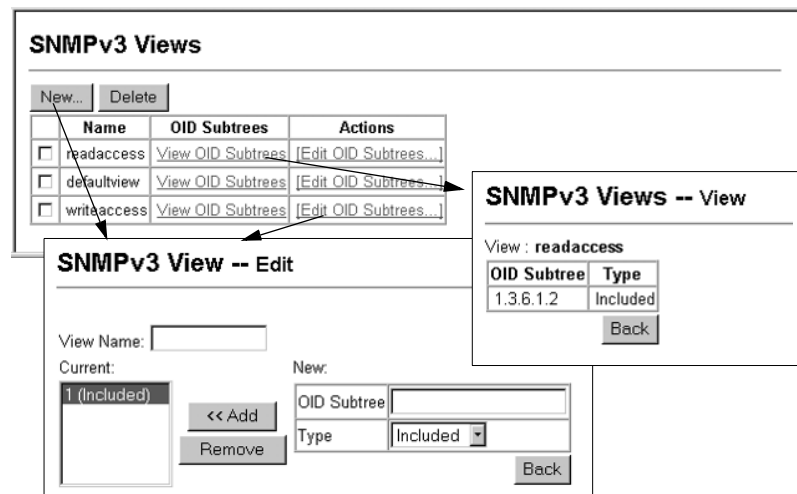


Figure 41 Configuring SNMPv3 Views

CLI – Use the **snmp-server view** command to configure a new view. This example view includes the MIB-2 interfaces table, and the wildcard mask selects all index entries.

```
Console(config)#snmp-server view ifEntry.a 1.3.6.1.2.1.2.2.1.1.*
    included
Console(config)#exit
Console#show snmp view
View Name: ifEntry.a
Subtree OID: 1.3.6.1.2.1.2.2.1.1.*
View Type: included
Storage Type: nonvolatile
Row Status: active

View Name: readaccess
Subtree OID: 1.3.6.1.2
View Type: included
Storage Type: nonvolatile
Row Status: active

View Name: defaultview
Subtree OID: 1
View Type: included
Storage Type: nonvolatile
Row Status: active

Console#
```

6.5 User Authentication

Management access to the ECN330-switch can be restricted using the following options:

- **User Accounts** – Manually configure management access rights for users.
- **Authentication Settings** – Use remote authentication to configure access rights.
- **HTTPS Settings** – Provide a secure web connection.
- **SSH Settings** – Provide a secure shell (for secure Telnet access).
- **Port Security** – Configure secure addresses for individual ports.
- **802.1X** – Use IEEE 802.1X port authentication to control access to specific ports.
- **IP Filter** – Filters management access to the web, SNMP or Telnet interface.

6.5.1 Configuring User Accounts

The guest only has read access for most configuration parameters. However, the administrator has write access for all parameters governing the onboard agent. Therefore assign a new administrator password as soon as possible, and store it in a safe place.

The default guest name is “guest” with the password “guest.” The default administrator name is “admin” with the password “admin.”

Command Attributes

- **Account List** – Displays the current list of user accounts and associated access levels. (Defaults: admin, and guest)
- **New Account** – Allows configuration of a new account.
 - **User Name** – The name of the user.
(Maximum length: 8 characters; maximum number of users: 16)
 - **Access Level** – Specifies the user level.
(Options: Normal and Privileged)

- **Password** – Specifies the user password.
(Range: 0-8 characters plain text, case sensitive)
- **Change Password** – Sets a new password for the specified user.

Web – Click Security, User Accounts. To configure a new user account, enter the user name, access level, and password, then click Add. To change the password for a specific user, enter the user name and new password, confirm the password by entering it again, then click Apply.

User Accounts

Account List

admin (Privileged)
guest (Normal)

<< Add Remove

New Account

User Name	mike
Access Level	Normal
Password	*****
Confirm Password	*****

Change Password

User Name	
New Password	
Confirm Password	

Change

Figure 42 User Accounts

CLI – Assign a user name to access-level 15 (that is, administrator), then specify the password.

```
Console(config)#username bob access-level 15
Console(config)#username bob password 0 smith
Console(config)#
```

6.5.2 Configuring Local/Remote Logon Authentication

Use the Authentication Settings menu to restrict management access based on specified user names and passwords. Access rights can be manually configured on the ECN330-switch, or a remote access authentication server based on RADIUS or TACACS+ protocols can be used.

Remote Authentication Dial-in User Service (RADIUS) and Terminal Access Controller Access Control System Plus (TACACS+) are logon authentication protocols that use software running on a central server to control access to RADIUS-aware or TACACS-aware devices on the network. An authentication server contains a database of multiple user name/password pairs with associated privilege levels for each user that requires management access to the ECN330-switch.

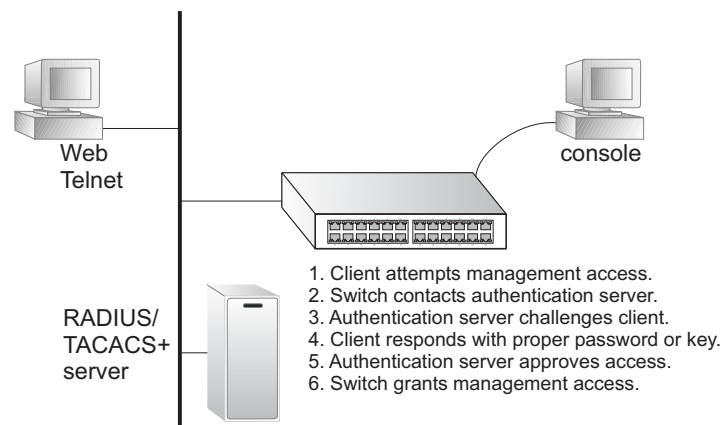


Figure 43 Authentication Server Operation

RADIUS uses UDP while TACACS+ uses TCP. UDP only offers best effort delivery, while TCP offers a connection-oriented transport. Also, note that RADIUS encrypts only the password in the access-request packet from the client to the server, while TACACS+ encrypts the entire body of the packet.

Command Usage

- By default, management access is always checked against the authentication database stored on the local ECN330-switch. If a remote authentication server is used, the authentication sequence and the corresponding parameters for the remote authentication protocol must

be specified. Local and remote logon authentication control management access through the console port, web browser, or Telnet.

- RADIUS and TACACS+ logon authentication assign a specific privilege level for each user name/password pair. The user name, password, and privilege level must be configured on the authentication server.
- Up to three authentication methods can be specified for any user to indicate the authentication sequence. For example, by selecting (1) RADIUS, (2) TACACS and (3) Local, the user name and password on the RADIUS server is verified first. If the RADIUS server is not available, then authentication is attempted using the TACACS+ server, and finally the local user name and password is checked.

Command Attributes

- **Authentication** – Select the authentication, or authentication sequence required:
 - **Local** – User authentication is performed only locally by the ECN330-switch.
 - **Radius** – User authentication is performed using a RADIUS server only.
 - **TACACS** – User authentication is performed using a TACACS+ server only.
 - [authentication sequence] – User authentication is performed by up to three authentication methods in the indicated sequence.
- RADIUS Settings
 - **Global** – Provides globally applicable RADIUS settings.
 - **ServerIndex** – Specifies one of five RADIUS servers that may be configured. The ECN330-switch attempts authentication using the listed sequence of servers. The process ends when a server either approves or denies access to a user.
 - **Server IP Address** – Address of authentication server. ServerIndex must be selected to display this field. (Default: 10.1.0.1)
 - **Server Port Number** – Network (UDP) port of authentication server used for authentication messages. (Range: 1-65535; Default: 1812)

- **Secret Text String** – Encryption key used to authenticate logon access for client. Do not use blank spaces in the string. (Maximum length: 20 characters)
- **Number of Server Transmits** – Number of times the ECN330-switch tries to authenticate logon access through the authentication server. (Range: 1-30; Default: 2)
- **Timeout for a reply** – The number of seconds the ECN330-switch waits for a reply from the RADIUS server before it resends the request. (Range: 1-65535; Default: 5)
- TACACS Settings
 - **Server IP Address** – Address of the TACACS+ server. (Default: 10.11.12.13)
 - **Server Port Number** – Network (TCP) port of TACACS+ server used for authentication messages. (Range: 1-65535; Default: 49)
 - **Secret Text String** – Encryption key used to authenticate logon access for client. Do not use blank spaces in the string. (Maximum length: 20 characters)

Note: The local ECN330-switch user database has to be set up by manually entering user names and passwords using the CLI. (See “username” on page 633.)

Web – Click Security, Authentication Settings. To configure local or remote authentication preferences, specify the authentication sequence (that is, one to three methods), fill in the parameters for RADIUS or TACACS+ authentication if selected, and click Apply.

Authentication Settings

Authentication
Local

RADIUS Settings:

☒ Global | ServerIndex: ☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5

Server Port Number (1-65535)
181

Secret Text String
XXXXXXXXXX

Number of Server Transmits (1-30)
5

Timeout for a reply (1-65535)
10
(sec)

TACACS Settings:

Server IP Address
10.11.12.13

Server Port Number (1-65535)
49

Secret Text String

Figure 44 Authentication Server Settings

CLI – Specify all the required parameters to enable logon authentication.

```

Console(config)#authentication login radius
Console(config)#radius-server host 192.168.1.25
Console(config)#radius-server port 181
Console(config)#radius-server key green
Console(config)#radius-server retransmit 5
Console(config)#radius-server timeout 10
Console#show radius-server

Remote RADIUS server configuration:

Global settings:
Communication key with RADIUS server: *****
Server port number:                181
Retransmit times:                  5
Request timeout:                   10

Server 1:
Server IP address: 192.168.1.25
Communication key with RADIUS server: *****
Server port number: 181
Retransmit times: 5
Request timeout: 10
Console(config)#authentication login tacacs
Console(config)#tacacs-server host 10.20.30.40
Console(config)#tacacs-server port 200
Console(config)#tacacs-server key green
Console#show tacacs-server
Server IP address:                10.20.30.40
Communication key with tacacs server:
Server port number:                200
Console(config)#

```

6.5.3 Configuring HTTPS

The ECN330-switch can be configured to enable the Secure Hypertext Transfer Protocol (HTTPS) over the Secure Socket Layer (SSL), providing secure access (that is, an encrypted connection) to the ECN330-switch's web interface.

Command Usage

- Both the HTTP and HTTPS service can be enabled independently on the ECN330-switch. However, both services cannot be configured to use the same UDP port.

- If HTTPS is enabled, it must be indicated in the URL that is specified in the browser: `https://device[:port_number]`
- When HTTPS is started, the connection is established in this way:
 - The client authenticates the server using the server's digital certificate.
 - The client and server negotiate a set of security protocols to use for the connection.
 - The client and server generate session keys for encrypting and decrypting data.
- The client and server establish a secure encrypted connection. A padlock icon should appear in the status bar for Internet Explorer 5.x or above and Netscape Navigator 4.x or above.
- The following web browsers and operating systems currently support HTTPS:

Table 11 HTTPS System Support

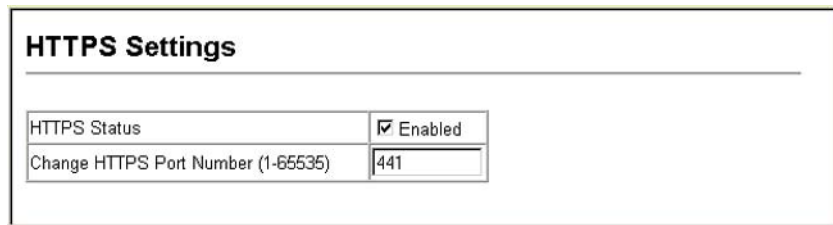
Web Browser	Operating System
Internet Explorer 5.0 or later	Windows 98, Windows NT (with service pack 6a), Windows 2000, Windows XP
Netscape Navigator 6.2 or later	Windows 98, Windows NT (with service pack 6a), Windows 2000, Windows XP, Solaris 2.6

- To specify a secure-site certificate, see 6.5.3.1 "Replacing the Default Secure-site Certificate" 134.

Command Attributes

- **HTTPS Status** – Enables/disables the HTTPS server feature on the ECN330-switch. (Default: Enabled)
- **Change HTTPS Port Number** – Specifies the UDP port number used for HTTPS/SSL connection to the ECN330-switch's web interface. (Default: Port 443)

Web – Click Security, HTTPS Settings. Enable HTTPS and specify the port number, then click Apply.



HTTPS Settings	
HTTPS Status	☒ Enabled
Change HTTPS Port Number (1-65535)	441

Figure 45 HTTPS Settings

CLI – This example enables the HTTP secure server and modifies the port number.

```
Console(config)#ip http secure-server
Console(config)#ip http secure-port 441
Console(config)#
```

6.5.3.1

Replacing the Default Secure-site Certificate

When using HTTPS (for secure access) to log onto the web interface, a Secure Sockets Layer (SSL) certificate appears for the ECN330-switch. By default, the certificate that Netscape and Internet Explorer display will be associated with a warning that the site is not recognized as a secure site. This is because the certificate has not been signed by an approved certification authority. To replace this warning by a message confirming that the connection to the ECN330-switch is secure, a unique certificate and a private key and password must be obtained from a recognized certification authority.

Note: For maximum security, it is recommended to obtain a unique Secure Sockets Layer certificate at the earliest opportunity. This is because the default certificate for the ECN330-switch is not unique to the hardware.

When a unique certificate and a private key and password have been obtained, place them on the TFTP server, and use the **copy tftp https-certificate** command at the ECN330-switch's command-line interface to replace the default (unrecognized) certificate with an authorized one:

```
Console#copy tftp https-certificate
TFTP server ip address: <server ip-address>
Source certificate file name: <certificate file name>
Source private file name: <private key file name>
Private password: <password for private key>
```

Note: The ECN330-switch must be reset for the new certificate to be activated. To reset the ECN330-switch, type “reload” at the command prompt:
Console#reload

6.5.4 Configuring the Secure Shell

The Berkley-standard includes remote access tools originally designed for Unix systems. Some of these tools have also been implemented for Microsoft Windows and other environments. These tools, including commands such as *rlogin* (remote login), *rsh* (remote shell), and *rcp* (remote copy), are not secure from hostile attacks.

The Secure Shell (SSH) includes server/client applications intended as a secure replacement for the older Berkley remote access tools. SSH can also provide remote management access to the ECN330-switch as a secure replacement for Telnet. When the client contacts the ECN330-switch through the SSH protocol, the ECN330-switch generates a public-key that the client uses along with a local user name and password for access authentication. SSH also encrypts all data transfers passing between the ECN330-switch and SSH-enabled management station clients, and ensures that data traveling over the network arrives unaltered.

Note that an SSH client needs to be installed on the management station to access the ECN330-switch for management using the SSH protocol.

Note: The ECN330-switch supports both SSH Version 1.5 and 2.0 clients.

Command Usage

The SSH server on the ECN330-switch supports both password and public key authentication. If password authentication is specified by the SSH client, then the password can be authenticated either locally or through a RADIUS or TACACS+ remote authentication server, as specified on the Authentication Settings page (page 128). If public key authentication is specified by the client, then authentication keys must be configured on both the client and the ECN330-switch as described in the following section. Note that regardless of whether public key or password authentication is used, authentication keys still have to be generated on the ECN330-switch (SSH Host Key Settings) and enable the SSH server (Authentication Settings).

To use the SSH server, complete these steps:

1. *Generate a Host Key Pair* – On the SSH Host Key Settings page, create a host public/private key pair.
2. *Provide Host Public Key to Clients* – Many SSH client programs automatically import the host public key during the initial connection setup with the ECN330-switch. Otherwise, a known hosts file needs to be manually created on the management station and the host public key placed in it. An entry for a public key in the known hosts file would appear similar to the following example:

```
10.1.0.54 1024 35 1568499540186766925933394677505461732531367
4890836547254 1502024559319986854435836165199992332978176606
5830956 10825913212890233 765468017262725714134287629413011
96195566782 59566410486957427888146206 51941746772984865468
61571773939016477935594230357741309802273708779454524083971
752646358058176716709574804776117
```

3. *Import Client's Public Key to the ECN330-switch* – Use the **copy tftp public-key** command (page 651) to copy a file containing the public key for all the SSH client's granted management access to the ECN330-switch. (Note that these clients must be configured locally on the ECN330-switch through the User Accounts page as described on page 126.) The clients are subsequently authenticated using these keys. The current firmware only accepts public key files based on standard UNIX format as shown in the following example for an RSA Version 1 key:

```
1024 35 134108168560989392104094492015542534763164192187295
8921143173880 055536161631051775940838686311092912322268285
19254374603100937187721199696317813662774141689851320491172
```

```
04830339254324101637997592371449011938006090253948408482717
81943722884025331159521348610229029789827213532671316294325
32818915045306393916643 steve@192.168.1.19
```

4. *Set the Optional Parameters* – On the SSH Settings page, configure the optional parameters, including the authentication timeout, the number of retries, and the server key size.
5. *Enable SSH Service* – On the SSH Settings page, enable the SSH server on the ECN330-switch.
6. *Challenge-Response Authentication* – When an SSH client attempts to contact the ECN330-switch, the SSH server uses the host key pair to negotiate a session key and encryption method. Only clients that have a private key corresponding to the public keys stored on the ECN330-switch can access it. The following exchanges take place during this process:
 - A The client sends its public key to the ECN330-switch.
 - B The ECN330-switch compares the client's public key to those stored in memory.
 - C If a match is found, the ECN330-switch uses the public key to encrypt a random sequence of bytes, and sends this string to the client.
 - D The client uses its private key to decrypt the bytes, and sends the decrypted bytes back to the ECN330-switch.
 - E The ECN330-switch compares the decrypted bytes to the original bytes it sent. If the two sets match, this means that the client's private key corresponds to an authorized public key, and the client is authenticated.

Note: To use SSH with only password authentication, the host public key must still be given to the client, either during initial connection or manually entered into the known host file. However, the client's keys do not need to be configured.

Note: The SSH server supports up to four client sessions. The maximum number of client sessions includes both current Telnet sessions and SSH sessions.

6.5.4.1 Generating the Host Key Pair

A host public/private key pair is used to provide secure communications between an SSH client and the ECN330-switch. After generating this key pair, the host public key must be provided to SSH clients and the client's public key imported to the ECN330-switch as described in the preceding section (Command Usage).

Field Attributes

- **Public-Key of Host-Key** – The public key for the host.
 - RSA (Version 1): The first field indicates the size of the host key (for example, 1024), the second field is the encoded public exponent (for example, 65537), and the last string is the encoded modulus.
 - DSA (Version 2): The first field indicates that the encryption method used by SSH is based on the Digital Signature Standard (DSS). The last string is the encoded modulus.
- **Host-Key Type** – The key type used to generate the host key pair (that is, public and private keys). (Range: RSA (Version 1), DSA (Version 2), Both: Default: Both)
The SSH server uses RSA or DSA for key exchange when the client first establishes a connection with the ECN330-switch, and then negotiates with the client to select either DES (56-bit) or 3DES (168-bit) for data encryption.
- **Save Host-Key from Memory to Flash** – Saves the host key from RAM (that is, volatile memory to flash memory). Otherwise, the host key pair is stored to RAM by default. Note that this item must be selected prior to generating the host-key pair.
- **Generate** – This button is used to generate the host key pair. Note that the host key pair must first be generated before the SSH server can be enabled on the SSH Server Settings page.
- **Clear** – This button clears the host key from both volatile memory (RAM) and non-volatile memory (Flash).

Web – Click Security, SSH, Host-Key Settings. Select the host-key type from the drop-down box, select the option to save the host key from memory to flash (if required) prior to generating the key, and then click Generate.

SSH Host-Key Settings

Public-Key of Host-Key

RSA

```
1024 65537
1309178972674789616152111712764979196296211551642422768028072510384048338276358290698941935742287566
1853076228099531413921379002210394737439417368512447371756369962704297907064627111321882467751081589
0431586119348954200209463340676128115040594681146425925732650943840347858370753955264123928004845007
811621891
```

DSA

```
ssh-dss
AAAAE3NzAc1Kc3MAAAcBAJBvdKEZjKtKEEBU3Ak1Fz72nOPSVp08BdqF2eZeNx17DQ/N4hYx/W427x1AwJ1/dEO41o8fnOdcH2Ub
KQX00BdqU9/IuvNMd+AEHx5nwoZDzrLWuyHJdowH0GpKwVSmVcZkIjs1FrQs6XTaC1r3ODWbovF0sc1ld+Jj3DC4tXq1AAAAFQCy
PELSe2E3S0Q+P32+SfpbFA+cQAAAIArYRgej1/ZfBvVhC9M/XuIVfApHEdY18fcrzpf1cSeBaIeE53gcH0uQrvFLGH+ZC1VV1ds
8VvYKHAUFQfnTK0GCGnhVQRj2bsEz0KRqKI7nWt2OtXk4z2BD0tvyF5vCQaret3b1Ud1/eB2q7eJvnruk00v1QbWFPB01pJX5op
QwAAAI89RK3JwMa9pBCT360x2H14sqQVbu70v5GVuxH6zaY92ZHPsuDvvI55wWenchwCaRpGfOJ1iWVHEmtcgeFzrAw5G3OT4iAR
qGqHc9p1vL4eVnxhRdx9O2H1WkjhWSHOPVH4Cw2FLHpfEBnPL3NHqcvFYjNTBxJReaqV0ZK6lknaGHQ==
```

Host-Key Type: Both

☒ Save Host-Key from Memory to Flash

Generate Clear

Figure 46 SSH Host-Key Settings

CLI – This example generates a host-key pair using both the RSA and DSA algorithms, stores the keys to flash memory, and then displays the host's public keys.

```

Console#ip ssh crypto host-key generate
Console#ip ssh save host-key
Console#show public-key host
Host:
RSA:
1024 65537
  127250922544926402131336514546131189679055192360076028653006761
  8240969094744832010252487896597759216832225584652387791546479807
  39631403386925793105105765212243052807865885485789272602937866089
  23684142327591212760325919683697053439336438445223335188287173896
  894511729290510813919642025190932104328579045764891
DSA:
ssh-dss AAAAB3NzaC1kc3MAAACBAN6zwIqCqDb3869jYVXlME1sHL0EcE/Re6hlasf
  EthIwmjhLY4O0jqJZpcEQUgCfYlum0Y2uoLka+Py9ieGWQ8f2gobUZKIIICuKg6vjO
  9XTs7XKc05xfzkBiKviDa+2OrIz6UK+6vFOgvUDFedlnixYTVo+h5v8r0ea2rpnO6
  DkZAAAAFQCZNzn/x17dwpW8RrVDQnSWw4Qk+6QAAAEApTkGeB6B5hwagH4gUOCY6i
  1TmrmsiJgfwO9OqRPUMbCAkCC+uzxatOo7drnIZypMx+Sx5RUdMGgKS+9ywsalcWq
  HeFY5ilc3lDCNBueeLykZzVS+RS+azTKIk/zrJh8GLGNq375R55yRxFvm cGIn/Q7
  IphPqyJ3o9MK8LFDfmJEAACAL8A6tESiswP2OFqX7VGoEbzVDSOIRTMFy3iUXtvG
  yQAOVSy67Mfc3lMtggPRUOYXDwiBp5NXgilCg5z7VqbmRm28mWc5a//f8 TUAgnPN
  WKV6W0hqmshQdotVzDR1e+XKNTZj0uTwWfjO5KytDn4MdoTHgrbl/DMDAfjnte8MZ
  Zs=
Console#

```

6.5.4.2 Configuring the SSH Server

The SSH server includes basic settings for authentication.

Note: The host key pair must first be generated using the SSH Host-Key Settings page (section 6.5.4.1 on page 138) before enabling the SSH server.

Field Attributes

- **SSH Server Status** – Enables/disables the SSH server on the ECN330-switch. (Default: Disabled)
- **Version** – The Secure Shell version number. Version 2.0 is displayed, but the ECN330-switch supports management access through either SSH Version 1.5 or 2.0 clients.

- **SSH Authentication Timeout** – Specifies the time interval in seconds that the SSH server waits for a response from a client during an authentication attempt.
(Range: 1 to 120 seconds; Default: 120 seconds)
- **SSH Authentication Retries** – Specifies the number of authentication attempts that a client is allowed before authentication fails and the client has to restart the authentication process. (Range: 1-5 times; Default: 3)
- **SSH Server-Key Size** – Specifies the SSH server key size. (Range: 512-896 bits; Default: 768)
 - The server key is a private key that is never shared outside the ECN330-switch.
 - The host key is shared with the SSH client, and is fixed at 1024 bits.

Web – Click Security, SSH, Settings. Enable SSH and adjust the authentication parameters as required, then click Apply. Note that the host key pair must first be generated on the SSH Host-Key Settings page before the SSH server can be enabled.

SSH Server Settings	
SSH Server Status	Enabled ▾
Version	2.0
SSH Authentication Timeout (1-120)	100 seconds
SSH Authentication Retries (1-5)	5
SSH Server-Key Size (512-896)	512

Figure 47 SSH Server Settings

CLI – This example enables SSH, sets the authentication parameters, and displays the current configuration. It shows that the administrator has made a connection through SSH, and then disables this connection.

```

Console(config)#ip ssh server
Console(config)#ip ssh timeout 100
Console(config)#ip ssh authentication-retries 5
Console(config)#ip ssh server-key size 512
Console(config)#end
Console#show ip ssh
SSH Enabled - version 2.0
Negotiation timeout: 120 secs; Authentication retries: 3
Server key size: 768 bits
Console#show ssh
Information of secure shell
Session Username Version Encrypt method Negotiation state
-----
0 admin 2.0 cipher-3des session-started
Console#disconnect 0
Console#

```

6.5.5 Configuring Port Security

Port security is a feature that allows an ECN330-switch port to be configured with one or more device MAC addresses that are authorized to access the network through that port.

When port security is enabled on a port, the ECN330-switch stops learning new MAC addresses on the specified port when it has reached a configured maximum number. Only incoming traffic with source addresses already stored in the dynamic or static address table will be accepted as authorized to access the network through that port. If a device with an unauthorized MAC address attempts to use the ECN330 port, the intrusion will be detected and the ECN330-switch can automatically take action by disabling the port and sending a trap message.

To use port security, specify a maximum number of addresses to allow on the port and then let the ECN330-switch dynamically learn the <source MAC address, VLAN> pair for frames received on the port. Note that secure addresses can also be manually added to the port using the Static Address Table (page 227). When the port has reached the maximum number of MAC addresses the selected port will stop learning. The MAC addresses already in the address table will be retained and will not age out. Any other device that attempts to use the port will be prevented from accessing the ECN330-switch.

Command Usage

- A secure port has the following restrictions:
 - It cannot use port monitoring.
 - It cannot be a multi-VLAN port.
 - It cannot be used as a member of a static or dynamic trunk.
 - It should not be connected to a network interconnection device.
- The default maximum number of MAC addresses allowed on a secure port is zero. A maximum address count from 1 - 20 must be configured for the port to allow access.
- If a port is disabled (shut down) due to a security violation, it must be manually re-enabled from the Port/Port Configuration page (page 187).

Command Attributes

- **Port** – Port number.
- **Name** – Descriptive text (page 187).
- **Disable MAC Learning** – Disables MAC address learning for the selected port, and flush all MAC addresses that have learned on this port.

Security Status cannot be configured when this option is selected. Also note that MAC address learning cannot be disabled if 802.1x Port Authentication has been globally enabled on the ECN330-switch (see “Configuring 802.1X Global Settings” on page 148), or GVRP has been enabled on a port (see “Configuring VLAN Behavior for Interfaces” on page 290).

- **Action** – Indicates the action to be taken when a port security violation is detected:
 - **None**: No action should be taken. (This is the default.)
 - **Trap**: Send an SNMP trap message.
 - **Shutdown**: Disable the port.
 - **Trap and Shutdown**: Send an SNMP trap message and disable the port.

- **Security Status** – Enables or disables port security on the port. (Default: Disabled)
- **Max MAC Count** – The maximum number of MAC addresses that can be learned on a port. (Range: 0 - 1024)

This parameter is only display in the web interface:

- **Trunk** – Indicates if a port is configured as a trunk member (page 191 and 193) and cannot be enabled as a secure port.

Web – Click Security, Port Security. Set the action to take when an invalid address is detected on a port, mark the checkbox in the Status column to enable security for a port, set the maximum number of MAC addresses allowed on a port, and click Apply.

Port Security

Configuration:

Port	Name	Disable MAC Learn	Action	Security Status	Max MAC Count (0-1024)	Trunk
1		☐ Disabled	None	☐ Enabled	0	
2		☐ Disabled	None	☐ Enabled	0	
3		☐ Disabled	None	☐ Enabled	0	
4		☐ Disabled	None	☐ Enabled	0	
5		☒ Disabled	Trap and Shutdown	☒ Enabled	20	
6		☒ Disabled	None	☐ Enabled	0	
7		☐ Disabled	None	☐ Enabled	0	
8		☐ Disabled	None	☐ Enabled	0	
9		☐ Disabled	None	☐ Enabled	0	
10		☐ Disabled	None	☐ Enabled	0	

Figure 48 Port Security

CLI – This example sets the command mode to Port 5, sets the port security action to send a trap and disable the port, and specifies a maximum address count. It then disables MAC address learning for Port 2.

```
Console(config)#interface ethernet 1/5
Console(config-if)#port security action trap-and-shutdown
Console(config-if)#port security max-mac-count 20
Console(config-if)#exit
Console(config)#interface ethernet 1/2
Console(config-if)#mac-learn disable
Console(config-if)#
```

6.5.6 Configuring 802.1X Port Authentication

Network switches can provide open and easy access to network resources by simply attaching a client PC. Although this automatic configuration and access is a desirable feature, it also allows unauthorized personnel to easily intrude and possibly gain access to sensitive network data.

The IEEE 802.1X (dot1x) standard defines a port-based access control procedure that prevents unauthorized access to a network by requiring users to first submit credentials for authentication. Access to all ECN330 ports in a network can be centrally controlled from a server, which means that authorized users can use the same credentials for authentication from any point within the network.

The ECN330-switch uses the Extensible Authentication Protocol over LANs (EAPOL) to exchange authentication protocol messages with the client, and a remote RADIUS authentication server to verify user identity and access rights. When a client (that is, Supplicant) connects to a ECN330 port, the ECN330-switch (that is, Authenticator) responds with an EAPOL identity request. The client provides its identity (such as a user name) in an EAPOL response to the ECN330-switch, which it forwards to the RADIUS server. The RADIUS server verifies the client identity and sends an access challenge back to the client. The EAP packet from the RADIUS server contains not only the challenge, but the authentication method to be used. The client can reject the authentication method and request another, depending on the configuration of the client software and the RADIUS server. The authentication method must be MD5. The client responds to the appropriate method with its credentials, such as a password or certificate. The RADIUS server verifies the client credentials and responds with an accept or reject packet. If authentication is successful, the ECN330-switch allows the client to access the network. Otherwise, network access is denied and the port remains blocked.

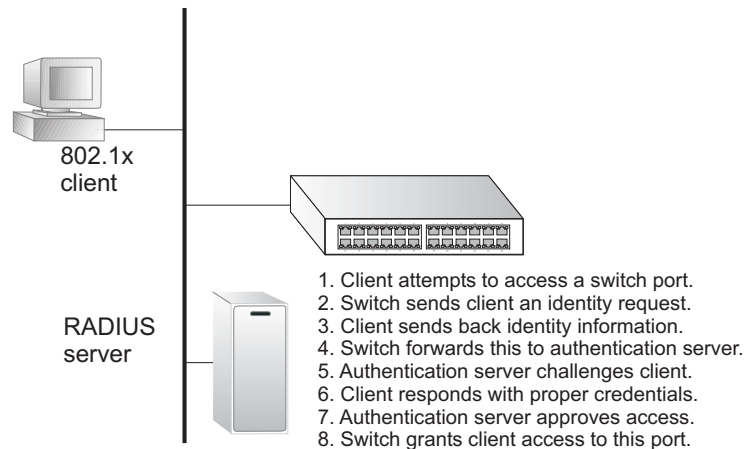


Figure 49 IEEE 802.1X Port Authentication

The operation of dot1x on the ECN330-switch requires the following:

- The ECN330-switch must have an IP address assigned.
- RADIUS authentication must be enabled on the ECN330-switch and the IP address of the RADIUS server specified.
- Each ECN330 port that will be used must be set to dot1x "Auto" mode.
- Each client that needs to be authenticated must have dot1x client software installed and properly configured.
- The RADIUS server and 802.1X client support EAP. (The ECN330-switch only supports EAPOL in order to pass the EAP packets from the server to the client.)
- The RADIUS server and client also have to support the same EAP authentication type – MD5. (Some clients have native support in Windows, otherwise the dot1x client must support it.)

6.5.6.1 Displaying 802.1X Global Settings

The 802.1X protocol provides port authentication.

Command Attributes

- **802.1X System Authentication Control** – The global setting for 802.1X.

Web – Click 802.1X, Information.



Figure 50 802.1X Global Information

CLI – This example shows the default global setting for 802.1X.

```
Console#show dot1x
Global 802.1X Parameters
  system-auth-control: enable

802.1X Port Summary

Port Name  Status      Operation Mode  Mode              Authorized
1/1        disabled   Single-Host     ForceAuthorized   n/a
1/2        disabled   Single-Host     ForceAuthorized   n/a
.
.
.
802.1X Port Details

802.1X is disabled on port 1/1
.
.
.
802.1X is disabled on port 28
Console#
```

6.5.6.2 Configuring 802.1X Global Settings

The 802.1X protocol provides port authentication. The 802.1X protocol must be enabled globally for the ECN330-switch system before port settings are active.

Command Attributes

- **802.1X System Authentication Control** – Sets the global setting for 802.1X. (Default: Disabled)

Web – Select Security, 802.1X, Configuration. Enable 802.1X globally for the ECN330-switch, and click Apply.



The screenshot shows a web configuration window titled "802.1X Configuration". Inside the window, there is a label "802.1X System Authentication Control" followed by a checked checkbox and the word "Enabled".

Figure 51 802.1X Global Configuration

CLI – This example enables 802.1X globally for the ECN330-switch.

```
Console(config)#dot1x system-auth-control
Console(config)#
```

6.5.6.3 Configuring Port Settings for 802.1X

When 802.1X is enabled, the parameters for the authentication process that runs between the client and the ECN330-switch (that is, authenticator), as well as the client identity lookup process that runs between the ECN330-switch and authentication server need to be configured. These parameters are described in this section.

Command Attributes

- **Status** – Indicates if authentication is enabled or disabled on the port. (Default: Disabled)
- **Operation Mode** – Allows single or multiple hosts (clients) to connect to an 802.1X-authorized port. (Range: Single-Host, Multi-Host; Default: Single-Host)

- **Max Count** – The maximum number of hosts that can connect to a port when the Multi-Host operation mode is selected. (Range: 1-1024; Default: 5)
- **Mode** – Sets the authentication mode to one of the following options:
 - **Auto** – Requires a dot1x-aware client to be authorized by the authentication server. Clients that are not dot1x-aware will be denied access.
 - **Force-Authorized** – Forces the port to grant access to all clients, either dot1x-aware or otherwise. (This is the default setting.)
 - **Force-Unauthorized** – Forces the port to deny access to all clients, either dot1x-aware or otherwise.
- **Re-authentication** – Sets the client to be re-authenticated after the interval specified by the Re-authentication Period. Re-authentication can be used to detect if a new device is plugged into an ECN330 port. (Default: Disabled)
- **Max Request** – Sets the maximum number of times the ECN330 port will retransmit an EAP request packet to the client before it times out the authentication session. (Range: 1-10; Default 2)
- **Quiet Period** – Sets the time that an ECN330 port waits after the Max Request count has been exceeded before attempting to acquire a new client. (Range: 1-65535 seconds; Default: 60 seconds)
- **Re-authentication Period** – Sets the time period after which a connected client must be re-authenticated. (Range: 1-65535 seconds; Default: 3600 seconds)
- **TX Period** – Sets the time period during an authentication session that the ECN330-switch waits before re-transmitting an EAP packet. (Range: 1-65535; Default: 30 seconds)
- **Authorized** –
 - **Yes** – Connected client is authorized.
 - **No** – Connected client is not authorized.
 - *Blank* – Displays nothing when dot1x is disabled on a port.
- **Supplicant** – Indicates the MAC address of a connected client.
- **Trunk** – Indicates if the port is configured as a trunk port.

Web – Click Security, 802.1X, Port Configuration. Modify the parameters required, and click Apply.

802.1X Port Configuration												
Port	Status	Operation Mode	Max Count (1-20)	Mode	Re-authen	Max-Req	Quiet/Period	Re-authen/Period	Tx Period	Authorized	Supplicant	Trunk
1	Disabled	Single-Host	5	Force-Unauthenticated	☐ Enable	2	60	3600	30	Yes	00-00-00-00-00-00	
2	Enabled	Single-Host	5	Force-Authenticated	☐ Enable	2	60	3600	30		00-00-00-00-00-00	
3	Disabled	Single-Host	5	Force-Authenticated	☐ Enable	2	60	3600	30		00-00-00-00-00-00	
4	Disabled	Single-Host	5	Force-Authenticated	☐ Enable	2	60	3600	30		00-00-00-00-00-00	
5	Disabled	Single-Host	5	Force-Authenticated	☐ Enable	2	60	3600	30		00-00-00-00-00-00	
6	Disabled	Single-Host	5	Force-Authenticated	☐ Enable	2	60	3600	30		00-00-00-00-00-00	

Figure 52 802.1X Port Configuration

CLI – This example sets the 802.1X parameters on port 2. For a description of the additional fields displayed in this example, see “show dot1x” on page 4-84.

```

Console(config)#interface ethernet 1/2
Console(config-if)#dot1x port-control auto
Console(config-if)#dot1x re-authentication
Console(config-if)#dot1x max-req 5
Console(config-if)#dot1x timeout quiet-period 40
Console(config-if)#dot1x timeout re-authperiod 5
Console(config-if)#dot1x timeout tx-period 40
Console(config-if)#end
Console#show dot1x

```

```

Global 802.1X Parameters
  system-auth-control: enable

```

802.1X Port Summary

Port Name	Status	Operation Mode	Mode	Authorized
1/1	disabled	Single-Host	ForceAuthorized	yes
1/2	enabled	Single-Host	Auto	yes
.				
.				
.				
1/27	disabled	Single-Host	ForceAuthorized	n/a
1/28	disabled	Single-Host	ForceAuthorized	n/a

802.1X Port Details

802.1X is disabled on port 1/1

802.1X is enabled on port 1/2

```

reauth-enabled:      Disable
reauth-period:       3600
quiet-period:        60
tx-period:           30
supplicant-timeout:  30
server-timeout:      10
reauth-max:          2
max-req:             2
Status               Authorized
Operation mode        Single-Host
Max count             5
Port-control          Auto
Supplicant            00-e0-29-94-34-65
Current Identifier    7

```

Authenticator State Machine

```

State                Authenticated
Reauth Count         0

```

Backend State Machine

```

State                Idle
Request Count        0
Identifier(Server)    6

```

Reauthentication State Machine

```

State                Initialize

```

```

.
.
.
.

```

802.1X is disabled on port 1/28

Console#

6.5.6.4 Displaying 802.1X Statistics

The ECN330-switch can display statistics for dot1x protocol exchanges for any port.

Table 12 802.1X Statistics

Parameter	Description
Rx EAPOL Start	The number of EAPOL Start frames that have been received by this Authenticator.
Rx EAPOL Logoff	The number of EAPOL Logoff frames that have been received by this Authenticator.
Rx EAPOL Invalid	The number of EAPOL frames that have been received by this Authenticator in which the frame type is not recognized.
Rx EAPOL Total	The number of valid EAPOL frames of any type that have been received by this Authenticator.
Rx EAP Resp/Id	The number of EAP Resp/Id frames that have been received by this Authenticator.
Rx EAP Resp/Oth	The number of valid EAP Response frames (other than Resp/Id frames) that have been received by this Authenticator.
Rx EAP LenError	The number of EAPOL frames that have been received by this Authenticator in which the Packet Body Length field is invalid.
Rx Last EAPOLVer	The protocol version number carried in the most recently received EAPOL frame.
Rx Last EAPOLSrc	The source MAC address carried in the most recently received EAPOL frame.
Tx EAPOL Total	The number of EAPOL frames of any type that have been transmitted by this Authenticator.

Parameter	Description
Tx EAP Req/Id	The number of EAP Req/Id frames that have been transmitted by this Authenticator.
Tx EAP Req/Oth	The number of EAP Request frames (other than Rq/Id frames) that have been transmitted by this Authenticator.

Web – Select Security, 802.1X, Statistics. Select the required port and then click Query. Click Refresh to update the statistics.

802.1X Statistics

Port

Query

Rx EXPOL Start	0	Rx EAP LenError	0
Rx EAPOL Logoff	0	Rx Last EAPOLVer	0
Rx EAPOL Invalid	0	Rx Last EAPOLSrc	00-00-00-00-00-00
Rx EAPOL Total	0	Tx EAPOL Total	1
Rx EAP Resp/Id	0	Tx EAP Req/Id	0
Rx EAP Resp/Oth	0	Tx EAP Req/Oth	0

Refresh

Figure 53 802.1X Statistics

CLI – This example displays the dot1x statistics for port 4.

```

Console#show dot1x statistics interface ethernet 1/4

Eth 1/4
Rx:  EXPOL      EAPOL      EAPOL      EAPOL      EAP      EAP      EAP
    Start      Logoff     Invalid    Total     Resp/Id  Resp/Oth LenError
        2          0          0       1007       672         0         0

    Last      Last
EAPOLVer     EAPOLSrc
    1       00-00-E8-98-73-21

Tx:  EAPOL      EAP      EAP
    Total     Req/Id  Req/Oth
    2017      1005      0
Console#

```

6.5.7 Filtering IP Addresses for Management Access

A list of up to 15 IP addresses or IP address groups can be created that are allowed management access to the ECN330-switch through the web interface, SNMP, or Telnet.

Command Usage

- The management interfaces are open to all IP addresses by default. Once an entry is added to a filter list, access to that interface is restricted to the specified addresses.
- If anyone tries to access a management interface on the ECN330-switch from an invalid address, the ECN330-switch will reject the connection, enter an event message in the system log, and send a trap message to the trap manager.
- IP address can be configured for SNMP, web and Telnet access respectively. Each of these groups can include up to five different sets of addresses, either individual addresses or address ranges.
- When entering addresses for the same group (that is, SNMP, web or Telnet), the ECN330-switch will not accept overlapping address ranges. When entering addresses for different groups, the ECN330-switch will accept overlapping address ranges.

- An individual address cannot be deleted from a specified range. The entire range must be deleted and the addresses reentered.
- An address range can be deleted just by specifying the start address, or by specifying both the start address and end address.

Command Attributes

- **Web IP Filter** – Configures IP address(es) for the web group.
- **SNMP IP Filter** – Configures IP address(es) for the SNMP group.
- **Telnet IP Filter** – Configures IP address(es) for the Telnet group.
- **IP Filter List** – IP address which are allowed management access to this interface.
- **Start IP Address** – A single IP address, or the starting address of a range.
- **End IP Address** – The end address of a range.

Web – Click Security, IP Filter. Enter the addresses that are allowed management access to an interface, and click Add IP Filtering Entry.

Telnet IP Filter	
Telnet IP Filter List	192.168.1.19 192.168.1.19 192.168.1.25 192.168.1.30
Start IP Address	
End IP Address	
Add Telnet IP Filtering Entry Remove Telnet IP Filtering Entry	

Figure 54 IP Filter

CLI – This example restricts management access for Telnet clients.

```

Console(config)#management telnet-client 192.168.1.19
Console(config)#management telnet-client 192.168.1.25 192.168.1.30
Console#show management all-client
Management IP Filter
  HTTP-Client:
    Start IP address      End IP address
    -----
    1. 192.168.1.19        192.168.1.19
    2. 192.168.1.25        192.168.1.30

  SNMP-Client:
    Start IP address      End IP address
    -----

  TELNET-Client:
    Start IP address      End IP address
    -----
1. 192.168.1.19          192.168.1.19
2. 192.168.1.25          192.168.1.30

Console#

```

6.6 Access Control Lists

Access Control Lists (ACL) provide packet filtering for IP frames (based on address, protocol, Layer 4 protocol port number or TCP control code), any frames (based on MAC address or Ethernet type), or for frame types within a specified VLAN. To filter incoming packets, first create an access list, add the required rules, specify a mask to modify the precedence in which the rules are checked, and then bind the list to a specific port.

6.6.1 Configuring Access Control Lists

An ACL is a sequential list of permit or deny conditions that apply to IP addresses, MAC addresses, or other more specific criteria. The ECN330-switch tests ingress or egress packets against the conditions in an ACL one by one. A packet will be accepted as soon as it matches a permit rule, or dropped as soon as it matches a deny rule. If no rules match for a list of all permit rules, the packet is dropped; and if no rules match for a list of all deny rules, the packet is accepted.

A mask must be configured for an ACL rule before it can be bound to a port or set the queue or frame priorities associated with the rule. This is done by

specifying masks that control the order in which ACL rules are checked. The ECN330-switch includes two system default masks that pass/filter packets matching the permit/deny rules specified in an ingress ACL. Up to seven user-defined masks can also be configured for an ACL. A mask must be bound exclusively to one of the basic ACL types (that is, Ingress IP ACL, Egress IP ACL, Ingress MAC ACL, Egress MAC ACL, or Ingress VLAN ACL), but a mask can be bound to up to four ACLs of the same type.

The following filtering modes are supported:

- Standard IP ACL mode (STD-ACL) filters packets based on the source IP address.
- Extended IP ACL mode (EXT-ACL) filters packets based on source or destination IP address, as well as protocol type and protocol port number. If the TCP protocol is specified, packets can also be filtered based on the TCP control code.
- MAC ACL mode (MAC-ACL) filters packets based on the source or destination MAC address and the Ethernet frame type (RFC 1060).
- VLAN ACL mode (VLAN ACL) controls filtering within a VLAN based on specified IP or MAC ACLs.

Command Usage

The following restrictions apply to ACLs:

General Restrictions

- The ECN330-switch supports ACLs for both ingress and egress filtering. However, only one IP ACL and one MAC ACL can be bound to any port for ingress filtering, and one IP ACL and one MAC ACL to any port for egress filtering. In other words, only four ACLs can be bound to an interface – Ingress IP ACL, Egress IP ACL, Ingress MAC ACL and Egress MAC ACL.
- When an ACL is bound to an interface as an egress filter, all entries in the ACL must be deny rules. Otherwise, the bind operation will fail.
- The maximum number of ACLs is:
 - Fast Ethernet ports - 193 rules, 2 masks shared by 8-port groups
 - Gigabit Ethernet ports - 65 rules, 2 masks

- Each ACL can have up to 32 rules.
- The maximum number of ACLs is also 32. However, due to resource restrictions, the average number of rules bound the ports should not exceed 20.
- A mask must be configured for an ACL rule before it can be bound to a port or set the queue or frame priorities associated with the rule.
- The ECN330-switch does not support the explicit “deny any any” rule for the egress IP ACL or the egress MAC ACLs. If these rules are included in an ACL, and an attempt is made to bind the ACL to an interface for egress checking, the bind operation will fail.
- Egress MAC ACLs only work for destination-mac-known packets, not for multicast, broadcast, or destination-mac-unknown packets.
- Both a MAC ACL mask and VLAN ACL MAC mask can configure the VLAN ID field, so the masks may be completely the same. If this happens, there will be only one copy in database, and deleting either one of these two entries will remove the mask from database.

VLAN ACL Restrictions

- A VLAN ACL may contain at most one IP-ACL and one MAC-ACL.
- VLAN ACLs only apply to ingress traffic entering member ports within the bound VLANs.
- VLAN ACLs can only be applied to static VLANs.
- A VLAN which has already been bound by a VLAN ACL cannot subsequently be bound by another VLAN ACL.
- If a VLAN which has already been bound by a VLAN ACL, is bound by another VLAN ACL, the newly bound VLAN ACL takes precedence.
- A port may be bound with multiple VLAN ACLs since a port may join multiple VLANs.
- When a VLAN ACL is bound to a VLAN, this VLAN ACL is bound to all member ports, either tagged or untagged.
- If a port is bound with both a port-based ACL and a VLAN-based ACL, mask priority depends on which mask was configured first — the port ACL Mask or the VLAN ACL Mask.

The order in which active ACLs are checked is as follows:

1. MAC ACLs and IP ACLs bound to ports are checked first.
 - A User-defined rules in the Egress MAC ACL for egress ports.
 - B User-defined rules in the Egress IP ACL for egress ports.
 - C User-defined rules in the Ingress MAC ACL for ingress ports.
 - D User-defined rules in the Ingress IP ACL for ingress ports.
 - E Explicit default rule (permit any any) in the ingress IP ACL for ingress ports.
 - F Explicit default rule (permit any any) in the ingress MAC ACL for ingress ports.
 - G If no explicit rule is matched, the implicit default is permit all.
2. VLAN ACLs are then checked.

6.6.1.1 Setting the ACL Name and Type

Use the ACL Configuration page to designate the name and type of an ACL.

Command Attributes

- **Name** – Name of the ACL. (Maximum length: 16 characters)
- **Type** – There are three filtering modes:
 - Standard: IP ACL mode that filters packets based on the source IP address.
 - Extended: IP ACL mode that filters packets based on source or destination IP address, as well as protocol type and protocol port number. If the “TCP” protocol is specified, then packets can also be filtered based on the TCP control code.
 - MAC: MAC ACL mode that filters packets based on the source or destination MAC address and the Ethernet frame type (RFC 1060).

Web – Click Security, ACL, Configuration. Enter an ACL name in the Name field, select the list type (IP Standard, IP Extended, or MAC), and click Add to open the configuration page for the new list.

Figure 55 Selecting ACL Type

CLI – This example creates a standard IP ACL named bill.

```
Console(config)#access-list ip standard bill
Console(config-std-acl)#
```

6.6.1.2

Configuring a Standard IP ACL

Command Attributes

- **Action** – An ACL can contain all permit rules or all deny rules. (Default: Permit rules)
- **Address Type** – Specifies the source IP address. Use “Any” to include all possible addresses, “Host” to specify a specific host address in the Address field, or “IP” to specify a range of addresses with the Address and SubMask fields. (Options: Any, Host, IP; Default: Any)
- **IP Address** – Source IP address.
- **Subnet Mask** – A subnet mask containing four integers from 0 to 255, each separated by a period. The mask uses 1 bits to indicate “match” and 0 bits to indicate “ignore.” The mask is bitwise ANDed with the specified source IP address, and compared with the address for each IP packet entering the port(s) to which this ACL has been assigned.

Web – Specify the action (that is, Permit or Deny). Select the address type (Any, Host, or IP). If “Host” is selected, enter a specific address. If “IP” is selected, enter a subnet address and the mask for an address range. Then click Add.

Standard ACL

Name: david

Action	IP Address	Subnet Mask	Remove
Permit	10.1.1.21	255.255.255.255	Remove

Action:
 Address Type:
 IP Address:
 Subnet Mask:

Figure 56 Configuring Standard IP ACLs

CLI – This example configures one permit rule for the specific address 10.1.1.21 and another rule for the address range 168.92.16.x – 168.92.31.x using a bitmask.

```
Console(config-std-acl)#permit host 10.1.1.21
Console(config-std-acl)#permit 168.92.16.0 255.255.240.0
Console(config-std-acl)#
```

6.6.1.3

Configuring an Extended IP ACL

Command Attributes

- **Action** – An ACL can contain permit rules, deny rules or a combination of both. (Default: Permit rules)
- **Source/Destination Address Type** – Specifies the source or destination IP address. Use “Any” to include all possible addresses, “Host” to specify a specific host address in the Address field, or “IP” to specify a range of addresses with the Address and SubMask fields. (Options: Any, Host, IP; Default: Any)
- **Source/Destination IP Address** – Source or destination IP address.

- **Source/Destination Subnet Mask** – Subnet mask for source or destination address. (See the description for SubMask on page 160.)
- **Service Type** – Packet priority settings based on the following criteria:
 - **Precedence** – IP precedence level. (Range: 0-8, 8 means any)
 - **TOS** – Type of Service level. (Range: 0-16, 16 means any)
 - **DSCP** – DSCP priority level. (Range: 0-64, 64 means any)
- **Protocol** – Specifies the protocol type to match as TCP, UDP or Others, where others indicates a specific protocol number (0-255). (Options: TCP, UDP, Others; Default: TCP)
- **Source/Destination Port** – Source/destination port number for the specified protocol type. (Range: 0-65535)
- **Source/Destination Port Bitmask** – Decimal number representing the port bits to match. (Range: 0-65535)
- **Control Code** – Decimal number (representing a bit string) that specifies flag bits in byte 14 of the TCP header. (Range: 0-63)
- **Control Code Bitmask** – Decimal number representing the code bits to match. The control bitmask is a decimal number (for an equivalent binary bit mask) that is applied to the control code. Enter a decimal number, where the equivalent binary bit “1” means to match a bit and “0” means to ignore a bit. The following bits may be specified:
 - 1 (fin) – Finish
 - 2 (syn) – Synchronize
 - 4 (rst) – Reset
 - 8 (psh) – Push
 - 16 (ack) – Acknowledgement
 - 32 (urg) – Urgent pointer
- For example, use the code value and mask below to catch packets with the following flags set:
 - SYN flag valid, use control-code 2, control bitmask 2
 - Both SYN and ACK valid, use control-code 18, control bitmask 18
 - SYN valid and ACK invalid, use control-code 2, control bitmask 18

Web – Specify the action (that is, Permit or Deny). Specify the source or destination addresses or both addresses. Select the address type (Any, Host, or IP). If "Host" is selected, enter a specific address. If "IP" is selected, enter a subnet address and the mask for an address range. Set any other required criteria, such as service type, protocol type, or TCP control code. Then click Add.

Extended ACL

Name: mike

Action	Source IP Address	Source Subnet Mask	Destination IP Address	Destination Subnet Mask	TOS	Precedence	DSCP	Protocol	Source Port	Source Port Bitmask	Destination Port	Destination Port Bitmask	Control Code	Control Code Bitmask	Remove
Permit	10.7.1.0	255.255.255.255	Any	Any	Any	Any	Any	6	Any	Any	Any	Any	Any	Any	Remove
Permit	192.168.1.0	255.255.255.255	Any	Any	Any	Any	Any	6	Any	Any	80	65535	Any	Any	Remove

Action:

Source Address Type:

Source IP Address:

Source Subnet Mask:

Destination Address Type:

Destination IP Address:

Destination Subnet Mask:

Service Type: ☒ TOS (0-16) ☐ Precedence (0-8) ☐ DSCP (0-64)

Protocol: ☒ TCP (6) ☐ UDP (17) ☐ Others

Source Port (0-65535):

Source Port Bitmask (0-65535):

Destination Port (0-65535):

Destination Port Bitmask (0-65535):

Control Code (0-63):

Control Code Bitmask (0-63):

Figure 57 Configuring Extended IP ACLs

CLI – This example adds three rules:

1. Accept any incoming packets if the source address is in subnet 10.7.1.x. For example, if the rule is matched; that is, the rule (10.7.1.0 & 255.255.255.0) equals the masked address (10.7.1.2 & 255.255.255.0), the packet passes through.
2. Allow TCP packets from class C addresses 192.168.1.0 to any destination address when set for destination TCP port 80 (that is, HTTP).

3. Permit all TCP packets from class C addresses 192.168.1.0 with the TCP control code set to "SYN."

```

Console(config-ext-acl)#permit 10.7.1.1 255.255.255.0 any
Console(config-ext-acl)#permit tcp 192.168.1.0 255.255.255.0 any
    destination-port 80
Console(config-ext-acl)#permit tcp 192.168.1.0 255.255.255.0 any
    control-flag 2 2
Console(config-std-acl)#

```

6.6.1.4

Configuring a MAC ACL

Command Attributes

- **Action** – An ACL can contain permit rules, deny rules, or a combination of both. (Default: Permit rules)
- **Source/Destination Address Type** – Use "Any" to include all possible addresses, "Host" to indicate a specific MAC address, or "MAC" to specify an address range with the Address and Bitmask fields. (Options: Any, Host, MAC; Default: Any)
- **Source/Destination MAC Address** – Source or destination MAC address.
- **Source/Destination MAC Bitmask** – Hexadecimal mask for source or destination MAC address.
- **VID** – VLAN ID. (Range: 1-4093)
- **VID Bitmask** – VLAN bitmask. (Range: 1-4095)
- **Ethernet Type** – This option can only be used to filter Ethernet II formatted packets. (Range: 600-fff hex.)
A detailed listing of Ethernet protocol types can be found in RFC 1060. A few of the common types include 0800 (IP), 0806 (ARP), 8137 (IPX).
- **Ethernet Type Bitmask** – Protocol bitmask. (Range: 600-fff hex.)
- **Packet Format** – This attribute includes the following packet types:
 - **Any** – Any Ethernet packet type.
 - **Untagged-eth2** – Untagged Ethernet II packets.
 - **Untagged-802.3** – Untagged Ethernet 802.3 packets.
 - **Tagged-eth2** – Tagged Ethernet II packets.

- **Tagged-802.3** – Tagged Ethernet 802.3 packets.

Command Usage

- Egress MAC ACLs only work for destination-mac-known packets, not for multicast, broadcast, or destination-mac-unknown packets.

Web – Specify the action (that is, Permit or Deny). Specify the source or destination addresses or both addresses. Select the address type (Any, Host, or MAC). If "Host" is selected, enter a specific address (for example, 11-22-33-44-55-66). If "MAC" is selected, enter a base address and a hexadecimal bitmask for an address range. Set any other required criteria, such as VID, Ethernet type, or packet format. Then click Add.

MAC ACL

Name: bob

Action	Source MAC Address	Source Bitmask	Destination MAC Address	Destination Bitmask	VID	VID Bitmask	Ethernet Type	Ethernet Type Bitmask	Packet Format	Remove
Permit	Any	Any	00-e0-29-94-34-de	ff-ff-ff-ff	Any	Any	2048	65535	Any	Remove

Action:
 Source Address Type:
 Source MAC Address:
 Source Bitmask:
 Destination Address Type:
 Destination MAC Address:
 Destination Bitmask:
 VID:
 VID Bitmask:
 Ethernet Type:
 Ethernet Type Bitmask:
 Packet Format:

Figure 58 Configuring MAC ACLs

CLI – This rule permits packets from any source MAC address to the destination address 00-e0-29-94-34-de where the Ethernet type is 0800.

```
Console(config-mac-acl)#permit any host 00-e0-29-94-34-de
ethertype 0800
Console(config-mac-acl)#
```

6.6.2 Configuring ACL Masks

Masks must be specified that control the order in which ACL rules are checked. For example, the order in which the rules shown in Figure 57 on page 163 are checked depends on the mask settings. ACL rules matching the first entry in the mask are checked first. Rules matching subsequent entries in the mask are then checked in the specified order.

The ECN330-switch includes two system default masks that pass/filter packets matching the permit/deny rules specified in an ingress ACL. Up to seven user-defined masks can also be configured for an ingress or egress ACL. A mask must be bound exclusively to one of the basic ACL types (that is, Ingress IP ACL, Egress IP ACL, Ingress MAC ACL or Egress MAC ACL), but a mask can be bound to up to four ACLs of the same type.

Command Usage

- Up to seven entries can be assigned to an ACL mask.
- Packets crossing a port are checked against all the rules in the ACL until a match is found. The order in which these packets are checked is determined by the mask, and not the order in which the ACL rules are entered.
- First create the required ACLs and the ingress or egress masks before mapping an ACL to an interface.
- A mask must be configured for an ACL rule before it can be bound to a port or the queue or frame priorities associated with the rule set.

6.6.2.1 Specifying the Mask Type

Use the ACL Mask Configuration page to edit the mask for the Ingress IP ACL, Egress IP ACL, Ingress MAC ACL or Egress MAC ACL.

Web – Click Security, ACL, ACL Mask Configuration. Click Edit for one of the basic mask types to open the configuration page.

ACL Mask Configuration		
Mask Type	Mask Action	Edit
IP	Ingress	Edit
IP	Egress	Edit
MAC	Ingress	Edit
MAC	Egress	Edit

Figure 59 Choosing ACL Mask Types

CLI – This example creates an IP ingress mask, and then adds two rules. Each rule is checked in order of precedence to look for a match in the ACL entries. The first entry matching a mask is applied to the inbound packet.

```
Console(config)#access-list ip mask-precedence in
Console(config-ip-mask-acl)#mask host any
Console(config-ip-mask-acl)#mask 255.255.255.0 any
Console(config-ip-mask-acl)#
```

6.6.2.2 Configuring an IP ACL Mask

This mask defines the fields to check in the IP header.

Command Usage

- Masks that include an entry for a Layer 4 protocol source port or destination port can only be applied to packets with a header length of exactly five bytes.

Command Attributes

- **Source/Destination Address Type** – Specifies the source or destination IP address. Use “Any” to match any address, “Host” to specify a host address (not a subnet), or “IP” to specify a range of addresses. (Options: Any, Host, IP; Default: Any)
- **Source/Destination Subnet Mask** – Source or destination address of rule must match this bitmask. (See the description for SubMask on page 160.)
- **Protocol Bitmask** – Check the protocol field.
- **Service Type Mask** – Check the rule for the specified priority type. (Options: Precedence, TOS, DSCP; Default: TOS)
- **Source/Destination Port Bitmask** – Protocol port of rule must match this bitmask. (Range: 0-65535)
- **Control Code Bitmask** – Control flags of rule must match this bitmask. (Range: 0-63)

Web – Configure the mask to match the required rules in the IP ingress or egress ACLs. Set the mask to check for any source or destination address, a specific host address, or an address range. Include other criteria to search for in the rules, such as a protocol type or one of the service types. Or use a bitmask to search for specific protocol port(s) or TCP control code(s). Then click Add.

ACL Mask IP Configuration

Mask IP Ingress Table

Source Subnet Mask	Destination Subnet Mask	Protocol Mask	TOS Mask	Precedence Mask	DSCP Mask	Source Port Bitmask	Destination Port Bitmask	Control Code Bitmask	Remove
255.255.255.255	192.168.1.0	Disabled	Disabled	Disabled	Disabled	Any	80	Any	Remove

Remove All Entries

Source Address Type: Any

Source Subnet Mask: 0.0.0.0

Destination Address Type: Any

Destination Subnet Mask: 0.0.0.0

Protocol Mask: ☐ Enabled

Service Type Mask: ☒ TOS Enabled ☐ Precedence Enabled ☐ DSCP Enabled

Source Port Bitmask (0-65535):

Destination Port Bitmask (0-65535):

Control Code Bitmask (0-63):

Add

Figure 60 Configuring an IP ACL Mask

CLI – This shows that the entries in the mask override the precedence in which the rules are entered into the ACL. In the following example, packets with the source address 10.1.1.1 are dropped because the “deny 10.1.1.1 255.255.255.255” rule has the higher precedence according to the “mask host any” entry.

```

Console(config)#access-list ip standard A2
Console(config-std-acl)#permit 10.1.1.0 255.255.255.0
Console(config-std-acl)#deny 10.1.1.1 255.255.255.255
Console(config-std-acl)#exit
Console(config)#access-list ip mask-precedence in
Console(config-ip-mask-acl)#mask host any
Console(config-ip-mask-acl)#mask 255.255.255.0 any
Console(config-ip-mask-acl)#

```

6.6.2.3 Configuring a MAC ACL Mask

This mask defines the fields to check in the packet header.

Command Usage

A mask must be configured for an ACL rule before it can be bound to a port.

Command Attributes

- **Source/Destination Address Type** – Use “Any” to match any address, “Host” to specify the host address for a single node, or “MAC” to specify a range of addresses. (Options: Any, Host, MAC; Default: Any)
- **Source/Destination Bitmask** – Address of rule must match this bitmask.
- **VID Bitmask** – VLAN ID of rule must match this bitmask.
- **Ethernet Type Bitmask** – Ethernet type of rule must match this bitmask.
- **Packet Format Mask** – A packet format must be specified in the rule.

Web – Configure the mask to match the required rules in the MAC ingress or egress ACLs. Set the mask to check for any source or destination address, a host address, or an address range. Use a bitmask to search for specific VLAN ID(s) or Ethernet type(s). Or check for rules where a packet format was specified. Then click Add.

ACL Mask MAC Configuration

Mask MAC Ingress Table

Source Bitmask	Destination Bitmask	VID Bitmask	Ethernet Type Bitmask	Packet Format Mask	Remove
00-11-11-11-11-11	Any	3	800	Enabled	Remove

Remove All Entries

Source Address Type

Any

Source Bitmask

00-00-00-00-00-00

Destination Address Type

Any

Destination Bitmask

00-00-00-00-00-00

VID Bitmask

Ethernet Type Bitmask

Packet Format Mask

☐ Enabled

Add

Figure 61 Configuring an ACL MAC Mask

CLI – This example shows how to create an Ingress MAC ACL and bind it to a port. It can be seen that the order of the rules have been changed by the mask.

```

Console(config)#access-list mac M4
Console(config-mac-acl)#permit any any
Console(config-mac-acl)#deny tagged-eth2 00-11-11-11-11-11 ff-ff-ff-ff-ff-ff any vid 3
Console(config-mac-acl)#end
Console#show mac access-list
MAC access-list M4:
  permit any any
  deny tagged-eth2 host 00-11-11-11-11-11 any vid 3
Console(config)#access-list mac mask-precedence in
Console(config-mac-mask-acl)#mask pktformat ff-ff-ff-ff-ff-ff any vid
Console(config-mac-mask-acl)#exit
Console(config)#interface ethernet 1/12
Console(config-if)#mac access-group M4 in
Console(config-if)#end
Console#show access-list
MAC access-list M4:
  deny tagged-eth2 host 00-11-11-11-11-11 any vid 3
  permit any any
MAC ingress mask ACL:
  mask pktformat host any vid
Console#

```

6.6.3 Binding a Port to an Access Control List

After configuring the Access Control Lists (ACL), bind the ports that need to filter traffic to the appropriate ACLs. Only bind a port to one ACL for each basic type – IP ingress, IP egress, MAC ingress and MAC egress.

Command Usage

- A mask must be configured for an ACL rule before it can be bound to a port.
- The ECN330-switch supports ACLs for both ingress and egress filtering. However, only bind one IP ACL and one MAC ACL to any port for ingress filtering, and one IP ACL and one MAC ACL to any port for egress filtering. In other words, only four ACLs can be bound to an interface – Ingress IP ACL, Egress IP ACL, Ingress MAC ACL and Egress MAC ACL.

- When an ACL is bound to an interface as an egress filter, all entries in the ACL must be deny rules. Otherwise, the bind operation will fail.
- The ECN330-switch does not support the explicit “deny any any” rule for the egress IP ACL or the egress MAC ACLs. If these rules are included in an ACL, and an attempt is made to bind the ACL to an interface for egress checking, the bind operation will fail.

Command Attributes

- **Port** – Fixed port or SFP module. (Range: 1-12)
- **IP** – Specifies the IP ACL to bind to a port.
- **MAC** – Specifies the MAC ACL to bind to a port.
- **IN** – ACL for ingress packets.
- **OUT** – ACL for egress packets.
- *ACL Name* – Name of the ACL.

Web – Click Security, ACL, Port Binding. Mark the Enable field for the port to be bound to an ACL for ingress or egress traffic, select the required ACL from the drop-down list, then click Apply.

Port	IP		MAC	
	IN	OUT	IN	OUT
1	☒ Enable david	☐ Enable david	☒ Enable jerry	☐ Enable jerry
2	☒ Enable david	☐ Enable david	☐ Enable jerry	☐ Enable jerry
3	☐ Enable david	☐ Enable david	☐ Enable jerry	☐ Enable jerry
4	☐ Enable david	☐ Enable david	☐ Enable jerry	☐ Enable jerry
5	☐ Enable david	☐ Enable david	☐ Enable jerry	☐ Enable jerry
6	☐ Enable david	☐ Enable david	☐ Enable jerry	☐ Enable jerry

Figure 62 Mapping ACLs to Port Ingress/Egress Queues

CLI – This examples assigns an IP and MAC ingress ACL to port 1, and an IP ingress ACL to port 2.

```
Console(config)#interface ethernet 1/1
Console(config-if)#ip access-group david in
Console(config-if)#mac access-group jerry in
Console(config-if)#exit
Console(config)#interface ethernet 1/2
Console(config-if)#ip access-group david in
Console(config-if)#
```

6.6.4 Configuring a VLAN Access Map

A VLAN access map controls traffic filtering within a VLAN based on source or destination addresses and other criteria specified in IP or MAC ACLs (see “Configuring a Standard IP ACL” on page 160, “Configuring an Extended IP ACL” on page 161, or “Configuring a MAC ACL” on page 164). An access map contains information about the ACLs to apply and the action to take when a packet matches the specified rules. Follow these steps to create a VLAN ACL:

1. Configure an access map (see “Setting the Name of a VLAN Access Map” on page 175 and “Specifying the Associated IP/MAC ACLs and Action” on page 175),
2. Create a mask to control the order in which ingress traffic is checked against the ACL rules (see “Configuring a VLAN Mask for IP ACLs” on page 178 and “Configuring a VLAN Mask for MAC ACLs” on page 180),
3. Bind the VLAN ACL to one or more VLANs (see “Binding a VLAN to an Access Map” on page 182).

Any input packets which meet the criteria specified in the ACL permit rules are forwarded or dropped according to the specified action. Note that if no rules match any of the permit rules, the packet is dropped.

The following additional guidelines apply to the use of VLAN ACLs:

- When a port is added to a VLAN which had been bound by a VLAN ACL, the VLAN ACL is automatically added to the new port member.
- After a VLAN is bound with a VLAN ACL, any modifications to this VLAN ACL are automatically applied to all of the VLAN member ports.

6.6.4.1 Setting the Name of a VLAN Access Map

Use the VLAN Access Map Configuration page to designate the name of a new VLAN access map, or to edit an existing access map.

Command Attributes

- **Name** – Name of the ACL. (Maximum length: 16 characters)

Web – Click Security, VLAN ACL, Configuration. Enter a name for a new access map in the Name field, and click Add to open the configuration page for the new access map.

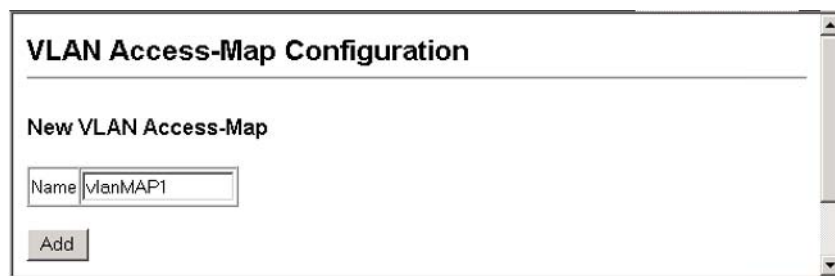


Figure 63 Creating a VLAN Access Map

CLI – This example creates a VLAN access map named RD.

```
Console(config)#vlan access-map vlanMAP1
Console(config-access-map)#match ip address ipACL1
Console(config-access-map)#action forward
Console(config-access-map)#
```

6.6.4.2 Specifying the Associated IP/MAC ACLs and Action

Command Usage

- Use existing IP or MAC ACLs to specify the match criteria for the VLAN access map. If the packets match, they will be forwarded or dropped, depending on the specified action.
- If the VLAN access map has at least one match clause for the packet type (IP or MAC) and the packet does not match any of the match

criteria, the default is to drop the packet. If there is no match criteria for that type of packet in the VLAN map, the default is to forward the packet.

- If the action is to drop matching packets, first define the access map, including configuring any access control list (ACL) containing the required match criteria before binding the map to a VLAN, or all packets could be dropped.

Command Attributes

- **IP** – Sets the access map to match packets against an IP ACL.
- **MAC** – Sets the access map to match packets against a MAC ACL.
- **Action** – Drops or forwards the packet when the specified conditions are matched.

Web – Click Security, VLAN ACL, Configuration. Enter a name for a new access map in the Name field, and click Add to open the configuration page for the new access map. Select an IP or MAC ACL from the scroll-down lists, set the Action to Drop or Forward, and then click Add.

VLAN Access-Map ACL Configuration

Name: vlanMAP1

ACL Type	IP	MAC
Name	☒ Enabled ipACL1	☐ Enabled (none)
Action	Forward	

Edit

Figure 64 Configuring a VLAN Access Map

CLI – The following command creates a VLAN access-map called vlanMAP1, sets the match criteria for an IP ACL called ipACL1, sets the action for forward matching packets, and then binds the VLAN ACL to VLANs 2 and 3.

```
Console(config)#vlan access-map vlanMAP1
Console(config-access-map)#match ip address ipACL1
Console(config-access-map)#action forward
Console(config-access-map)#exit
Console(config)#vlan filter vlanMAP1 vlan-lists 2-3
Console(config)#
```

6.6.5 Configuring VLAN ACL Masks

Masks must be specified that control the order in which ACL rules are checked. For example, the order in which the rules shown in Figure 57 on page 163 are checked depends on the mask settings. ACL rules matching the first entry in the mask are checked first. Rules matching subsequent entries in the mask are then checked in the specified order.

The ECN330-switch includes two system default masks that pass/filter packets matching the permit/deny rules specified in ingress IP ACLs or ingress MAC ACLs.

Command Usage

- Up to seven entries can be assigned to an ACL mask.
- Packets entering a VLAN member port are checked against all the rules in the ACL until a match is found. The order in which these packets are checked is determined by the mask, and not the order in which the ACL rules are entered.
- A mask must be configured for a VLAN access map before it can be bound to a VLAN or the queue or frame priorities associated with the rule set. Otherwise, any attempt to bind the access map to a VLAN will fail.
- The VLAN ID field is not specified in IP or MAC masks used for VLAN ACLs. The ECN330-switch automatically appends the VID filed for these masks when the VLAN ACL is bound to an interface.
- When an ACL port binding is removed, the ECN330-switch removes the mask settings from ASIC but keeps this information in RAM. When creating a VLAN mask, the ECN330-switch first checks whether there

are enough available masks based on the current mask information stored in RAM. If there are not enough available masks, the ECN330-switch responds with an error to the console interface such as "There are 4 user masks available, 3 used for port ACL, 1 used for VLAN ACL, no mask available now." If this kind of message appears, remove a port ACL mask (see section 6.6.2 on page 166). Enough masks should then be made available to create a VLAN ACL.

6.6.5.1 Configuring a VLAN Mask for IP ACLs

This mask defines the fields to check in the IP header.

Command Usage

- If Service Type "DSCP" is enabled, neither "TOS" nor (IP) "Precedence" can be enabled. However, both "TOS" and "Precedence" can be enabled if "DSCP" is not selected.
- Masks that include an entry for a Layer 4 protocol source port or destination port can only be applied to packets with a header length of exactly five bytes.

Command Attributes

- **Source/Destination Address Type** – Specifies the source or destination IP address. Use "Any" to match any address, "Host" to specify a host address (not a subnet), or "IP" to specify a range of addresses. (Options: Any, Host, IP; Default: Any)
- **Source/Destination Subnet Mask** – Source or destination address of rule must match this bitmask. (See the description for Subnet Mask on page 160.)
- **Protocol Bitmask** – Checks the protocol field.
- **Service Type Mask** – Check the rule for the specified priority type. (Options: Precedence, TOS, DSCP; Default: TOS)
- **Source/Destination Port Bit Mask** – Protocol port of rule must match this bitmask. (Range: 0-65535)
- **Control Code Bit Mask** – Control flags of rule must match this bitmask. (Range: 0-63)

Web – Configure the mask to match the required rules in the IP ingress ACLs. Set the mask to check for any source or destination address, a specific host address, or an address range. Include other criteria to search for in the rules, such as a protocol type or one of the service types. Or use a bitmask to search for specific protocol port(s) or TCP control code(s). Then click Add.

VLAN ACL Mask IP Configuration

Mask IP Table

Src IP BitMask	Dst IP BitMask	Protocol	TOS	Precedence	DSCP	Src Port BitMask	Dst Port BitMask	Control BitMask	Remove
255.255.255.255	192.168.1.0	Disabled	Disabled	Disabled	Disabled	Any	80	Any	Remove

Src IP:

Src IP BitMask:

Dst IP:

Dst IP BitMask:

Protocol BitMask: ☐ Enabled

Service Type: ☒ ☐ TOS Enabled ☐ Precedence Enabled ☐ ☐ DSCP Enabled

Src Port BitMask (0-65535):

Dst Port BitMask (0-65535):

Control BitMask (0-63):

Figure 65 Configuring an VLAN IP ACL Mask

CLI – The following example creates a mask that checks the protocol field in the IP header. It matches any source IP addresses, allows destination IP addresses that match the bitmask 192.168.1.0, and checks for destination port 80.

```
Console(config-ip-mask-acl)#mask protocol host 192.168.1.0
destination-port 80
Console(config-ip-mask-acl)#
```

6.6.5.2 Configuring a VLAN Mask for MAC ACLs

This mask defines the fields to check in the packet header.

Command Usage

A mask must be configured for an ACL rule before it can be bound to a port.

Command Attributes

- **Source/Destination Address Type** – Use “Any” to match any address, “Host” to specify the host address for a single node, or “MAC” to specify a range of addresses. (Options: Any, Host, MAC; Default: Any)
- **Source/Destination Bitmask** – Address of rule must match this bitmask.
- **Ethernet Type Bitmask** – Ethernet type of rule must match this bitmask.
- **Packet Format Mask** – A packet format must be specified in the rule.

Web – Configure the mask to match the required rules in the MAC ingress ACLs. Set the mask to check for any source or destination address, a host address, or an address range. Use a bitmask to search for specific Ethernet type(s). Or check for rules where a packet format was specified. Then click Add.

VLAN ACL Mask MAC Configuration

Mask MAC Table

Source MAC BitMask	Destination MAC BitMask	Ethernet Type Bitmask	Packet Format Bitmask	Remove
00-11-11-11-11-11	Any	800	Enabled	Remove

Source MAC	Any
Source MAC BitMask	00-00-00-00-00-00
Destination MAC	Any
Destination MAC BitMask	00-00-00-00-00-00
Ethernet Type Bitmask	
Packet Format Bitmask	☐ Enable

Figure 66 Configuring an VLAN MAC ACL Mask

CLI – The following example creates a mask that checks packet format, matches the source MAC address 00-11-11-11-11-11 but allows any destination MAC address in the MAC header, and checks the Ethernet type field for Ethernet II packet types.

```
Console(config-mac-mask-acl)#mask pktformat 00-11-11-11-11-11 any
ethertype 800
Console(config-mac-mask-acl)#
```

6.6.6 Binding a VLAN to an Access Map

After configuring the VLAN access map, bind one or more VLANs that need to filter traffic to the appropriate access map. Note that a VLAN can only be bound to one access map.

Command Usage

- A mask must be configured for any access map before it can be bound to a VLAN.
- Only one VLAN access map can be bound to a VLAN. If more than one access map is bound to the same VLAN, only the later one will be used.
- When an IP or MAC access list is bound to a port interface, and a VLAN map is subsequently bound to a VLAN containing that port, the VLAN access map takes precedence over the port ACL.

Command Attributes

- **VLAN Access Map Name** – Name of VLAN access map. (Maximum length: 16 characters)
- **VLAN Filter List** – A list of one or more VLANs to which the selected access map is bound. (Range: 1-4094)

Web – Click Security, VLAN ACL, VLAN Filtering. Select the required access map from the drop-down list, use the Binding and Remove buttons to select the VLANs to which the access map is bound, then click Apply.

VLAN Access-Map Filter Configuration

VLAN Access-Map Name
 vlanMAP1

Filter Vlan List

2

<<Binding Remove

VLAN ID (1-4094)

Figure 67 Mapping Access Maps to VLANs

CLI – This examples binds vlanMAP1 to VLAN 2.

```
Console(config)#vlan filter vlanMAP1 vlan-lists 2
Console(config)#
Console#show vlan filter access-map vlanMAP1
Access-map: vlanMAP1
  Applied VLAN Lists: 2
  Match IP VLANACL: ipACL1
  Match MAC VLANACL: macACL1
  Action: forward
Console#
```

6.7 Port Configuration

6.7.1 Displaying Connection Status

The Port Information or Trunk Information pages can be used to display the current connection status, including link state, speed/duplex mode, flow control, and auto-negotiation.

Field Attributes (Web)

- **Name** – Interface label.
- **Type** – Indicates the port type. (100BASE-TX, 1000BASE-T, or SFP)
- **Admin Status** – Shows if the interface is enabled or disabled.
- **Oper Status** – Indicates if the link is Up or Down.
- **Speed Duplex Status** – Shows the current speed and duplex mode. (Auto or fixed choice)
- **Flow Control Status** – Indicates the type of flow control currently in use. (IEEE 802.3x, Back-Pressure or None)
- **Autonegotiation** – Shows if auto-negotiation is enabled or disabled.
- **Media Type** – Shows the forced or preferred port type to use for combination ports 25-26. (Copper-Forced, SFP-Forced, SFP-Preferred-Auto) (This parameter is displayed for Port Information only.)
- **Trunk Member** – Shows if port is a trunk member. (This parameter is displayed for Port Information only.)
- **Creation** – Shows if a trunk is manually configured or dynamically set through LACP. (This parameter is displayed for Trunk Information only.)

Web – Click Port, Port Information or Trunk Information.

Port Information								
Port Name	Type	Admin Status	Oper Status	Speed Duplex Status	Flow Control Status	Autonegotiation	Media Type	Trunk Member
1	100Base-TX	Enabled	Up	100full	None	Enabled	None	
2	100Base-TX	Enabled	Up	100full	None	Enabled	None	
3	100Base-TX	Enabled	Down	100full	None	Enabled	None	
4	100Base-TX	Enabled	Down	100full	None	Enabled	None	
5	100Base-TX	Enabled	Down	100full	None	Enabled	None	
6	100Base-TX	Enabled	Down	100full	None	Enabled	None	
7	100Base-TX	Enabled	Down	100full	None	Enabled	None	
8	100Base-TX	Enabled	Down	100full	None	Enabled	None	
9	100Base-TX	Enabled	Down	100full	None	Enabled	None	
10	100Base-TX	Enabled	Down	100full	None	Enabled	None	
11	100Base-TX	Enabled	Down	100full	None	Enabled	None	
12	100Base-TX	Enabled	Down	100full	None	Enabled	None	

Figure 68 Port - Port Information

Field Attributes (CLI)

Basic information:

- **Port type** – Indicates the port type. (100BASE-TX, 1000BASE-T, or SFP)
- **MAC address** – The physical layer address for this port. (To access this item on the web, see “Setting the ECN330-switch’s IP Address” on page 80.)

Configuration:

- **Name** – Interface label.
- **Port Admin** – Shows if the interface is enabled or disabled (that is, up or down).
- **Speed-duplex** – Shows the current speed and duplex mode. (Auto, or fixed choice)
- **Capabilities** – Specifies the capabilities to be advertised for a port during auto-negotiation. (To access this item on the web, see “Configuring Interface Connections” on page 3-48.) The following capabilities are supported.
 - **10half** - Supports 10 Mbps half-duplex operation
 - **10full** - Supports 10 Mbps full-duplex operation
 - **100half** - Supports 100 Mbps half-duplex operation

- **100full** - Supports 100 Mbps full-duplex operation
- **1000full** - Supports 1000 Mbps full-duplex operation
- **Sym** - Transmits and receives pause frames for flow control
- **FC** - Supports flow control
- **Broadcast Storm** – Shows if broadcast storm control is enabled or disabled.
- **Broadcast Storm Limit** – Shows the broadcast storm threshold. (500 - 262143 packets per second)
- **Flow Control** – Shows if flow control is enabled or disabled.
- **LACP** – Shows if LACP is enabled or disabled.
- **Port Security** – Shows if port security is enabled or disabled.
- **Max MAC Count** – Shows the maximum number of MAC address that can be learned by a port. (0 - 1024 addresses)
- **Port Security Action** – Shows the response to take when a security violation is detected. (shutdown, trap, trap-and-shutdown)
- **Port MAC Learning** – Shows whether or not MAC address learning is enabled on this interface.
- **Media Type** – Shows the forced or preferred port type to use for combination ports 25-26. (copper forced, SFP forced, SFP preferred auto)

Current status:

- **Link Status** – Indicates if the link is up or down.
- **Port Operation Status** – Provides detailed information on port state. (Displayed only when the link is up.).
- **Operation Speed-Duplex** – Shows the current speed and duplex mode.
- **Flow Control Type** – Indicates the type of flow control currently in use. (IEEE 802.3x, Back-Pressure or none)

CLI – This example shows the connection status for Port 5.

```

Console#show interfaces status ethernet 1/5
Information of Eth 1/5
Basic information:
  Port Type:          100TX
  Mac address:        00-30-f1-47-58-46
Configuration:
  Port Admin:         Up
  Speed-duplex:       Auto
  Capabilities:       10half, 10full, 100half, 100full
  Broadcast Storm:    Enabled
  Broadcast Storm Limit: 500 packets/second
  Flow Control:       Disabled
  LACP:               Disabled
  Port Security:      Disabled
  Max MAC Count:      0
  Port Security Action: None
  Port MAC Learning:  Enabled
  Media Type:         None
Current status:
  Link Status:        Up
  Port Operation Status: Up
  Operation Speed-duplex: 100full
  Flow Control Type:  None
Console#

```

6.7.2

Configuring Interface Connections

The Port Configuration or Trunk Configuration page can be used to enable/disable an interface, set auto-negotiation and the interface capabilities to advertise, or manually fix the speed, duplex mode, and flow control for Fast Ethernet ports.

Command Attributes

- **Name** – Allows an interface to be labeled. (Range: 1-64 characters)
- **Admin** – Allows an interface to be manually disabled. An interface can be disabled due to abnormal behavior (for example, excessive collisions), and then reenabled after the problem has been resolved. An interface may also be disabled for security reasons.
- **Speed/Duplex** – Allows the port speed and duplex mode to be manually set.

Note: The 1000BASE-T standard does not support forced mode. Auto-negotiation must always be used to establish a connection over any 1000BASE-T port or trunk.

- **Flow Control** – Allows automatic or manual selection of flow control (that is, with auto-negotiation disabled for Fast Ethernet ports).
- **Autonegotiation** (Port Capabilities) – Allows auto-negotiation to be enabled/disabled. When auto-negotiation is enabled, the capabilities to be advertised need to be specified. When auto-negotiation is disabled for Fast Ethernet ports, the settings for speed, mode, and flow control can be forced. Note that autonegotiation cannot be disabled for Gigabit Ethernet ports, which only operate at 1000full (1 Gbps full-duplex). The following capabilities are supported.
 - **10half** - Supports 10 Mbps half-duplex operation
 - **10full** - Supports 10 Mbps full-duplex operation
 - **100half** - Supports 100 Mbps half-duplex operation
 - **100full** - Supports 100 Mbps full-duplex operation
 - **1000full** - Supports 1000 Mbps full-duplex operation
 - **Sym** (Gigabit only) - Check this item to transmit and receive pause frames, or clear it to auto-negotiate the sender and receiver for asymmetric pause frames. (*The current ECN330-switch chip only supports symmetric pause frames.*)
 - **FC** - Supports flow control.

Flow control can eliminate frame loss by “blocking” traffic from end stations or segments connected directly to the ECN330-switch when its buffers fill. When enabled, back pressure is used for half-duplex operation and IEEE 802.3x for full-duplex operation. (Avoid using flow control on a port connected to a hub unless it is actually required to solve a problem. Otherwise back pressure jamming signals may degrade overall performance for the segment attached to the hub.)

(Default: Autonegotiation enabled)

Auto-negotiation cannot be disabled for Gigabit Ethernet ports, which only operate at 1000full (1 Gbps full-duplex).

Advertised capabilities for RJ45:

100BASE-TX – 10half, 10full, 100half, 100full;

1000BASE-T – 10half, 10full, 100half, 100full, 1000full;

Advertised capabilities for SFP: 1000BASE-SX/LX/LH – 1000full)

- **Media Type** – Shows the forced/preferred port type to use for the combination ports. (Ports 25-26)
 - **Copper-Forced** - Always uses the built-in RJ45 port.
 - **SFP-Forced** - Always uses the SFP port (even if module is not installed).
 - **SFP-Preferred-Auto** - Uses SFP port if both combination types are functioning and the SFP port has a valid link. (This is the default.)
- **Trunk** – Indicates if a port is a member of a trunk. To create trunks and select port members, see 6.7.3 "Creating Trunk Groups" 190.

Note: Auto-negotiation must be disabled for Fast Ethernet ports before an interface can be configured or forced to use the Speed/Duplex Mode or Flow Control options. Auto-negotiation cannot be disabled for Gigabit Ethernet ports, which only operate at 1000full (1 Gbps full-duplex).

Web – Click Port, Port Configuration or Trunk Configuration. Modify the required interface settings, and click Apply.

Port Configuration											
Port	Name	Admin	Speed Duplex	Autonegotiation						Media Type	Trunk
1		☒ Enabled	100full	☒ Enabled	☒ 10h	☒ 100h	☐ 1000h	☐ 10Gh	☐ Sym	None	
				☒ 10f	☒ 100f	☒ 1000f	☐ 10Gf	☐ FC			
2		☒ Enabled	100full	☒ Enabled	☒ 10h	☒ 100h	☐ 1000h	☐ 10Gh	☐ Sym	None	
				☒ 10f	☒ 100f	☒ 1000f	☐ 10Gf	☐ FC			
3		☒ Enabled	100full	☒ Enabled	☒ 10h	☒ 100h	☐ 1000h	☐ 10Gh	☐ Sym	None	
				☒ 10f	☒ 100f	☒ 1000f	☐ 10Gf	☐ FC			
4		☒ Enabled	100full	☒ Enabled	☒ 10h	☒ 100h	☐ 1000h	☐ 10Gh	☐ Sym	None	
				☒ 10f	☒ 100f	☒ 1000f	☐ 10Gf	☐ FC			
5		☒ Enabled	100full	☒ Enabled	☒ 10h	☒ 100h	☐ 1000h	☐ 10Gh	☐ Sym	None	
				☒ 10f	☒ 100f	☒ 1000f	☐ 10Gf	☒ FC			
6		☒ Enabled	100full	☒ Enabled	☒ 10h	☒ 100h	☐ 1000h	☐ 10Gh	☐ Sym	None	
				☒ 10f	☒ 100f	☒ 1000f	☐ 10Gf	☐ FC			
7		☒ Enabled	100full	☒ Enabled	☒ 10h	☒ 100h	☐ 1000h	☐ 10Gh	☐ Sym	None	
				☒ 10f	☒ 100f	☒ 1000f	☐ 10Gf	☐ FC			
8		☒ Enabled	100full	☒ Enabled	☒ 10h	☒ 100h	☐ 1000h	☐ 10Gh	☐ Sym	None	
				☒ 10f	☒ 100f	☒ 1000f	☐ 10Gf	☐ FC			

Figure 69 Port - Port Configuration

CLI – Select the interface, and then enter the required settings.

```
Console(config)#interface ethernet 1/13
Console(config-if)#description RD SW#13
Console(config-if)#shutdown
.
Console(config-if)#no shutdown
Console(config-if)#no negotiation
Console(config-if)#speed-duplex 100half
Console(config-if)#flowcontrol
.
Console(config-if)#negotiation
Console(config-if)#capabilities 100half
Console(config-if)#capabilities 100full
Console(config-if)#capabilities flowcontrol
Console(config-if)#
```

6.7.3 Creating Trunk Groups

Multiple links can be created between devices that work as one virtual, aggregate link. A port trunk offers a dramatic increase in bandwidth for network segments where bottlenecks exist, as well as providing a fault-tolerant link between two devices. Up to 13 trunks can be created at a time.

The ECN330-switch supports both static trunking and dynamic Link Aggregation Control Protocol (LACP). Static trunks have to be manually configured at both ends of the link, and the switches must comply with the Cisco EtherChannel standard. On the other hand, LACP configured ports can automatically negotiate a trunked link with LACP-configured ports on another device. Any number of ports on the ECN330-switch can be configured as LACP, as long as they are not already configured as part of a static trunk. If ports on another device are also configured as LACP, the ECN330-switch and the other device will negotiate a trunk link between them. If an LACP trunk consists of more than eight ports, all other ports will be placed in a standby mode. Should one link in the trunk fail, one of the standby ports will automatically be activated to replace it.

Command Usage

Besides balancing the load across each port in the trunk, the other ports provide redundancy by taking over the load if a port in the trunk fails. However, before making any physical connections between devices, use the web interface or CLI

to specify the trunk on the devices at both ends. When using a port trunk, take note of the following points:

- Finish configuring port trunks before connecting the corresponding network cables between switches to avoid creating a loop.
- Up to 13 trunks can be created on the ECN330-switch, with up to eight ports per trunk.
- The ports at both ends of a connection must be configured as trunk ports.
- When configuring static trunks on switches of different types, they must be compatible with the Cisco EtherChannel standard.
- The ports at both ends of a trunk must be configured in an identical manner, including communication mode (that is, speed, duplex mode and flow control), VLAN assignments, and CoS settings.
- Any of the Gigabit ports on the front panel can be trunked together, including ports of different media types.
- All the ports in a trunk have to be treated as a whole when moved from/to, added or deleted from a VLAN.
- STP, VLAN, and IGMP settings can only be made for the entire trunk.

6.7.3.1

Statically Configuring a Trunk

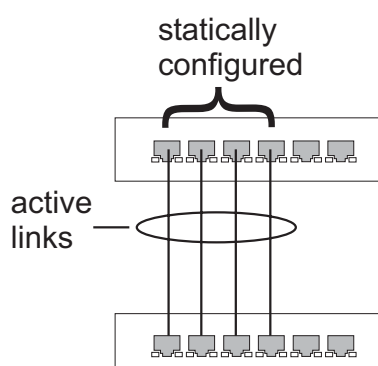


Figure 70 Configuring Static Trunks

Command Usage

- When configuring static trunks, switches of different types may not be able to link, depending on the manufacturer's implementation. However, note that the static trunks on the ECN330-switch are Cisco EtherChannel compatible.
- To avoid creating a loop in the network, add a static trunk through the configuration interface before connecting the ports, and also disconnect the ports before removing a static trunk through the configuration interface.

Command Attributes

- **Current** (Member List) – Shows configured trunks (Trunk ID, Unit, Port).
- **New** – Includes entry fields for creating new trunks.
 - **Trunk** – Trunk identifier. (Range: 1-13)
 - **Port** – Port identifier. (Range: 1-28)

Web – Click Trunk, Trunk Membership. Enter a trunk ID of 1-13 in the Trunk field, select any of the ECN330-switch ports from the scroll-down port list, and click Add. After adding the ports to the member list, click Apply.

Figure 71 Static Trunk Configuration

CLI – This example creates trunk 1 with ports 9 and 10. Just connect these ports to two static trunk ports on another switch to form a trunk.

```

Console(config)#interface port-channel 1
Console(config-if)#exit
Console(config)#interface ethernet 1/9
Console(config-if)#channel-group 1
Console(config-if)#exit
Console(config)#interface ethernet 1/10
Console(config-if)#channel-group 1
Console(config-if)#end
Console#show interfaces status port-channel 1
Information of Trunk 1
Basic information:
  Port Type:          100TX
  Mac address:        00-00-E8-AA-AA-01
Configuration:
  Name:
  Port Admin:         Up
  Speed-duplex:        Auto
  Capabilities:        10half, 10full, 100half, 100full
  Flow Control:        Disabled
  Port Security:       Disabled
Current status:
  Created By:          User
  Link Status:         Up
  Operation speed-duplex: 100full
  Flow control type:   None
  Member Ports: Eth1/9, Eth1/10,
Console#

```

6.7.3.2

Enabling LACP on Selected Ports

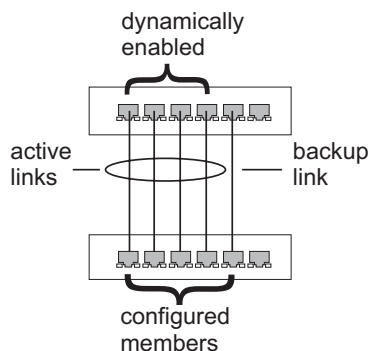


Figure 72 Configuring Dynamic Trunks

Command Usage

- To avoid creating a loop in the network, be sure to enable LACP before connecting the ports, and also disconnect the ports before disabling LACP.
- If the target switch has also enabled LACP on the connected ports, the trunk will be activated automatically.
- A trunk formed with another switch using LACP will automatically be assigned the next available trunk ID.
- If more than eight ports attached to the same target switch have LACP enabled, the additional ports will be placed in standby mode, and will only be enabled if one of the active links fails.
- All ports on both ends of an LACP trunk must be configured for full duplex, either by forced mode or auto-negotiation.
- Trunks dynamically established through LACP will also be shown in the Member List on the Trunk Membership menu (see page 191).

Command Attributes

- **Current** (Member List) – Shows configured trunks (Unit, Port).
- **New** – Selects a port to add to the current LACP-enabled port list.
 - **Port** – Port identifier. (Range: 1-28)

Web – Click Port, LACP, Configuration. Select any of the ECN330-switch ports from the scroll-down port list and click Add. After completing adding ports to the member list, click Apply.

The screenshot shows a web interface titled "LACP Configuration". Under the "Member List:" section, there are two columns: "Current:" and "New:". The "Current:" column contains a scrollable list of ports: Unit1 Port1, Unit1 Port2, Unit1 Port3, Unit1 Port4, Unit1 Port5, Unit1 Port6, Unit1 Port7, and Unit1 Port8. To the right of this list are two buttons: "<<Add" and "Remove". The "New:" column contains a "Port" label followed by a dropdown menu currently showing the value "1".

Figure 73 LACP Trunk Configuration

CLI – The following example enables LACP for ports 1 to 6. Just connect these ports to LACP-enabled trunk ports on another switch to form a trunk.

```

Console(config)#interface ethernet 1/1
Console(config-if)#lacp
Console(config-if)#exit
.
.
.
Console(config)#interface ethernet 1/6
Console(config-if)#lacp
Console(config-if)#end
Console#show interfaces status port-channel 1
Information of Trunk 1
Basic information:
  Port Type:          100TX
  Mac Address:        00-00-12-33-89-7F
Configuration:
  Name:
  Port Admin:         Up
  Speed-duplex:       Auto
  Capabilities:       10half, 10full, 100half, 100full
  Flow Control:       Disabled
  Port Security:      Disabled
  Max MAC Count:      0
Current status:
  Created by:         LACP
  Link status:        Up
  Port operation status: Up
  Operation Speed-duplex: 100full
  Flow Control Type:  None
  Member Ports: Eth1/1, Eth1/2, Eth1/3, Eth1/4, Eth1/5, Eth1/6,

```

6.7.3.3 Configuring LACP Parameters

Dynamically Creating a Port Channel –

Ports assigned to a common port channel must meet the following criteria:

- Ports must have the same LACP System Priority.
- Ports must have the same LACP port Admin Key.
- However, if the “port channel” Admin Key is set (page 763), then the port Admin Key must be set to the same value for a port to be allowed to join a channel group.

Note – If the port channel admin key (lacp admin key, page 763) is not set (through the CLI) when a channel group is formed (that is, it has a null value of 0), this key is set to the same value as the port admin key used by the interfaces that joined the group (lacp admin key, as described in this section and on page 762).

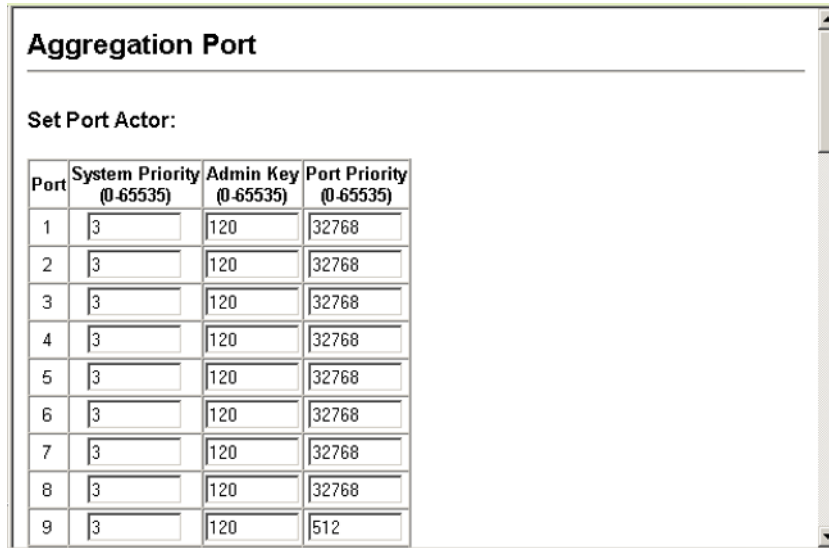
Command Attributes

Set Port Actor – This menu sets the local side of an aggregate link; that is, the ports on the ECN330-switch.

- **Port** – Port number. (Range: 1-28)
- **System Priority** – LACP system priority is used to determine link aggregation group (LAG) membership, and to identify this device to other switches during LAG negotiations. (Range: 0-65535; Default: 32768)
 - Ports must be configured with the same system priority to join the same LAG.
 - System priority is combined with the ECN330-switch's MAC address to form the LAG identifier. This identifier is used to indicate a specific LAG during LACP negotiations with other systems.
- **Admin Key** – The LACP administration key must be set to the same value for ports that belong to the same LAG. (Range: 0-65535; Default: 1)
- **Port Priority** – If a link goes down, LACP port priority is used to select a backup link. (Range: 0-65535; Default: 32768)

Set Port Partner – This menu sets the remote side of an aggregate link; that is, the ports on the attached device. The command attributes have the same meaning as those used for the port actor. However, configuring LACP settings for the partner only applies to its administrative state, not its operational state, and will only take effect the next time an aggregate link is established with the partner.

Web – Click Port, LACP, Aggregation Port. Set the System Priority, Admin Key, and Port Priority for the Port Actor. These settings can also be configured for the Port Partner. (However, note that these settings only affect the administrative state of the partner, and will not take effect until the next time an aggregate link is formed with this device.) After setting the port LACP parameters, click Apply.



Aggregation Port

Set Port Actor:

Port	System Priority (0-65535)	Admin Key (0-65535)	Port Priority (0-65535)
1	3	120	32768
2	3	120	32768
3	3	120	32768
4	3	120	32768
5	3	120	32768
6	3	120	32768
7	3	120	32768
8	3	120	32768
9	3	120	512

Figure 74 LACP - Aggregation Port

CLI – The following example configures LACP parameters for ports 1-10. Ports 1-8 are used as active members of the LAG, ports 9 and 10 are set to backup mode.

```

Console(config)#interface ethernet 1/1
Console(config-if)#lacp actor system-priority 3
Console(config-if)#lacp actor admin-key 120
Console(config-if)#lacp actor port-priority 128
Console(config-if)#exit
.
.
.
Console(config)#interface ethernet 1/10
Console(config-if)#lacp actor system-priority 3
Console(config-if)#lacp actor admin-key 120
Console(config-if)#lacp actor port-priority 512
Console(config-if)#end
Console#show lacp sysid

```

Channel Group	System Priority	System MAC Address
1	3	00-00-E9-31-31-31
2	32768	00-00-E9-31-31-31
3	32768	00-00-E9-31-31-31

```

.
.
.
Console#show lacp 1 internal
Port channel: 1
-----
Oper Key: 120
Admin Key: 0
Eth 1/ 1
-----
LACPDUs Internal: 30 sec
LACP System Priority: 3
LACP Port Priority: 128
Admin Key: 120
Oper Key: 120
Admin State: defaulted, aggregation, long timeout, LACP-activity
Oper State: distributing, collecting, synchronization,
aggregation, long timeout, LACP-activity
.
.
.

```

6.7.3.4 Displaying LACP Port Counters

Statistics for LACP protocol messages can be displayed.

Table 13 LACP Port Counters

Parameter	Description
LACPDUs Sent	Number of valid LACPDUs transmitted from this channel group.
LACPDUs Received	Number of valid LACPDUs received by this channel group.
Marker Sent	Number of valid Marker PDUs transmitted from this channel group.
Marker Received	Number of valid Marker PDUs received by this channel group.
Marker Unknown Pkts	Number of frames received that either (1) Carry the Slow Protocols Ethernet Type value, but contain an unknown PDU, or (2) are addressed to the Slow Protocols group MAC Address, but do not carry the Slow Protocols Ethernet Type.
Marker Illegal Pkts	Number of frames that carry the Slow Protocols Ethernet Type value, but contain a badly formed PDU or an illegal value of Protocol Subtype.

Web – Click Port, LACP, Port Counters Information. Select a member port to display the corresponding information.

LACP Port Counters Information

Member Port 1

Trunk ID : 2

LACPDU's Sent	307	LACPDU's Receive	296
Marker Sent	0	Marker Receive	0
Marker Unknown Pkts	0	Marker Illegal Pkts	0

Figure 75 LACP - Port Counters Information

CLI – The following example displays LACP counters for port channel 1.

```

Console#show lacp 1 counters
Port channel: 1
-----
Eth 1/ 2
-----
LACPDU's Sent:      19
LACPDU's Receive:   10
Marker Sent:        0
Marker Receive:     0
LACPDU's Unknown Pkts: 0
LACPDU's Illegal Pkts: 0
.
.
.

```

6.7.3.5 Displaying LACP Settings and Status for the Local Side

The configuration settings and operational state for the local side of a link aggregation can be displayed.

Table 14 LACP Internal Configuration Information

Field	Description
LACP System Priority	LACP system priority assigned to this port channel.
LACP Port Priority	LACP port priority assigned to this interface within the channel group.
Admin Key	Current administrative value of the key for the aggregation port.
Oper Key	Current operational value of the key for the aggregation port.
LACPDUs Internal	Number of seconds before invalidating received LACPDU information.

Field	Description
Admin State, Oper State	Administrative or operational values of the actor's state parameters: • Expired – The actor's receive machine is in the expired state; • Defaulted – The actor's receive machine is using defaulted operational partner information, administratively configured for the partner. • Distributing – If false, distribution of outgoing frames on this link is disabled; that is, distribution is currently disabled and is not expected to be enabled in the absence of administrative changes or changes in received protocol information. • Collecting – Collection of incoming frames on this link is enabled; that is, collection is currently enabled and is not expected to be disabled in the absence of administrative changes or changes in received protocol information. • Synchronization – The System considers this link to be IN_SYNC; that is, it has been allocated to the correct Link Aggregation Group, the group has been associated with a compatible Aggregator, and the identity of the Link Aggregation Group is consistent with the System ID and operational Key information transmitted. • Aggregation – The system considers this link to be aggregatable; that is, a potential candidate for aggregation. • Long timeout – Periodic transmission of LACPDUs uses a slow transmission rate. • LACP-Activity – Activity control value with regard to this link. (0: Passive; 1: Active)

Web – Click Port, LACP, Port Internal Information. Select a port channel to display the corresponding information.

LACP Port Internal Information

Interface Port 2

Trunk ID : 1

LACP System Priority	32768	LACP Port Priority	32768
Admin Key	3	Oper Key	3
LACPDUS Interval (secs)	30 seconds		
Admin State : Expired		Oper State : Expired	
Admin State : Defaulted	✓	Oper State : Defaulted	
Admin State : Distributing		Oper State : Distributing	✓
Admin State : Collecting		Oper State : Collecting	✓
Admin State : Synchronization		Oper State : Synchronization	✓
Admin State : Aggregation	✓	Oper State : Aggregation	✓
Admin State : Timeout	Long	Oper State : Timeout	Long
Admin State : LACP-Activity	✓	Oper State : LACP-Activity	✓

Figure 76 LACP - Port Internal Information

CLI – The following example displays the LACP configuration settings and operational state for the local side of port channel 1.

```

Console#show lacp 1 internal
Port channel: 1
-----
Oper Key: 3
Admin Key: 0
Eth 1/ 2
-----

LACPDUs Internal: 30 sec
LACP System Priority: 32768
LACP Port Priority: 32768
Admin Key: 3
Oper Key: 3
Admin State: defaulted, aggregation, long timeout, LACP-activity
Oper State: distributing, collecting, synchronization,
            aggregation, long timeout, LACP-activity
.
.
.

```

6.7.3.6 Displaying LACP Settings and Status for the Remote Side

The configuration settings and operational state for the remote side of a link aggregation can be displayed.

Table 15 LACP Neighbor Configuration Information

Field	Description
Partner Admin System ID	LAG partner's system ID assigned by the user.
Partner Oper System ID	LAG partner's system ID assigned by the LACP protocol.
Partner Admin Port Number	Current administrative value of the port number for the protocol Partner.
Partner Oper Port Number	Operational port number assigned to this aggregation port by the port's protocol partner.
Port Admin Priority	Current administrative value of the port priority for the protocol partner.
Port Oper Priority	Priority value assigned to this aggregation port by the partner.
Admin Key	Current administrative value of the Key for the protocol partner.
Oper Key	Current operational value of the Key for the protocol partner.
Admin State	Administrative values of the partner's state parameters. (See preceding table.)
Oper State	Operational values of the partner's state parameters. (See preceding table.)

Web – Click Port, LACP, Port Neighbors Information. Select a port channel to display the corresponding information.

LACP Port Neighbors Information

Interface Port 2

Trunk ID : 1

Partner Admin System ID	32768,00-00-00-00-00-00	Partner Oper System ID	32768,00-01-F4-78-AE-C0
Partner Admin Port Number	2	Partner Oper Port Number	2
Port Admin Priority	32768	Port Oper Priority	32768
Admin Key	0	Oper Key	3
Admin State : Expired		Oper State : Expired	
Admin State : Defaulted	✓	Oper State : Defaulted	
Admin State : Distributing	✓	Oper State : Distributing	✓
Admin State : Collecting	✓	Oper State : Collecting	✓
Admin State : Synchronization	✓	Oper State : Synchronization	✓
Admin State : Aggregation		Oper State : Aggregation	✓
Admin State : Timeout	Long	Oper State : Timeout	Long
Admin State : LACP-Activity		Oper State : LACP-Activity	✓

Figure 77 LACP - Port Neighbors Information

CLI – The following example displays the LACP configuration settings and operational state for the remote side of port channel 1.

```

Console#show lacp 1 neighbors
Port channel 1 neighbors
-----
Eth 1/2
-----
Partner Admin System ID: 32768, 00-00-00-00-00-00
Partner Oper System ID: 32768, 00-01-F4-78-AE-C0
Partner Admin Port Number: 2
Partner Oper Port Number: 2
Port Admin Priority: 32768
Port Oper Priority: 32768
Admin Key: 0
Oper Key: 3
Admin State: defaulted, distributing, collecting,
              synchronization, long timeout,
Oper State: distributing, collecting,
              synchronization, aggregation,
              long timeout, LACP-activity
.
.
.

```

6.7.4 Setting Broadcast Storm Thresholds

Broadcast storms may occur when a device on the network is malfunctioning, or if application programs are not well designed or properly configured. If there is too much broadcast traffic on the network, performance can be severely degraded or everything can come to complete halt.

The network can be protected from broadcast storms by setting a threshold for broadcast traffic for each port. Any broadcast packets exceeding the specified threshold will then be dropped.

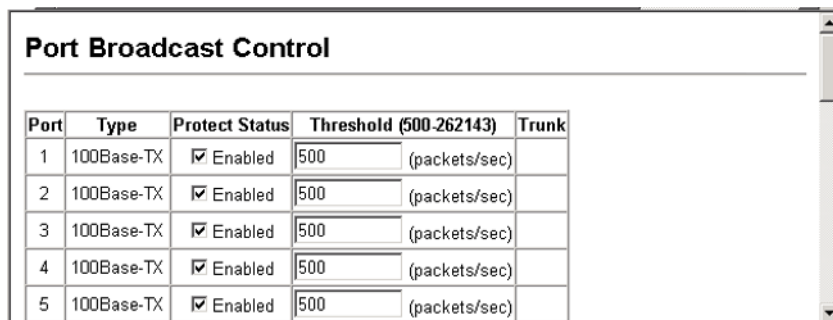
Command Usage

- Broadcast Storm Control is enabled by default.
- Broadcast control does not effect IP multicast traffic.

Command Attributes

- **Port** – Port number. (Port Broadcast Control)
- **Trunk** – Trunk number. (Trunk Broadcast Control)
- **Type** – Indicates the port type. (100BASE-TX, 1000BASE-T, or SFP)
- **Protect Status** – Shows whether or not broadcast storm control has been enabled. (Default: Enabled)
- **Threshold** – Threshold as percentage of port bandwidth. (Options: 500-262143 packets per second; Default: 500 packets per second)
- **Trunk** – Shows if port is a trunk member. (Port Broadcast Control)

Web – Click Port, Port Broadcast Control. Set the threshold any port, click Apply.



Port	Type	Protect Status	Threshold (500-262143)	Trunk
1	100Base-TX	☒ Enabled	500 (packets/sec)	
2	100Base-TX	☒ Enabled	500 (packets/sec)	
3	100Base-TX	☒ Enabled	500 (packets/sec)	
4	100Base-TX	☒ Enabled	500 (packets/sec)	
5	100Base-TX	☒ Enabled	500 (packets/sec)	

Figure 78 Port Broadcast Control

CLI – Specify any interface, and then enter the threshold. The following disables broadcast storm control for port 1, and then sets broadcast suppression at 600 packets per second for port 2.

```

Console(config)#interface ethernet 1/1
Console(config-if)#no switchport broadcast
Console(config-if)#exit
Console(config)#interface ethernet 1/2
Console(config-if)#switchport broadcast packet-rate 600
Console(config-if)#end
Console#show interfaces switchport ethernet 1/2
Information of Eth 1/2
Broadcast threshold: Enabled, 600 packets/second
Lacp status: Disabled
Ingress rate limit: disable,1000M bits per second
Egress rate limit: disable,1000M bits per second
VLAN membership mode: Hybrid
Ingress rule: Disabled
Acceptable frame type: All frames
Native VLAN: 1
Priority for untagged traffic: 0
Gvrp status: Disabled
Allowed Vlan: 1(u),
Forbidden Vlan:
Console#

```

6.7.5 Configuring Port Mirroring

Traffic can be mirrored from any source port to a target port for real-time analysis. A logic analyzer or RMON probe can then be attached to the target port to study the traffic crossing the source port in a completely unobtrusive manner.

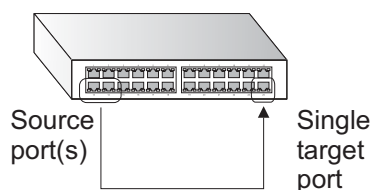


Figure 79 Configuring Port Mirroring

Command Usage

- Monitor port speed should match or exceed source port speed, otherwise traffic may be dropped from the monitor port.
- All mirror sessions have to share the same destination port.
- When mirroring port traffic, the target port must be included in the same VLAN as the source port.

Command Attributes

- **Mirror Sessions** – Displays a list of current mirror sessions.
- **Source Port** – The port whose traffic will be monitored. (Range: 1-28)
- **Type** – Selects which traffic to mirror to the target port. (Options: Rx, Tx, Both; Default: Both)
- **Target Port** – The port that will “duplicate” or “mirror” the traffic on the source port. (Range: 1-28)

Web – Click Port, Mirror Port Configuration. Specify the source port, the traffic type to be mirrored, and the monitor port, then click Add.

Mirror Port Configuration

Mirror Sessions:

Source: 1/1 Rx Destination: 1/2

New:

Source Port 1

Type Rx

Target Port 1

<<Add

Remove

Figure 80 Mirror Port Configuration

CLI – Use the interface command to select the monitor port, then use the port monitor command to specify the source port. Note that default mirroring under the CLI is for both received and transmitted packets.

```
Console(config)#interface ethernet 1/1
Console(config-if)#port monitor ethernet 1/2
Console(config-if)#
```

6.7.6 Configuring Rate Limits

This function allows the network manager to control the maximum rate for traffic transmitted or received on an interface. Rate limiting is configured on interfaces at the edge of a network to limit traffic into or out of the ECN330-switch. Traffic that falls within the rate limit is transmitted, while packets that exceed the acceptable amount of traffic are dropped.

Rate limiting can be applied to individual ports or trunks. The input rate limit for any port within a specific VLAN can also be configured. When an interface is configured with this feature, the traffic rate will be monitored by the hardware to verify conformity. Non-conforming traffic is dropped, conforming traffic is forwarded without any changes.

6.7.6.1 Setting Rate Limits for Individual Ports or Trunks

Command Attributes

- **Port** – Port number. (Range: 1-28)
- **Rate Limit Status** – Enables or disables rate limiting on the selected interface. (Default: Disabled)
- **Input/Output Rate Limit** – Sets the output rate limit for an interface. (Default: Fast Ethernet: 100000 Kbps; Gigabit Ethernet: 1000000 Kbps; Range: Fast Ethernet: 1-100000 Kbps; Gigabit Ethernet: 1-1000000 Kbps in multiples of 64 Kbps)
- **Trunk** – Shows if this port is a member of a trunk. (This item is only displayed for the Input/Output Port Configuration menus.)

Web - Click Rate Limit, Input/Output Port/Trunk Configuration. Set the Input Rate Limit Status or Output Rate Limit Status, then set the rate limit for the individual interfaces, and click Apply.

Port	Input Rate Limit Status	Input Rate Limit (Kbps)	Trunk
1	☒ Enabled	64000	
2	☐ Enabled	100032	
3	☐ Enabled	100032	
4	☐ Enabled	100032	
5	☐ Enabled	100032	
6	☐ Enabled	100032	
7	☐ Enabled	100032	
8	☐ Enabled	100032	
9	☐ Enabled	100032	
10	☐ Enabled	100032	

Figure 81 Rate Limit Configuration for an Interface

CLI - This example sets the rate limit for input and output traffic passing through port 1 to 64000 Kbps (640 Mbps).

```
Console(config)#interface ethernet 1/1
Console(config-if)#rate-limit input 64000
Console(config-if)#rate-limit output 64000
Console(config-if)#
```

6.7.6.2

Setting Rate Limits for Ports within Each VLAN

Command Attributes

- **Port** – Port number. (Range: 1-28)
- **Rate Limit List** – Rate limits applied to specified VLANs for each port.
- **VLAN ID** – ID of configured VLAN (1-4094).

- **Rate Limit** – Sets the output rate limit for an interface.
(Default: Fast Ethernet: 100000 Kbps; Gigabit Ethernet: 1000000 Kbps;
Range: Fast Ethernet: 1-100000 Kbps; Gigabit Ethernet: 1-1000000
Kbps in multiples of 64 Kbps)

Web - Click Rate Limit, Input Port Configuration per VLAN. Select a port and a VLAN to which this port has been assigned, then set the rate limit, and click Apply.

Figure 82 Rate Limit Configuration On a VLAN Basis

CLI - This example sets the rate limit for input traffic passing through port 1 on VLAN 1 to 6400 Kbps (6.4 Mbps) and 12800 kbps (12.8 Mbps) on VLAN 248.

```
Console(config)#interface ethernet 1/1
Console(config-if)#rate-limit input 6400 vlan 1
Console(config-if)#rate-limit input 12800 vlan 248
Console(config-if)#
```

6.7.7

Showing Port Statistics

Standard statistics can be displayed for network traffic from the Interfaces Group and Ethernet-like MIBs, as well as a detailed breakdown of traffic based on the RMON MIB. Interfaces and Ethernet-like statistics display errors on the traffic passing through each port. This information can be used to identify potential problems with the ECN330-switch (such as a faulty port or unusually heavy loading). RMON statistics provide access to a broad range of statistics, including a total count of different frame types and sizes passing through each port. All values displayed have been accumulated since the last system reboot, and are

shown as counts per second. Statistics are refreshed every 60 seconds by default.

Note: RMON groups 2, 3 and 9 can only be accessed using SNMP management software such as HP OpenView.

Table 16 Port Statistics

Parameter	Description
<i>Interface Statistics</i>	
Received Octets	The total number of octets received on the interface, including framing characters.
Received Unicast Packets	The number of subnetwork-unicast packets delivered to a higher-layer protocol.
Received Multicast Packets	The number of packets, delivered by this sub-layer to a higher (sub-)layer, which were addressed to a multicast address at this sub-layer.
Received Broadcast Packets	The number of packets, delivered by this sub-layer to a higher (sub-)layer, which were addressed to a broadcast address at this sub-layer.
Received Discarded Packets	The number of inbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. One possible reason for discarding such a packet could be to free up buffer space.
Received Unknown Packets	The number of packets received through the interface which were discarded because of an unknown or unsupported protocol.
Received Errors	The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.

Parameter	Description
Transmit Octets	The total number of octets transmitted out of the interface, including framing characters.
Transmit Unicast Packets	The total number of packets that higher-level protocols requested be transmitted to a subnetwork-unicast address, including those that were discarded or not sent.
Transmit Multicast Packets	The total number of packets that higher-level protocols requested be transmitted, and which were addressed to a multicast address at this sub-layer, including those that were discarded or not sent.
Transmit Broadcast Packets	The total number of packets that higher-level protocols requested be transmitted, and which were addressed to a broadcast address at this sub-layer, including those that were discarded or not sent.
Transmit Discarded Packets	The number of outbound packets which were chosen to be discarded even though no errors had been detected to prevent their being transmitted. One possible reason for discarding such a packet could be to free up buffer space.
Transmit Errors	The number of outbound packets that could not be transmitted because of errors.
<i>Etherlike Statistics</i>	
Alignment Errors	The number of alignment errors (missynchronized data packets).
Late Collisions	The number of times that a collision is detected later than 512 bit-times into the transmission of a packet.

Parameter	Description
FCS Errors	A count of frames received on a particular interface that are an integral number of octets in length but do not pass the FCS check. This count does not include frames received with frame-too-long or frame-too-short error.
Excessive Collisions	A count of frames for which transmission on a particular interface fails due to excessive collisions. This counter does not increment when the interface is operating in full-duplex mode.
Single Collision Frames	The number of successfully transmitted frames for which transmission is inhibited by exactly one collision.
Internal MAC Transmit Errors	A count of frames for which transmission on a particular interface fails due to an internal MAC sublayer transmit error.
Multiple Collision Frames	A count of successfully transmitted frames for which transmission is inhibited by more than one collision.
Carrier Sense Errors	The number of times that the carrier sense condition was lost or never asserted when attempting to transmit a frame.
SQE Test Errors	A count of times that the SQE TEST ERROR message is generated by the PLS sublayer for a particular interface.
Frames Too Long	A count of frames received on a particular interface that exceed the maximum permitted frame size.
Deferred Transmissions	A count of frames for which the first transmission attempt on a particular interface is delayed because the medium was busy.

Parameter	Description
Internal MAC Receive Errors	A count of frames for which reception on a particular interface fails due to an internal MAC sublayer receive error.
<i>RMON Statistics</i>	
Drop Events	The total number of events in which packets were dropped due to lack of resources.
Jabbers	The total number of frames received that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either an FCS or alignment error.
Received Bytes	Total number of bytes of data received on the network. This statistic can be used as a reasonable indication of Ethernet utilization.
Collisions	The best estimate of the total number of collisions on this Ethernet segment.
Received Frames	The total number of frames (bad, broadcast and multicast) received.
Broadcast Frames	The total number of good frames received that were directed to the broadcast address. Note that this does not include multicast packets.
Multicast Frames	The total number of good frames received that were directed to this multicast address.
CRC/Alignment Errors	The number of CRC/alignment errors (FCS or alignment errors).
Undersize Frames	The total number of frames received that were less than 64 octets long (excluding framing bits, but including FCS octets) and were otherwise well formed.

Parameter	Description
Oversize Frames	The total number of frames received that were longer than 1518 octets (excluding framing bits, but including FCS octets) and were otherwise well formed.
Fragments	The total number of frames received that were less than 64 octets in length (excluding framing bits, but including FCS octets) and had either an FCS or alignment error.
64 Bytes Frames	The total number of frames (including bad packets) received and transmitted that were 64 octets in length (excluding framing bits but including FCS octets).
65-127 Byte Frames 128-255 Byte Frames 256-511 Byte Frames 512-1023 Byte Frames 1024-1518 Byte Frames 1519-1536 Byte Frames	The total number of frames (including bad packets) received and transmitted where the number of octets fall within the specified range (excluding framing bits but including FCS octets).

Web – Click Port, Port Statistics. Select the required interface, and click Query. To update the screen, use the Refresh button at the bottom of the page.

Port Statistics

Interface
☒ Port 1
☐ Trunk

Query

Interface Statistics:

Received Octets	15020	Received Unicast Packets	0
Received Multicast Packets	177	Received Broadcast Packets	0
Received Discarded Packets	0	Received Unknown Packets	0
Received Errors	0	Transmit Octets	168087
Transmit Unicast Packets	0	Transmit Multicast Packets	2420
Transmit Broadcast Packets	47	Transmit Discarded Packets	0
Transmit Errors	0		

Etherlike Statistics:

Alignment Errors	0	Late Collisions	0
FCS Errors	0	Excessive Collisions	0
Single Collision Frames	0	Internal MAC Transmit Errors	0
Multiple Collision Frames	0	Carrier Sense Errors	0
SQE Test Errors	0	Frames Too Long	0
Deferred Transmissions	0	Internal MAC Receive Errors	0

RMON Statistics:

Drop Events	0	Jabbers	0
Received Bytes	188155	Collisions	0
Received Frames	0	64 Bytes Frames	2249
Broadcast Frames	47	65-127 Bytes Frames	459
Multicast Frames	2672	128-255 Bytes Frames	11
CRC/Alignment Errors	0	256-511 Bytes Frames	0
Undersize Frames	0	512-1023 Bytes Frames	0
Oversize Frames	0	1024-1518 Bytes Frames	0
Fragments	0		

Refresh

Figure 83 Port Statistics

CLI – This example shows statistics for port 12.

```
Console#show interfaces counters ethernet 1/12
Ethernet 1/12
Iftable stats:
  Octets input: 868453, Octets output: 3492122
  Unicast input: 7315, Unitcast output: 6658
  Discard input: 0, Discard output: 0
  Error input: 0, Error output: 0
  Unknown protos input: 0, QLen output: 0
Extended iftable stats:
  Multi-cast input: 0, Multi-cast output: 17027
  Broadcast input: 231, Broadcast output: 7
Ether-like stats:
  Alignment errors: 0, FCS errors: 0
  Single Collision frames: 0, Multiple collision frames: 0
  SQE Test errors: 0, Deferred transmissions: 0
  Late collisions: 0, Excessive collisions: 0
  Internal mac transmit errors: 0, Internal mac receive errors: 0
  Frame too longs: 0, Carrier sense errors: 0
  Symbol errors: 0
RMON stats:
  Drop events: 0, Octets: 4422579, Packets: 31552
  Broadcast pkts: 238, Multi-cast pkts: 17033
  Undersize pkts: 0, Oversize pkts: 0
  Fragments: 0, Jabbers: 0
  CRC align errors: 0, Collisions: 0
  Packet size <= 64 octets: 25568, Packet size 65 to 127 octets: 1616
  Packet size 128 to 255 octets: 1249, Packet size 256 to 511 octets: 1449
  Packet size 512 to 1023 octets: 802, Packet size 1024 to 1518 octets: 871
Console#
```

6.8 Power Over Ethernet Settings

The ECN330 can provide DC power to a wide range of connected devices, eliminating the need for an additional power source and cutting down on the amount of cables attached to each device. Once configured to supply power, an automatic detection process is initialized by the ECN330-switch that is authenticated by a PoE signature from the connected device. Detection and authentication prevent damage to non-compliant devices.

The ECN330-switch's power management enables total switch power and individual port power to be controlled within a configured power budget. Port power can be automatically turned on and off for connected devices, and a per-port power priority can be set so that the ECN330-switch never exceeds its allocated power budget. When a device is connected to an ECN330 port, its power requirements are detected by the ECN330-switch before power is supplied. If the power required by a device exceeds the power budget of the port or the whole switch, power is not supplied.

Ports can be set to one of three power priority levels, critical, high, or low. To control the power supply within the ECN330-switch's budget, ports set at critical or high priority have power enabled in preference to those ports set at low priority. For example, when a device is connected to a port set to critical priority, the ECN330-switch supplies the required power, if necessary by dropping power to ports set for a lower priority. If power is dropped to some low-priority ports and later the power demands on the ECN330-switch fall back within its budget, the dropped power is automatically restored.

6.8.1 ECN330-switch Power Status

Displays the Power over Ethernet parameters for the ECN330-switch.

Command Attributes

- **Maximum Available Power** – The configured power budget for the ECN330-switch.
- **System Operation Status** – The PoE power service provided to the ECN330 ports.
- **Mainpower Consumption** – The amount of power being consumed by PoE devices connected to the ECN330.

- **Thermal Temperature** – The internal temperature of the ECN330. (This parameter is not supported for the current hardware.)
- **Software Version** – The version of software running on the PoE controller subsystem in the ECN330-switch.

Web – Click PoE, Power Status.

Mainpower Status	
Maximum Available Power	555 watts
System Operation Status	on
Mainpower Consumption	0 watts
Thermal Temperature	(in Celsius)
Software Version	Version 0x1B6F, Build 0x07

Figure 84 Displaying the Global PoE Status

CLI – This example displays the current power status for the ECN330-switch.

```

Console#show power mainpower
Unit 1 Mainpower Status
Maximum Available Power : 555 watts
System Operation Status : on
Mainpower Consumption   : 0 watts
Software Version        : Version 0x1B6F, Build 0x07
Console#
    
```

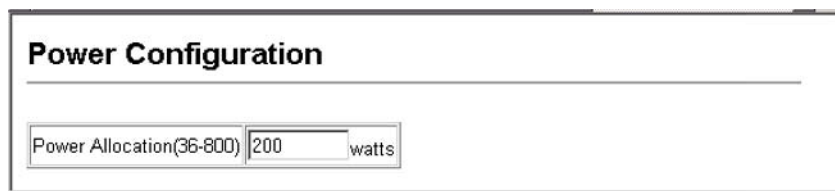

6.8.2 Setting the ECN330-switch Power Budget

A maximum PoE power budget for the ECN330-switch (power available to all ECN330 ports) can be defined so that power can be centrally managed, preventing overload conditions at the power source. If the power demand from devices connected to the ECN330 exceeds the power budget setting, the ECN330-switch uses port power priority settings to limit the supplied power.

Command Attributes

- **Power Allocation** – The power budget for the ECN330. If devices connected to the ECN330 require more power than the ECN330-switch budget, the port power priority settings are used to control the supplied power. (Range: 36 - 800 watts; Default: 555 Watts)

Web – Click PoE, Power Config. Specify the desired power budget for the ECN330-switch. Click Apply.



The screenshot shows a web interface titled "Power Configuration". Below the title is a horizontal line. Underneath the line is a text input field labeled "Power Allocation(36-800)" with the value "200" entered and a unit "watts" to its right.

Figure 85 Setting the ECN330-switch Power Budget

CLI – Use the **power mainpower maximum allocation** command to set the PoE power budget for the ECN330.

```
Console(config)#power mainpower maximum allocation 200
Console(config)#
```

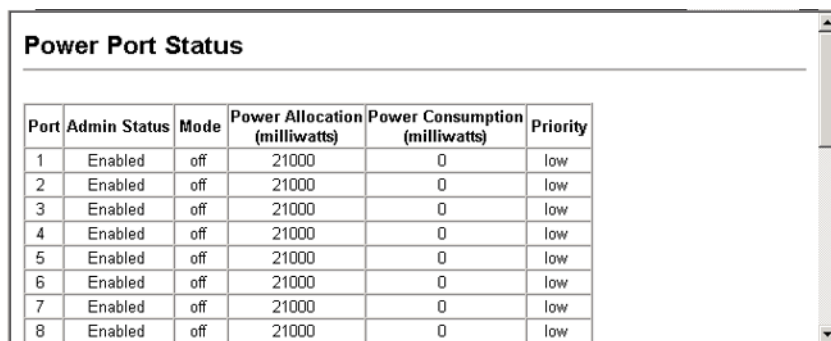
6.8.3 Displaying Port Power Status

Use the Power Port Status page to display the current PoE power status for all ports.

Command Attributes

- **Port** – The port number.
- **Admin Status** – The administrative status of PoE power on the port.
- **Mode** – The current operating status of PoE power on the port.
- **Power Allocation** – The configured power budget for the port.
- **Power Consumption** – The current power consumption on the port.
- **Priority** – The port's configured power priority setting.

Web – Click PoE, Power Port Status.



Port	Admin Status	Mode	Power Allocation (milliwatts)	Power Consumption (milliwatts)	Priority
1	Enabled	off	21000	0	low
2	Enabled	off	21000	0	low
3	Enabled	off	21000	0	low
4	Enabled	off	21000	0	low
5	Enabled	off	21000	0	low
6	Enabled	off	21000	0	low
7	Enabled	off	21000	0	low
8	Enabled	off	21000	0	low

Figure 86 Displaying Port PoE Status

CLI – This example displays the PoE status and priority of port 1.

```

Console#show power inline status
Interface  Admin   Oper  Power(mWatt)  Power(used)  Priority
-----
Eth  1/ 1  enable  off           21000         0          low
Eth  1/ 2  enable  off           21000         0          low
Eth  1/ 3  enable  off           21000         0          low
Eth  1/ 4  enable  off           21000         0          low
Eth  1/ 5  enable  off           21000         0          low
Eth  1/ 6  enable  off           21000         0          low
Eth  1/ 7  enable  off           21000         0          low
.
.
.
Eth  1/23  enable  off           21000         0          low
Eth  1/24  enable  off           21000         0          low
Console#

```

6.8.4 Configuring Port PoE Power

If a device is connected to an ECN330 port and the ECN330-switch detects that it requires more than the power budget of the port, no power is supplied to the device (that is, port power remains off).

If the power demand from devices connected to ECN330 ports exceeds the power budget set for the ECN330, the port power priority settings are used to control the supplied power. For example:

- If a device is connected to a low-priority port and causes the ECN330-switch to exceed its budget, port power is not turned on.
- If a device is connected to a critical or high-priority port and causes the ECN330-switch to exceed its budget, port power is turned on, but the ECN330-switch drops power to one or more lower-priority ports.

Note: Power is dropped from low-priority ports in sequence starting from port number 1.

Command Attributes

- **Port** – The port number on the ECN330.
- **Admin Status** – Enables PoE power on the port. Power is automatically supplied when a device is detected on the port, providing that the power

demanded does not exceed the ECN330 or port power budget.
(Default: Enabled)

- **Priority** – Sets the power priority for the port. (Options: low, high, or critical; Default: low)
- **Power Allocation** – Sets the power budget for the port.
(Range: 3000- 24700 milliwatts; Default: 24700 milliwatts)

Note: The maximum power allocation that configured is 24700 milliwatts. However, the maximum guaranteed power that can be delivered to any port is only 23100 miliwatts.

Web – Click PoE, Power Port Configuration. Enable PoE power on selected ports, set the priority and the power budget, and then click Apply.

Port	Admin Status	Priority	Power Allocation (3000-24700 milliwatts)
1	☒ Enabled	low	13000
2	☒ Enabled	critical	23100
3	☒ Enabled	low	24700
4	☒ Enabled	high	24700
5	☒ Enabled	high	24700

Figure 87 Configuring Port PoE Power

CLI – This example sets the PoE power budget for port 1 to 8 watts, the priority to high (2), and then enables the power.

```
Console(config)#interface ethernet 1/1
Console(config-if)#power inline maximum allocation 13000
Console(config-if)#power inline priority 2
Console(config-if)#power inline auto
Console(config-if)#
```

6.9 Address Table Settings

Switches store the addresses for all known devices. This information is used to pass traffic directly between the inbound and outbound ports. All the addresses learned by monitoring traffic are stored in the dynamic address table. Static addresses that are bound to a specific port can also be manually configured.

6.9.1 Setting Static Addresses

A static address can be assigned to a specific interface on the ECN330-switch. Static addresses are bound to the assigned interface and will not be moved. When a static address is seen on another interface, the address will be ignored and will not be written to the address table.

Command Attributes

- **Current Static Address Table** – Lists all the static addresses.
- **Interface** – Port or trunk associated with the device assigned a static address.
- **MAC Address** – Physical address of a device mapped to this interface.
- **VLAN** – ID of configured VLAN (1-4094).

The following parameter is displayed in the web interface only.

- **Static Address Counts** – The number of manually configured addresses.

Web – Click Address Table, Static Addresses. Specify the interface, the MAC address and VLAN, then click Add Static Address.

The screenshot shows a web interface titled "Static Addresses". It contains a form with the following fields and controls:

- Static Address Counts:** A text input field containing the number "1".
- Current Static Address Table:** A text area displaying the entry "00-E0-29-94-34-DE, VLAN 1, Unit 1, Port 1, Permanent".
- Interface:** A section with two radio buttons: "Port" (selected) and "Trunk". The "Port" option has a dropdown menu showing "1".
- MAC Address:** A text input field with a placeholder "(XX-XX-XX-XX-XX-XX)".
- VLAN:** A dropdown menu showing "1".
- Buttons:** Two buttons at the bottom: "Add Static Address" and "Remove Static Address".

Figure 88 Static Addresses

CLI – This example adds an address to the static address table, but sets it to be deleted when the ECN330-switch is reset.

```
Console(config)#mac-address-table static 00-e0-29-94-34-de interface
                ethernet 1/1 vlan 1 delete-on-reset
Console(config)#
```

6.9.2 Displaying the Address Table

The Dynamic Address Table contains the MAC addresses learned by monitoring the source address for traffic entering the ECN330-switch. When the destination address for inbound traffic is found in the database, the packets intended for that address are forwarded directly to the associated port. Otherwise, the traffic is flooded to all ports.

Command Attributes

- **Interface** – Indicates a port or trunk.
- **MAC Address** – Physical address associated with this interface.

- **VLAN** – ID of configured VLAN (1-4094).
- **Address Table Sort Key** – Sorts the information displayed based on MAC address, VLAN or interface (port or trunk).
- **Dynamic Address Counts** – The number of addresses dynamically learned.
- **Current Dynamic Address Table** – Lists all the dynamic addresses.

Web – Click Address Table, Dynamic Addresses. Specify the search type (that is, mark the Interface, MAC Address, or VLAN checkbox), select the method of sorting the displayed addresses, and then click Query.

Dynamic Addresses

Query by:

☒ Interface ☐ MAC Address ☐ VLAN

☒ Port 1 ☐ Trunk

Address Table Sort Key: Address

Dynamic Address Table

Dynamic Address Counts: 1

00-20-9C-23-CD-60, VLAN 2, Unit 1, Port 1, Dynamic

Current Dynamic Address Table

Figure 89 Dynamic Addresses

CLI – This example also displays the address table entries for port 1.

```
Console#show mac-address-table interface ethernet 1/1
Interface Mac Address      Vlan Type
-----
Eth 1/ 1 00-E0-29-94-34-DE  1 Permanent
Eth 1/ 1 00-20-9C-23-CD-60  2 Learned
Console#
```

6.9.3 Changing the Aging Time

The aging time can be set for entries in the dynamic address table.

Command Attributes

- **Aging Status** – Enables/disables the aging function.
- **Aging Time** – The time after which a learned entry is discarded. (Range: 10-1000000 seconds; Default: 300 seconds)

Web – Click Address Table, Address Aging. Specify the new aging time, click Apply.



Figure 90 Address Aging

CLI – This example sets the aging time to 400 seconds.

```
Console(config)#mac-address-table aging-time 400
Console(config)#
```

6.9.4 Setting an Address Threshold

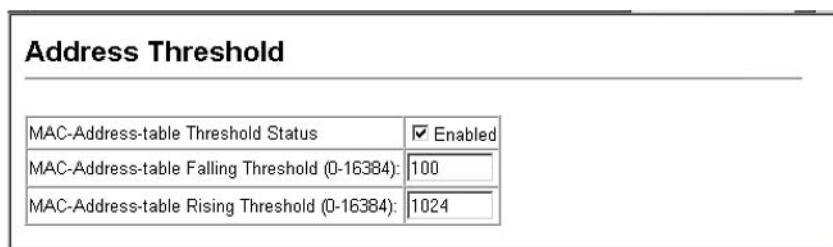
A trap message can be sent when entries in the address table exceed a specified threshold.

Command Attributes

- **MAC-Address-Table Threshold Status** – Sends a trap when entries in the MAC address table exceed the rising threshold. Note that once this trap has been sent, the next trigger time for this trap is after the MAC address entries fall below the falling threshold, and then exceed the rising threshold again.

- **MAC-Address-Table Falling Threshold (0-16384)** – Falling threshold for the address table. (Default: 0; Range 0-16384)
- **MAC-Address-Table Rising Threshold (0-16384)** – Rising threshold for the address table. (Default: 1024; Range 0-16384)

Web – Click Address Table, Address Threshold. Enable the trap, set the falling and rising thresholds, then click Apply.



Address Threshold	
MAC-Address-table Threshold Status	☒ Enabled
MAC-Address-table Falling Threshold (0-16384):	100
MAC-Address-table Rising Threshold (0-16384):	1024

Figure 91 Address Threshold

CLI – This example sets the aging time to 400 seconds.

```
Console(config)#mac-address-table threshold enable
Console(config)#mac-address-table threshold falling-threshold 100
Console(config)#mac-address-table threshold rising-threshold 1024
Console(config)#
```

6.10 Spanning Tree Algorithm Configuration

The Spanning Tree Algorithm (STA) can be used to detect and disable network loops, and to provide backup links between switches, bridges or routers. This allows the ECN330-switch to interact with other bridging devices (an STA-compliant switch, bridge or router) in the network to ensure that only one route exists between any two stations on the network, and provide backup links which automatically take over when a primary link goes down.

The spanning tree algorithms supported by the ECN330-switch include these versions:

- STP – Spanning Tree Protocol (IEEE 802.1D)
- RSTP – Rapid Spanning Tree Protocol (IEEE 802.1w)
- MSTP – Multiple Spanning Tree Protocol (IEEE 802.1s)

STP – STP uses a distributed algorithm to select a bridging device (STP-compliant switch, bridge or router) that serves as the root of the spanning tree network. It selects a root port on each bridging device (except for the root device) which incurs the lowest path cost when forwarding a packet from that device to the root device. Then it selects a designated bridging device from each LAN which incurs the lowest path cost when forwarding a packet from that LAN to the root device. All ports connected to designated bridging devices are assigned as designated ports. After determining the lowest cost spanning tree, it enables all root ports and designated ports, and disables all other ports. Network packets are therefore only forwarded between root ports and designated ports, eliminating any possible network loops.

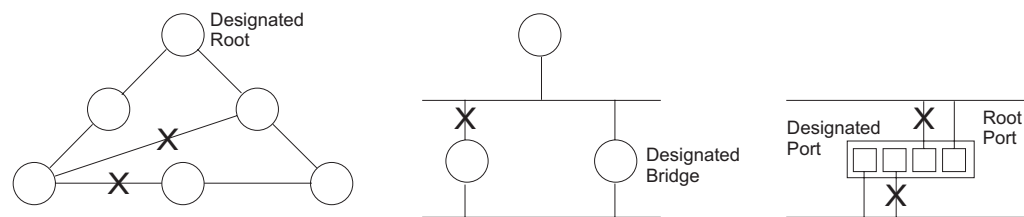


Figure 92 STP Root Ports and Designated Ports

Once a stable network topology has been established, all bridges listen for Hello BPDUs (Bridge Protocol Data Units) transmitted from the Root Bridge. If a bridge does not get a Hello BPDU after a predefined interval (Maximum Age), the bridge assumes that the link to the Root Bridge is down. This bridge will then initiate negotiations with other bridges to reconfigure the network to reestablish a valid network topology.

RSTP – RSTP is designed as a general replacement for the slower, legacy STP. RSTP is also incorporated into MSTP. RSTP achieves much faster reconfiguration (that is, around 1 to 3 seconds, compared to 30 seconds or more for STP) by reducing the number of state changes before active ports start learning, predefining an alternate route that can be used when a node or port fails, and retaining the forwarding database for ports insensitive to changes in the tree structure when reconfiguration occurs.

MSTP – When using STP or RSTP, it may be difficult to maintain a stable path between all VLAN members. Frequent changes in the tree structure can easily isolate some of the group members. MSTP (which is based on RSTP for fast convergence) is designed to support independent spanning trees based on VLAN groups. Using multiple spanning trees can provide multiple forwarding paths and enable load balancing. One or more VLANs can be grouped into a Multiple Spanning Tree Instance (MSTI). MSTP builds a separate Multiple

Spanning Tree (MST) for each instance to maintain connectivity among each of the assigned VLAN groups. MSTP then builds a Internal Spanning Tree (IST) for the Region containing all commonly configured MSTP bridges.

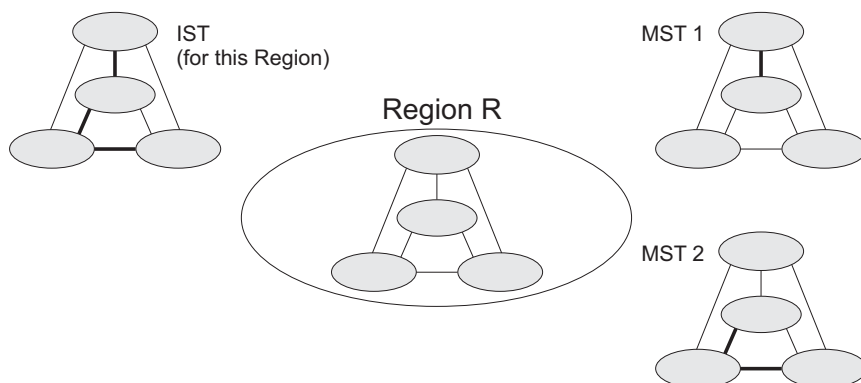


Figure 93 MSTP Region, Internal Spanning Tree, and Multiple Spanning Tree

An MST Region consists of a group of interconnected bridges that have the same MST Configuration Identifiers (including Region Name, Revision Level and Configuration Digest – see “Configuration Settings for MSTP” on page 241). An MST Region may contain multiple MSTP Instances. An Internal Spanning Tree (IST) is used to connect all the MSTP switches within an MST region. A Common Spanning Tree (CST) interconnects all adjacent MST Regions, and acts as a virtual bridge node for communications with STP or RSTP nodes in the global network.

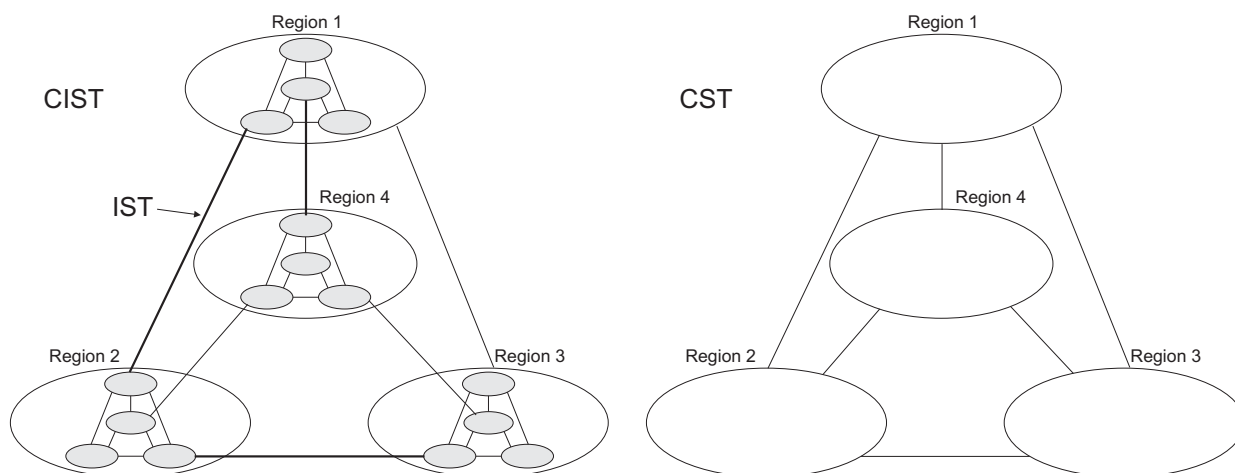


Figure 94 Common Internal Spanning Tree, Common Spanning Tree and Internal Spanning Tree

MSTP connects all bridges and LAN segments with a single Common and Internal Spanning Tree (CIST). The CIST is formed as a result of the running spanning tree algorithm between switches that support the STP, RSTP, MSTP protocols.

6.10.1 Displaying Global Settings

Using the STA Information screen, a summary of the current bridge STA information that applies to the entire ECN330-switch can be displayed.

Field Attributes

- **Spanning Tree State** – Shows if the ECN330-switch is enabled to participate in an STA-compliant network.
- **Bridge ID** – A unique identifier for this bridge, consisting of the bridge priority, the MST Instance ID 0 for the Common Spanning Tree when spanning tree mode is set to MSTP (see “Configuring Global Settings” on page 238), and the MAC address (where the address is taken from the ECN330-switch system).
- **Max Age** – The maximum time (in seconds) a device can wait without receiving a configuration message before attempting to reconfigure. All device ports (except for designated ports) should receive configuration messages at regular intervals. Any port that ages out STA information (provided in the last configuration message) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the device ports attached to the network. (References to “ports” in this section mean “interfaces,” which includes both ports and trunks.)
- **Hello Time** – Interval (in seconds) at which the root device transmits a configuration message.
- **Forward Delay** – The maximum time (in seconds) the root device will wait before changing states (that is, discarding to learning to forwarding). This delay is required because every device must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a discarding state; otherwise, temporary data loops might result.
- **Designated Root** – The priority and MAC address of the device in the Spanning Tree that the ECN330-switch has accepted as the root device.

- **Root Port** – The number of the port on the ECN330-switch that is closest to the root. The ECN330-switch communicates with the root device through this port. If there is no root port, then the ECN330-switch has been accepted as the root device of the Spanning Tree network.
- **Root Path Cost** – The path cost from the root port on the ECN330-switch to the root device.
- **Configuration Changes** – The number of times the Spanning Tree has been reconfigured.
- **Last Topology Change** – Time since the Spanning Tree was last reconfigured.

These additional parameters are only displayed for the CLI:

- **Spanning tree mode** – Specifies the type of spanning tree used on the ECN330-switch:
 - **STP**: Spanning Tree Protocol (IEEE 802.1D)
 - **RSTP**: Rapid Spanning Tree (IEEE 802.1w)
 - **MSTP**: Multiple Spanning Tree (IEEE 802.1s)
- **Instance** – Instance identifier of this spanning tree. (This is always 0 for the CIST.)
- **VLANs configuration** – VLANs assigned to the CIST.
- **Priority** – Bridge priority is used in selecting the root device, root port, and designated port. The device with the highest priority becomes the STA root device. However, if all devices have the same priority, the device with the lowest MAC address will then become the root device.
- **Root Hello Time** – Interval (in seconds) at which this device transmits a configuration message.
- **Root Maximum Age** – The maximum time (in seconds) this device can wait without receiving a configuration message before attempting to reconfigure. All device ports (except for designated ports) should receive configuration messages at regular intervals. If the root port ages out STA information (provided in the last configuration message), a new root port is selected from among the device ports attached to the network. (References to “ports” in this section means “interfaces,” which includes both ports and trunks.)

- **Root Forward Delay** – The maximum time (in seconds) this device will wait before changing states (discarding to learning to forwarding). This delay is required because every device must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a discarding state; otherwise, temporary data loops might result.
- **Max hops** – The max number of hop counts for the MST region.
- **Remaining hops** – The remaining number of hop counts for the MST instance.
- **Transmission limit** – The minimum interval between the transmission of consecutive RSTP/MSTP BPDUs.
- **Path Cost Method** – The path cost is used to determine the best path between devices. The path cost method is used to determine the range of values that can be assigned to each interface.

Web – Click Spanning Tree, STA, Information.

STA Information			
Spanning Tree:			
Spanning Tree State	Enabled	Designated Root	32768.0000ABCD0000
Bridge ID	32768.0000ABCD0000	Root Port	0
Max Age	20	Root Path Cost	0
Hello Time	2	Configuration Changes	2
Forward Delay	15	Last Topology Change	0 d 0 h 0 min 35 s

Figure 95 STA Information

CLI – This command displays global STA settings, followed by settings for each port.

```

Console#show spanning-tree
Spanning-tree information
-----
Spanning tree mode                :RSTP
Spanning tree enable/disable     :enable
Instance                          :0
Vlans configuration              :1-4094
Priority                          :32768
Bridge Hello Time (sec.)         :2
Bridge Max Age (sec.)            :20
Bridge Forward Delay (sec.)      :15
Root Hello Time (sec.)           :2
Root Max Age (sec.)              :20
Root Forward Delay (sec.)        :15
Max hops                         :20
Remaining hops                   :20
Designated Root                  :32768.0.0000ABCD0000
Current root port                 :1
Current root cost                 :200000
Number of topology changes       :1
Last topology changes time (sec.):13380
Transmission limit               :3
Path Cost Method                  :long
-----

Eth 1/ 1 information
-----
Admin status      : enable
Role              : disable
State             : discarding
External path cost : 10000
Internal path cost : 10000
Priority           : 128
Designated cost    : 5000
Designated port    : 128.1
Designated root:    32768.0.0000E8AAAA00
Designated bridge:  32768.0.0030F18FD550
Fast forwarding    : disable
Forward transitions : 0
Admin edge port     : disable
Oper edge port      : disable
Admin Link type     : auto
Oper Link type      : point-to-point
Spanning Tree Status : enable
.
.
.

```

Note: The current root port and current root cost display as zero when this device is not connected to the network.

6.10.2 Configuring Global Settings

Global settings apply to the entire ECN330-switch.

Command Usage

- **Spanning Tree Protocol**
Uses RSTP for the internal state machine, but sends only 802.1D BPDUs. This creates one spanning tree instance for the entire network. If multiple VLANs are implemented on a network, the path between specific VLAN members may be inadvertently disabled to prevent network loops, thus isolating group members. When operating multiple VLANs, it is recommended to select the MSTP option.
- **Rapid Spanning Tree Protocol**
RSTP supports connections to either STP or RSTP nodes by monitoring the incoming protocol messages and dynamically adjusting the type of protocol messages the RSTP node transmits, as described below:
 - **STP Mode** – If the ECN330-switch receives an 802.1D BPDU (STP BPDU) after a port's migration delay timer expires, the ECN330-switch assumes it is connected to an 802.1D bridge and starts using only 802.1D BPDUs.
 - **RSTP Mode** – If RSTP is using 802.1D BPDUs on a port and receives an RSTP BPDU after the migration delay expires, RSTP restarts the migration delay timer and begins using RSTP BPDUs on that port.
- **Multiple Spanning Tree Protocol**
 - To allow multiple spanning trees to operate over the network, configure a related set of bridges with the same MSTP configuration, allowing them to participate in a specific set of spanning tree instances.
 - A spanning tree instance can exist only on bridges that have compatible VLAN instance assignments.

- Be careful when switching between spanning tree modes. Changing modes stops all spanning-tree instances for the previous mode and restarts the system in the new mode, temporarily disrupting user traffic.

Note: STP and RSTP BPDUs are transmitted as untagged frames, and will cross any VLAN boundaries.

Command Attributes

Basic Configuration of Global Settings

- **Spanning Tree State** – Enables/disables STA on the ECN330-switch. (Default: Disabled)
- **Spanning Tree Type** – Specifies the type of spanning tree used on the ECN330-switch:
 - **STP:** Spanning Tree Protocol (IEEE 802.1D); when this option is selected, the ECN330-switch will use RSTP set to STP forced compatibility mode).
 - **RSTP:** Rapid Spanning Tree (IEEE 802.1w); RSTP is the default.
 - **MSTP:** Multiple Spanning Tree (IEEE 802.1s)
- **Priority** – Bridge priority is used in selecting the root device, root port, and designated port. The device with the highest priority becomes the STA root device. However, if all devices have the same priority, the device with the lowest MAC address will then become the root device. (Note that lower numeric values indicate higher priority.)
 - Default: 32768
 - Range: 0-61440, in steps of 4096
 - Options: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440

Root Device Configuration

- **Hello Time** – Interval (in seconds) at which the root device transmits a configuration message.
 - Default: 2
 - Minimum: 1
 - Maximum: The lower of 10 or $[(\text{Max. Message Age} / 2) - 1]$
- **Maximum Age** – The maximum time (in seconds) a device can wait without receiving a configuration message before attempting to reconfigure. All device ports (except for designated ports) should receive configuration messages at regular intervals. Any port that ages out STA information (provided in the last configuration message) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the device ports attached to the network. (References to “ports” in this section mean “interfaces,” which includes both ports and trunks.)
 - Default: 20
 - Minimum: The higher of 6 or $[2 \times (\text{Hello Time} + 1)]$.
 - Maximum: The lower of 40 or $[2 \times (\text{Forward Delay} - 1)]$
- **Forward Delay** – The maximum time (in seconds) this device will wait before changing states (discarding to learning to forwarding). This delay is required because every device must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a discarding state; otherwise, temporary data loops might result.
 - Default: 15
 - Minimum: The higher of 4 or $[(\text{Max. Message Age} / 2) + 1]$
 - Maximum: 30

Configuration Settings for RSTP

The following attributes apply to both RSTP and MSTP:

- **Path Cost Method** – The path cost is used to determine the best path between devices. The path cost method is used to determine the range of values that can be assigned to each interface.
 - Long: Specifies 32-bit based values that range from 1-200,000,000. (This is the default.)
 - Short: Specifies 16-bit based values that range from 1-65535.
- **Transmission Limit** – The maximum transmission rate for BPDUs is specified by setting the minimum interval between the transmission of consecutive protocol messages. (Range: 1-10; Default: 3)

Configuration Settings for MSTP

- **Max Instance Numbers** – The maximum number of MSTP instances to which the ECN330-switch can be assigned. (Default: 33)
- **Configuration Digest** – An MD5 signature key that contains the VLAN ID to MST ID mapping table. In other words, this key is a mapping of all VLANs to the CIST.
- **Region Revision** – The revision for this MSTI. (Range: 0-65535; Default: 0)
- **Region Name** – The name for this MSTI. (Maximum length: 32 characters)
- **Maximum Hop Count** – The maximum number of hops allowed in the MST region before a BPDU is discarded. (Range: 1-40; Default: 20)

Note: The MST name, revision number, and configuration digest are all required to uniquely identify an MST region.

Web – Click Spanning Tree, STA, Configuration. Modify the required attributes, and click Apply.

STA Configuration

Switch:

Spanning Tree State	☒ Enabled
Spanning Tree Type	MSTP
Priority (0-61440), in steps of 4096	32768

When The Switch Becomes Root:

Input Format: $2 * (\text{hello time} + 1) \leq \text{max age} \leq 2 * (\text{forward delay} - 1)$

Hello Time (1-10)	2	seconds
Maximum Age (6-40)	20	seconds
Forward Delay (4-30)	15	seconds

RSTP Configuration:

Path Cost Method	Long
Transmission Limit (1-10)	3

MSTP Configuration:

Max Instance Numbers	33
Configuration Digest	0xAC36177F50283CD4B83821D8AB26DE62
Region Revision (0-65535)	0
Region Name	00 00 12 33 89 76
Max Hop Count (1-40)	20

Figure 96 STA Configuration

CLI – This example enables Spanning Tree Protocol, sets the mode to MST, and then configures the STA and MSTP parameters.

```
Console(config)#spanning-tree
Console(config)#spanning-tree mode mst
Console(config)#spanning-tree priority 40000
Console(config)#spanning-tree hello-time 5
Console(config)#spanning-tree max-age 38
Console(config)#spanning-tree forward-time 20
Console(config)#spanning-tree pathcost method long
Console(config)#spanning-tree transmission-limit 4
Console(config)#spanning-tree mst-configuration
Console(config-mstp)#revision 1
Console(config-mstp)#name R&D
Console(config-mstp)#max-hops 30
Console(config-mstp)#
```

6.10.3

Displaying Interface Settings

The STA Port Information and STA Trunk Information pages display the current status of ports and trunks in the Spanning Tree.

Field Attributes

- **Spanning Tree** – Shows if STA has been enabled on this interface.
- **STA Status** – Displays current state of this port within the Spanning Tree:
 - **Discarding** - Port receives STA configuration messages, but does not forward packets.
 - **Learning** - Port has transmitted configuration messages for an interval set by the Forward Delay parameter without receiving contradictory information. Port address table is cleared, and the port begins learning addresses.
 - **Forwarding** - Port forwards packets, and continues learning addresses.

The rules defining port status are:

- A port on a network segment with no other STA compliant bridging device is always forwarding.

- If two ports of an ECN330 are connected to the same segment and there is no other STA device attached to this segment, the port with the smaller ID forwards packets and the other port is set to discarding.
- All ports are discarding when the ECN330 is booted, then some of them change state to learning, and then to forwarding.
- **Forward Transitions** – The number of times this port has transitioned from the Learning state to the Forwarding state.
- **Designated Cost** – The cost for a packet to travel from this port to the root in the current Spanning Tree configuration. The slower the media, the higher the cost.
- **Designated Bridge** – The bridge priority, the MST Instance ID 0 for the Common Spanning Tree when spanning tree mode is set to MSTP, and MAC address of the device through which this port must communicate to reach the root of the Spanning Tree.
- **Designated Port** – The port priority and number of the port on the designated bridging device through which the ECN330-switch must communicate with the root of the Spanning Tree.
- **Oper Path Cost** (Operational Path Cost) – The contribution of this port to the cost of paths towards the spanning tree root which includes this port.
- **Oper Link Type** (Operational Link Type) – The operational point-to-point status of the LAN segment attached to this interface. This parameter is determined by manual configuration or by auto-detection, as described for Admin Link Type in STA Port Configuration on page 256.
- **Oper Edge Port** (Operational Edge Port) – This parameter is initialized to the setting for Admin Edge Port in STA Port Configuration on page 247 (true or false), but will be set to false if a BPDU is received, indicating that another bridge is attached to this port.
- **Port Role** – Roles are assigned according to whether the port is part of the active topology connecting the bridge to the root bridge (**root** port), connecting a LAN through the bridge to the root bridge (that is, **designated** port), or is the MSTI regional root (**master** port); or is an **alternate** or **backup** port that may provide connectivity if other bridges, bridge ports, or LANs fail or are removed. The role is set to disabled (**disabled** port) if a port has no role within the spanning tree.

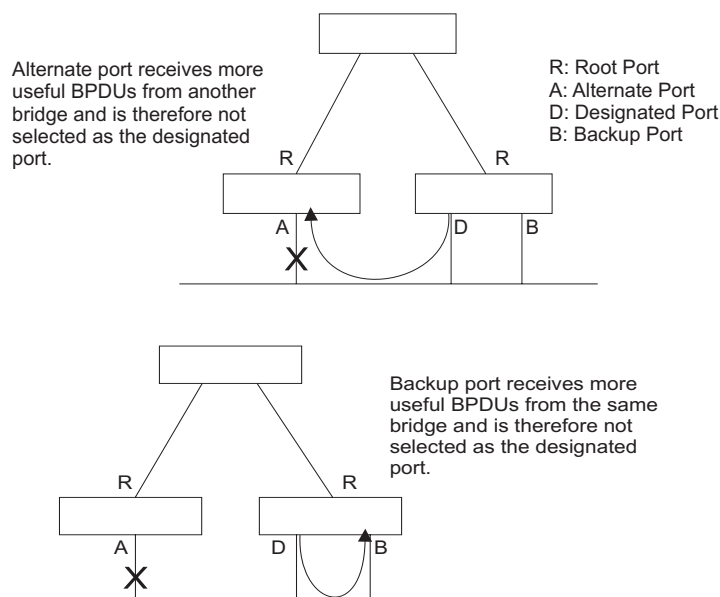


Figure 97 STA Port Roles

- **Trunk Member** – Indicates if a port is a member of a trunk. (STA Port Information only)

These additional parameters are only displayed for the CLI:

- **Admin status** – Shows if this interface is enabled.
- **External path cost** – The path cost for the IST. This parameter is used by the STA to determine the best path between devices. Therefore, lower values should be assigned to ports attached to faster media, and higher values assigned to ports with slower media. (Path cost takes precedence over port priority.)
- **Internal path cost** – The path cost for the MST. See the preceding item.
- **Priority** – Defines the priority used for this port in the Spanning Tree Algorithm. If the path cost for all ports on an ECN330-switch is the same, the port with the highest priority (lowest value) will be configured as an active link in the Spanning Tree. This makes a port with higher priority less likely to be blocked if the Spanning Tree Algorithm is detecting network loops. Where more than one port is assigned the highest priority, the port with the lowest numeric identifier will be enabled.

- **Designated root** – The priority and MAC address of the device in the Spanning Tree that the ECN330-switch has accepted as the root device.
- **Fast forwarding** – This field provides the same information as Admin Edge port, and is only included for backward compatibility with earlier products.
- **Admin Edge Port** – Enable this option if an interface is attached to a LAN segment at the end of a bridged LAN or to an end node. Since end nodes **cannot** cause forwarding loops, they can pass directly through to the spanning tree forwarding state. Specifying Edge Ports provides quicker convergence for devices such as workstations or servers, retains the current forwarding database to reduce the amount of frame flooding required to rebuild address tables during reconfiguration events, does not cause the spanning tree to reconfigure when the interface changes state, and also overcomes other STA-related timeout problems. However, remember that Edge Port should only be enabled for ports connected to an end-node device.
- **Admin Link Type** – The link type attached to this interface.
 - Point-to-Point – A connection to exactly one other bridge.
 - Shared – A connection to two or more bridges.
 - Auto – The ECN330-switch automatically determines if the interface is attached to a point-to-point link or to shared media.

Web – Click Spanning Tree, STA, Port Information or STA Trunk Information.

STA Port Information											
Port	Spanning Tree	STA Status	Forward Transitions	Designated Cost	Designated Bridge	Designated Port	Oper Path Cost	Oper Link Type	Oper Edge Port	Port Role	Trunk Member
1	Enabled	Forwarding	3	0	32768.0.000012338976	128.1	100000	Point-to-Point	Disabled	Designated	
2	Enabled	Forwarding	5	0	32768.0.000012338976	128.2	100000	Point-to-Point	Disabled	Designated	
3	Enabled	Discarding	0	0	32768.0.000012338976	128.3	100000	Point-to-Point	Disabled	Disabled	
4	Enabled	Discarding	0	0	32768.0.000012338976	128.4	100000	Point-to-Point	Disabled	Disabled	
5	Enabled	Discarding	0	0	32768.0.000012338976	128.5	100000	Point-to-Point	Disabled	Disabled	
6	Enabled	Discarding	0	0	32768.0.000012338976	128.6	100000	Point-to-Point	Disabled	Disabled	
7	Enabled	Discarding	0	0	32768.0.000012338976	128.7	100000	Point-to-Point	Disabled	Disabled	
8	Enabled	Discarding	0	0	32768.0.000012338976	128.8	100000	Point-to-Point	Disabled	Disabled	
9	Enabled	Discarding	0	0	32768.0.000012338976	128.9	100000	Point-to-Point	Disabled	Disabled	
10	Enabled	Discarding	0	0	32768.0.000012338976	128.10	100000	Point-to-Point	Disabled	Disabled	

Figure 98 STA Port Information

CLI – This example shows the STA attributes for port 5.

```

Console#show spanning-tree ethernet 1/5
Eth 1/ 5 information
-----
Admin Status:           Enabled
Role:                   Designate
State:                  Forwarding
External Admin Path Cost: 100000
Internal Admin Path Cost: 100000
External Oper Path Cost: 100000
Internal Oper Path Cost: 100000
Priority:                128
Designated Cost:         0
Designated Port:         128.1
Designated Root:         32768.0.000012338976
Designated Bridge:       32768.0.000012338976
Fast Forwarding:         Disabled
Forward Transitions:     3
Admin Edge Port:         Disabled
Oper Edge Port:          Disabled
Admin Link Type:         Auto
Oper Link Type:          Point-to-point
Spanning Tree Status:    Enabled

Console#

```

6.10.4

Configuring Interface Settings

RSTP and MSTP attributes can be configured for specific interfaces, including port priority, path cost, link type, and edge port. Use a different priority or path cost for ports of the same media type to indicate the preferred path, link type to indicate a point-to-point connection or shared-media connection, and edge port to indicate if the attached device can support fast forwarding. (References to “ports” in this section means “interfaces,” which includes both ports and trunks.)

Command Attributes

The following attributes are read-only and cannot be changed:

- **STA State** – Displays current state of this port within the Spanning Tree. (See Displaying Interface Settings on page 243 for additional information.)

- **Discarding** - Port receives STA configuration messages, but does not forward packets.
- **Learning** - Port has transmitted configuration messages for an interval set by the Forward Delay parameter without receiving contradictory information. Port address table is cleared, and the port begins learning addresses.
- **Forwarding** - Port forwards packets, and continues learning addresses.
- **Trunk** – Indicates if a port is a member of a trunk. (STA Port Configuration only)

The following interface attributes can be configured:

- **Spanning Tree** – Enables/disables STA on this interface. (Default: Enabled).
- **Priority** – Defines the priority used for this port in the Spanning Tree Algorithm. If the path cost for all ports on an ECN330-switch are the same, the port with the highest priority (lowest value) will be configured as an active link in the Spanning Tree. This makes a port with higher priority less likely to be blocked if the Spanning Tree Protocol is detecting network loops. Where more than one port is assigned the highest priority, the port with lowest numeric identifier will be enabled.
 - Default: 128
 - Range: 0-240, in steps of 16
- **Admin Path Cost** – This parameter is used by the STA to determine the best path between devices. Therefore, lower values should be assigned to ports attached to faster media, and higher values assigned to ports with slower media. (Path cost takes precedence over port priority.) Note that when the Path Cost Method is set to short (page 241), the maximum path cost is 65,535.

By default, the system automatically detects the speed and duplex mode used on each port, and configures the path cost according to the values shown below. Path cost “0” is used to indicate auto-configuration mode.

- Range –
 - Ethernet: 200,000-20,000,000
 - Fast Ethernet: 20,000-2,000,000
 - Gigabit Ethernet: 2,000-200,000

- **Default –**
 Ethernet – Half duplex: 2,000,000; full duplex: 1,000,000; trunk: 500,000
 Fast Ethernet – Half duplex: 200,000; full duplex: 100,000; trunk: 50,000
 Gigabit Ethernet – Full duplex: 10,000; trunk: 5,000
- **Admin Link Type** – The link type attached to this interface.
 - Point-to-Point – A connection to exactly one other bridge.
 - Shared – A connection to two or more bridges.
 - Auto – The ECN330-switch automatically determines if the interface is attached to a point-to-point link or to shared media. (This is the default setting.)
- **Admin Edge Port (Fast Forwarding)** – Enable this option if an interface is attached to a LAN segment at the end of a bridged LAN or to an end node. Since end nodes **cannot** cause forwarding loops, they can pass directly through to the spanning tree forwarding state. Specifying Edge Ports provides quicker convergence for devices such as workstations or servers, retains the current forwarding database to reduce the amount of frame flooding required to rebuild address tables during reconfiguration events, does not cause the spanning tree to initiate reconfiguration when the interface changes state, and also overcomes other STA-related timeout problems. However, remember that Edge Port should only be enabled for ports connected to an end-node device. (Default: Disabled)
- **Migration** – If at any time the ECN330-switch detects STP BPDUs, including Configuration or Topology Change Notification BPDUs, it automatically sets the selected interface to forced STP-compatible mode. However, the Protocol Migration button can also be used to manually re-check the appropriate BPDU format (RSTP or STP-compatible) to send on the selected interfaces. (Default: Disabled)

Web – Click Spanning Tree, STA, Port Configuration or Trunk Configuration. Modify the required attributes, then click Apply.

STA Port Configuration								
Port	Spanning Tree	STA State	Priority (0-240), in steps of 16	Admin Path Cost (1-200000000, 0:Auto)	Admin Link Type	Admin Edge Port (Fast Forwarding)	Migration	Trunk
1	☒ Enabled	Forwarding	128	0	Auto	☐ Enabled	☐ Enabled	
2	☒ Enabled	Discarding	128	0	Auto	☐ Enabled	☐ Enabled	
3	☒ Enabled	Discarding	128	0	Auto	☐ Enabled	☐ Enabled	
4	☒ Enabled	Discarding	128	0	Auto	☐ Enabled	☐ Enabled	
5	☒ Enabled	Discarding	128	0	Auto	☐ Enabled	☐ Enabled	
6	☒ Enabled	Discarding	128	0	Auto	☐ Enabled	☐ Enabled	
7	☐ Enabled	Discarding	0	50	Auto	☒ Enabled	☒ Enabled	

Figure 99 STA Port Configuration

CLI – This example sets STA attributes for port 7.

```
Console(config)#interface ethernet 1/7
Console(config-if)#no spanning-tree spanning-disabled
Console(config-if)#spanning-tree port-priority 0
Console(config-if)#spanning-tree cost 50
Console(config-if)#spanning-tree link-type auto
Console(config-if)#no spanning-tree edge-port
Console(config-if)#end
Console#spanning-tree protocol-migration ethernet 1/7
Console#
```

6.10.5 Configuring Multiple Spanning Trees

MSTP generates a unique spanning tree for each instance. This provides multiple pathways across the network, thereby balancing the traffic load, preventing wide-scale disruption when a bridge node in a single instance fails, and allowing for faster convergence of a new topology for the failed instance.

By default all VLANs are assigned to the Internal Spanning Tree (MST Instance 0) that connects all bridges and LANs within the MST region. The ECN330-switch supports up to 65 instances. Try to group VLANs which cover the same general area of the network. However, remember that all bridges within the same MSTP Region (page 241) must be configured with the same set of instances, and the same instance (on each bridge) with the same set of VLANs. Also, note that RSTP treats each MSTI region as a single node, connecting all regions to the Common Spanning Tree (CST).

To use multiple spanning trees:

1. Set the spanning tree type to MSTP (STA Configuration, page 238).
2. Enter the spanning tree priority for the selected MST instance (MSTP VLAN Configuration).
3. Add the VLANs that will share this MSTI (MSTP VLAN Configuration).

Note: All VLANs are automatically added to the IST (Instance 0).

To ensure that the MSTI maintains connectivity across the network, configure a related set of bridges with the same MSTI settings.

Command Attributes

- **MST Instance** – Instance identifier of this spanning tree. (Default: 0)
- **Priority** – The priority of a spanning tree instance. (Range: 0-61440 in steps of 4096; Options: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440; Default: 32768)
- **VLANs in MST Instance** – VLANs assigned this instance.
- **MST ID** – Instance identifier to configure. (Range: 0-4094; Default: 0)
- **VLAN ID** – VLAN assigned to the MST instance. (Range: 1-4094)

The other global attributes are described under “Displaying Global Settings,” page 234. The attributes displayed by the CLI for individual interfaces are described under “Displaying Interface Settings,” page 243

Web – Click Spanning Tree, MSTP, VLAN Configuration. Select an instance identifier from the list, set the instance priority, and click Apply. To add the VLAN members to an MSTI instance, enter the instance identifier, the VLAN identifier, and click Add.

MSTP VLAN Configuration

MST Instance ID: 1

Spanning Tree State	Enabled	Designated Root	32768.1.0030F1D473A0
Bridge ID	32768.1.0030F1D473A0	Root Port	0
Max Age	20	Root Path Cost	0
Hello Time	2	Configuration Changes	1
Forward Delay	15	Last Topology Change	0 d 0 h 0 min 1 s

Priority (0-61440): 32768

MSTP VLAN Configuration:

VLAN in MST Instance:

VLAN 1

Remove

MST ID (0-4094): VLAN ID: Add

Figure 100 MSTP VLAN Configuration

CLI – This displays STA settings for instance 2, followed by settings for each port.

```

Console#show spanning-tree mst 2
Spanning-tree information
-----
Spanning tree mode                :MSTP
Spanning tree enable/disable     :enable
Instance                          :2
Vlans configuration              :2
Priority                          :4096
Bridge Hello Time (sec.)         :2
Bridge Max Age (sec.)            :20
Bridge Forward Delay (sec.)      :15
Root Hello Time (sec.)           :2
Root Max Age (sec.)              :20
Root Forward Delay (sec.)        :15
Max hops                         :20
Remaining hops                   :20
Designated Root                  :4096.2.0000E9313131
Current root port                 :0
Current root cost                 :0
Number of topology changes       :0
Last topology changes time (sec.):646
Transmission limit               :3
Path Cost Method                  :long
-----

Eth 1/ 7 information
-----
Admin status      : enable
Role              : disable
State             : discarding
External path cost : 10000
Internal path cost : 10000
Priority           : 128
Designated cost   : 0
Designated port   : 128.7
Designated root   : 4096.2.0000E9313131
Designated bridge : 4096.2.0000E9313131
Fast forwarding   : enable
Forward transitions : 0
Admin edge port   : enable
Oper edge port    : enable
Admin Link type   : auto
Oper Link type    : point-to-point
Spanning Tree Status : enable
.
.
.

```

CLI – This example sets the priority for MSTI 1, and adds VLANs 1-5 to this MSTI.

```
Console(config)#spanning-tree mst-configuration
Console(config-mst)#mst 1 priority 4096
Console(config-mstp)#mst 1 vlan 1-5
Console(config-mst)#
```

6.10.6 Displaying Interface Settings for MSTP

The MSTP Port Information and MSTP Trunk Information pages display the current status of ports and trunks in the selected MST instance.

Field Attributes

MST Instance ID – Instance identifier to configure. (Range: 0-4094; Default: 0)

The other attributes are described under “Displaying Interface Settings,” page 243.

Web – Click Spanning Tree, MSTP, Port Information or Trunk Information. Select the required MST instance to display the current spanning tree values.

MSTP Port Information										
MST Instance ID: 0										
Port	STA Status	Forward Transitions	Designated Cost	Designated Bridge	Designated Port	Oper Path Cost	Oper Link Type	Oper Edge Port	Port Role	Trunk Member
1	Forwarding	3	0	32768.0.000012338976	128.1	100000	Point-to-Point	Disabled	Designated	
2	Forwarding	5	0	32768.0.000012338976	128.2	100000	Point-to-Point	Disabled	Designated	
3	Discarding	0	0	32768.0.000012338976	128.3	100000	Point-to-Point	Disabled	Disabled	
4	Discarding	0	0	32768.0.000012338976	128.4	100000	Point-to-Point	Disabled	Disabled	
5	Discarding	0	0	32768.0.000012338976	128.5	100000	Point-to-Point	Disabled	Disabled	
6	Discarding	0	0	32768.0.000012338976	128.6	100000	Point-to-Point	Disabled	Disabled	

Figure 101 MSTP Port Information

CLI – This displays STA settings for instance 0, followed by settings for each port. The settings for instance 0 are global settings that apply to the IST (page 234), the settings for other instances only apply to the local spanning tree.

```

Console#show spanning-tree mst 0
Spanning-tree information
-----
Spanning tree mode                :MSTP
Spanning tree enable/disable     :enable
Instance                          :0
Vlans configuration               :1-4094
Priority                          :32768
Bridge Hello Time (sec.)         :2
Bridge Max Age (sec.)            :20
Bridge Forward Delay (sec.)      :15
Root Hello Time (sec.)           :2
Root Max Age (sec.)              :20
Root Forward Delay (sec.)        :15
Max hops                         :20
Remaining hops                   :20
Designated Root                  :32768.0.0000ABCD0000
Current root port                 :1
Current root cost                 :200000
Number of topology changes       :1
Last topology changes time (sec.):645
Transmission limit               :3
Path Cost Method                  :long
-----

Eth 1/ 1 information
-----
Admin Status:                    Enabled
Role:                            Designate
State:                           Forwarding
External Admin Path Cost: 100000
Internal Admin Path Cost: 100000
External Oper Path Cost: 100000
Internal Oper Path Cost: 100000
Priority:                         128
Designated Cost:                  0
Designated Port:                  128.1
Designated Root:                  32768.0.000012338976
Designated Bridge:                32768.0.000012338976
Fast Forwarding:                  Disabled
Forward Transitions:              3
Admin Edge Port:                  Disabled
Oper Edge Port:                   Disabled
Admin Link Type:                  Auto
Oper Link Type:                   Point-to-point
Spanning Tree Status:             Enabled

```

6.10.7 Configuring Interface Settings for MSTP

The STA interface settings for an MST Instance can be configured using the MSTP Port Configuration and MSTP Trunk Configuration pages.

Field Attributes

The following attributes are read-only and cannot be changed:

- **STA State** – Displays current state of this port within the Spanning Tree. (See Displaying Interface Settings on page 243 for additional information.)
 - **Discarding** - Port receives STA configuration messages, but does not forward packets.
 - **Learning** - Port has transmitted configuration messages for an interval set by the Forward Delay parameter without receiving contradictory information. Port address table is cleared, and the port begins learning addresses.
 - **Forwarding** - Port forwards packets, and continues learning addresses.
- **Trunk** – Indicates if a port is a member of a trunk. (STA Port Configuration only)

The following interface attributes can be configured:

- **MST Instance ID** – Instance identifier to configure. (Range: 0-4094; Default: 0)
- **Priority** – Defines the priority used for this port in the Spanning Tree Protocol. If the path cost for all ports on an ECN330-switch are the same, the port with the highest priority (lowest value) will be configured as an active link in the Spanning Tree. This makes a port with higher priority less likely to be blocked if the Spanning Tree Protocol is detecting network loops. Where more than one port is assigned the highest priority, the port with lowest numeric identifier will be enabled.
 - Default: 128
 - Range: 0-240, in steps of 16

- **Admin MST Path Cost** – This parameter is used by the MSTP to determine the best path between devices. Therefore, lower values should be assigned to ports attached to faster media, and higher values assigned to ports with slower media. (Path cost takes precedence over port priority.) Note that when the Path Cost Method is set to short (page 241), the maximum path cost is 65,535.

By default, the system automatically detects the speed and duplex mode used on each port, and configures the path cost according to the values shown below. Path cost “0” is used to indicate auto-configuration mode.

- Range –
Ethernet: 200,000-20,000,000
Fast Ethernet: 20,000-2,000,000
Gigabit Ethernet: 2,000-200,000
- Default –
Ethernet – Half duplex: 2,000,000; full duplex: 1,000,000; trunk: 500,000
Fast Ethernet – Half duplex: 200,000; full duplex: 100,000; trunk: 50,000
Gigabit Ethernet – Full duplex: 10,000; trunk: 5,000

Web – Click Spanning Tree, MSTP, Port Configuration or Trunk Configuration. Enter the priority and path cost for an interface, and click Apply.

MSTP Port Configuration

MST Instance ID:

Port	STA State	Priority (0-240), in steps of 16	Admin MST Path Cost (1-200000000, 0:Auto)	Trunk
1	Forwarding	128	0	☐
2	Forwarding	128	0	☐
3	Discarding	0	50	☐
4	Discarding	128	0	☐
5	Discarding	128	0	☐

Figure 102 MSTP Port Configuration

CLI – This example sets the MSTP attributes for port 4.

```
Console(config)#interface ethernet 1/4
Console(config-if)#spanning-tree mst port-priority 0
Console(config-if)#spanning-tree mst cost 50
Console(config-if)
```

6.11 Ethernet Automatic Protection Switching Configuration

Note: The information provided in this section is based on RFC 3619.

Ethernet Automatic Protection Switching™ (EAPS) can be used to increase the availability and robustness of Ethernet rings. An Ethernet ring built using EAPS can have resilience comparable to that provided by SONET BSHR or SDH MS-SPRing configurations, at a lower cost and with fewer constraints (for example, ring size).

Many Metropolitan Area Networks (MANs) use a ring topology. EAPS works well in ring topologies for either MANs or LANs. MAN operators want to minimize the recovery time in the event of a fibre cut. EAPS technology converges in less than one second, often in less than 500 milliseconds. Also, EAPS does not limit the number of nodes in the ring, and the convergence time is independent of the number of nodes in the ring.

Operational Concept – An EAPS Domain exists on a single Ethernet ring. Any VLAN that is to be protected is configured on all ports in the ring for the given EAPS Domain. Each EAPS Domain has a single designated "master node." All other nodes on that ring are referred to as "transit nodes."

Each node has two ports connected to the ring. One port of the master node is designated as the "primary port" to the ring, carrying control messages and data, while the other port is designated as the "secondary port" and runs in backup mode.

In normal operation, the master node blocks the secondary port for all non-control Ethernet frames belonging to the given EAPS Domain, thereby avoiding a loop in the ring. Existing Ethernet switching and learning mechanisms operate per existing standards on this ring. This is possible because the master node makes the ring appear as though there is no loop from the perspective of the Ethernet standard algorithms used for switching and learning. If the master node detects a ring fault, it unblocks its secondary port and allows Ethernet data

frames to pass through that port. There is also a special "Control VLAN" that can always pass through all ports in the EAPS Domain, including the secondary port of the master node.

EAPS uses both a polling mechanism and an alert mechanism, described below, to verify the connectivity of the ring and quickly detect any faults.

Link Down Alert – When a transit node detects a link-down on any of its ports in the EAPS Domain, that transit node immediately sends a "link down" control frame on the Control VLAN to the master node.

When the master node receives this "link down" control frame, the master node moves from the "normal" state to the ring-fault state and unblocks its secondary port. The master node also flushes its bridging table, and sends a control frame to all other ring nodes, instructing them to flush their bridging tables as well. Immediately after flushing its bridging table, each node begins learning the new topology.

Ring Polling – The master node sends a health-check frame on the Control VLAN at a user-configurable interval. If the ring is complete, the health-check frame will be received on its secondary port, and the master node resets its fail-period timer and continues normal operation.

If the master node does not receive the health-check frame before the fail-period timer expires, the master node moves from normal state to "ring-fault" state and unblocks its secondary port. The master node flushes its bridging table and sends a control frame to all other nodes, instructing them to also flush their bridging tables. Immediately after flushing its bridge table, each node starts learning the new topology. This ring polling mechanism provides a backup in the event that the Link Down Alert frame should get lost for some unforeseen reason.

Ring Restoration – The master node continues sending periodic health-check frames out its primary port even when operating in the ring-fault state. Once the ring is restored, the next health-check frame will be received on the master node's secondary port. This will cause the master node to transition back to the normal state, logically block non-control frames on the secondary port, flush its own bridge table, and send a control frame to the transit nodes, instructing them to flush their bridging tables and re-learn the topology.

During the time between the transit node detecting that its link is restored and the master node detecting that the ring is restored, the secondary port of the

master node is still open – creating the possibility of a temporary loop in the topology. To prevent this, the transit node will place all the protected VLANs transiting the newly restored port into a temporary blocked state, remember which port has been temporarily blocked, and then transition into the "pre-forwarding" state. When the transit node in the "pre-forwarding" state receives a control frame instructing it to flush its bridging table, it will flush the bridging table, unblock the previously blocked protected VLANs on the newly restored port, and transition to the "normal" state.

Multiple EAPS Domains – An EAPS-enabled ECN330-switch can be part of more than one ring. Hence, an EAPS-enabled ECN330-switch can belong to more than one EAPS Domain at the same time. Each EAPS Domain on an ECN330-switch requires a separate instance of the EAPS protocol on that same ECN330-switch, one instance per EAPS-protected ring.

There can also be more than one EAPS domain running on the same ring at the same time. Each EAPS Domain has its own unique master node and its own set of protected VLANs. This facilitates reuse of the ring's bandwidth.

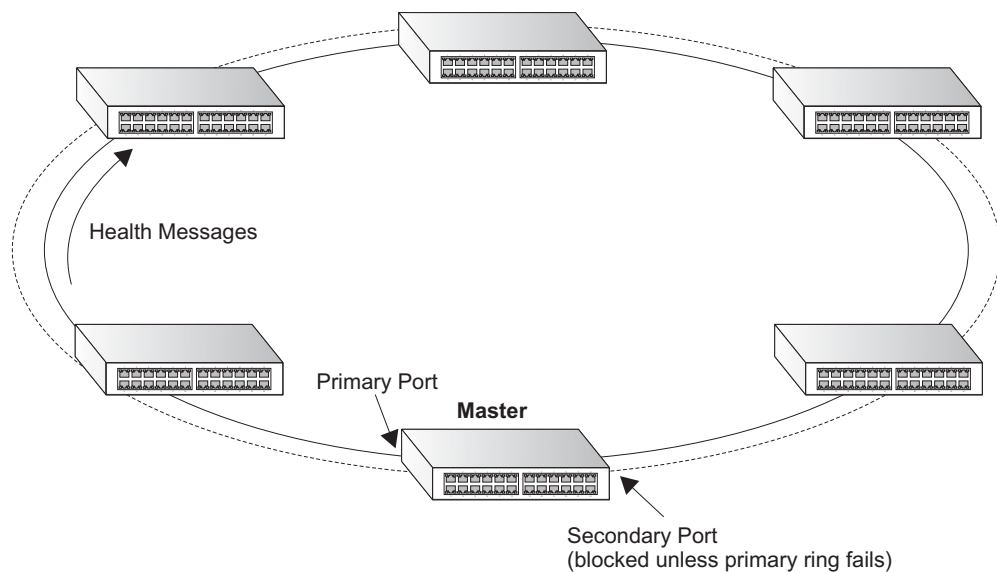


Figure 103 EAPS Ring Components

Configuration Guidelines

1. Create or delete an EAPS domain: Create or delete a domain (EAPS Domain Configuration, section 6.11.2 on page 265). The domain name is

used as the index for this domain in EAPS database. When deleting an EAPS Domain, first release the Control VLAN (CVLAN) and Protected VLANs (PVLANS) configured on this domain (as described in Step 6 and 7). If a port on the domain ring has not been added to another domain ring, this port will be reset to operate as a normal port. The database of this domain will then be cleared.

2. Define the EAPS mode of the ECN330-switch: After creating an EAPS domain, define the EAPS mode for this node (EAPS Domain Configuration - EAPS Mode, section 6.11.2 on page 265). Only one node can be defined as the master node on a domain ring, all the other ports should be defined as transit nodes.
3. Configure EAPS polling timers: Set the values of the polling timers the master node uses for the EAPS health-check packet that is circulated around the ring for an EAPS domain (EAPS Domain Configuration - Hello Timer and Fail Timer, section 6.11.2 on page 265). The hello-timer is the periodic time at which the master node sends a health-check packet, and the fail-time is the time the master node waits to receive back a health-check packet from the other direction in the ring.
4. Configure the primary and secondary ports: Each node on the ring connects to it through two ring ports. Configure one port as the primary port and the other as the secondary port (EAPS Domain Configuration - Primary Port and Secondary Port, section 6.11.2 on page 265).
5. Configure the EAPS Control VLAN (CVLAN): Specify the VLAN used to pass ring integrity commands (EAPS Domain Configuration - Control VLAN, section 6.11.2 on page 265). The CVLAN is automatically assigned a QoS profile of Qp8 (with the QoS High priority setting). The CVLAN must NOT be configured with an IP address. In addition, only ring ports may be added to the CVLAN. No other ports can be members of this VLAN. Also, the ring ports of the CVLAN must be tagged. Failure to observe these restrictions can result in a loop in the network.

Note that the CVLAN must be cleared prior to deleting an EAPS Domain. To release the CVLAN, clear the check box in the Control VLAN field.

6. Configuring EAPS Protected VLANs (PVLAN): Specify the protected VLANs that carry normal traffic and are protected by the EAPS ring integrity mechanism (EAPS Domain Protected VLAN Configuration, section 6.11.2 on page 265). One EAPS domain can be assigned 10 VLANs – 1 control VLAN and 9 protected VLANs. The ring ports of a protected VLAN must be tagged. The protected VLANs will be blocked on the secondary port.

Note that the protected VLANs must be cleared prior to deleting an EAPS Domain. To release the Protected VLANs, click the Modify Protected VLAN button (EAPS Domain Configuration, section 6.11.2 on page 265), and remove all of the entries in the VLAN list (EAPS Domain Protected VLAN Configuration, section 6.11.2 on page 265).

7. Enable or disable EAPS: Before enabling a domain as described in the next step, globally enable the EAPS function on the ECN330-switch (EAPS Configuration, section 6.11.1 on page 264). If EAPS has not yet been enabled or has been disabled, no EAPS domains will work.
8. Enable or disable an EAPS domain: Before an EAPS domain can work, it must be enabled (EAPS Domain Configuration - Domain Status, section 6.11.2 on page 265). When configuration is completed and the domain is enabled, it will start running on the ring. To stop a domain running on a ring, it can be disabled on any node.
9. Unconfigure an EAPS ring port: To unconfigure an EAPS primary or secondary ring port for an EAPS domain, clear the check box in the required field (EAPS Domain Configuration - Primary Port or Secondary Port, section 6.11.2 on page 265).
10. Display EAPS status information: Refer to the EAPS Domain List to view EAPS status information (EAPS Domain Configuration, section 6.11.2 on page 265). The output displayed depends on whether the node is a transit node or a master node.

Functional Description

- Setting port status on the master node: When the master node is in the Complete state, the primary and secondary ports will be set to the status described below. On the CVLAN, the secondary port will trap control messages to the CPU and not forward them to any port. On Protected VLANs, the secondary port will block all data flow except for EAPS domain control messages.
- Setting port status on the transit node: The port on the domain ring will periodically receive a control message. This message is copied to the CPU and forwarded to the next port on the domain ring. When the port on the domain ring link changes from up to down, this port will be temporarily blocked on the Protected VLANs. This port is opened on the Protected VLANs again only when the transit node in "pre-forwarding" state receives a control frame instructing it to flush its bridging table and unblock the previously blocked protected VLANs.

- Handling a hardware link down event: If this event occurs on the primary port of the master node, the master node will unblock the blocked port on the Protected VLAN and send a message to flush the forwarding database (FDB) to all transit nodes. If this event occurs on the secondary port, the master node will enter failed state. If this event occurs on a transit node, the transit node will send a link down control message to the master node, and the master node will unblock the blocked port and send a control message to make the transit nodes flush their FDB. The master node also enters the failed state.
- Handling a hardware link up event: If this event occurs on the master node, the secondary port will be blocked on the Protected VLAN, and the master node will send a message to flush the FDB to all transit nodes. If this event occurs on a transit node, the new linked port will be blocked until it receives RING-UP-FLUSH-FDB message.
- Handling health-check packet hello timer events: The master node sends a health-check packet to ensure the ring status, and starts the health-check packet fair timer at once.
- Handling health-check packet fail timer events: If this event occurs, the ring topology has changed, and the link down control message lost. The master node enters failed state and sends a control message to make all transit nodes flush their FDB.
- Handling EAPS control message events: Control messages are sent to nodes on the domain ring to maintain ring status. The master node sends health-check packets to ensure that the domain ring is unchanged. The master node sends RING-DOWN-FLUSH-FDB and RING-UP-FLUSH-FDB messages to inform the transit nodes to flush their FDB. Transit nodes send a link-down message to the master node to make master enter failed state immediately.

Note: The port MAC address, not the system MAC address, is used as the source address for all EAPS protocol packets.

Configuration Limitations for EAPS

The following configuration limitations apply to EAPS:

- One ECN330-switch only supports two EAPS domains – each domain must have one control VLAN and at most nine Protected VLANs.
- Either Gigabit Ethernet or Fast Ethernet ports can be configured as EAPS ring ports, but these ports should not be a member of any trunk.

- Each EAPS domain can have only one master node.
- The hello timer and fail timer must be configured on the master node. Afterwards, the master node will send timer configuration messages to the transit nodes to reset their hello-timer and fail-timer.
- One VLAN must be added to an EAPS domain as the CVLAN. This can be designated as any VLAN, other than the management VLANs (246-249, 4093). The CVLAN should only contain ring ports, and must NOT be configured with an IP address.

6.11.1 EAPS Configuration

Use the EAPS Configuration page to globally enable or disable EAPS on the ECN330-switch.

Command Usage

The EAPS function must be enabled on the ECN330-switch before an EAPS domain can start running on the ring (EAPS Domain Configuration, section 6.11.2 on page 265). Once enabled, the master node and transit node state machines will start, and the domain will enter the active state. When the domain is in the active state, no EAPS configuration changes can be made.

Command Attribute

- **EAPS Status** – Enables or disables EAPS on the ECN330-switch. (Default: Disabled)

Web – Click EAPS, Configuration. Mark the check box to enable EAPS globally on the ECN330-switch, and click Apply.



The screenshot shows a web interface titled "EAPS Configuration". Below the title, there is a label "EAPS Status :" followed by a checkbox that is checked, and the word "Enabled" next to it.

Figure 104 Setting EAPS Global Status

CLI – This example enables EAPS globally on the ECN330-switch.

```
Console(config)#eaps
Console(config)#
```

6.11.2 EAPS Domain Configuration

Use the EAPS Domain Configuration page to configure EAPS domains.

Command Usage

An EAPS domain containing one Control VLAN and one or more Protected VLANs must be configured, and the EAPS function enabled on the ECN330-switch (EAPS Configuration, section 6.11.1 on page 264) before a domain can start running on the ring. Once enabled, the master node and transit node state machines will start, and the domain will enter the active state.

To create an EAPS domain:

1. Enter a suitable name in the "Domain Name" field on the EAPS Domain Configuration page, and click the New button.
2. Configure the EAPS domain parameters for this node, including the control VLAN, the primary and secondary ports, the timers, EAPS node type, and domain status.
3. Click the Modify Protected VLAN button, and add the data VLANs that will be protected by the EAPS mechanism.

Command Attributes

New EAPS Domain

- **Domain Name** – Name of a specific EAPS domain. (Range: 1-32 characters)

EAPS Domain List

- **Domain Name** – Name of a configured EAPS domain.
- **Bridge-Links** – The number of Protected VLANs configured on the EAPS domain.

- **State** – Shows the following EAPS states:

Master Node

- **Idle** – The EAPS domain has been enabled, but the configuration is not complete.
- **Init** – The EAPS domain has started but has not yet determined the status of the ring.
- **Complete** – The ring is in the COMPLETE state for this EAPS domain.
- **Failed** – There is a break in the ring for this EAPS domain.

Transit Node

- **Idle** – The EAPS domain has been enabled, but the configuration is not complete.
- **Link-Up** – The EAPS domain is running, and both of its ports are up and in the FORWARDING state.
- **Link-Down** – This EAPS domain is running, but one or both of its ports are down.
- **Preforwarding** – This EAPS domain is running, but the new link port is temporarily blocked. When the state changes from link-down to link-up on a transit node, the new link port is temporarily blocked until the master node enters the Complete state. This transition time is known as the preforwarding time.
- **Mode** – Shows if the ECN330-switch is a master or transit node.
- **Status** – Shows if the specified domain is enabled.
- **Hello Timer (secs)** – The interval at which the master node sends health-check packets on the domain ring.
- **Fail Timer (secs)** – The time the master node waits for a health-check packet before declaring a break in the ring.
- **Preforwarding Timer (secs)** – The interval a transit node waits before transitioning from BLOCKED state to forwarding state.
- **Primary Port** – Shows the primary port on this node.
- **Primary Port Status** – Shows the port connection status or link status (Up, Down, Block).

- **Secondary Port** – Shows the secondary port on this node.
- **Secondary Port Status** – Shows the port connection status or link status (Up, Down, Block).
- **Control VLAN** – Shows the Control VLAN ID.
- **Protected VLANs** – Shows the name and VLAN ID of Protected VLANs.

EAPS Domain Configuration

- **Control VLAN** – The Control VLAN (CVLAN) is used only to send and receive EAPS ring maintenance messages.

Only one CVLAN can be configured in an EAPS domain. First create the VLAN to be used as the CVLAN (see “Creating VLANs” on page 284), and then add the CVLAN to the EAPS domain.

The CVLAN must not be configured with an IP address. In addition, only ring ports may be added to the CVLAN. No other ports can be members of this VLAN. Also, the ring ports of the CVLAN must be tagged. Failure to observe these restrictions can result in a loop in the network.

Once the domain has been activated by setting the Domain Status to Enabled, the configuration of the Control VLAN cannot be modified. The Domain Status must first be set to Disabled to stop the EAPS domain before making any configuration changes to this VLAN.

- **Primary Port** – This port is open on the Protected VLAN and is used for passing both control messages and data traffic. The master node sends control messages from this port. (Range: Port 1-27)

Each node must connect to the ring through two ports as part of the protection switching scheme – one port as the primary port and another as the secondary port.

The primary port must be removed from an EAPS domain before specifying a new primary port.

- **Secondary Port** – This port is blocked on the Protected VLAN and is used only to receive control messages on the master node. (Range: Port 1-27)

If the ring is complete, the master node prevents a loop by logically blocking all data traffic in the transmit and receive directions on its secondary port. If the master node subsequently detects a break in the ring, it unblocks its secondary port and allows data traffic to be transmitted and received through it.

The secondary port must be removed from an EAPS domain, before specifying a new secondary port.

- **Hello Timer (1-3 secs)** – The interval at which the master node sends hello-check packets. (Default: 1 second)

The hello time should be set on the master node. Once set, the master node will send a hello-check packet at the interval specified by this timer to all transit nodes. The transit nodes check for a health-check packet at the interval specified by the fail time.

- **Fail Timer (3-9 secs)** – The interval after which a node declares a link down if no hello-check packet is received. (Default: 3 seconds)

The fail time should be set on the master node. Once set, the master node will send the newly configured fail time to all transit nodes, forcing each node to update its fail timer. The transit nodes then check for a health-check packet at the interval specified by the fail time, and report a link down event to the master node if a health-check packet is not received during this interval.

On transit nodes, the default value for the fail time can be used until receiving a control message from the master node to update their timers.

- **EAPS Mode** – This parameter configures the ECN330-switch as a master node or transit node on the ring.
 - **Master** – The master node is the control node of the EAPS domain. This node actively monitors ring integrity and sends health check and state change messages to transit nodes. Only one master node can be set for a domain.
 - **Transit** – Transit nodes receive master control messages, detect ring topology changes, and send status messages to the master node. The transit node also receives control messages from the master node to synchronize the hello and fail timers. Note that all other configuration parameters for a transit node should be configured to be the same as that the EAPS domain's master node.

- **Domain Status** – This parameter is used to activate an EAPS domain.

EAPS Domain Protected VLAN Configuration

- **EAPS Domain Name** – Name of a configured EAPS domain.
- **VLAN List** – Protected VLANs are used to send and receive data traffic on the EAPS ring. (Range: 1-4094)

Up to nine Protected VLANs can be configured in an EAPS domain. First create the VLANs to be used as Protected VLANs (see “Creating VLANs” on page 284), and then add the Protected VLAN to the EAPS domain.

Once the domain has been activated (EAPS Domain Configuration - Domain Status, section 6.11.2 on page 265), the configuration of the Protected VLAN cannot be modified. The Domain Status must first be set to Disabled to stop the EAPS domain before making any configuration changes to this domain.

Web – Click EAPS, Domain Configuration. Enter a domain name, and click New to open the EAPS Domain Configuration page. Configure the EAPS parameters for this node, including the control VLAN, the primary and secondary ports, the timers, EAPS node type, and domain status, and click Apply. Then click the "Modify Protected VLAN" button to open the EAPS Domain Protected VLAN Configuration page, select the protected VLANs, and click Apply.

EAPS Domain Configuration

New VLAN Access-Map

Domain Name

EAPS Domain Configuration

Name: rd

Control Vlan	☒	3
Primary Port(1-27)	☒	26
Secondary Port(1-27)	☒	27
Hello Timer(1-3 Secs)		2
Fail Timer(3-9 Secs)		3
EAPS Mode		Master
Domain Status		Disabled

Note : Fail Timer should be longer than Hello Timer

EAPS Domain Protected Vlan Configuration

EAPS Domain Name: rd

Vlans List

<<Add

VLAN ID (1-4094)

Figure 105 Configuring EAPS Domains

Click EAPS, Domain Configuration to display the EAPS domain settings.

EAPS Domain Configuration

New VLAN Access-Map

Domain Name:

EAPS Domain List
Domain Name: rd

Bridge-Links	State	Mode	Status	Hello Timer (Secs)	Fail Timer (Secs)	Preforwarding Timer(Secs)	Primary Port	Pri-Port Status	Secondary Port	Sec.Port Status	Control Vlan	Protected Vlan	Remove	Edit
1	COMPLETE	MASTER	ENABLED	2	3	6	port 26	Up	port 27	Block	vlan 3	vlan: 2	Remove	Edit

Figure 106 Displaying EAPS Domain Settings

CLI – This example enables EAPS globally on the ECN330-switch.

```
Console(config)#eaps domain rd
Console(config-eaps)#control-vlan 3
Console(config-eaps)#port primary 26
Console(config-eaps)#port secondary 27
Console(config-eaps)#hellotime 2
Console(config-eaps)#failtime 3
Console(config-eaps)#mode master
Console(config-eaps)#protect-vlan 2
Console(config-eaps)#protect-vlan 246
Console(config-eaps)#protect-vlan 247
Console(config-eaps)#protect-vlan 248
Console(config-eaps)#enable
Console(config-eaps)#
```

6.12 VLAN Configuration

6.12.1 IEEE 802.1Q VLANs

In large networks, routers are used to isolate broadcast traffic for each subnet into separate domains. The ECN330-switch provides a similar service at Layer 2 by using VLANs to organize any group of network nodes into separate broadcast domains. VLANs confine broadcast traffic to the originating group, and can eliminate broadcast storms in large networks. This also provides a more secure and cleaner network environment.

An IEEE 802.1Q VLAN is a group of ports that can be located anywhere in the network, but communicate as though they belong to the same physical segment.

VLANs help to simplify network management by allowing devices to move to a new VLAN without having to change any physical connections. VLANs can be easily organized to reflect departmental groups (such as Marketing or R&D), usage groups (such as e-mail), or multicast groups (used for multimedia applications such as videoconferencing).

VLANs provide greater network efficiency by reducing broadcast traffic, and allow network changes to be made without having to update IP addresses or IP subnets. VLANs inherently provide a high level of network security since traffic must pass through a configured Layer 3 link to reach a different VLAN.

The ECN330-switch supports the following VLAN features:

- Up to 4094 VLANs based on the IEEE 802.1Q standard
- Distributed VLAN learning across multiple switches using explicit or implicit tagging and GVRP protocol
- Port overlapping, allowing a port to participate in multiple VLANs
- End stations can belong to multiple VLANs
- Passing traffic between devices that support VLANs and devices that do not support VLANs
- Priority tagging

6.12.1.1 Assigning Ports to VLANs

Before enabling VLANs for the ECN330-switch, first assign each port to the VLAN group(s) in which it will participate. The default VLAN assignment for all ports under ECN330 mode and ECN330-switch mode are shown in Table 17.

Table 17 Default VLAN Assignments

Port	ECN330 Mode						ECN330-switch Mode	
	VLAN						VLAN	
	1	246	247	248	249	4093	1	246
1-24			T	U	T		U	T
25	U	T					U	T
26	U	T					U	T
27	U	T		T		T	U	T
28		T	T	T	T	T	U	T

T: Tagged; U: Untagged

Add a port as a tagged port if it has to carry traffic for one or more VLANs, and any intermediate network devices or the host at the other end of the connection supports VLANs. Then assign ports on the other VLAN-compliant devices along the path that will carry this traffic to the same VLAN(s), either manually or dynamically using GVRP. However, if a port on the ECN330-switch has to participate in one or more VLANs, but none of the intermediate network devices nor the host at the other end of the connection supports VLANs, then add this port to the VLAN as an untagged port.

Note: VLAN-tagged frames can pass through any network interconnection devices regardless of whether or not they support VLANs, but the VLAN tags should be stripped off before passing it on to any end-node host that does not support VLAN tagging.

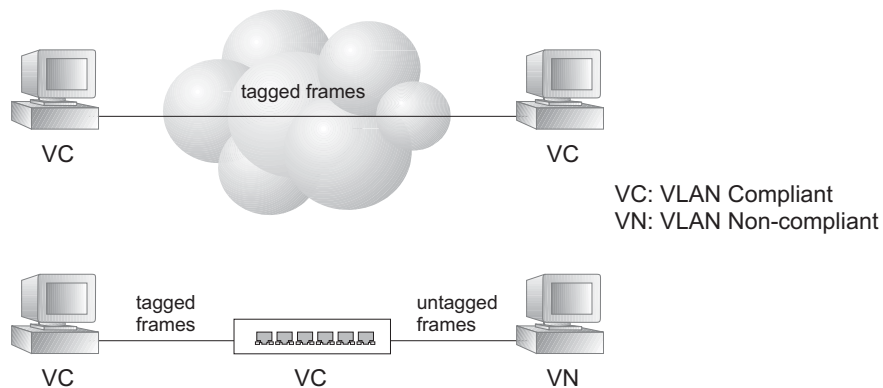


Figure 107 VLAN Compliant and VLAN Non-compliant Devices

VLAN Classification – When the ECN330-switch receives a frame, it classifies the frame in one of two ways. If the frame is untagged, the ECN330-switch assigns the frame to an associated VLAN (based on the default VLAN ID of the receiving port). But if the frame is tagged, the ECN330-switch uses the tagged VLAN ID to identify the port broadcast domain of the frame.

Port Overlapping – Port overlapping can be used to allow access to commonly shared network resources among different VLAN groups, such as file servers or printers. Note that if VLANs are implemented that do not overlap, but still need to communicate, they can be connected by enabling routing on the ECN330-switch.

Untagged VLANs – Untagged (or static) VLANs are typically used to reduce broadcast traffic and to increase security. A group of network users assigned to a VLAN form a broadcast domain that is separate from other VLANs configured on the ECN330-switch. Packets are forwarded only between ports that are designated for the same VLAN. Untagged VLANs can be used to manually isolate user groups or subnets. However, use IEEE 802.3 tagged VLANs with GVRP whenever possible to fully automate VLAN registration.

Automatic VLAN Registration – GVRP (GARP VLAN Registration Protocol) defines a system whereby the ECN330-switch can automatically learn the VLANs to which each end station should be assigned. If an end station (or its network adapter) supports the IEEE 802.1Q VLAN protocol, it can be configured to broadcast a message to the network indicating the VLAN groups it wants to join. When the ECN330-switch receives these messages, it will automatically place the receiving port in the specified VLANs, and then forward the message to all other ports. When the message arrives at another switch that supports

GVRP, it will also place the receiving port in the specified VLANs, and pass the message on to all other ports. VLAN requirements are propagated in this way throughout the network. This allows GVRP-compliant devices to be automatically configured for VLAN groups based solely on endstation requests.

Caution!

It is not recommended to use GVRP in the EDA network.

To implement GVRP in a network, first add the host devices to the required VLANs (using the operating system or other application software), so that these VLANs can be propagated onto the network. For both the edge switches attached directly to these hosts, and core switches in the network, enable GVRP on the links between these devices. Also, determine security boundaries in the network and disable GVRP on the boundary ports to prevent advertisements from being propagated, or forbid those ports from joining restricted VLANs.

Note: If host devices do not support GVRP, configure static or untagged VLANs for the ECN330-switch ports connected to these devices (as described in 6.12.1.8 "Adding Static Members to VLANs (VLAN Index)" 287). GVRP can still be enabled on these edge switches, as well as on the core switches in the network.

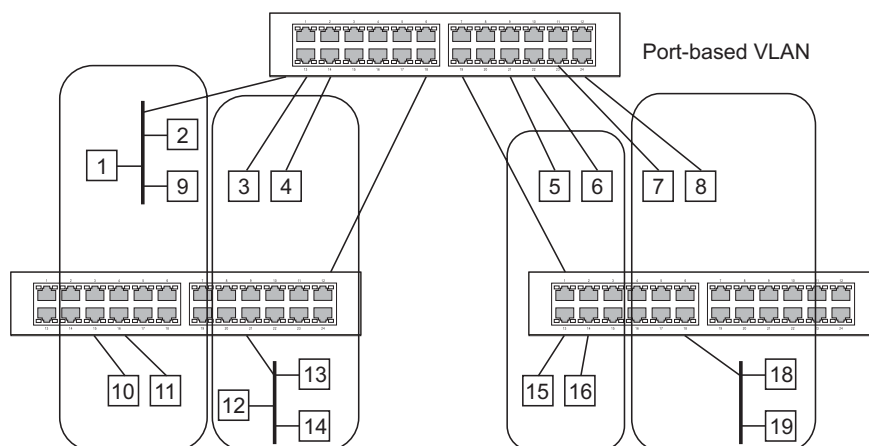


Figure 108 GVRP

6.12.1.2 Forwarding Tagged/Untagged Frames

To create a small port-based VLAN for devices attached directly to a single ECN330-switch, assign ports to the same untagged VLAN. Also ensure that VLAN tagging is not supported or is disabled on the attached devices. However, to participate in a VLAN group that crosses several switches, create a VLAN for that group and enable tagging on all ports.

Ports can be assigned to multiple tagged or untagged VLANs. Each port on the ECN330-switch is therefore capable of passing tagged or untagged frames. When forwarding a frame from the ECN330-switch along a path that contains any VLAN-compliant devices, the ECN330-switch should include VLAN tags. When forwarding a frame from the ECN330-switch along a path that does not contain any VLAN-compliant devices (including the destination host), the ECN330-switch must first strip off the VLAN tag before forwarding the frame. When the ECN330-switch receives a tagged frame, it will pass this frame onto the VLAN(s) indicated by the frame tag. However, when the ECN330-switch receives an untagged frame from a device that does not support VLANs, it first decides where to forward the frame, and then inserts a VLAN tag reflecting the ingress port's default VID.

6.12.1.3 Enabling or Disabling GVRP (Global Setting)

GARP VLAN Registration Protocol (GVRP) defines a way for switches to exchange VLAN information in order to register VLAN members on ports across the network. VLANs are dynamically configured based on join messages issued by host devices and propagated throughout the network. GVRP must be enabled to permit automatic VLAN registration, and to support VLANs which extend beyond the local switch. (Default: Disabled)

Web – Click VLAN, 802.1Q VLAN, GVRP Status. Enable or disable GVRP, click Apply



The screenshot shows a web interface titled "GVRP Status". Below the title is a horizontal line. Underneath the line, there is a checkbox labeled "GVRP" which is checked, followed by the text "Enable".

Figure 109 Enabling GVRP

CLI – This example enables GVRP for the ECN330-switch.

```
Console(config)#bridge-ext gvrp
Console(config)#
```

6.12.1.4 Displaying Basic VLAN Information

The VLAN Basic Information page displays basic information on the VLAN type supported by the ECN330-switch.

Field Attributes

- **VLAN Basic Information**
 - **VLAN Version Number** – The VLAN version used by the ECN330-switch as specified in the IEEE 802.1Q standard. (This parameter is displayed in the web interface only.)
 - **Maximum VLAN ID** – Maximum VLAN ID recognized by the ECN330-switch (4094).
 - **Maximum Number of Supported VLANs** – Maximum number of VLANs that can be configured on the ECN330-switch.
- **Management VLAN** – See “Configuring Management VLANs” on page 278.

Web – Click VLAN, 802.1Q VLAN, Basic Information.

VLAN Basic Information

VLAN Version Number	1
Maximum VLAN ID	4094
Maximum Number of Supported VLANs	4094

Management Vlan

Type	VLAN ID
Internal	247
Dynamic	248
External	246
Native	4093
FSA	249

Figure 110 VLAN Basic Information

CLI – Enter the following command to display the basic VLAN information.

```

Console#show bridge-ext
Max Support VLAN Numbers:          4094
Max Support VLAN ID:               4094
Extended Multicast Filtering Services: No
Static Entry Individual Port:       Yes
VLAN Learning:                     IVL
Configurable PVID Tagging:          Yes
Local VLAN Capable:                 No
Traffic Classes:                    Enabled
Global GVRP Status:                 Disabled
GMRP:                               Disabled
Console#

```

6.12.1.5 Configuring Management VLANs

Management VLANs can be defined for secure management access to the ECN330-switch. Only IP addresses assigned to these management VLANs can be used to manage the ECN330-switch.

The default management VLANs assigned to the switch are described under “Enabling the SBC to Access Advanced Management Tools” on page 74.

Command Usage

- The management VLAN applies to management access through the web, Telnet, SSH, and SNMP.
- There may be one or more management VLANs on the ECN330-switch, depending on whether the switch is set the ECN330 mode or ECN330-switch mode (see “Enabling the SBC to Access Advanced Management Tools” on page 74).
- When a management VLAN is defined, IP addresses assigned to other non-management VLAN interfaces cannot be used for management access. When no management VLAN is defined, the ECN330-switch can be managed through any IP address assigned to any VLAN interface.
- Management VLANs operate as an isolated VLAN. Data traffic is not routed to or from other VLANs, routing protocols cannot be enabled on these interfaces, nor is the management IP interface advertised by routing protocols to other routers.
- A management VLAN cannot be deleted when a IP address is assigned to the interface.
- To change a management VLAN, first set up a new VLAN without naming it (see “Creating VLANs” on page 284), add the required port members as tagged or untagged (see “Adding Static Members to VLANs (VLAN Index)” on page 287), remove the current management VLAN (see “Creating VLANs” on page 284), and then set the newly created VLAN as the new management VLAN on the Basic VLAN Information page.

Command Attributes

Management VLAN

Type – The ECN330-switch acts as a Network Address Translator (NAT) for management traffic, connecting and hiding the embedded nodes from the Access Domain Management. The following interfaces (each configured independently) are utilized:

- **Internal** – Internal Management VLAN is the gateway for the embedded nodes (such as ECN330-switch, IP DSLAM, ESN108). By default, it is configured through DHCP with an internal IP

address for the ECN330-switch. (Default VID: 247;
Default Members: 1-24, 28 tagged)

Downlink ports (1-24) are configured automatically with the Internal Management VLAN ID (default 247).

- **Dynamic** – Dynamic Management VLAN (DMV) ensures that embedded nodes will be automatically reconfigured if their configured management VLAN is not the same as the internal VLAN in the EAN (for example, if an IP DSLAM that was connected directly to the EDA network using VLAN ID 247, is connected as an embedded node using VLAN ID 248).

Any untagged traffic entering a downlink port is tagged with the Untagged VLAN ID (default 248). The embedded nodes can use untagged frames to get information about the used management VLAN. (Default VID: 248; Default Members: 1-24 untagged, 28 tagged)

For more information about the DMV, please refer the *Management VLAN Configuration Guide*. Note that the ECN330-switch does not have to be configured for the DMV. It automatically supports the DMV for all embedded nodes.

- **External** – External Management VLAN is used by PEM to manage the SBC. This interface represents the EAN to the outside network. By default, it must be manually configured with an IP address for the ECN330-switch, using the same management VLAN as that used by the EDA network. (Default VID: 246; Default Members: 25-28 tagged)

Uplink ports (25-27) are configured automatically with the External Management VLAN ID (default 246). Any untagged traffic entering an uplink port is tagged with VLAN ID 1, which in effect is the same as discarded, since the data will not be forwarded to any other port.

- **Native** – Native Management VLAN is used internally to terminate untagged traffic passed from or to the SBC (for example, when using a QinQ tunnel). (Default VID: 4093; Default Members: 28 untagged)
- **FSA** – FSA (Flexible Service Access) Management VLAN is used by end users to subscribe to the different services. Authentication is

done in the SBC. (Default VID: 249; Default Members: 1-24,28 tagged)

- **VLAN ID** – The VLAN ID of the management VLAN. If the field is blank or zero, no VLAN is defined for the corresponding management VLAN on the ECN330-switch. (Range: 0-4094; Default: Internal - 247, Dynamic - 248, External - 246, Native - 4093, FSA - 249)

Web – Click VLAN, 802.1Q VLAN, Basic Information. Create an new management VLAN as described under Command Usage in this section, enter the VLAN ID for the new management VLAN, and click Apply.

VLAN Basic Information

VLAN Version Number	1
Maximum VLAN ID	4094
Maximum Number of Supported VLANs	4094

Management Vlan

Type	VLAN ID
Internal	247
Dynamic	248
External	246
Native	4093
FSA	349

Figure 111 Configuring Management VLANs

CLI – This example shows how to change a management VLAN. First set up a new VLAN with the required port members (without naming the VLAN), remove the current FSA management VLAN, and then configure the newly configured VLAN as the new FSA management VLAN.

```
Console#configure
Console(config)#vlan database
Console(config-vlan)#vlan 349 media ethernet state active
Console(config)#exit
Console(config)#interface ethernet 1/1
Console(config-if)#switchport allowed vlan add 349 tagged
.
.
.
Console(config)#exit
Console(config)#interface ethernet 1/24
Console(config-if)#switchport allowed vlan add 349 tagged
Console(config)#exit
Console(config)#interface ethernet 1/28
Console(config-if)#switchport allowed vlan add 349 tagged
Console(config)#exit
Console(config)#no management vlan fsa
Console(config)#management vlan fsa 349
Console#show management vlan
Current Internal Management VLAN: 247
Current Dynamic Management VLAN: 248
Current External Management VLAN: 246
Current Native Management VLAN: 4093
Current FSA Management VLAN: 349
Console#
```

6.12.1.6 Displaying Current VLANs

The VLAN Current Table shows the current port members of each VLAN and whether or not the port supports VLAN tagging. Ports assigned to a large VLAN group that crosses several switches should use VLAN tagging. However, for a small port-based VLAN using one or two switches, tagging can be disabled.

Command Attributes (Web)

- **VLAN ID** – ID of configured VLAN (1-4094).
- **Up Time at Creation** – Time this VLAN was created (System Up Time).
- **Status** – Shows how this VLAN was added to the ECN330-switch.
 - **Dynamic GVRP**: Automatically learned through GVRP.
 - **Permanent**: Added as a static entry.
- **Egress Ports** – Shows all the VLAN port members.
- **Untagged Ports** – Shows the untagged VLAN port members.

Web – Click VLAN, 802.1Q VLAN, Current Table. Select any ID from the scroll-down list.

VLAN Current Table

VLAN ID:

Up Time at Creation: 0 d 0 h 0 min 7 s

Status: Permanent

Egress Ports	Untagged Ports
Unit1 Port1	Unit1 Port1
Unit1 Port2	Unit1 Port2
Unit1 Port3	Unit1 Port3
Unit1 Port4	Unit1 Port4
Unit1 Port6	Unit1 Port6
Unit1 Port7	Unit1 Port7
Unit1 Port8	Unit1 Port8
Unit1 Port9	Unit1 Port9

Figure 112 VLAN Current Table

Command Attributes (CLI)

- **VLAN** – ID of configured VLAN (1-4094, no leading zeroes).
- **Type** – Shows how this VLAN was added to the ECN330-switch.
 - **Dynamic:** Automatically learned through GVRP.
 - **Static:** Added as a static entry.
- **Name** – Name of the VLAN (1 to 32 characters).
- **Status** – Shows if this VLAN is enabled or disabled.
 - **Active:** VLAN is operational.
 - **Suspend:** VLAN is suspended; that is, does not pass packets.
- **Ports / Channel groups** – Shows the VLAN interface members.

CLI – Current VLAN information can be displayed with the following command.

```

Console#show vlan id 1
Console#sh vlan id 1
Default VLAN ID : 1

VLAN ID:          1
Type:             Static
Name:             DefaultVlan
Status:           Active
Ports/Port Channels:  Eth1/25(S) Eth1/26(S) Eth1/27(S)

Console#

```

6.12.1.7**Creating VLANs**

Use the VLAN Static List to create or remove VLAN groups. To propagate information about VLAN groups used on the ECN330-switch to external network devices, specify a VLAN ID for each of these groups.

Command Attributes

- **Current** – Lists all the current VLAN groups created for this system. Up to 4094 VLAN groups can be defined. VLAN 1 is the default untagged VLAN.

- **New** – Specifies the name and numeric identifier for a new VLAN group. (The VLAN name is only used for management on this system; it is not added to the VLAN tag.)
- **VLAN ID** – ID of configured VLAN (1-4094, no leading zeroes).
- **VLAN Name** – Name of the VLAN (1 to 32 characters).
- **Status (Web)** – Enables or disables the specified VLAN.
 - **Enable:** VLAN is operational.
 - **Disable:** VLAN is suspended; that is, does not pass packets.
- **State (CLI)** – Enables or disables the specified VLAN.
 - **Active:** VLAN is operational.
 - **Suspend:** VLAN is suspended; that is, does not pass packets.
- **Add** – Adds a new VLAN group to the current list.
- **Remove** – Removes a VLAN group from the current list. If any port is assigned to this group as untagged, it will be reassigned to VLAN group 1 as untagged.

Web – Click VLAN, 802.1Q VLAN, Static List. To create a new VLAN, enter the VLAN ID and VLAN name, mark the Enable checkbox to activate the VLAN, and then click Add.

VLAN Static List							
Current: 1, DefaultVlan, Enabled 246, extmgm, Enabled 247, intmgm, Enabled 248, dynvlan, Enabled 4093, intuntag, Enabled	New: <table border="1"> <tr> <td>VLAN ID (1-4094)</td> <td>2</td> </tr> <tr> <td>VLAN Name</td> <td>R&D</td> </tr> <tr> <td>Status</td> <td>☒ Enabled</td> </tr> </table>	VLAN ID (1-4094)	2	VLAN Name	R&D	Status	☒ Enabled
VLAN ID (1-4094)	2						
VLAN Name	R&D						
Status	☒ Enabled						
<<Add Remove							

Figure 113 VLAN Static List - Creating VLANs

CLI – This example creates a new VLAN.

```

Console(config)#vlan database
Console(config-vlan)#vlan 2 name R&D media ethernet state active
Console(config-vlan)#end
Console#show vlan
Default VLAN ID : 1

VLAN ID:          1
Type:             Static
Name:             DefaultVlan
Status:           Active
Ports/Port Channels:  Eth1/25(S) Eth1/26(S) Eth1/27(S)

VLAN ID:          2
Type:             Static
Name:             R&D
Status:           Active
Ports/Port Channels:

VLAN ID:          246
Type:             Static
Name:             extmgm
Status:           Active
Ports/Port Channels:  Eth1/25(S) Eth1/26(S) Eth1/27(S) Eth1/28(S)

VLAN ID:          247
Type:             Static
Name:             intmgm
Status:           Active
Ports/Port Channels:  Eth1/ 1(S) Eth1/ 2(S) Eth1/ 3(S) Eth1/ 4(S) Eth1/ 5(S)
                      Eth1/ 6(S) Eth1/ 7(S) Eth1/ 8(S) Eth1/ 9(S) Eth1/10(S)
                      Eth1/11(S) Eth1/12(S) Eth1/13(S) Eth1/14(S) Eth1/15(S)
                      Eth1/16(S) Eth1/17(S) Eth1/18(S) Eth1/19(S) Eth1/20(S)
                      Eth1/21(S) Eth1/22(S) Eth1/23(S) Eth1/24(S) Eth1/28(S)

VLAN ID:          248
Type:             Static
Name:             dynvlan
Status:           Active
Ports/Port Channels:  Eth1/ 1(S) Eth1/ 2(S) Eth1/ 3(S) Eth1/ 4(S) Eth1/ 5(S)
                      Eth1/ 6(S) Eth1/ 7(S) Eth1/ 8(S) Eth1/ 9(S) Eth1/10(S)
                      Eth1/11(S) Eth1/12(S) Eth1/13(S) Eth1/14(S) Eth1/15(S)
                      Eth1/16(S) Eth1/17(S) Eth1/18(S) Eth1/19(S) Eth1/20(S)
                      Eth1/21(S) Eth1/22(S) Eth1/23(S) Eth1/24(S) Eth1/28(S)

```



```

VLAN ID:          249
Type:             Static
Name:            fsavlan
Status:          Active
Ports/Port Channels:  Eth1/ 1(S) Eth1/ 2(S) Eth1/ 3(S) Eth1/ 4(S) Eth1/ 5(S)
                    Eth1/ 6(S) Eth1/ 7(S) Eth1/ 8(S) Eth1/ 9(S) Eth1/10(S)
                    Eth1/11(S) Eth1/12(S) Eth1/13(S) Eth1/14(S) Eth1/15(S)
                    Eth1/16(S) Eth1/17(S) Eth1/18(S) Eth1/19(S) Eth1/20(S)
                    Eth1/21(S) Eth1/22(S) Eth1/23(S) Eth1/24(S) Eth1/28(S)

VLAN ID:          4093
Type:             Static
Name:            intuntag
Status:          Active
Ports/Port Channels:  Eth1/28(S)

Console#

```

6.12.1.8 Adding Static Members to VLANs (VLAN Index)

Use the VLAN Static Table to configure port members for the selected VLAN index. Assign ports as tagged if they are connected to 802.1Q VLAN compliant devices, or untagged they are not connected to any VLAN-compliant devices. Or configure a port as forbidden to prevent the ECN330-switch from automatically adding it to a VLAN through the GVRP protocol.

Note: The VLAN Static Membership by Port page can also be used to configure VLAN groups based on the port index (page 289). However, note that this configuration page can only add ports to a VLAN as tagged members.

Note: VLAN 1 is the default untagged VLAN containing all ports on the ECN330-switch, and can only be modified by first reassigning the default port VLAN ID as described under 6.12.1.10 "Configuring VLAN Behavior for Interfaces" 290.

Command Attributes

- **VLAN** – ID of configured VLAN (1-4094, no leading zeroes).
- **Name** – Name of the VLAN (1 to 32 characters).
- **Status** – Enables or disables the specified VLAN.
 - **Enable:** VLAN is operational.
 - **Disable:** VLAN is suspended; that is, does not pass packets.

- **Port** – Port identifier.
- **Trunk** – Trunk identifier.
- Membership Type – Select VLAN membership for each interface by marking the appropriate radio button for a port or trunk:
 - **Tagged**: Interface is a member of the VLAN. All packets transmitted by the port will be tagged, that is, carry a tag and therefore carry VLAN or CoS information.
 - **Untagged**: Interface is a member of the VLAN. All packets transmitted by the port will be untagged, that is, not carry a tag and therefore not carry VLAN or CoS information. Note that an interface must be assigned to at least one group as an untagged port.
 - **Forbidden**: Interface is forbidden from automatically joining the VLAN through GVRP. For more information, see “Automatic VLAN Registration” on page 274.
 - **None**: Interface is not a member of the VLAN. Packets associated with this VLAN will not be transmitted by the interface.
- **Trunk Member** – Indicates if a port is a member of a trunk. To add a trunk to the selected VLAN, use the last table on the VLAN Static Table page.

Web – Click VLAN, 802.1Q VLAN, Static Table. Select a VLAN ID from the scroll-down list. Modify the VLAN name and status if required. Select the membership type by marking the appropriate radio button in the list of ports or trunks. Click Apply.

Port	Tagged	Untagged	Forbidden	None	Trunk Member
1	☒	☐	☐	☐	
2	☐	☒	☐	☐	
3	☐	☐	☐	☒	
4	☐	☐	☐	☒	
5	☐	☐	☐	☒	

Figure 114 VLAN Static Table - Adding Static Members

CLI – The following example adds tagged and untagged ports to VLAN 2.

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport allowed vlan add 2 tagged
Console(config-if)#exit
Console(config)#interface ethernet 1/2
Console(config-if)#switchport allowed vlan add 2 untagged
Console(config-if)#exit
Console(config)#interface ethernet 1/13
Console(config-if)#switchport allowed vlan add 2 tagged
```

6.12.1.9 Adding Static Members to VLANs (Port Index)

Use the VLAN Static Membership by Port menu to assign VLAN groups to the selected interface as a tagged member.

Command Attributes

- **Interface** – Port or trunk identifier.
- **Member** – VLANs for which the selected interface is a tagged member.

- **Non-Member** – VLANs for which the selected interface is not a tagged member.

Web – Open VLAN, 802.1Q VLAN, Static Membership by Port. Select an interface from the scroll-down box (Port or Trunk). Click Query to display membership information for the interface. Select a VLAN ID, and then click Add to add the interface as a tagged member, or click Remove to remove the interface. After configuring VLAN membership for each interface, click Apply.

Figure 115 VLAN Static Membership

CLI – This example adds Port 3 to VLAN 1 as a tagged port, and removes Port 3 from VLAN 2.

```
Console(config)#interface ethernet 1/3
Console(config-if)#switchport allowed vlan add 1 tagged
Console(config-if)#switchport allowed vlan remove 2
```

6.12.1.10

Configuring VLAN Behavior for Interfaces

VLAN behavior can be configured for specific interfaces, including the default VLAN identifier (PVID), accepted frame types, ingress filtering, GVRP status, and GARP timers.

Command Usage

- **GVRP** – GARP VLAN Registration Protocol defines a way for switches to exchange VLAN information in order to automatically register VLAN members on interfaces across the network.

- **GARP** – Group Address Registration Protocol is used by GVRP to register or deregister client attributes for client services within a bridged LAN. The default values for the GARP timers are independent of the media access method or data rate. These values should not be changed unless difficulties are experienced with GVRP registration/deregistration.

Command Attributes

- **PVID** – VLAN ID assigned to untagged frames received on the interface. (Default: 1)
 - If an interface is not a member of VLAN 1 and its PVID is assigned to this VLAN, the interface will automatically be added to VLAN 1 as an untagged member. For all other VLANs, an interface must first be configured as an untagged member before its PVID can be assigned to that group.
- **Acceptable Frame Type** – Sets the interface to accept all frame types, including tagged or untagged frames, or only tagged frames. When set to receive all frame types, any received frames that are untagged are assigned to the default VLAN. (Option: All, Tagged; Default: All)
- **Ingress Filtering** – Determines how to process frames tagged for VLANs for which the ingress port is not a member. (Default: Enabled)
 - Ingress filtering only affects tagged frames.
 - If ingress filtering is disabled and a port receives frames tagged for VLANs for which it is not a member, these frames will be flooded to all other ports (except for those VLANs explicitly forbidden on this port).
 - If ingress filtering is enabled and a port receives frames tagged for VLANs for which it is not a member, these frames will be discarded.
 - Ingress filtering does not affect VLAN independent BPDU frames, such as GVRP or STP. However, they do affect VLAN dependent BPDU frames, such as GMRP.
- **GVRP Status** – Enables/disables GVRP for the interface. GVRP must be globally enabled for the ECN330-switch before this setting can take effect. (See “Displaying Bridge Extension Capabilities” on page 77.) When disabled, any GVRP packets received on this port will be discarded and no GVRP registrations will be propagated from other ports. (Default: Disabled)

- **GARP Join Timer** – The interval between transmitting requests/queries to participate in a VLAN group. (Range: 20-1000 centiseconds; Default: 20)
- **GARP Leave Timer** – The interval a port waits before leaving a VLAN group. This time should be set to more than twice the join time. This ensures that after a Leave or LeaveAll message has been issued, the applicants can rejoin before the port actually leaves the group. (Range: 60-3000 centiseconds; Default: 60)
- **GARP LeaveAll Timer** – The interval between sending out a LeaveAll query message for VLAN group participants and the port leaving the group. This interval should be considerably larger than the Leave Time to minimize the amount of traffic generated by nodes rejoining the group. (Range: 500-18000 centiseconds; Default: 1000)

Note: GARP timer settings must follow this rule: $2 \times (\text{join timer}) < \text{leave timer} < \text{leaveAll timer}$

- **Mode** – Indicates VLAN membership mode for an interface. (Default: Hybrid)
 - **1Q Trunk** – Specifies a port as an end-point for a VLAN trunk. A trunk is a direct link between two switches, so the port transmits tagged frames that identify the source VLAN. Note that frames belonging to the port's default VLAN (that is, associated with the PVID) are also transmitted as tagged frames.
 - **Hybrid** – Specifies a hybrid VLAN interface. The port may transmit tagged or untagged frames.
 - **Dot1q-Tunnel** – Configures IEEE 802.1Q tunneling (QinQ) to segregate and preserve customer VLAN IDs for traffic crossing the service provider network. See "Configuring IEEE 802.1Q Tunneling" on page 296 for a detailed description of this feature.
- **TPID (0-65535)** – Tag Protocol Identifier specifies the ether-type of incoming packets on a tunnel port. See "Configuring IEEE 802.1Q Tunneling" on page 296 for a detailed description of this parameter.
- **Address Monitor Mode** – This feature must be enabled on a QinQ tunnel port to properly forward traffic for the internal management VLANs (VIDs 247-249) between the QinQ tunnel port and the SBC connected to port 28. For a more detailed description, see "Configuring IEEE 802.1Q Tunneling" on page 296.

- **Trunk Member** – Indicates if a port is a member of a trunk. To add a trunk to the selected VLAN, use the last table on the VLAN Static Table page.

Web – Click VLAN, 802.1Q VLAN, Port Configuration or VLAN Trunk Configuration. Fill in the required settings for each interface, click Apply.

VLAN Port Configuration											
Port	PVID	Acceptable Frame Type	Ingress Filtering	GVRP Status	GARP Join Timer (Centi Seconds) (20-1000)	GARP Leave Timer (Centi Seconds) (60-3000)	GARP LeaveAll Timer (Centi Seconds) (500-18000)	Mode	TPID(0-65535)	AddressMonitorMode	Trunk Member
1	1	ALL	☒ Enabled	☐ Enabled	20	60	1000	Hybrid		☐ Enabled	
2	248	ALL	☒ Enabled	☐ Enabled	20	60	1000	Hybrid		☐ Enabled	
3	3	Tagged	☒ Enabled	☒ Enabled	20	90	2000	Hybrid		☐ Enabled	
4	248	ALL	☒ Enabled	☐ Enabled	20	60	1000	Hybrid		☐ Enabled	
5	248	ALL	☒ Enabled	☐ Enabled	20	60	1000	Hybrid		☐ Enabled	
6	248	ALL	☒ Enabled	☐ Enabled	20	60	1000	Hybrid		☐ Enabled	
7	248	ALL	☒ Enabled	☐ Enabled	20	60	1000	Hybrid		☐ Enabled	
8	248	ALL	☒ Enabled	☐ Enabled	20	60	1000	Hybrid		☐ Enabled	
9	248	ALL	☒ Enabled	☐ Enabled	20	60	1000	Hybrid		☐ Enabled	

Figure 116 VLAN Port Configuration

CLI – This example sets port 3 to accept only tagged frames, assigns PVID 3 as the native VLAN ID, enables GVRP, sets the GARP timers, and then sets the switchport mode to hybrid.

```

Console(config)#interface ethernet 1/3
Console(config-if)#switchport acceptable-frame-types tagged
Console(config-if)#switchport ingress-filtering
Console(config-if)#switchport native vlan 3
Console(config-if)#switchport gvrp
Console(config-if)#garp timer join 20
Console(config-if)#garp timer leave 90
Console(config-if)#garp timer leaveall 2000
Console(config-if)#switchport mode hybrid
Console(config-if)#

```

6.12.1.11 Configuring the MAC Address for a VLAN

Use the VLAN MAC Address page to configure the MAC address of any VLAN on the ECN330-switch.

Command Usage

- It may be necessary to configure a unique MAC address for a VLAN to ensure proper operation of service provider applications, or to simplify troubleshooting.
- After configuring a MAC address for a VLAN, all Layer 3 traffic originating from this VLAN will use the specified MAC address.
- MAC addresses used for VLANs have the following restrictions:
 - Cannot be a broadcast MAC address.
 - Cannot be a multicast MAC address.
 - Cannot be a MAC address or all zeroes.

Command Attributes

- **VLAN** – ID of configured VLAN. (Range: 1-4094)
- **MAC Address** – MAC address of the selected VLAN.
(Format examples: 00-01-02-03-0d-0e or 000102030d0e)
- **Set Default MAC Address** – Sets the MAC address to the same as that used by the ECN330-switch.
- **Set MAC Address** – Sets the MAC address to the specified value.

Web – Click VLAN, 802.1Q VLAN, VLAN MAC Address. Select a VLAN, enter the required MAC address, and click Set MAC Address.

Figure 117 VLAN MAC Address Configuration

CLI – This example sets the MAC address for VLAN 3.

```

Console(config)#interface vlan 3
Console(config-if)#mac-address 00-01-02-03-0d-0e
Console(config-if)#exit
Console#show vlan mac-address
  VLAN MAC Address          Status    Type      Name
  ----  -
  1      00-01-02-03-0d-0e    Active    Static    DefaultVlan
  246    00-00-12-33-89-76    Active    Static    extmgm
  247    00-00-12-33-89-76    Active    Static    intmgm
  248    00-00-12-33-89-76    Active    Static    dynvlan
  249    00-00-12-33-89-76    Active    Static    fsavlan
  4093   00-00-12-33-89-76    Active    Static    intuntag
Console#

```

6.12.1.12 Configuring IEEE 802.1Q Tunneling

IEEE 802.1Q Tunneling (QinQ) is designed for service providers carrying traffic for multiple customers across their networks. QinQ tunneling is used to maintain customer-specific VLAN and Layer 2 protocol configurations even when different customers use the same internal VLAN IDs. This is accomplished by inserting Service Provider VLAN (SPVLAN) tags into the customer's frames when they enter the service provider's network, and then stripping the tags when the frames leave the network.

A service provider's customers may have specific requirements for their internal VLAN IDs and number of VLANs supported. VLAN ranges required by different customers in the same service-provider network might easily overlap, and traffic passing through the infrastructure might be mixed. Assigning a unique range of VLAN IDs to each customer would restrict customer configurations, require intensive processing of VLAN mapping tables, and could easily exceed the maximum VLAN limit of 4096.

QinQ tunneling uses a single Service Provider VLAN (SPVLAN) for customers who have multiple VLANs. Customer VLAN IDs are preserved and traffic from different customers is segregated within the service provider's network even when they use the same customer-specific VLAN IDs. QinQ tunneling expands VLAN space by using a VLAN-in-VLAN hierarchy, preserving the customer's original tagged packets, and adding SPVLAN tags to each frame (also called double tagging).

A port configured to support QinQ tunneling must be set to tunnel port mode. The Service Provider VLAN (SPVLAN) ID for the specific customer must be assigned to the QinQ tunnel port on the edge switch where the customer traffic enters the service provider's network. Each customer requires a separate SPVLAN, but this VLAN supports all of the customer's internal VLANs. The QinQ uplink port that passes traffic from the edge switch into the service provider's metro network must also be added to this SPVLAN. The uplink port can be added to multiple SPVLANs to carry inbound traffic for different customers onto the service provider's network.

When a double-tagged packet enters another trunk port in an intermediate or core switch in the service provider's network, the outer tag is stripped for packet processing. When the packet exits another trunk port on the same core switch, the same SPVLAN tag is again added to the packet.

When a packet enters the trunk port on the service provider's egress switch, the outer tag is again stripped for packet processing. However, the SPVLAN tag is not added when it is sent out the tunnel port on the edge switch into the customer's network. The packet is sent as a normal IEEE 802.1Q-tagged frame, preserving the original VLAN numbers used in the customer's network.

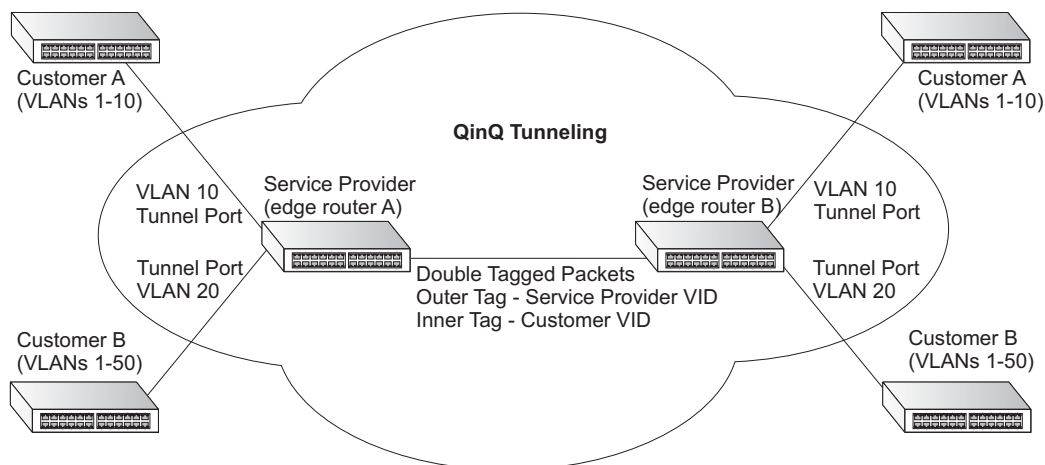


Figure 118 QinQ Operational Concept

Layer 2 Flow for Packets Coming into a Tunnel Port

A QinQ tunnel port may receive either tagged or untagged packets. No matter how many tags the incoming packet has, it is treated as tagged packet.

The ingress process does source and destination lookups. If both lookups are successful, the ingress process writes the packet to memory. Then the egress process transmits the packet. Packets entering a QinQ tunnel port are processed in the following manner:

1. New SPVLAN tags are added to all incoming packets, no matter how many tags they already have. The ingress process constructs and inserts the outer tag (SPVLAN) into the packet based on the default VLAN ID and Tag Protocol Identifier (TPID, that is, the ether-type of the tag). This outer tag is used for learning and switching packets. The priority of the inner tag is copied to the outer tag if it is a tagged or priority tagged packet.
2. After successful source and destination lookup, the ingress process sends the packet to the switching process with two tags. If the incoming packet is untagged, the outer tag is an SPVLAN tag, and the inner tag is a dummy tag

(8100 0000). If the incoming packet is tagged, the outer tag is an SPVLAN tag, and the inner tag is a CVLAN tag.

3. After packet classification through the switching process, the packet is written to memory with one tag (an outer tag) or with two tags (both an outer tag and inner tag).
4. The ECN330-switch sends the packet to the proper egress port.
5. If the egress port is an untagged member of the SPVLAN, the outer tag will be stripped. If it is a tagged member, the outgoing packets will have two tags.

Layer 2 Flow for Packets Coming into an Uplink Port

An uplink port receives one of the following packets:

- Untagged
- One tag (CVLAN or SPVLAN)
- Double tag (CVLAN + SPVLAN)

The ingress process does source and destination lookups. If both lookups are successful, the ingress process writes the packet to memory. Then the egress process transmits the packet. Packets entering a QinQ uplink port are processed in the following manner:

1. If incoming packets are untagged, the PVID VLAN native tag is added.
2. If the ether-type of an incoming packet (single or double tagged) is not equal to the TPID of the uplink port, the VLAN tag is determined to be a Customer VLAN (CVLAN) tag. The uplink port's PVID VLAN native tag is added to the packet. This outer tag is used for learning and switching packets within the service provider's network. The TPID must be configured on a per port basis, and the verification cannot be disabled.
3. If the ether-type of an incoming packet (single or double tagged) is equal to the TPID of the uplink port, no new VLAN tag is added. If the uplink port is not the member of the outer VLAN of the incoming packets, the packet will be dropped when ingress filtering is enabled. If ingress filtering is not enabled, the packet will still be forwarded. If the VLAN is not listed in the VLAN table, the packet will be dropped.
4. After successful source and destination lookup, the packet is double tagged. The ECN330-switch uses the TPID of 0x8100 to indicate that an incoming packet is double-tagged. If the outer tag of an incoming double-tagged

packet is equal to the port TPID and the inner tag is 0x8100, it is treated as a double-tagged packet. If a single-tagged packet has 0x8100 as its TPID, and port TPID is not 0x8100, a new VLAN tag is added and it is also treated as double-tagged packet.

5. If the destination address lookup fails, the packet is sent to all member ports of the outer tag's VLAN.
6. After packet classification, the packet is written to memory for processing as a single-tagged or double-tagged packet.
7. The ECN330-switch sends the packet to the proper egress port.
8. If the egress port is an untagged member of the SPVLAN, the outer tag will be stripped. If it is a tagged member, the outgoing packet will have two tags.

Configuration Limitations for QinQ

- The native VLAN of uplink ports should not be used as the SPVLAN. If the SPVLAN is the uplink port's native VLAN, the uplink port must be an untagged member of the SPVLAN. Then the outer SPVLAN tag will be stripped when the packets are sent out. Another reason is that it causes none-customer packets will be forwarded to SPVLAN.
- Static trunk port groups are compatible with QinQ tunnel ports as long as the QinQ configuration is consistent within a trunk port group.
- QinQ and L2MPLS mode cannot be supported at the same time.
- The native VLAN (VLAN 1) is not normally added to transmitted frames. Avoiding using VLAN 1 as an SPVLAN tag for customer traffic to reduce the risk of misconfiguration. Instead, use VLAN 1 as a management VLAN instead of a data VLAN in the service provider network.
- There are some inherent incompatibilities between Layer 2 and Layer 3 switching:
 - A tunnel port cannot be a routed port.
 - Tunnel ports do not support IP Access Control Lists.
 - Layer 3 Quality of Service (QoS) and other QoS features containing Layer 3 information are not supported on tunnel ports.
 - Spanning tree bridge protocol data unit (BPDU) filtering is automatically disabled on a tunnel port.

General Configuration Guidelines for QinQ

1. Configure the ECN330-switch to QinQ mode (see “Configuring the ECN330-switch for Normal Operation or Tunneling Mode” on page 71).
2. Create a Service Provider VLAN, also referred to as an SPVLAN (see “Creating VLANs” on page 284).
3. Configure the QinQ tunnel port to dot1Q tunnel port mode (see “Adding an Interface to a QinQ Tunnel” on page 300).
4. Set the Tag Protocol Identifier (TPID) value of the tunnel port. This step is required if the attached client is using a nonstandard 2-byte ethertype to identify 802.1Q tagged frames. The standard ethertype value is 0x8100. (See “Adding an Interface to a QinQ Tunnel” on page 300.)
5. Configure the QinQ tunnel port to join the SPVLAN as an untagged member (see “Adding Static Members to VLANs (VLAN Index)” on page 287).
6. Configure the SPVLAN ID as the native VID on the QinQ tunnel port (see “Configuring VLAN Behavior for Interfaces” on page 290).
7. Configure system MTU to 1526 if jumbo frames are not enabled (see “Configuring the Maximum Frame Size” on page 72).
8. Configure the QinQ uplink port to join the SPVLAN as a tagged member (see “Adding Static Members to VLANs (VLAN Index)” on page 287).

Adding an Interface to a QinQ Tunnel

Follow the guidelines in the preceding section to set up a QinQ tunnel on the ECN330-switch. Use the VLAN Port Configuration or VLAN Trunk Configuration page to set the ingress port on the edge switch to dot1Q tunnel mode. Also set the Tag Protocol Identifier (TPID) value of the tunnel port if the attached client is using a nonstandard 2-byte ethertype to identify 802.1Q tagged frames.

Command Usage

- Use the System Mode page to set the ECN330-switch to QinQ mode before configuring a tunnel port (see “Configuring the ECN330-switch for Normal Operation or Tunneling Mode” on page 71).
- Use the TPID field to set a custom 802.1Q ethertype value on the selected interface. This feature allows the ECN330-switch to interoperate with third-party switches that do not use the standard 0x8100 ethertype to identify 802.1Q-tagged frames. For example,

0x1234 is set as the custom 802.1Q ethertype on a trunk port, incoming frames containing that ethertype are assigned to the VLAN contained in the tag following the ethertype field, as they would be with a standard 802.1Q trunk. Frames arriving on the port containing any other ethertype are looked upon as untagged frames, and assigned to the native VLAN of that port.

- All members of a VLAN should be set to the same ethertype.

Command Attributes

- **Mode** – Set the VLAN membership mode dot1Q-Tunnel. (Default: Hybrid)
 - **Dot1q-Tunnel** – Configures IEEE 802.1Q tunneling (QinQ) to segregate and preserve customer VLAN IDs for traffic crossing the service provider network.
- **TPID (0-65535)** – Tag Protocol Identifier specifies the ethertype of incoming packets on a tunnel port.
- **Address Monitor Mode** – Address monitoring must be enabled on a QinQ tunnel port to properly forward traffic for the internal management VLANs (VIDs 247-249) between the QinQ tunnel port and the SBC connected to port 28. (Default: Automatically enabled for any QinQ tunnel port)

Before enabling address monitoring, the ECN330-switch must first be set to QinQ mode (see “Configuring the ECN330-switch for Normal Operation or Tunneling Mode” on page 71), and the access port set to a QinQ tunnel port.

When address monitoring for the QinQ tunnel port is enabled, and incoming traffic is tagged for the internal management VLAN (247) or the FSA VLAN (249), an outer VLAN tag of 4093 is inserted and the packet redirected to port 28. The outer tag is removed at port 28 and the SBC processes the packet. When a packet for VLAN 247 or 249 is sent from port 28 to the tunnel port, a single inner tag is used and the packet is sent as in any normal forwarding operation.

When address monitoring for the QinQ tunnel port is enabled, and the tunnel port is a member of the dynamic management VLAN (248) and an incoming untagged packet enters this port, the ECN330-switch inserts an inner dummy tag, an outer tag of 248, and the packet is

redirected to port 28. The outer VLAN tag is retained because port 28 is tagged member of 248, and the SBC processes the packet. When a packet for VLAN 248 is sent from port 28 to the tunnel port, a single inner tag is used and the packet is sent as in any normal forwarding operation. However, note that the tag will be stripped from the packet by the tunnel port because it is an untagged member of VLAN 248.

When a tunnel port changes to QinQ Tunnel mode from normal mode, address monitoring is automatically enabled on this port, and all dynamic MAC address entries are deleted. If a new address entry is subsequently learned at the tunnel port, a static address entry for any internal management VLAN is added to the address table. If multiple internal management VLANs are configured, multiple entries are added to the address table.

When a tunnel port changes to normal mode from QinQ Tunnel mode, address monitoring is automatically disabled on this port, and all static internal management VLAN address entries are deleted.

If the internal management VLAN ID is changed, all dynamic MAC address and static internal management VLAN address entries are deleted.

When the PVID of a tunnel port is changed, all dynamic MAC address and static internal management VLAN address entries are deleted.

Web – Click VLAN, 802.1Q VLAN, Port Configuration or Trunk Configuration. Set the mode for the tunnel port to Dot1q-Tunnel, and set the TPID if the client is using a non-standard ethertype to identify 802.1Q tagged frames, then click Apply.

Port	PVID	Acceptable Frame Type	Ingress Filtering	GVRP Status	GARP Join Timer(Centi Seconds) (20-1000)	GARP Leave Timer(Centi Seconds)(60-3000)	GARP LeaveAll Timer(Centi Seconds) (500-18000)	Mode	TPID(0-65535)	AddressMonitorMode	Trunk Member
1	248	ALL	☒ Enabled	☐ Enabled	20	60	1000	Hybrid	33024	☐ Enabled	
2	248	ALL	☒ Enabled	☐ Enabled	20	60	1000	Dot1q-Tunnel	608	☒ Enabled	
3	248	ALL	☒ Enabled	☐ Enabled	20	60	1000	Hybrid	33024	☐ Enabled	
4	248	ALL	☒ Enabled	☐ Enabled	20	60	1000	Hybrid	33024	☐ Enabled	
5	248	ALL	☒ Enabled	☐ Enabled	20	60	1000	Hybrid	33024	☐ Enabled	
6	248	ALL	☒ Enabled	☐ Enabled	20	60	1000	Hybrid	33024	☐ Enabled	

Figure 119 Tunnel Port Configuration

CLI – This example sets port 2 to tunnel mode, indicates that the TPID used for 802.1Q tagged frames will be 9100 hexadecimal, and enables address monitor mode to pass traffic between the management VLANs and the tunnel port.

```
Console(config)#interface ethernet 1/2
Console(config-if)#switchport mode dot1q-tunnel
Console(config-if)#switchport dot1q-ethertype 9100
Console(config-if)#address-monitor qinq
Console(config-if)#
```

6.12.2 Configuring Private VLANs

Private VLANs provide port-based security and isolation between ports within the assigned VLAN. The ECN330-switch supports private VLANs in the form of primary/secondary associated groups, where the secondary groups are isolated VLANs whose members cannot directly communicate with each other, and can only send/receive traffic outside of the group through promiscuous ports that have been assigned to an associated primary VLAN. In other words, a primary VLAN contains promiscuous ports that can communicate with all other ports in the primary VLAN group and with members of any isolated VLAN group that has been associated with the primary group. An isolated VLAN contains isolated ports that cannot communicate with any other hosts within the isolated VLAN, and can only communicate with promiscuous ports in the associated primary VLAN. In all cases, the promiscuous ports are designed to provide open access to an external network such as the Internet, while the isolated ports provide restricted access to local users.

One or more isolated VLAN can be configured. An isolated port can also join a normal VLAN, but at most host-associate to one isolated VLAN. A promiscuous port can join to normal VLAN but at most be mapped to one primary VLAN. (Note that private VLANs and normal VLANs can exist simultaneously within the same ECN330-switch.)

Multiple primary VLANs can be configured on the ECN330-switch, an isolated VLAN can only be associated with only one primary VLAN, but multiple isolated VLANs can be associated with each primary VLAN.

To configure primary/secondary associated groups, follow these steps:

1. Use the Private VLAN Configuration menu (section 6.12.2.2 on page 306) to designate the primary VLAN that will be used to channel traffic outside of the isolated VLAN(s), and one or more isolated VLANs.
2. Use the Private VLAN Association menu (section 6.12.2.3 on page 307) to map the isolated VLAN(s) to a primary VLAN.
3. Use the Private VLAN Port Configuration menu (section 6.12.2.5 on page 309) to configure one or more promiscuous port (that is, having access to all ports in the primary VLAN and all ports in the associated isolated VLANs), and one or more isolated ports.

Note that a promiscuous port can join a normal VLAN, but at most be mapped to one primary VLAN. Because private VLAN ports can belong to a normal VLAN and private VLAN concurrently, the native VLAN of a private port will not automatically change to the private VLAN when assigning a promiscuous port to a primary VLAN or assigning an isolated port to an isolated VLAN as described in the following steps.

4. Use the Private VLAN Port Configuration menu (section 6.12.2.5 on page 309) to assign a promiscuous port to a primary VLAN.
5. Use the Private VLAN Port Configuration menu (section 6.12.2.5 on page 309) to assign an isolated port to an isolated VLAN.
6. Private VLANs can support tagged or untagged members. Use the VLAN Static Table (section 6.12.1.8 on page 287) to specify tagged or untagged members.

6.12.2.1 Displaying Current Private VLANs

The Private VLAN Information page displays information on the private VLANs configured on the ECN330-switch, including primary and isolated VLANs, and their assigned interfaces.

Command Attributes

- **VLAN ID** – ID of configured VLAN (1-4094), and VLAN type.
- **Primary VLAN** – The VLAN with which the selected VLAN ID is associated. A primary VLAN displays its own ID, and an isolated VLAN displays the associated primary VLAN.

- **Ports List** – The list of ports (and assigned port type) in the selected private VLAN.

Web – Click VLAN, Private VLAN, Information. Select the desired port from the VLAN ID drop-down menu.

Private VLAN Information

VLAN ID: 3, Primary VLAN ▼

Primary VLAN/VLAN 3

Ports List

- Unit 1, Port 3, Promiscuous
- Unit 1, Port 4, Isolated
- Unit 1, Port 5, Isolated

Figure 120 Private VLAN Information

CLI – This example shows the ECN330-switch configured with primary VLAN 3 and isolated VLANs 4 and 5. The isolated VLANs are associated with VLAN 3. Port 3 has then been configured as a promiscuous port and mapped to the Primary VLAN, while ports 4 and 5 have been configured as isolated ports and assigned to isolated VLAN 4 and 5 respectively. This means that traffic for port 4 and 5 can only pass through port 3.

```

Console#show vlan private-vlan

```

Primary	Secondary	Type	Interfaces
3		Primary	Eth1/ 3
3	4	Isolated	Eth1/ 4
3	5	Isolated	Eth1/ 5

```

Console#

```

6.12.2.2 Configuring Private VLANs

The Private VLAN Configuration page is used to create/remove primary or isolated VLANs.

Command Attributes

- **VLAN ID** – ID of configured VLAN (1-4094).
- **Type** – There are two types of private VLANs:
 - **Primary** – Conveys traffic between promiscuous ports in the primary VLAN, and to isolated ports within any associated isolated VLANs.
 - **Isolated** – Conveys traffic only between the VLAN's isolated ports and to promiscuous ports in the associated primary VLAN. Traffic between isolated ports within the VLAN is blocked.
- **Current** – Displays a list of the currently configured VLANs.

Web – Click VLAN, Private VLAN, Configuration. Enter the VLAN ID number, select Primary or Isolated type, then click Add. To remove a private VLAN from the ECN330-switch, highlight an entry in the Current list box and then click Remove. Note that all member ports must be removed from the VLAN before it can be deleted.

Private VLAN Configuration

Current:

3, Primary VLAN
4, Isolated VLAN
5, Isolated VLAN

<<Add Remove

New:

VLAN ID (1-4094) Type Primary

Figure 121 Private VLAN Configuration

CLI – This example configures VLAN 5 as a primary VLAN, and VLAN 6 as a community VLAN and VLAN 7 as an isolated VLAN.

```
Console(config)#vlan database
Console(config-vlan)#private-vlan 3 primary
Console(config-vlan)#private-vlan 4 isolated
Console(config-vlan)#private-vlan 5 isolated
Console(config-vlan)#
```

6.12.2.3 Associating VLANs

Each isolated VLAN must be associated with a primary VLAN.

Command Attributes

- **Primary VLAN ID** – ID of primary VLAN (1-4094).
- **Association** – Isolated VLANs associated with the selected primary VLAN.
- **Non-Association** – Isolated VLANs not associated with the selected primary VLAN.

Web – Click VLAN, Private VLAN, Association. Select the required primary VLAN from the scroll-down box, highlight one or more isolated VLANs in the Non-Association list box, and click Add to associate these entries with the selected primary VLAN. (An isolated VLAN can only be associated with one primary VLAN.)

Private VLAN Association

Primary VLAN ID: 3

Association:

- 4, Isolated VLAN
- 5, Isolated VLAN

Non-Association:

- (none)

<<Add Remove

Figure 122 Private VLAN Association

CLI – This example associates isolated VLANs 4 and 5 with primary VLAN 3.

```
Console(config)#vlan database
Console(config-vlan)#private-vlan 3 association 4
Console(config-vlan)#private-vlan 3 association 5
Console(config)#
```

6.12.2.4

Displaying Private VLAN Interface Information

Use the Private VLAN Port Information and Private VLAN Trunk Information menus to display the interfaces associated with private VLANs.

Command Attributes

- **Port/Trunk** – The ECN330 interface.
- **PVLAN Port Type** – Displays private VLAN port types.
 - **Normal** – The port is not configured in a private VLAN.
 - **Promiscuous** – A promiscuous port can communicate with all the interfaces within the assigned primary VLAN, and with interfaces within any isolated VLANs associated with the primary VLAN.
 - **Isolated** – An isolated port that can only communicate with the promiscuous ports in the associated primary VLAN.
- **Primary VLAN** – Conveys traffic between promiscuous ports within the primary VLAN, and between promiscuous ports and isolated ports within the associated isolated VLANs.
- **Isolated VLAN** – Conveys traffic only between the VLAN's isolated ports and promiscuous ports within the associated primary VLAN. Traffic between isolated ports within the VLAN is blocked.
- **Trunk** – The trunk identifier. (Port Information only)

Web – Click VLAN, Private VLAN, Port Information or Trunk Information.

Private VLAN Port Information				
Port	PVLAN Port Type	Primary VLAN	Secondary VLAN	Trunk
1	Normal			
2	Normal			
3	Promiscuous	3		
4	Isolated		4	
5	Isolated		5	
6	Normal			
7	Normal			
8	Normal			

Figure 123 Private VLAN Port Information

CLI – This example shows the ECN330-switch configured with primary VLAN 3 and isolated VLANs 4 and 5. Port 3 has been configured as a promiscuous port and mapped to VLAN 3, while ports 4 and 5 have been configured as isolated ports and associated with VLAN 4 and 5 respectively. This means that traffic for port 4 and 5 can only pass through port 3.

```

Console#show vlan private-vlan
Primary      Secondary      Type           Interfaces
-----
          3              Primary      Eth1/ 3
          3              4          Isolated      Eth1/ 4
          3              5          Isolated      Eth1/ 5
Console#

```

6.12.2.5 Configuring Private VLAN Interfaces

Use the Private VLAN Port Configuration and Private VLAN Trunk Configuration menus to set the private VLAN interface type, and assign the interfaces to a private VLAN.

Command Attributes

- **Port/Trunk** – The ECN330 interface.
- **PVLAN Port Type** – Sets the private VLAN port types.
 - **Normal** – The port is not configured in a private VLAN.

- **Promiscuous** – A promiscuous port can communicate with all the interfaces within the assigned primary VLAN, and with interfaces within any isolated VLANs associated with the primary VLAN.
- **Isolated** – An isolated port that can only communicate with the promiscuous ports in the associated primary VLAN.
- **Primary VLAN** – Conveys traffic between promiscuous ports within the primary VLAN, and between promiscuous ports and isolated ports within the associated isolated VLANs.
- **Isolated VLAN** – Conveys traffic only between the VLAN's isolated ports and promiscuous ports within the associated primary VLAN. Traffic between isolated ports within the VLAN is blocked.

Web – Click VLAN, Private VLAN, Port Configuration or Trunk Configuration. Set the PVLAN Port Type for each port that will join a private VLAN. Assign promiscuous ports to a primary VLAN. Assign isolated ports to an isolated VLAN. After all the ports have been configured, click Apply.

Private VLAN Port Configuration

Port	PVLAN Port Type	Primary VLAN	Secondary VLAN	Trunk
1	Normal	(none)	(none)	
2	Normal	(none)	(none)	
3	Promiscuous	3	(none)	
4	Isolated	(none)	4	
5	Isolated	(none)	5	
6	Normal	(none)	(none)	
7	Normal	(none)	(none)	
8	Normal	(none)	(none)	

Figure 124 Private VLAN Port Configuration

CLI – This example shows the ECN330-switch configured with primary VLAN 3 and isolated VLANs 4 and 5. Port 3 has been configured as a promiscuous port and mapped to VLAN 3, while ports 4 and 5 have been configured as isolated ports and associated with VLAN 4 and 5 respectively. This means that traffic for port 4 and 5 can only pass through port 3.

```
Console(config)#interface ethernet 1/3
Console(config-if)#switchport mode private-vlan promiscuous
Console(config-if)#switchport private-vlan mapping 3
Console(config-if)#exit
Console(config)#interface ethernet 1/4
Console(config-if)#switchport mode private-vlan isolated
Console(config-if)#switchport private-vlan host-association 4
Console(config-if)#exit
Console(config)#interface ethernet 1/5
Console(config-if)#switchport mode private-vlan isolated
Console(config-if)#switchport private-vlan host-association 6
Console(config-if)#
```

6.12.3

Configuring Protocol-Based VLANs

The network devices required to support multiple protocols cannot be easily grouped into a common VLAN. This may require non-standard devices to pass traffic between different VLANs in order to encompass all the devices participating in a specific protocol. This kind of configuration deprives users of the basic benefits of VLANs, including security and easy accessibility.

To avoid these problems, configure the ECN330-switch with protocol-based VLANs that divide the physical network into logical VLAN groups for each required protocol. When a frame is received at a port, its VLAN membership can then be determined based on the protocol type being used by the inbound packets.

Command Usage

To configure protocol-based VLANs, follow these steps:

1. Configure VLAN groups for the protocols to be used (page 284). Although not mandatory, it is suggested to configure a separate VLAN for each major protocol running on the network. Do not add port members at this time.
2. Create a protocol group for each of the protocols to be assigned to a VLAN using the Protocol VLAN Configuration page.

3. Map the protocol for each interface to the appropriate VLAN using the Protocol VLAN Port Configuration page.

6.12.3.1 Configuring Protocol Groups

Create a protocol group for one or more protocols.

Command Attributes

- **Protocol Group ID** – Group identifier of this protocol group. (Range: 1-2147483647)
- **Frame Type** – Frame type used by this protocol. (Options: Ethernet, RFC_1042, LLC_other)
- **Protocol Type** – The only option for the LLC_other frame type is IPX_raw. The options for all other frames types include: IP, ARP, RARP.

Note: SNAP frame types are not supported by the ECN330-switch due to hardware limitations.

Web – Click VLAN, Protocol VLAN, Configuration. Enter a protocol group ID, frame type and protocol type, then click Apply.

Figure 125 Protocol VLAN Configuration

CLI – The following creates protocol group 1, and then specifies Ethernet frames with IP and ARP protocol types.

```
Console(config)#protocol-vlan protocol-group 1 add frame-
type ethernet protocol-type ip
Console(config)#protocol-vlan protocol-group 1 add frame-
type ethernet protocol-type arp
Console(config)#
```

6.12.3.2 Mapping Protocols to VLANs

Map a protocol group to a VLAN for each interface that will participate in the group.

Command Usage

- When creating a protocol-based VLAN, only assign interfaces using this configuration screen. Assigning interfaces using any of the other VLAN commands, such as VLAN Static Table (page 287) or VLAN Static Membership (page 289), these interfaces will admit traffic of any protocol type into the associated VLAN.
- When a frame enters a port that has been assigned to a protocol VLAN, it is processed in the following manner:
 - If the frame is tagged, it will be processed according to the standard rules applied to tagged frames.
 - If the frame is untagged and the protocol type matches, the frame is forwarded to the appropriate VLAN.
 - If the frame is untagged but the protocol type does not match, the frame is forwarded to the default VLAN for this interface.

Command Attributes

- **Interface** – Port or trunk identifier.
- **Protocol Group ID** – Group identifier of this protocol group.
(Range: 1-2147483647)
- **VLAN ID** – VLAN to which matching protocol traffic is forwarded.
(Range: 1-4094)

Web – Click VLAN, Protocol VLAN, Port Configuration. Select a a port or trunk, enter a protocol group ID, the corresponding VLAN ID, and click Apply.

Figure 126 Protocol VLAN Port Configuration

CLI – The following maps the traffic entering Port 1 which matches the protocol type specified in protocol group 1 to VLAN 3.

```
Console(config)#interface ethernet 1/1
Console(config-if)#protocol-vlan protocol-group 1 vlan 3
Console(config-if)#
```

6.13 Layer 2 over MPLS Configuration

Layer 2 over MPLS (also referred to as L2MPLS or Ethernet over MPLS) is a solution for transporting Layer 2 packets over an MPLS network, allowing service providers to use an MPLS network to provide connectivity between customer sites over existing Layer 2 networks. Instead of using separate networks for each customer, service providers can use a common MPLS network to transport Layer 2 Ethernet traffic for different customers.

L2MPLS can provide customers with a virtual Ethernet link between remote sites using the service provider's existing MPLS backbone. It also simplifies service provider provisioning, since the edge switches on the service provider's network only need to support Layer 2 connectivity to the customer's equipment.

L2MPLS encapsulates Ethernet frames in MPLS packets and uses label stacking to forward them across an MPLS tunnel. Tunnel labels define the path

across the MPLS network and virtual channel labels define the entry and exit points to the customer. The edge switches connected to the service provider's network add and remove these labels as appropriate for packet encapsulation.

The MPLS network uses tunnel labels to transport packets between the service provider's switches. The egress service provider switch uses the virtual channel (VC) label to select the outgoing interface for the Ethernet packet. L2MPLS tunnels are unidirectional. For bi-directional L2MPLS to function properly, one tunnel must be configured in each direction.

L2MPLS uses a two label stack to transport Layer 2 frames, where the inner label is the VC label and the outer label is the tunnel label. The point-to-point virtual channel requires VC endpoints to be configured at the two edge switches. Only the edge switches at the ingress and egress points of the MPLS backbone know about the VCs dedicated to transporting Layer 2 traffic. Other routers do not have table entries for these VCs. This allows two physically separated customer switches to appear as if they are directly connected on the same physical LAN.

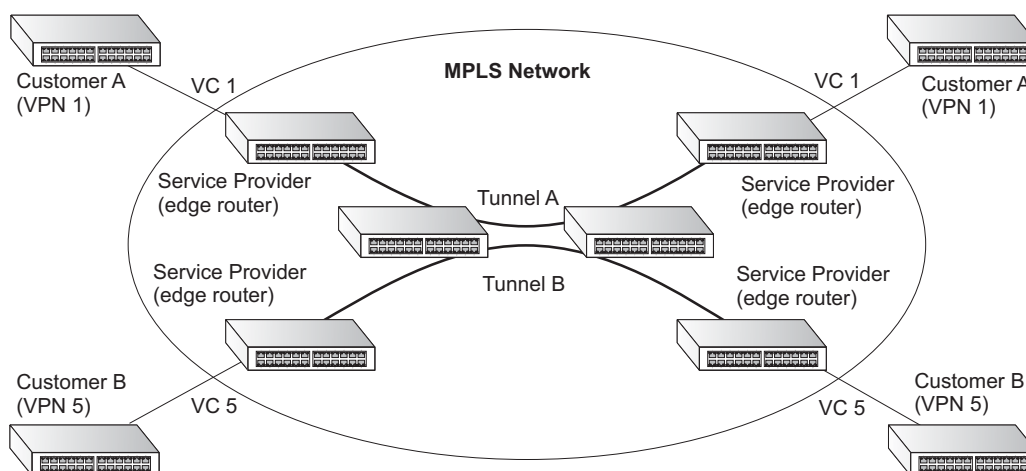


Figure 127 L2MPLS Functional Concept

Note: The priority bits of an incoming MPLS frame's VLAN tag are used to determine the input COS queue. To specify the MPLS EXP bits (experimental bits used to define Class of Service) for outgoing MPLS frames, first modify the priority bits of the VLAN tag with the priority commands provided by the ECN330-switch. The priority bits in the VLAN tag will then be copied to the outgoing frames as MPLS EXP bits.

Packet Flow for L2MPLS Tunnel

1. The ingress Provider Equipment (PE) switch receives an Ethernet frame and encapsulates the packet by removing the preamble, the start of frame delimiter (SFD), and the frame check sequence (FCS). The rest of the packet header is not changed.
2. If a port based VC label is configured, it will be added to all incoming packets.
3. If a packet has multiple VLAN tags, the access port uses the outer VLAN ID as an index to search its VC table. If a valid VC entry is found and the destination port is an uplink port, the ingress Provider Equipment (PE) switch adds the VC label and an optional tunnel label to the packet for normal MPLS routing through the MPLS backbone. If the packet already has a port-based VC label, it will be replaced with the new VC label.

One VLAN can only be mapped to one input VC and one output VC. However, one VC can be mapped to multiple VLANs. The input VC and output VC should normally be configured to the same value. Also, note that a maximum 8 input VCs and 8 output VCs are supported on the ECN330-switch.

4. The network core routers use the tunnel label to move the packet through the MPLS backbone and do not distinguish Ethernet traffic from any other types of packets in the MPLS backbone.
5. At the other end of the MPLS backbone, the egress PE switch receives the packet and de-encapsulates the packet by removing the tunnel label if one is present. The PE switch also removes the VC label from the packet. Any inbound traffic is not an MPLS packet is dropped.
6. The PE switch updates the header, if necessary, and sends the packet out the appropriate interface to the destination switch.

Configuration Limitations for L2MPLS

The following configuration limitations apply to L2MPLS:

- Only one Gigabit Ethernet (GE) port can be configured to L2MPLS uplink mode.
- L2MPLS does not support packet fragmentation and reassembly. Therefore, the maximum transmission unit (MTU) of all intermediate links between endpoints must be sufficient to carry the largest Layer 2

VLAN frame received. The ingress and egress PE switches must have the same MTU value. If single VLAN tagged packets are supported, the MTU should be 1544 bytes when jumbo frame is not enabled.

- L2MPLS only supports VLAN packets that conform to IEEE 802.1Q standard frames.
- The native VLAN of a trunk cannot be an L2MPLS VLAN, otherwise untagged packets would be forwarded onto the L2MPLS VLAN.
- QinQ and L2MPLS mode cannot be supported at the same time.
- The tunnel label is based on the uplink port. Each GE port has a register to store the tunnel label. All outgoing MPLS packets will use this register value to construct an MPLS header. It is not VLAN or VC based. So only one uplink port can be connected with one remote PE device.
- No VC redundancy is supported.
- L2MPLS link redundancy can be supported only if the entire network supports STP or EAPS.
- A VC can be associated with multiple VLANs. But a VLAN can only be associated with one input VC and one output VC.
- MPLS packets with Control Word cannot be received correctly. See the following section.
- If a VC is associated with the VLAN (see “Binding a VLAN to an MPLS Tunnel” on page 319), then the same VC cannot be configured as a port-based VC (see “Configuring an MPLS Uplink Port” on page 320), and vice versa.
- If the VC label is port-based (see “Configuring an MPLS Uplink Port” on page 320), the PVID (port’s native VID) is 0. When an untagged packet is received at the ingress port, the PVID is used to build a VLAN tag for this packet. This PVID is then used to search the VC table. If an entry is found, the ECN330-switch adds a VC label and tunnel label, and sends the packet out the uplink port.

When an untagged MPLS packet (has MPLS header but no VLAN tag) is received at the MPLS uplink port, the VID of the VC entry is used to build a VLAN tag for this packet instead of the PVID. So if the VC is port-based, incoming untagged MPLS packets with this VC are dropped.

Points of Non-compliance with the Martini Draft

The ECN330-switch does not comply the following items in the draft-martini-l2circuit-trans-mpls-16:

- **Withdrawing label after port disabled**
[2.2.5 Martini] – If the Label Switching Router (LSR) detects a failure on the Ethernet physical port, or the port is administratively disabled, it **MUST** withdraw the label mappings for all VCs associated with the port.

DOES NOT COMPLY – L2MPLS will not withdraw the label mapping for all VCs associated with the port if the port is administratively disabled.

- **Missing support for Control Word**
[2.2.6 Martini] – When transporting Ethernet and VLAN frames, the Martini Control Word is optional.

It must be supported to both send and receive without the Control Word!

And it must be supported to receive a Control Word from an implementation having implemented the optional Control Word, and the egress R2 (Martini tunnel end-point, defined in the draft and used in 3.1 Martini Draft Introduction) must be aware of this from configuration (or Label Distribution Protocol - LDP signalling)!

It must also be specified how to handle a received sequence number (in the Control Word), is it ignored or is it processed according to the Martini-draft!

DOES NOT COMPLY – L2MPLS does not support Martini Control Word. (T, E, C, U and "Optional sequence number") The implementation does not comply with the Martini draft at this point. An MPLS packet with a Control Word cannot be received correctly. It will just be treated as a normal L2MPLS packet. The ECN330-switch will use the Control Word as the first 32 bits of CDA MAC (destination MAC address of original packet). The CDA, CSA (source MAC address of original packet), CVLAN tag and payload will all be mismatched.

- **Modification of the frame header at R2**
[2.3.3 Martini] – The 4-byte VLAN tag is transported as is, and MAY be overwritten by the egress router.

DOES NOT COMPLY – The VLAN tag will not be modified by egress R2 switch.

General Configuration Guidelines for L2MPLS

1. Configure ECN330-switch to L2MPLS mode (“Configuring the ECN330-switch for Normal Operation or Tunneling Mode” on page 71).
2. Create a normal VLAN (“Creating VLANs” on page 284).
3. Enable L2MPLS mode in the VLAN interface (L2MPLS VLAN Binding – VLAN Mode, section 6.13.1 on page 319).
4. Associate L2MPLS VLAN to a Virtual Channel, specifying the MPLS input and output labels (MPLS VLAN Binding – Input Label and Output Label, section 6.13.1 on page 319).
5. Configure a Gigabit Ethernet port to L2MPLS uplink mode (L2MPLS Port Configuration – Status, section 6.13.2 on page 320).
6. Specify the tunnel label, virtual channel (VC), next hop, and maximum transfer unit (MTU) used by the uplink port (L2MPLS Port Configuration – Tunnel Label, VC Label, Next-Hop, and MTU, section 6.13.2 on page 320). Note that the MTU for the uplink port must be bigger than 1544 bytes.

6.13.1 Binding a VLAN to an MPLS Tunnel

Use the L2MPLS VLAN Configuration page to configure a VLAN to operate as an L2MPLS tunnel, and associate the MPLS input and output labels with the VLAN.

Command Attributes

- **VLAN** – ID of configured VLAN. (Default: 1, Range: 1-4094)
- **VLAN Mode** – Configures a VLAN to operate in normal IEEE 802.1Q mode or to operate as an L2MPLS tunnel. (Default: Normal Mode)
- **Input Label (0-1048574)** – MPLS input label. (Range: 0-1048574)
- **Output Label (0-1048574)** – MPLS output label. (Range: 0-1048574)

Web – Click L2MPLS, VLAN Configuration. Specify the VLAN that will be bound to the L2MPLS tunnel, set the status to enabled, set the mode to L2MPLS, and enter the input and output labels, then click Apply.

L2MPLS VLAN Configuration

VLAN: 9

VLAN Mode: L2MPLS Mode

Input Label (0-1048574): 5

Output Label (0-1048574): 5

Figure 128 L2MPLS VLAN Binding

CLI – The following example configures VLAN 9 to operate as an L2MPLS tunnel, and associates the MPLS input and output labels with the VLAN.

```
Console(config)#interface vlan 9
Console(config-if)#mpls l2
Console(config-if)#exit
Console(config)#mpls static binding vlan 9 input 5 output 5
Console(config)#
```

6.13.2 Configuring an MPLS Uplink Port

Use the L2MPLS Port Configuration page to set the operational characteristics for an MPLS uplink port.

Command Attributes

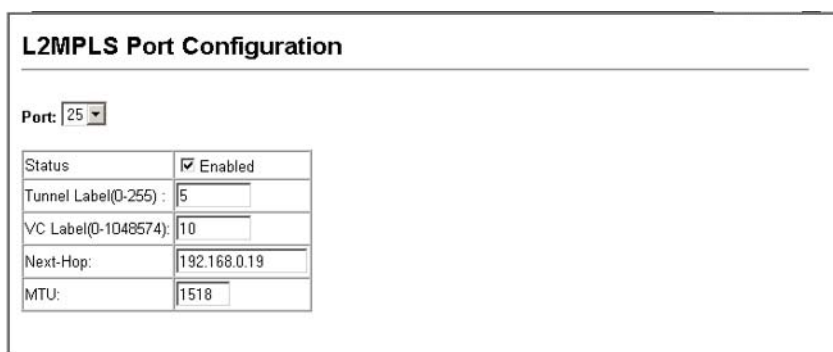
- **Port** – Port number. (Range: 1-27)
- **Status** – Configures a port to enter L2MPLS uplink port mode.
- **Tunnel Label (0-255)** – Sets the MPLS tunnel label that will be used to construct the MPLS header on the L2MPLS uplink port. This label is used by switches within the MPLS core network to establish a path from the entry point to the exit point. (Range: 0-255)
- **VC Label (0-1048574)** – Sets the MPLS port-based virtual channel (VC) label. All incoming packets forwarded to MPLS ports will use this

VC to generate MPLS labels. The VC is used to map traffic to a specific customer port on the edge switches at the boundaries of the MPLS network. (Range: 0-1048574)

- **Next Hop** – Configures the next hop MPLS switch/router IP address. This IP address will be used to identify the next hop across the MPLS network or, more commonly, the edge switch where traffic is passed on to the customer.
- **MTU** – Specifies the Maximum Transfer Unit (MTU) size for the specified port. (Range: 1500-9216 bytes)

The MTU setting for the uplink port takes precedence over the System MTU (see “Configuring the Maximum Frame Size” on page 72). Also, note that if the MTU setting for the uplink port has been specified, then setting the system MTU will not change the port MTU.

Web – Click L2MPLS, Port Configuration or Trunk Configuration. Configure the operational characteristics for the L2MPLS uplink port, and click Apply.



L2MPLS Port Configuration	
Port:	25
Status	☒ Enabled
Tunnel Label(0-255) :	5
VC Label(0-1048574):	10
Next-Hop:	192.168.0.19
MTU:	1518

Figure 129 Configuring an L2MPLS Uplink Port

CLI – The following example configures port 25 as an L2MPLS uplink port, and then specifies the tunnel label, the VC, the next hop, and the port MTU.

```
Console(config)#interface ethernet 1/25
Console(config-if)#mpls tunnel 5
Console(config-if)#mpls vc 10
Console(config-if)#mpls next-hop 192.168.0.19
Console(config-if)#switchport mtu 1518
Console(config-if)#
```

6.13.3 Displaying MPLS Virtual Channel Settings

Use the VPN Information page to display the L2MPLS tunnel settings.

Field Attributes

MPLS VLAN Information

- **Client Interface** – A VLAN configured to operate as an L2MPLS tunnel. This VLAN is connected to the client interface on the edge switch of the service provider's network.
- **VC State** – The status of the Virtual Channel can be one of the following:
 - UP – The VC can carry traffic between the two endpoints.
 - DOWN – The VC is not ready to carry traffic between the two endpoints. When no input and output labels are configured, the VC state is down
 - ADMIN DOWN—The VC has been administratively disabled.
- **Local VC Label** – This label determines the egress interface of a packet arriving from the MPLS backbone.
- **Remote VC Label** – This label is used by a remote peer switch.

MPLS Uplink Port Information

- **Uplink Interface** – The uplink port connected to the client interface.
- **Tunnel Label** – The MPLS tunnel label that is used by switches within the MPLS core network to establish a path from the entry point to the exit point.
- **VC Label** – The Virtual Channel identifier that is used to map traffic to a specific customer port on the edge switches at the boundaries of the MPLS network.
- **Next Hop IP** – The IP address of the next hop across the MPLS network.
- **DA MAC** – The MAC address of the remote switch's interface at the other end of the VC. The default DA-MAC of MPLS uplink port is 00-00-00-00-00-00.

Web – Click L2MPLS, VPN Information.

L2MPLS VPN Information

MPLS VLAN Information

Client Intf	VC State	Local VC Label	Remote VC Label
Vlan9	UP	5	5

MPLS Up-Link Port Information

Up-Link Intf	Tunnel Label	VC Label	Next Hop IP	DA-MAC
port25	0x5	0xa	192.168.0.10	00-00-00-00-00-00

Figure 130 Configuring an L2MPLS Uplink Port

CLI – The following example displays the settings for an L2MPLS tunnel and uplink port.

```

Console#sh mpls l2trnasport
MPLS Vlan Infomation :
[Client Intf]  [VC State]  [Local VC Label]  [Remote VC Label]
Vlan9          UP          5                  5

MPLS Up-link Port Information :
[Up-Link Intf]  [Tunnel Label]  [Vc Label]  [NextHopIP]  [Da-Mac]
port:25         5          10          192.168.0.19  00-00-00-00-00-00
Console#

```

6.14 Class of Service Configuration

Class of Service (CoS) specifies which data packets have greater precedence when traffic is buffered in the ECN330-switch due to congestion. The ECN330-switch supports CoS with eight priority queues for each port. Data packets in a port's high-priority queue will be transmitted before those in the lower-priority queues. The default priority for each interface can be set and the mapping of frame priority tags to the ECN330-switch's priority queues can be configured.

6.14.1 Layer 2 Queue Settings

6.14.1.1 Setting the Default Priority for Interfaces

The default port priority for each interface on the ECN330-switch can be specified. All untagged packets entering the ECN330-switch are tagged with the specified default port priority, and then sorted into the appropriate priority queue at the output port.

Command Usage

- The ECN330-switch provides eight priority queues for each port. It can use Weighted Round Robin or Weighted Fair Queuing to prevent head-of-queue blockage.
- The default priority applies for an untagged frame received on a port set to accept all frame types (i.e, receives both untagged and tagged frames). This priority does not apply to IEEE 802.1Q VLAN tagged frames. If the incoming frame is an IEEE 802.1Q VLAN tagged frame, the IEEE 802.1p User Priority bits will be used.
- If the output port is an untagged member of the associated VLAN, these frames are stripped of all VLAN tags prior to transmission.

Command Attributes

- **Default Priority** – The priority that is assigned to untagged frames received on the specified port. (Range: 0 - 7, Default: 0)

Note: This parameter is displayed in the CLI as "Priority for untagged traffic."

- **Number of Egress Traffic Classes** – The number of queue buffers provided for each port.

Web – Click Priority, Default Port Priority or Default Trunk Priority. Modify the default priority for any interface, then click Apply.

Default Port Priority			
Port	Default Priority (0-7)	Number of Egress Traffic Classes	Trunk
1	0	8	
2	0	8	
3	0	8	
4	0	8	
5	0	8	
6	0	8	
7	0	8	
8	0	8	
9	0	8	
10	0	8	
11	0	8	
12	0	8	

Figure 131 Default Port Priority

CLI – This example assigns a default priority of 5 to port 3.

```

Console(config)#interface ethernet 1/1
Console(config-if)#switchport priority default 5
Console(config-if)#end
Console#show interfaces switchport ethernet 1/1
Information of Eth 1/1
Broadcast Threshold:           Enabled, 500 packets/second
LACP Status:                   Disabled
Ingress Rate Limit:            Disabled, 100M bits per second
Egress Rate Limit:             Disabled, 100M bits per second
VLAN Membership Mode:          Hybrid
Ingress Rule:                  Enabled
Acceptable Frame Type:         All frames
Native VLAN:                   248
Priority for Untagged Traffic:  5
GVRP Status:                   Disabled
Allowed VLAN:                   247(t), 248(u),
Forbidden VLAN:
Private-VLAN Mode:             NONE
Private-VLAN host-association: NONE
Private-VLAN Mapping:          NONE
Console#

```

6.14.1.2 Mapping CoS Values to Egress Queues

The ECN330-switch processes Class of Service (CoS) priority tagged traffic by using eight priority queues for each port, with service schedules based on strict, Weighted Round Robin (WRR), Weighted Fair Queueing (WFQ), or a combination of strict and weighted queueing. Up to eight separate traffic priorities are defined in IEEE 802.1p. The default priority levels are assigned according to recommendations in the IEEE 802.1p standard as shown in Table 18.

Table 18 Egress Queue Priority Mapping

Queue	0	1	2	3	4	5	6	7
Priority	2	0	1	3	4	5	6	7

The priority levels recommended in the IEEE 802.1p standard for various network applications are shown in Table 19. However, priority levels can be mapped to the ECN330-switch's output queues in any way that benefits application traffic for the network.

Table 19 CoS Priority Levels

Priority Level	Traffic Type
0 (default)	Best Effort
1	Background
2	(Spare)
3	Excellent Effort
4	Controlled Load
5	Video, less than 100 milliseconds latency and jitter
6	Voice, less than 10 milliseconds latency and jitter
7	Network Control

Command Attributes

- **Priority** – CoS value. (Range: 0-7, where 7 is the highest priority)
- **Traffic Class** – Output queue buffer. (Range: 0-7, where 7 is the highest CoS priority queue)

Note: This parameter is displayed in the CLI as "Queue ID."

Web – Click Priority, Traffic Classes. Assign priorities to the traffic classes (that is, output queues) for the selected interface, then click Apply.

Traffic Classes

Priority	Traffic Class
0	2 (0-7)
1	0 (0-7)
2	1 (0-7)
3	3 (0-7)
4	4 (0-7)
5	5 (0-7)
6	6 (0-7)
7	7 (0-7)

Figure 132 Traffic Classes

CLI – The following example shows how to change the CoS assignments to a one-to-one mapping.

```

Console(config)#interface ethernet 1/1
Console(config)#queue cos-map 0 0
Console(config)#queue cos-map 1 1
Console(config)#queue cos-map 2 2
Console(config)#exit
Console#show queue cos-map ethernet 1/1
Information of Eth 1/1
  Traffic Class : 0 1 2 3 4 5 6 7
  Priority Queue: 0 1 2 3 4 5 6 7
Information of Eth 1/2
  CoS Value:      0 1 2 3 4 5 6 7
  Priority Queue: 0 1 2 3 4 5 6 7
.
.
.

```

Note: Mapping specific values for CoS priorities is implemented as an interface configuration command, but any changes will apply to the all interfaces on the ECN330-switch.

6.14.1.3 Selecting the Queue Mode

The ECN330-switch can be set to service the queues based on a strict rule that requires all traffic in a higher priority queue to be processed before lower priority queues are serviced, Weighted Round-Robin (WRR) queuing that specifies a relative weight of each queue, Weighted Fair Queuing (WFQ) that specifies a minimum bandwidth for each queue, or a combination of strict service for the high priority queues and either WRR or WFQ for the remaining queues.

Command Attributes

- **Port** – The port number on the ECN330.
- **Queue Mode**
 - **Strict** - Services the egress queues in sequential order, transmitting all traffic in the higher priority queues before servicing lower priority queues. (This is the default selection.)
 - **WFQ** - Shares bandwidth at the egress ports by specifying a minimum bandwidth for each queue. Guaranteed bandwidth is first supplied to each queue, any remaining bandwidth is distributed in a round-robin fashion.
 - **WRR** - Uses a predefined relative weight for each queue that determines the percentage of service time the ECN330-switch services each queue before moving on to the next queue. This prevents head-of-line blocking that can occur with strict priority queuing. WRR shares bandwidth at the egress ports by using scheduling weights 1, 2, 4, 6, 8, 10, 12, 14 for queues 0 through 7 respectively.
 - **Strict-WFQ** - Uses strict priority service on the high-priority queues, and WFQ on the remaining queues.
 - **Strict-WRR** - Uses strict priority service on the high-priority queues, and WRR on the remaining queues.
- **Strict Queue Split Value (0-7)** - Specifies the strict priority queues used for the Strict-WFQ and Strict-WRR options. This assigns the specified queue up to the highest priority queue. (Range: 0-7)

Web – Click Priority, Queue Mode. Select a queueing option, set the lowest queue that uses strict priority when Strict-WFQ or Strict-WRR mode is selected, then click Apply.

Figure 133 Queue Mode

Note: Mapping specific values for Queue Mode is implemented as an interface configuration command, but any changes will apply to the all interfaces on the ECN330-switch.

CLI – The following sets the queue mode to Strict-WFQ, with queue 5-7 using strict priority and the other queues using WFQ

```
Console(config)#queue mode strict-wfq sp-queue 5
Console(config)#exit
Console#show queue mode
  Queue Mode: strict-wfq
    wfq      queue: 0-4
    strict queue: 5-7
Console#
```

6.14.1.4

Setting the Service Weight for Traffic Classes

The ECN330-switch can use the Weighted Round Robin (WRR) algorithm to determine the frequency at which it services each priority queue. As described in 6.14.1.2 "Mapping CoS Values to Egress Queues" 326, the traffic classes are mapped to one of the eight egress queues provided for each port. A weight can be assigned to each of these queues (and thereby to the corresponding traffic priorities). This weight sets the frequency at which each queue will be polled for service, and subsequently affects the response time for software applications assigned a specific priority value.

Command Attributes

- **WRR Setting Table** – Displays a list of weights for each traffic class (that is, queue).

Note: This parameter is displayed in the CLI as “Queue ID.”

- **Weight Value** – Set a new weight for the selected traffic class. (Range: 1-15)

Web – Click Priority, Queue Scheduling. Select the interface, highlight a traffic class (that is, output queue), enter a weight, then click Apply.

Queue Scheduling

Interface ☒ Port 1 ☐ Trunk

Select

WRR Setting Table	Traffic Class 0 - weight 1 Traffic Class 1 - weight 2 Traffic Class 2 - weight 4 Traffic Class 3 - weight 6 Traffic Class 4 - weight 8
Weight Value	2 (1-15)

Figure 134 Queue Scheduling

CLI – The following example shows how to assign WRR weights to each of the priority queues.

```

Console(config)#queue bandwidth 1 3 5 7 9 11 13 15
Console(config)#exit
Console#show queue bandwidth
Information of Eth 1/1
  Queue ID  Weight
  -----  -
      0      1
      1      2
      2      4
      3      6
      4      8
      5     10
      6     12
      7     14
Information of Eth 1/2
  Queue ID  Weight
  .
  .
  .

```

6.14.1.5

Setting the Minimum Bandwidth for WFQ

Use the WFQ Minimum Bandwidth Configuration page to assign a minimum bandwidth to each of the priority queues when using Weighted Fair Queueing (WFQ).

Command Usage

- WFQ shares bandwidth at the egress ports by specifying a minimum bandwidth for each queue. Guaranteed bandwidth is first supplied to each queue, any remaining bandwidth is distributed in a round-robin fashion.
- Use the Queue Mode page (see “Selecting the Queue Mode” on page 329) to set the queue mode to WFQ or Strict-WFQ before setting the minimum queue bandwidths.

Command Attributes

- **Interface** – Selects the port or trunk interface to which the settings apply.
- **Minimum Bandwidth Table** – The minimum bandwidth currently assigned to each of the priority queues when using WFQ.
- **Minimum Bandwidth Value** – The value to assign to a entry in the bandwidth table. (Range: 1-100000 kbps for Fast Ethernet ports, 1-100000000 kbps for Gigabit Ethernet ports; Granularity: 64 kbps)

Web – Click Priority, WFQ Minimum Bandwidth. Select an interface, highlight a queue in the Minimum Bandwidth Table, enter a minimum bandwidth for the selected queue, and click Apply.

WFQ Minimum BandWidth Configuration

Interface ☒ Port ☐ Trunk

Queue ID - Min BandWidth(Unit: 1kbps, Step: 64kbps)

Queue ID	Min BandWidth
0	1754
1	3508
2	7017
3	10526
4	14035

Minimum BandWidth Value: 64

Figure 135 Configuring WFQ Minimum Bandwidth

CLI – The following example assign a minimum bandwidth to each of the CoS priority queues.

```
Console#configure
Console(config)#queue mode wfq
Console(config)#int eth 1/5
Console(config-if)#queue min-bandwidth 64 128 256 512 1024 2048 4096
8190
Console(config-if)#
```

6.14.2 Layer 3/4 Priority Settings

6.14.2.1 Mapping Layer 3/4 Priorities to CoS Values

The ECN330-switch supports several common methods of prioritizing layer 3/4 traffic to meet application requirements. Traffic priorities can be specified in the IP header of a frame, using the priority bits in the Type of Service (ToS) octet or the number of the TCP port. If priority bits are used, the ToS octet may contain three bits for IP Precedence or six bits for Differentiated Services Code Point (DSCP) service. When these services are enabled, the priorities are mapped to a Class of Service value by the ECN330-switch, and the traffic then sent to the corresponding output queue.

Because different priority information may be contained in the traffic, the ECN330-switch maps priority values to the output queues in the following manner:

- The precedence for priority mapping is IP Port Priority, IP Precedence or DSCP Priority, and then Default Port Priority.
- IP Precedence and DSCP Priority cannot both be enabled. Enabling one of these priority types will automatically disable the other.

6.14.2.2 Selecting IP Precedence/DSCP Priority

The ECN330-switch allows a choice between using IP Precedence or DSCP priority. Select one of the methods or disable this feature.

Command Attributes

- **Disabled** – Disables both priority services. (This is the default setting.)
- **IP Precedence** – Maps layer 3/4 priorities using IP Precedence.
- **IP DSCP** – Maps layer 3/4 priorities using Differentiated Services Code Point Mapping.

Web – Click Priority, IP Precedence/DSCP Priority Status. Select Disabled, IP Precedence or IP DSCP from the scroll-down menu, then click Apply.

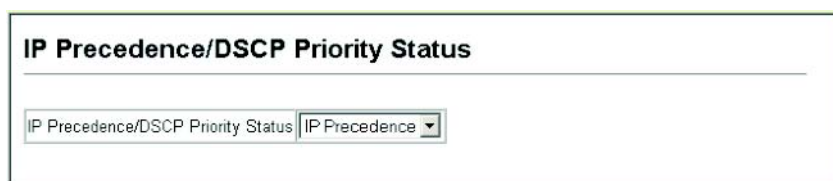


Figure 136 IP Precedence/DSCP Priority Status

CLI – The following example enables IP Precedence service on the ECN330-switch.

```
Console(config)#map ip precedence
Console(config)#
```

6.14.2.3

Mapping IP Precedence

The Type of Service (ToS) octet in the IPv4 header includes three precedence bits defining eight different priority levels ranging from highest priority for network control packets to lowest priority for routine traffic. The default IP Precedence values are mapped one-to-one to Class of Service values (that is, Precedence value 0 maps to CoS value 0, and so forth). Bits 6 and 7 are used for network control, and the other bits for various application types. ToS bits are defined in Table 20.

Table 20 Mapping IP Precedence

Priority Level	Traffic Type	Priority Level	Traffic Type
7	Network Control	3	Flash
6	Internetwork Control	2	Immediate
5	Critical	1	Priority
4	Flash Override	0	Routine

Command Attributes

- **IP Precedence Priority Table** – Shows the IP Precedence to CoS map.
- **Class of Service Value** – Maps a CoS value to the selected IP Precedence value. Note that “0” represents low priority and “7” represent high priority.

Web – Click Priority, IP Precedence Priority. Select an entry from the IP Precedence Priority Table, enter a value in the Class of Service Value field, and then click Apply.

The screenshot shows a web interface titled "IP Precedence Priority". It contains a table labeled "IP Precedence Priority Table" with a dropdown menu. The dropdown menu lists eight options: "IP Precedence 0 - CoS 0", "IP Precedence 1 - CoS 1" (which is highlighted in blue), "IP Precedence 2 - CoS 2", "IP Precedence 3 - CoS 3", "IP Precedence 4 - CoS 4", "IP Precedence 5 - CoS 5", "IP Precedence 6 - CoS 6", and "IP Precedence 7 - CoS 7". Below the table is a field labeled "Class of Service Value (0-7)" with the value "0" entered. At the bottom of the form is a button labeled "Restore Default".

Figure 137 IP Precedence Priority

CLI – The following example globally enables IP Precedence service on the ECN330-switch, maps IP Precedence value 1 to CoS value 0 (on port 1), and then displays the IP Precedence settings.

```

Console(config)#map ip precedence
Console(config)#interface ethernet 1/1
Console(config-if)#map ip precedence 1 cos 0
Console(config-if)#end
Console#show map ip precedence ethernet 1/1
Precedence mapping status: disabled
  Port          Precedence COS
  -----
  Eth 1/ 1      0    0
  Eth 1/ 1      1    0
  Eth 1/ 1      2    2
  Eth 1/ 1      3    3
  Eth 1/ 1      4    4
  Eth 1/ 1      5    5
  Eth 1/ 1      6    6
  Eth 1/ 1      7    7
Console#

```

Note: Mapping specific values for IP Precedence is implemented as an interface configuration command, but any changes will apply to the all interfaces on the ECN330-switch.

6.14.2.4 Mapping DSCP Priority

The DSCP is six bits wide, allowing coding for up to 64 different forwarding behaviors. The DSCP replaces the ToS bits, but it retains backward compatibility with the three precedence bits so that non-DSCP compliant, ToS-enabled devices, will not conflict with the DSCP mapping. Based on network policies, different kinds of traffic can be marked for different kinds of forwarding. The DSCP default values are defined in Table 21. Note that all the DSCP values that are not specified are mapped to CoS value 0.

Table 21 Mapping DSCP Priority

IP DSCP Value	CoS Value
0	0
8	1
10, 12, 14, 16	2
18, 20, 22, 24	3
26, 28, 30, 32, 34, 36	4
38, 40, 42	5
48	6
46, 56	7

Command Attributes

- **DSCP Priority Table** – Shows the DSCP Priority to CoS map.
- **Class of Service Value** – Maps a CoS value to the selected DSCP Priority value. Note that “0” represents low priority and “7” represent high priority.

Note: IP DSCP settings apply to all interfaces.

Web – Click Priority, IP DSCP Priority. Select an entry from the DSCP table, enter a value in the Class of Service Value field, then click Apply.

Figure 138 IP DSCP Priority

CLI – The following example globally enables DSCP Priority service on the ECN330-switch, maps DSCP value 0 to CoS value 1 (on port 1), and then displays the DSCP Priority settings.

```

Console(config)#map ip dscp
Console(config)#interface ethernet 1/1
Console(config-if)#map ip dscp 1 cos 0
Console(config-if)#end
Console#show map ip dscp ethernet 1/1
DSCP mapping status: disabled

  Port          DSCP COS
  -----
  Eth 1/ 1      0    0
  Eth 1/ 1      1    0
  Eth 1/ 1      2    0
  Eth 1/ 1      3    0
  .
  .
  .
  Eth 1/ 1      61   0
  Eth 1/ 1      62   0
  Eth 1/ 1      63   0
Console#

```

Note: Mapping specific values for IP DSCP is implemented as an interface configuration command, but any changes will apply to the all interfaces on the ECN330-switch.

6.14.2.5 Mapping IP Port Priority

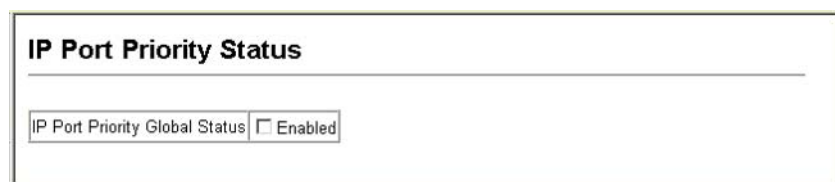
Network applications can also be mapped to Class of Service values based on the IP port number (that is, TCP/UDP port number) in the frame header. Some of the more common TCP service ports include: HTTP: 80, FTP: 21, Telnet: 23 and POP3: 110.

Command Attributes

- **IP Port Priority Status** – Enables or disables the IP port priority.
- **Interface** – Selects the port or trunk interface to which the settings apply.
- **IP Port Priority Table** – Shows the IP port to CoS map.
- **IP Port Number (TCP/UDP)** – Set a new IP port number.
- **Class of Service Value** – Sets a CoS value for a new IP port. Note that “0” represents low priority and “7” represent high priority.

Note: IP Port Priority settings apply to all interfaces.

Web – Click Priority, IP Port Status. Set IP Port Priority Status to Enabled.



IP Port Priority Status

IP Port Priority Global Status ☐ Enabled

Figure 139 IP Port Priority Status

Click Priority, IP Port Priority. Enter the port number for a network application in the IP Port Number box and the new CoS value in the Class of Service box, and then click Add IP Port.

IP Port Priority

Interface ☒ Port ☐ Trunk

Select

IP Port Priority Table

IP Port Number (TCP/UDP)	Class of Service Value (0-7)
80	0

Remove IP Port

Figure 140 IP Port Priority

CLI – The following example globally enables IP Port Priority service on the ECN330-switch, maps HTTP traffic (on port 1) to CoS value 0, and then displays the IP Port Priority settings.

```
Console(config)#map ip port
Console(config)#interface ethernet 1/1
Console(config-if)#map ip port 80 cos 0
Console(config-if)#end
Console#show map ip port ethernet 1/1
TCP port mapping status: disabled

Port          Port no. COS
-----
Eth 1/ 1      80    0
Console#
```

Note: Mapping specific values for IP Port Priority is implemented as an interface configuration command, but any changes will apply to the all interfaces on the ECN330-switch.

6.15 Quality of Service

The commands described in this section are used to configure Quality of Service (QoS) classification criteria and service policies. Differentiated Services (DiffServ) provides policy-based management mechanisms used for prioritizing network resources to meet the requirements of specific traffic types on a per hop basis. Each packet is classified upon entry into the network based on access lists, IP Precedence, DSCP values, or VLAN lists. Using access lists allows traffic to be selected based on Layer 2, Layer 3, or Layer 4 information contained in each packet. Based on configured network policies, different kinds of traffic can be marked for different kinds of forwarding.

All switches or routers that access the Internet rely on class information to provide the same forwarding treatment to packets in the same class. Class information can be assigned by end hosts, or switches or routers along the path. Priority can then be assigned based on a general policy, or a detailed examination of the packet. However, note that detailed examination of packets should take place close to the network edge so that core switches and routers are not overloaded.

Switches and routers along the path can use class information to prioritize the resources allocated to different traffic classes. The manner in which an individual device handles traffic in the DiffServ architecture is called per-hop behavior. All devices along a path should be configured in a consistent manner to construct a consistent end-to-end QoS solution.

Note: Only one rule per Class Map can be configured. However, multiple classes can be included in a Policy Map.

Note: A Class Map must be created before creating a Policy Map.

6.15.1 Configuring Quality of Service Parameters

To create a service policy for a specific category or ingress traffic, follow these steps:

1. Use the “Class Map” to designate a class name for a specific category of traffic.
2. Edit the rules for each class to specify a type of traffic based on an access list, a DSCP or IP Precedence value, or a VLAN.

3. Set an ACL mask to enable filtering for the criteria specified in the Class Map. (See “Configuring an IP ACL Mask” on page 168 or “Configuring a MAC ACL Mask” on page 170.)
4. Use the “Policy Map” to designate a policy name for a specific manner in which ingress traffic will be handled.
5. Add one or more classes to the Policy Map. Assign policy rules to each class by “setting” the QoS value to be assigned to the matching traffic class. The policy rule can also be configured to monitor the average flow and burst rate, and drop any traffic that exceeds the specified rate, or just reduce the DSCP service level for traffic exceeding the specified rate.
6. Use the “Service Policy” to assign a policy map to a specific interface.

6.15.1.1 **Configuring a Class Map**

A class map is used for matching packets to a specified class.

Command Usage

- To configure a Class Map, follow these steps:
 - Open the Class Map page, and click Add Class.
 - When the Class Configuration page opens, fill in the “Class Name” field, and click Add.
 - When the Match Class Settings page opens, specify type of traffic for this class based on an access list, a DSCP or IP Precedence value, or a VLAN, and click the Add button next to the field for the selected traffic criteria. Only one item can be specified to match when assigning ingress traffic to a class map.
- The class map uses the Access Control List filtering engine, so an ACL mask must also be set to enable filtering for the criteria specified in the Class Map. See “Configuring an IP ACL Mask” on page 168 or “Configuring a MAC ACL Mask” on page 170 for information on configuring an appropriate ACL mask.
- The class map is used with a policy map (page 346) to create a service policy (page 350) for a specific interface that defines packet classification, service tagging, and bandwidth policing. Note that one or more class maps can be assigned to a policy map.

Command Attributes

Class Map

- **Modify Name and Description** – Configures the name and a brief description of a class map. (Range: 1-16 characters for the name; 1-64 characters for the description)
- **Edit Rules** – Opens the “Match Class Settings” page for the selected class entry. Modify the criteria used to classify ingress traffic on this page.
- **Add Class** – Opens the “Class Configuration” page. Enter a class name and description on this page, and click Add to open the “Match Class Settings” page. Enter the criteria used to classify ingress traffic on this page.
- **Remove Class** – Removes the selected class.

Class Configuration

- **Class Name** – Name of the class map. (Range: 1-16 characters)
- **Type** – Only one match command is permitted per class map, so the match-any field refers to the criteria specified by the lone match command.
- **Description** – A brief description of a class map. (Range: 1-64 characters)
- **Add** – Adds the specified class.
- **Back** – Returns to previous page with making any changes.

Match Class Settings

- **Class Name** – List of class maps.
- **ACL List** – Name of an access control list. Any type of ACL can be specified, including standard or extended IP ACLs and MAC ACLs. (Range: 1-16 characters)
- **IP DSCP** – A DSCP value. (Range: 0-63)
- **IP Precedence** – An IP Precedence value. (Range: 0-7)
- **VLAN** – A VLAN. (Range:1-4094)

- **Add** – Adds the specified criteria to the class. Only one entry is permitted per class.
- **Remove** – Deletes the selected criteria from the class.

Web – Click QoS, DiffServ, then click Add Class to create a new class, or Edit Rules to change the rules of an existing class.

Class Map

	Class Name	Type	Description
☒	rd_class	match-any	R&D service for DSCP 3

Class Configuration

Class Name:

Type:

Description:

Match Class Settings

Class Name: **rd_class**

ACL List	(none)	Add
IP DSCP (0-63)		Add
IP Precedence (0-7)		Add
VLAN (1-4093)		Add

Figure 141 Configuring Class Maps

CLI - This example creates a class map call “rd-class,” and sets it to match packets marked for DSCP service value 3.

```
Console(config)#class-map rd_class match-any
Console(config-cmap)#match ip dscp 3
Console(config-cmap)#exit
Console(config)#access-list ip mask-precedence in
Console(config-ip-mask-acl)#mask any any dscp
Console(config-ip-mask-acl)#
```

6.15.1.2 Creating QoS Policies

This function creates a policy map that can be attached to multiple interfaces.

Command Usage

- To configure a Policy Map, follow these steps:
 - Create a Class Map as described on page 343.
 - Open the Policy Map page, and click Add Policy.
 - When the Policy Configuration page opens, fill in the “Policy Name” field, and click Add.
 - When the Policy Rule Settings page opens, select a class name from the scroll-down list (Class Name field). Configure a policy for traffic that matches criteria defined in this class by setting the quality of service that an IP packet will receive (in the Action field), defining the maximum throughput and burst rate (in the Meter field), and the action that results from a policy violation (in the Exceed field). Then finally click Add to register the new policy.
- A policy map can contain multiple class statements that can be applied to the same interface with the Service Policy Settings (page 350). Up to 63 policers (that is, class maps) can be configured for Fast Ethernet and Gigabit Ethernet ingress ports.

Policing is based on a token bucket, where bucket depth (that is, the maximum burst before the bucket overflows) is by specified the “Burst” field, and the average rate tokens are removed from the bucket is by specified by the “Rate” option.

- After using the policy map to define packet classification, service tagging, and bandwidth policing, it must be assigned to a specific interface by a service policy (page 350) to take effect.

Command Attributes

Policy Map

- **Modify Name and Description** – Configures the name and a brief description of a policy map. (Range: 1-16 characters for the name; 1-64 characters for the description)
- **Edit Classes** – Opens the “Policy Rule Settings” page for the selected class entry. Modify the criteria used to service ingress traffic on this page.
- **Add Policy** – Opens the “Policy Configuration” page. Enter a policy name and description on this page, and click Add to open the “Policy Rule Settings” page. Enter the criteria used to service ingress traffic on this page.
- **Remove Policy** – Deletes a specified policy.

Policy Configuration

- **Policy Name** — Name of policy map. (Range: 1-16 characters)
- **Description** – A brief description of a policy map. (Range: 1-64 characters)
- **Add** – Adds the specified policy.
- **Back** – Returns to previous page with making any changes.

Policy Rule Settings

- Class Settings -

- **Class Name** – Name of class map.
- **Action** – Shows the service provided to ingress traffic by setting a CoS, DSCP, or IP Precedence value in a matching packet (as specified in Match Class Settings on page 343).

- **Meter** – The maximum throughput and burst rate.
 - **Rate (kbps)** – Rate in kilobits per second.
 - **Burst (byte)** – Burst in bytes.
- **Exceed Action** – Specifies whether the traffic that exceeds the specified rate will be dropped or the DSCP service level will be reduced.
- **Remove Class** – Deletes a class.

- Policy Options -

- **Class Name** – Name of class map.
- **Action** – Configures the service provided to ingress traffic by setting a CoS, DSCP, or IP Precedence value in a matching packet (as specified in Match Class Settings on page 343). (Range - CoS: 0-7, DSCP: 0-63, IP Precedence: 0-7)
- **Meter** – Check this to define the maximum throughput, burst rate, and the action that results from a policy violation.
 - **Rate (kbps)** – Rate in kilobits per second. (Range: 1-100000 kbps or maximum port speed, whichever is lower)
 - **Burst (byte)** – Burst in bytes. (Range: 64-1522)
- **Exceed** – Specifies whether the traffic that exceeds the specified rate or burst will be dropped or the DSCP service level will be reduced.
 - **Set** – Decreases DSCP priority for out of conformance traffic. (Range: 0-63).
 - **Drop** – Drops out of conformance traffic.
- **Add** – Adds the specified criteria to the policy map.

Web – Click QoS, DiffServ, Policy Map to display the list of existing policy maps. To add a new policy map click Add Policy. To configure the policy rule settings click Edit Classes.

Policy Map

Policy Name	Description
☐ rd_policy	R&D service for QoS
☐ rd_policy#2	R&D service for IP Precedence

Policy Configuration

Policy Name:

Description:

Policy Rule Settings

Policy Name: **rd_policy#3**

Class Name	Action	Meter		Exceed Action
		Rate (bps)	Burst (byte)	

Class Name:

Action:

☒ Meter

Rate (1-100000): bps

Burst (64-1522): byte

Exceed:

Figure 142 Configuring Policy Maps

CLI – This example creates a policy map called “rd-policy,” sets the average bandwidth the 1 Mbps, the burst rate to 1522 bps, and the response to reduce the DSCP value for violating packets to 0.

```
Console(config)#policy-map rd_policy#3
Console(config-pmap)#class rd_class#3
Console(config-pmap-c)#set ip dscp 4
Console(config-pmap-c)#police 100000 1522 exceed-action
    set ip dscp 0
Console(config-pmap-c)#
```

6.15.1.3 Attaching a Policy Map to Ingress Queues

This function binds a policy map to the ingress queue of a particular interface.

Command Usage

- First define a class map, set an ACL mask to match the criteria defined in the class map, then define a policy map, and finally bind the service policy to the required interface.
- Only one policy map can be bound to an interface.
- The current firmware does not allow a policy map to be bound to an egress queue.

Command Attributes

- **Ports** – Specifies a port.
- **Ingress** – Applies the rule to ingress traffic.
- **Enabled** – Check this to enable a policy map on the specified port.
- **Policy Map** – Select the appropriate policy map from the scroll-down box.

Web – Click QoS, DiffServ, Service Policy Settings. Check Enabled and choose a Policy Map for a port from the scroll-down box, then click Apply.

Ports	Ingress
1	☐ Enabled rd_policy
2	☐ Enabled rd_policy
3	☐ Enabled rd_policy
4	☐ Enabled rd_policy
5	☒ Enabled rd_policy#3
6	☐ Enabled rd_policy

Figure 143 Service Policy Settings

CLI - This example applies a service policy to an ingress interface.

```
Console(config)#interface ethernet 1/5
Console(config-if)#service-policy input rd_policy#3
Console(config-if)#
```

6.16 Multicast Filtering

Multicasting is used to support real-time applications such as videoconferencing or streaming audio. A multicast server does not have to establish a separate connection with each client. It merely broadcasts its service to the network, and any hosts that want to receive the multicast register with their local multicast switch/router. Although this approach reduces the network overhead required by a multicast server, the broadcast traffic must be carefully pruned at every multicast switch/router it passes through to ensure that traffic is only passed on to the hosts which subscribed to this service.

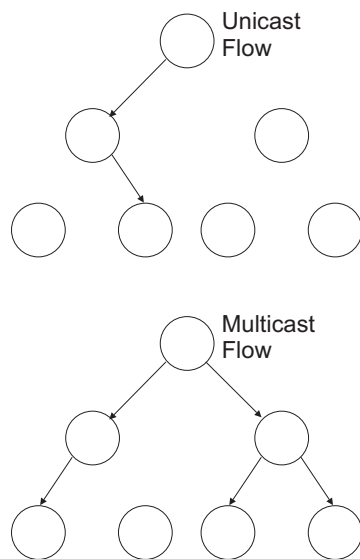


Figure 144 Multicast Filtering Concept

The ECN330-switch can use Internet Group Management Protocol (IGMP) to filter multicast traffic. IGMP Snooping can be used to passively monitor or "snoop" on exchanges between attached hosts and an IGMP-enabled device, most commonly a multicast router. In this way, the ECN330-switch can discover the ports that want to join a multicast group, and set its filters accordingly.

If there is no multicast router attached to the local subnet, multicast traffic and query messages may not be received by the ECN330-switch. In this case (Layer 2) IGMP Query can be used to actively ask the attached hosts if they want to receive a specific multicast service. IGMP Query thereby identifies the ports containing hosts requesting to join the service and sends data out to those ports

only. It then propagates the service request up to any neighboring multicast switch/router to ensure that it will continue to receive the multicast service.

The purpose of IP multicast filtering is to optimize a switched network's performance, so multicast packets will only be forwarded to those ports containing multicast group hosts or multicast routers/switches, instead of flooding traffic to all ports in the subnet (VLAN).

The ECN330-switch not only supports IP multicast filtering by passively monitoring IGMP query, report messages and multicast routing probe messages to register end-stations as multicast group members, but also supports the DVMRP and PIM multicast routing protocols required to forward multicast traffic to other subnets (page 473 and 484).

6.16.1 IGMP Protocol

The Internet Group Management Protocol (IGMP) runs between hosts and their immediately adjacent multicast router/switch. IGMP is a multicast host registration protocol that allows any host to inform its local router that it wants to receive transmissions addressed to a specific multicast group.

A router, or multicast-enabled switch, can periodically ask their hosts if they want to receive multicast traffic. If there is more than one router/switch on the LAN performing IP multicasting, one of these devices is elected "querier" and assumes the role of querying the LAN for group members. It then propagates the service requests on to any adjacent multicast switch/router to ensure that it will continue to receive the multicast service.

Based on the group membership information learned from IGMP, a router/switch can determine which (if any) multicast traffic needs to be forwarded to each of its ports. At Layer 3, multicast routers use this information, along with a multicast routing protocol such as Distance Vector Multicast Routing Protocol (DVMRP) or Protocol Independent Multicasting (PIM), to support IP multicasting across the Internet.

Note that IGMP neither alters nor routes IP multicast packets. A multicast routing protocol must be used to deliver IP multicast packets across different subnetworks. Therefore, when DVMRP or PIM routing is enabled for a subnet on the ECN330-switch, IGMP also needs to be enabled.

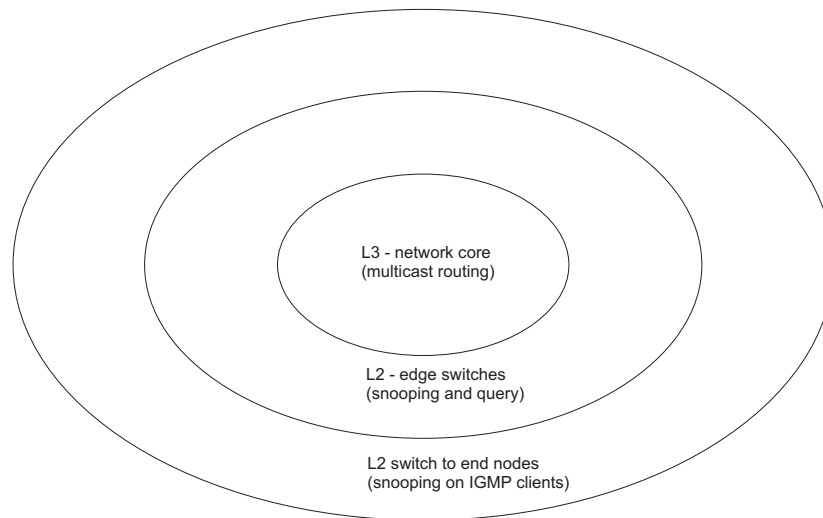


Figure 145 IGMP Protocol

6.16.2 Layer 2 IGMP (Snooping and Query)

IGMP Snooping and Query – If multicast routing is not supported on other switches in the network, use IGMP Snooping and IGMP Query (page 355) to monitor IGMP service requests passing between multicast clients and servers, and dynamically configure the ECN330 ports which need to forward multicast traffic.

Static IGMP Router Interface – If IGMP snooping cannot locate the IGMP querier, manually designate a known IGMP querier (that is, a multicast router/switch) connected over the network to an interface on the ECN330. This interface will then join all the current multicast groups supported by the attached router/switch to ensure that multicast traffic is passed to all appropriate interfaces within the ECN330.

Static IGMP Host Interface – To control multicast applications more carefully, manually assign a multicast service to specific interfaces on the ECN330 (page 361).

IGMP Query (Layer 2 or 3) – IGMP Query can only be enabled globally at Layer 2, but can be enabled for individual VLAN interfaces at Layer 3 (page 362). However, note that Layer 2 query is disabled if Layer 3 query is enabled.

6.16.2.1 Configuring IGMP Snooping and Query Parameters

The ECN330-switch can be configured to forward multicast traffic intelligently. Based on the IGMP query and report messages, the ECN330-switch forwards traffic only to the ports that request multicast traffic. This prevents the ECN330-switch from broadcasting the traffic to all ports and possibly disrupting network performance.

Command Usage

- **IGMP Snooping** – The ECN330-switch can passively snoop on IGMP Query and Report packets transferred between IP multicast routers/switches and IP multicast host groups to identify the IP multicast group members. It simply monitors the IGMP packets passing through it, picks out the group registration information, and configures the multicast filters accordingly.

Note: Unknown multicast traffic is flooded to all ports in the VLAN for several seconds when first received. If a multicast output port exists on the VLAN, the traffic will be filtered by subjecting it to IGMP snooping. If no output port exists on the VLAN, the traffic will simply be dropped.

- **IGMP Querier** – A router, or multicast-enabled switch, can periodically ask their hosts if they want to receive multicast traffic. If there is more than one router/switch on the LAN performing IP multicasting, one of these devices is elected “querier” and assumes the role of querying the LAN for group members. It then propagates the service requests on to any upstream multicast switch/router to ensure that it will continue to receive the multicast service.

Note: Multicast routers use this information, along with a multicast routing protocol such as DVMRP or PIM, to support IP multicasting across the Internet.

Command Attributes

- **IGMP Status** — When enabled, the ECN330-switch will monitor network traffic to determine which hosts want to receive multicast traffic. This is also referred to as IGMP Snooping. (Default: Enabled)
- **Report Suppression** — When enabled, the ECN330-switch forwards only one IGMP report per query to multicast devices, sending only the first report from all hosts within a group. Note that report suppression is not supported when multicast query messages include IGMPv3 reports. (Default: Enabled)

- **Act as IGMP Querier** — When enabled, the ECN330-switch can serve as the Querier, which is responsible for asking hosts if they want to receive multicast traffic. (Default: Disabled)
- **IGMP Query Count** — Sets the maximum number of queries issued for which there has been no response before the ECN330-switch takes action to drop a client from the multicast group. (Range: 1-10, Default: 2)
- **IGMP Query Interval** — Sets the frequency at which the ECN330-switch sends IGMP host-query messages. (Range: 60-125 seconds, Default: 125)
- **IGMP Report Delay** — Sets the time between receiving an IGMP Report for an IP multicast address on a port before the ECN330-switch sends an IGMP Query out of that port and removes the entry from its list. (Range: 1-225 tenths of a second, Default: 100)
- **IGMP Query Timeout** — The time the ECN330-switch waits after the previous querier stops before it considers the router port (the interface which had been receiving query packets) to have expired. (Range: 300-500 seconds, Default: 300)
- **IGMP Version** — Sets the protocol version for compatibility with other devices on the network. This is the IGMP Version the ECN330-switch uses for snooping. (Range: 1-3; Default: 2)

Note: All systems on the subnet must support the same version.

Note: Some attributes are only enabled for IGMPv2 and v3 snooping, including IGMP Report Delay and IGMP Query Timeout.

Note: The current software can snoop on IGMPv3 packets, but cannot generate a source/group (S,G) entry in service requests propagated to upstream multicast routers. It only sends an all-sources/group (*,G) entry, the same as done by IGMPv2. In other words, multicast traffic will be flooded to the required ports according to the group address only, and not according to the source IP address and group address as required by the IGMPv3 standard.

Web – Click IGMP Snooping, IGMP Configuration. Adjust the IGMP settings as required, and then click Apply. (The default settings are shown in Figure 146.)

IGMP Configuration	
IGMP Status	☒ Enabled
Report Suppression	☒ Enabled
Act as IGMP Querier	☐ Enabled
IGMP Query Count (1-10)	2
IGMP Query Interval (60-125)	125 seconds
IGMP Report Delay (1-255)	100 tenths of seconds
IGMP Query Timeout (300-500)	300 seconds
IGMP Version (1,2,3)	2

Figure 146 IGMP Configuration

CLI – This example modifies the settings for multicast filtering, and then displays the current status.

```

Console(config)#ip igmp snooping
Console(config)#ip igmp snooping report-suppression
Console(config)#ip igmp snooping querier
Console(config)#ip igmp snooping query-count 10
Console(config)#ip igmp snooping query-interval 100
Console(config)#ip igmp snooping query-max-response-time 100
Console(config)#ip igmp snooping report suppression
Console(config)#ip igmp snooping router-port-expire-time 300
Console(config)#ip igmp snooping version 2
Console(config)#exit
Console#show ip igmp snooping
Service Status:           Enabled
Report Suppression:       Enabled
Querier Status:           Disabled
Query Count:              2
Query Interval:           125 sec
Query Max Response Time:  100 (tenths of sec)
Router Port Expire Time:  300 sec
IGMP Snooping Version:    Version 2
Console#

```

6.16.2.2 Displaying Interfaces Attached to a Multicast Router

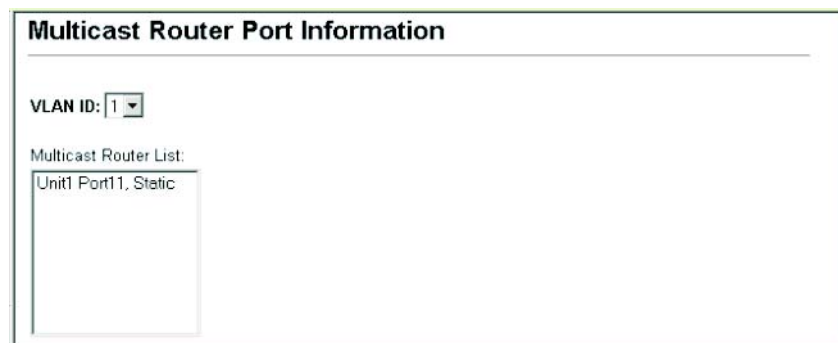
Multicast routers that are attached to ports on the ECN330-switch use information obtained from IGMP, along with a multicast routing protocol such as DVMRP or PIM, to support IP multicasting across the Internet. These routers may be dynamically discovered by the ECN330-switch or statically assigned to an interface on the ECN330-switch.

The Multicast Router Port Information page can be used to display the ports on the ECN330-switch attached to a neighboring multicast router/switch for each VLAN ID.

Command Attributes

- **VLAN ID** – ID of configured VLAN (1-4094).
- **Multicast Router List** – A list of ECN330 ports that are attached to multicast routers. These multicast routers have either been dynamically discovered by the ECN330-switch or have been statically assigned to an interface on the ECN330-switch.

Web – Click IGMP Snooping, Multicast Router Port Information. Select the required VLAN ID from the scroll-down list to display the associated multicast routers.



Multicast Router Port Information

VLAN ID: 1

Multicast Router List:

Unit1 Port11, Static

Figure 147 Multicast Router Port Information

CLI – This example shows that Port 11 has been statically configured as a port attached to a multicast router.

```
Console#show ip igmp snooping mrouter vlan 1
VLAN M'cast Router Port Type
-----
1          Eth 1/11 Static
```

6.16.2.3

Specifying Static Interfaces for a Multicast Router

Depending on network connections, IGMP snooping may not always be able to locate the IGMP querier. Therefore, if the IGMP querier is a known multicast router/ switch connected over the network to an interface (port or trunk) on the ECN330, the interface (and a specified VLAN) can be manually configured to join all the current multicast groups supported by the attached router. This can ensure that multicast traffic is passed to all the appropriate interfaces within the ECN330.

Command Attributes

- **Interface** – Activates the Port or Trunk scroll down list.
- **VLAN ID** – Selects the VLAN to propagate all multicast traffic coming from the attached multicast router.
- **Port or Trunk** – Specifies the interface attached to a multicast router.

Web – Click IGMP Snooping, Static Multicast Router Port Configuration. Specify the interfaces attached to a multicast router, indicate the VLAN which will forward all the corresponding multicast traffic, and then click Add. After adding interfaces to the list, click Apply.

Static Multicast Router Port Configuration

Current: Vlan1, Unit1 Port11

New:

Interface: Port

VLAN ID: 1

Port: 1

Trunk: ☐

<<Add Remove

Figure 148 Static Multicast Router Port Configuration

CLI – This example configures port 11 as a multicast router port within VLAN 1.

```
Console(config)#ip igmp snooping vlan 1 mrouter ethernet 1/11
Console(config)#exit
Console#show ip igmp snooping mrouter vlan 1
  VLAN M'cast Router Port Type
  ----
      1          Eth 1/11  Static
```

6.16.2.4 Displaying Port Members of Multicast Services

The port members associated with a specified VLAN and multicast service can be displayed.

Command Attribute

- **VLAN ID** – Selects the VLAN for which to display port members.
- **Multicast IP Address** – The IP address for a specific multicast service.
- **Multicast Group Port List** – Shows the interfaces that have already been assigned to the selected VLAN to propagate a specific multicast service.

Web – Click IGMP Snooping, IP Multicast Registration Table. Select a VLAN ID and the IP address for a multicast service from the scroll-down lists. The ECN330-switch will display all the interfaces that are propagating this multicast service.

IP Multicast Registration Table

VLAN ID:

Multicast IP Address:

Multicast Group Port List:

Unit1 Port1, User

Figure 149 IP Multicast Registration Table

CLI – This example displays all the known multicast services supported on VLAN 1, along with the ports propagating the corresponding services. The Type field shows if this entry was learned dynamically or was statically configured.

```

Console#show bridge 1 multicast vlan 1
VLAN M'cast IP addr. Member ports Type
-----
      1      224.1.1.12      Eth1/12      USER
      1      224.1.2.3       Eth1/12      IGMP
Console#

```

6.16.2.5 Assigning Ports to Multicast Services

Multicast filtering can be dynamically configured using IGMP Snooping and IGMP Query messages as described in 6.16.2.1 "Configuring IGMP Snooping and Query Parameters" 355. For certain applications that require tighter control, it may be necessary to statically configure a multicast service on the ECN330-switch. First add all the ports attached to participating hosts to a common VLAN, and then assign the multicast service to that VLAN group.

Command Usage

- Static multicast addresses are never aged out.
- When a multicast address is assigned to an interface in a specific VLAN, the corresponding traffic can only be forwarded to ports within that VLAN.

Command Attributes

- **Interface** – Activates the Port or Trunk scroll down list.
- **VLAN ID** – Selects the VLAN to propagate all multicast traffic coming from the attached multicast router.
- **Multicast IP** – The IP address for a specific multicast service
- **Port or Trunk** – Specifies the interface attached to a multicast router.

Web – Click IGMP Snooping, IGMP Member Port Table. Specify the interface attached to a multicast service (through an IGMP-enabled switch or multicast router), indicate the VLAN that will propagate the multicast service, specify the multicast IP address, and click Add. After adding ports to the member list, click Apply.

Figure 150 IGMP Member Port Table

CLI – This example assigns a multicast address to VLAN 1, and then displays all the known multicast services supported on VLAN 1.

```
Console(config)#ip igmp snooping vlan 1 static 224.1.1.12
                  ethernet 1/12
Console(config)#exit
Console#show mac-address-table multicast vlan 1
VLAN M'cast IP addr. Member ports Type
-----
1      224.1.1.12      Eth1/12      USER
1      224.1.2.3       Eth1/12      IGMP
Console#
```

6.16.2.6 Setting IGMP Snooping Status per Interface

IGMP Snooping status can be configured both globally for the ECN330-switch or per VLAN interface. To configure snooping globally, use the IGMP Configuration screen as described on page 355.

Command Usage

- When IGMP snooping is enabled globally, the per VLAN interface settings for IGMP snooping take precedence.

- When IGMP snooping is disabled globally, snooping can still be configured per VLAN interface, but the interface settings will not take effect until snooping is re-enabled globally.

Command Attributes

- **Enabled VLAN** – Displays the list of VLAN interfaces for which IGMP Snooping has been enabled.
- **VLAN ID** – ID of configured VLANs.

Web – Click IGMP Snooping, IGMP Snooping Status per VLAN. Use the Add or Remove buttons to edit the entries displayed in the list of enabled VLANs, and then click Apply.

Figure 151 IGMP Snooping Status per VLAN

CLI – This example enables IGMP snooping on VLAN 1.

```
Console(config)#interface vlan 1
Console(config-if)#ip igmp snooping
Console(config-if)#
```

6.16.3 Layer 3 IGMP (Query used with Multicast Routing)

IGMP Snooping – IGMP Snooping is a Layer 2 function (page 355) that can be used to provide multicast filtering when no other switches in the network support multicast routing. (Note that IGMP Snooping can only be globally enabled.)

IGMP Query – Multicast query is used to poll each known multicast group for active members, and dynamically configure the ECN330 ports which need to forward multicast traffic. Although the implementation differs slightly, IGMP Query is used in conjunction with both Layer 2 IGMP Snooping and multicast routing. Note that when using IGMP Snooping, multicast query is automatically enabled. (See 6.16.2.1 "Configuring IGMP Snooping and Query Parameters" 355.)

Layer 3 IGMP – This protocol includes a form of multicast query specifically designed to work with multicast routing. A router periodically asks its hosts if they want to receive multicast traffic. It then propagates service requests on to any upstream multicast router to ensure that it will continue to receive the multicast service. Layer 3 IGMP can be enabled for individual VLAN interfaces (page 362). (Note that Layer 2 snooping and query is disabled if Layer 3 IGMP is enabled.)

6.16.3.1 Configuring IGMP Interface Parameters

The ECN330-switch uses IGMP (Internet Group Management Protocol) to query for any attached hosts that want to receive a specific multicast service. The hosts may respond with several types of IP multicast messages. Hosts respond to queries with report messages that indicate which groups they want to join or the groups to which they already belong. If a router does not receive a report message within a specified period of time, it will prune that interface from the multicast tree. A host can also submit a join message at any time without waiting for a query from the router. Host can also signal when they no longer want to receive traffic for a specific group by sending a leave-group message.

These IGMP messages are used by the router to identify ports containing multicast hosts and to restrict the downstream flow of multicast data to only these ports. If more than one router on the LAN is performing IP multicasting, one of these is elected as the "querier" and assumes the role of querying for group members. It then propagates the service request up to any neighboring multicast router to ensure that it will continue to receive the multicast service. The following parameters are used to control Layer 3 IGMP and query functions.

Command Attributes

- **VLAN** (Interface) – VLAN interface bound to a primary IP address. (Range: 1-4094)
- **IGMP Protocol Status** (Admin Status) – Enables IGMP on a VLAN interface. (Default: Disabled)
- **Last Member Query Interval** – A multicast client sends an IGMP leave message when it leaves a group. The router then checks to see if this was the last host in the group by sending an IGMP query and starting a timer based on this command. If no reports are received before the timer expires, the group is deleted. (Range: 0-25 seconds; Default: 1 second)
 - This value may be tuned to modify the leave latency of the network. A reduced value results in reduced time to detect the loss of the last member of a group.
- **Max Query Response Time** – Configures the maximum response time advertised in IGMP queries. (Range: 0-25 seconds; Default: 10 seconds)
 - The ECN330-switch must be using IGMPv2 for this command to take effect.
 - This command defines how long any responder (that is, client or router) still in the group has to respond to a query message before the router deletes the group.
 - By varying the Maximum Query Response Time, the burstiness of IGMP messages passed on the subnet can be tuned; where larger values make the traffic less bursty, as host responses are spread out over a larger interval.
 - The number of seconds represented by the maximum response interval must be less than the Query Interval.
- **Query Interval** – Configures the frequency at which host query messages are sent. (Range: 1-255; Default: 125 seconds)
 - Multicast routers send host query messages to determine the interfaces that are connected to downstream hosts requesting a specific multicast service. Only the designated multicast router for a subnet sends host query messages, which are addressed to the multicast address 224.0.0.1.

- For IGMP Version 1, the designated router is elected according to the multicast routing protocol that runs on the LAN. But for IGMP Version 2, the designated querier is the lowest IP-addressed multicast router on the subnet.
- **Robustness Variable** – Specifies the robustness (that is, expected packet loss) for this interface. The robustness value is used in calculating the appropriate range for other IGMP variables, such as the Last Member Query Interval (Group Membership Interval), as well as the Other Querier Present Interval, and the Startup Query Count (RFC 2236). (Range: 1-255; Default: 2)
- **Version** – Configures the IGMP version used on an interface. (Options: Version 1-2; Default: Version 2)
 - All routers on the subnet must support the same version. However, the multicast hosts on the subnet may support IGMP version 1 or 2.
 - The ECN330-switch must be set to version 2 to enable the Max Query Response Time.
- **Querier** – Device currently serving as the IGMP querier for this multicast service.

Web – Click IP, IGMP, Interface Settings. Specify each interface that will support IGMP (Layer 3), specify the IGMP parameters for each interface, then click Apply.

IGMP Interface Information

Interface	Admin Status	Version	Robustness Variable	Query Interval	Max Query Response Time	Last Member Query Interval	Querier	Configure
VLAN2	Enabled	2	2	125	10	1	10.1.0.253	Configure
VLAN3	Enabled	2	2	125	10	1	10.1.5.253	Configure

Entry Count: 2

IGMP Interface Settings

VLAN: 2

IGMP Protocol Status	Enabled	Query Interval (seconds)	125
Last Member Query Interval (0 - 25 seconds)	1	Robustness Variable (1 - 255)	2
Max Query Response Time (0 - 25 seconds)	10	Version	2

Figure 152 IGMP Interface Settings

CLI – This example configures the IGMP parameters for VLAN 1.

```

Console(config)#interface vlan 1
Console(config-if)#ip igmp
Console(config-if)#ip igmp last-memb-query-interval 10
Console(config-if)#ip igmp max-resp-interval 20
Console(config-if)#ip igmp query-interval 100
Console(config-if)#ip igmp robustval 3
Console(config-if)#ip igmp version 1
Console(config-if)#end
Console#show ip igmp interface vlan 1
Vlan 1 is up
  IGMP is enable, version is 2
  Robustness variable is 2
  Query interval is 125 sec
  Query Max Response Time is 10 sec, Last Member Query Interval is 1 sec
  Querier is 10.1.0.253
Console#

```

6.16.3.2 Displaying Multicast Group Information

When IGMP (Layer 3) is enabled on the ECN330-switch the current multicast groups learned through IGMP can be displayed in the IP/IGMP/Group Information page. When IGMP (Layer 3) is disabled and IGMP (Layer 2) is enabled, the active multicast groups can be viewed in the IGMP Snooping/IP Multicast Registration Table (see page 360).

Command Usage

To display information about multicast groups, IGMP must first be enabled on the interface to which a group has been assigned (see “Configuring IGMP Interface Parameters” on page 364), and multicast routing must be enabled globally on the system (see “Configuring Global Settings for Multicast Routing” on page 469).

Command Attributes

- **Group Address** – IP multicast group address with subscribers directly attached or downstream from the ECN330-switch.
- **Interface** – The interface on the ECN330-switch that has received traffic directed to the multicast group address.
- **Last Reporter** – The IP address of the source of the last membership report received for this multicast group address on this interface. If no membership report has been received, this object has the value 0.0.0.0.
- **Up time** – The time elapsed since this entry was created.
- **Expire** – The time remaining before this entry will be aged out. (Default: 260 seconds)
- **V1 Timer** – The time remaining until the ECN330-switch assumes that there are no longer any IGMP Version 1 members on the IP subnet attached to this interface. (Default: 400 seconds)
 - If the ECN330-switch receives an IGMP Version 1 Membership Report, it sets a timer to note that there are Version 1 hosts present which are members of the group for which it heard the report.
 - If there are Version 1 hosts present for a particular group, the ECN330-switch will ignore any Leave Group messages that it receives for that group.

Web – Click IP, IGMP, IGMP Group Membership.

IGMP Group Membership					
Group Address	Interface	Last Reporter	Up time	Expire	V1 Timer
234.5.6.7	VLAN2	10.1.0.19	6077	209	0
234.5.6.8	VLAN3	10.1.5.19	6067	226	0

Entry Count: 2

Figure 153 IGMP Group Membership

CLI – The following shows the IGMP groups currently active on VLAN 1.

```
Console#show ip igmp groups vlan 1
```

GroupAddress	InterfaceVlan	Lastreporter	Uptime	Expire	V1Timer
234.5.6.8	1	10.1.5.19	7068	220	0

```
Console#
```

6.17 Configuring Domain Name Service

The Domain Naming System (DNS) service on the ECN330-switch allows host names to be mapped to IP addresses using static table entries or by redirection to other name servers on the network. When a client device designates the ECN330-switch as a DNS server, the client will attempt to resolve host names into IP addresses by forwarding DNS queries to the ECN330-switch, and waiting for a response.

The DNS table allows entries to be manually configured for mapping domain names to IP addresses, default domain names configured, and one or more name servers specified for domain name to address translation.

6.17.1 Configuring General DNS Server Parameters

Command Usage

- To enable DNS service on the ECN330-switch, first configure one or more name servers, and then enable domain lookup status.
- To append domain names to incomplete host names received from a DNS client (that is, not formatted with dotted notation), specify a default domain name or a list of domain names to be tried in sequential order.
- If there is no domain list, the default domain name is used. If there is a domain list, the default domain name is not used.
- When an incomplete host name is received by the DNS server on the ECN330-switch and a domain name list has been specified, the ECN330-switch will work through the domain list, appending each domain name in the list to the host name, and checking with the specified name servers for a match.
- When more than one name server is specified, the servers are queried in the specified sequence until a response is received, or the end of the list is reached with no response.
- Note that if all name servers are deleted, DNS will automatically be disabled.

Command Attributes

- **Domain Lookup Status** – Enables DNS host name-to-address translation.
- **Default Domain Name** – Defines the default domain name appended to incomplete host names. (Range: 1-64 alphanumeric characters)
- **Domain Name List** – Defines define a list of domain names that can be appended to incomplete host names. (Range: 1-64 alphanumeric characters. 1-5 names)
- **Name Server List** – Specifies the address of one or more domain name servers to use for name-to-address resolution. (Range: 1-6 IP addresses)

Note: When specifying names, do not include the initial dot that separates the host name from the domain name.

Web – Select DNS, General Configuration. Set the default domain name or list of domain names, specify one or more name servers to use to use for address resolution, enable domain lookup status, and click Apply.

The screenshot shows the 'General Configuration' page for DNS. It includes the following sections:

- Domain Lookup Status:** A checkbox labeled 'Enable' is checked.
- Default Domain Name:** A text input field containing 'sample.com'.
- Domain Name List:**
 - Current:** A list box containing 'sample.com.uk' and 'sample.com.jp'.
 - New:** A section with a '<< Add' button, a 'Domain Name' text input field, and a 'Remove' button.
- Name Server List:**
 - Current:** A list box containing '192.168.1.55' and '10.1.0.55'.
 - New:** A section with a '<< Add' button, a 'Name Server IP' text input field, and a 'Remove' button.

Figure 154 DNS General Configuration

CLI - This example sets a default domain name and a domain list. However, remember that if a domain list is specified, the default domain name is not used.

```

Console(config)#ip domain-name sample.com
Console(config)#ip domain-list sample.com.uk
Console(config)#ip domain-list sample.com.jp
Console(config)#ip domain-server 192.168.1.55 10.1.0.55
Console(config)#ip domain-lookup
Console#show dns
Domain Lookup Status:
    DNS enabled
Default Domain Name:
    .sample.com
Domain Name List:
    .sample.com.uk
    .sample.com.jp
Name Server List:
    192.168.1.55
    10.1.0.55
Console#

```

6.17.2 Configuring Static DNS Host to Address Entries

Static entries can be manually configured in the DNS table that are used to map domain names to IP addresses.

Command Usage

- Static entries may be used for local devices connected directly to the attached network, or for commonly used resources located elsewhere on the network.
- Servers or other network devices may support one or more connections through multiple IP addresses. If more than one IP address is associated with a host name in the static table or through information returned from a name server, a DNS client can try each address in succession, until it establishes a connection with the target device.

Field Attributes

- **Host Name** – Name of a host device that is mapped to one or more IP addresses. (Range: 1-64 characters)
- **IP Address** – Internet address(es) associated with a host name. (Range: 1-8 addresses)

- **Alias** – Displays the host names that are mapped to the same address(es) as a previously configured entry.

Web – Select DNS, Static Host Table. Enter a host name and one or more corresponding addresses, then click Apply.

Host Name	IP Address	Alias		
rd5	10.1.0.55	rd6	Delete	Edit
	192.168.1.55			

Clear

Add Static Host:

Host Name

IP Address 1

IP Address 2

IP Address 3

IP Address 4

IP Address 5

IP Address 6

IP Address 7

IP Address 8

Add

Figure 155 DNS Static Host Table

CLI - This example maps two address to a host name, and then configures an alias host name for the same addresses.

```
Console(config)#ip host rd5 192.168.1.55 10.1.0.55
Console(config)#ip host rd6 10.1.0.55
Console#show host

Hostname
  rd5
Inet address
  10.1.0.55 192.168.1.55
Alias
  1.rd6
```

6.17.3 Displaying the DNS Cache

Entries in the DNS cache can be displayed that have been learned through the designated name servers.

Field Attributes

- **No** – The entry number for each resource record.
- **Flag** – The flag is always “4” indicating a cache entry and therefore unreliable.
- **Type** – This field includes CNAME which specifies the canonical or primary name for the owner, and ALIAS which specifies multiple domain names which are mapped to the same IP address as an existing entry.
- **IP** – The IP address associated with this record.
- **TTL** – The time to live reported by the name server.
- **Domain** – The domain name associated with this record.

Web – Select DNS, Cache.

Cache					
No	Flag	Type	IP	TTL	Domain
0	4	CNAME	207.46.134.222	51	www.microsoft.akadns.net
1	4	CNAME	207.46.134.190	51	www.microsoft.akadns.net
2	4	CNAME	207.46.134.155	51	www.microsoft.akadns.net
3	4	CNAME	207.46.249.222	51	www.microsoft.akadns.net
4	4	CNAME	207.46.249.27	51	www.microsoft.akadns.net
5	4	ALIAS	POINTER TO:4	51	www.microsoft.com
6	4	CNAME	207.46.68.27	71964	msn.com.tw
7	4	ALIAS	POINTER TO:6	71964	www.msn.com.tw
8	4	CNAME	65.54.131.192	605	passportimages.com
9	4	ALIAS	POINTER TO:8	605	www.passportimages.com
10	4	CNAME	165.193.72.190	87	global.msads.net

Figure 156 DNS Cache

CLI - This example displays all the resource records learned from the designated name servers.

```

Console#show dns cache
NO      FLAG    TYPE      IP            TTL      DOMAIN
0       4       CNAME     207.46.134.222 51       www.microsoft.akadns.net
1       4       CNAME     207.46.134.190 51       www.microsoft.akadns.net
2       4       CNAME     207.46.134.155 51       www.microsoft.akadns.net
3       4       CNAME     207.46.249.222 51       www.microsoft.akadns.net
4       4       CNAME     207.46.249.27  51       www.microsoft.akadns.net
5       4       ALIAS     POINTER TO:4   51       www.microsoft.com
6       4       CNAME     207.46.68.27  71964    msn.com.tw
7       4       ALIAS     POINTER TO:6   71964    www.msn.com.tw
8       4       CNAME     65.54.131.192 605      passportimages.com
9       4       ALIAS     POINTER TO:8   605      www.passportimages.com
10      4       CNAME     165.193.72.190 87       global.msads.net
Console#

```

6.18 Dynamic Host Configuration Protocol

Dynamic Host Configuration Protocol (DHCP) can dynamically allocate an IP address and other configuration information to network clients when they boot up. If a subnet does not already include a BOOTP or DHCP server, DHCP client requests can be relayed to a DHCP server on another subnet, or the DHCP server can be configured on the ECN330-switch to support that subnet.

When configuring the DHCP server on the ECN330-switch, an address pool can be configured for each unique IP interface, or a static IP address manually assigned to clients based on their hardware address or client identifier. The DHCP server can provide the host's IP address, domain name, gateway router and DNS server, information about the host's boot image including the TFTP server to access for download and the name of the boot file, or boot information for NetBIOS Windows Internet Naming Service (WINS).

6.18.1 Configuring DHCP Relay Service

The ECN330-switch supports DHCP relay service for attached host devices. If DHCP relay is enabled, and the ECN330-switch sees a DHCP request broadcast, it inserts its own IP address into the request so that the DHCP server will know the subnet where the client is located. Then, the ECN330-switch forwards the packet to the DHCP server. When the server receives the DHCP request, it allocates a free IP address for the DHCP client from its defined scope for the DHCP client's subnet, and sends a DHCP response back to the DHCP relay agent (that is, the ECN330-switch). The ECN330-switch then broadcasts the DHCP response received from the server to the client.

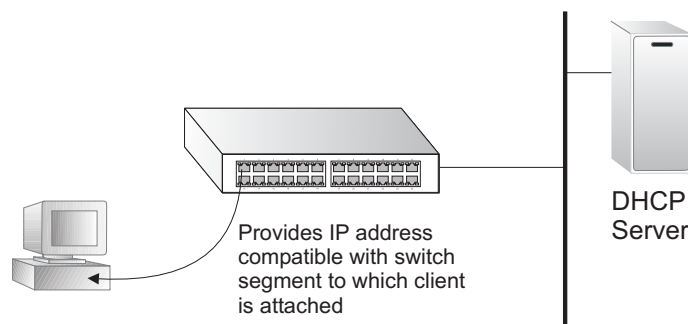


Figure 157 DHCP Relay Service

Command Usage

The IP address for at least one DHCP server must be specified. Otherwise, the ECN330-switch's DHCP relay agent will not forward client requests to a DHCP server.

Command Attributes

- **VLAN ID** – ID of configured VLAN.
- **VLAN Name** – Name of the VLAN.
- **Server IP Address** – Addresses of DHCP servers to be used by the ECN330-switch's DHCP relay agent in order of preference.
- **Restart DHCP Relay** – Use this button to enable or re-initialize DHCP relay service.

Web – Click DHCP, Relay Configuration. Enter up to five IP addresses for any VLAN, then click Restart DHCP Relay to start the relay service.

Relay Configuration

Note: DHCP relay configuration will be disabled if an active DHCP server is detected on the same network segment.

VLAN ID	VLAN Name	Server IP Address				
1	DefaultVlan	10.1.0.99	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0
246	extmgm	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0
248	dynvlan	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0
4093	intuntag	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0

Restart DHCP Relay

Figure 158 DHCP Relay Configuration

CLI – This example specifies one DHCP relay server for VLAN 1, and enables the relay service.

```
Console(config)#interface vlan 1
Console(config-if)#dhcp relay server 10.1.0.99
Console(config-if)#ip dhcp relay
Console(config-if)#
```

6.18.2 Configuring the DHCP Server

The ECN330-switch includes a Dynamic Host Configuration Protocol (DHCP) server that can assign temporary IP addresses to any attached host requesting service. It can also provide other network settings such as the domain name, default gateway, Domain Name Servers (DNS), Windows Internet Naming Service (WINS) name servers, or information on the bootup file for the host device to download.

Addresses can be assigned to clients from a common address pool configured for a specific IP interface on the ECN330-switch, or fixed addresses can be assigned to hosts based on the client identifier code or MAC address.

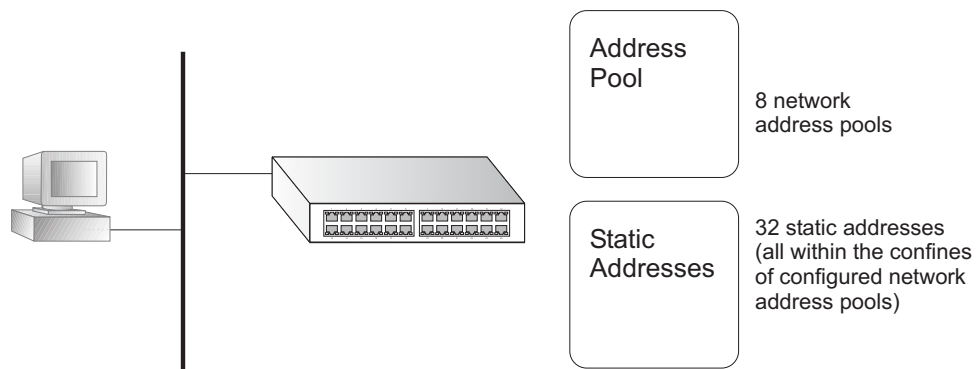


Figure 159 DHCP Server

Command Usage

- First configure any excluded addresses, including the address for the ECN330-switch.
- Then configure address pools for the network interfaces. Up to 8 network address pools can be configured. An address can also be

manually bound to a specific client if required. However, any fixed addresses must fall within the range of an existing network address pool. Up to 32 fixed host addresses (that is, entering one address per pool) can be configured.

- If the DHCP server is running, it must be disabled and then reenabled to implement any configuration changes. This can be done on the DHCP, Server, General page.

6.18.2.1 Enabling the Server, Setting Excluded Addresses

Enable the DHCP Server and specify the IP addresses that it should not be assigned to clients.

Command Attributes

- **DHCP Server** – Enables or disables the DHCP server on the ECN330-switch. (Default: Disabled)
- **Excluded Addresses** – Specifies IP addresses that the DHCP server should not assign to DHCP clients. A single address or an address range can be specified.
- **New (Excluded Addresses)** – New entries for excluded addresses can be specified as a single address or an address range.

Note: Be sure to exclude the address for the ECN330-switch and other key network devices.

Web – Click DHCP, Server, General. Enter a single address or an address range, and click Add.

Figure 160 DHCP Server General Configuration

CLI – This example enables the DHCP and sets an excluded address range.

```
Console(config)#service dhcp
Console(config)#ip dhcp excluded-address 10.1.0.250 10.1.0.254
Console#
```

6.18.2.2 Configuring Address Pools

IP address pools must be configured for each IP interface that will provide addresses to attached clients through the DHCP server.

Command Usage

- First configure address pools for the network interfaces. Then manually bind an address to a specific client if required. However, note that any static host address must fall within the range of an existing network address pool. Up to 8 network address pools and up to 32 manually

bound host address pools (that is, one address per host pool) can be configured.

- When a client request is received, the ECN330-switch first checks for a network address pool matching the gateway where the request originated (that is, if the request was forwarded by a relay server). If there is no gateway in the client request (that is, the request was not forwarded by a relay server), the ECN330-switch searches for a network pool matching the interface through which the client request was received. It then searches for a manually configured host address that falls within the matching network pool. If no manually configured host address is found, it assigns an address from the matching network address pool. However, if no matching address pool is found the request is ignored.
- When searching for a manual binding, the ECN330-switch compares the client identifier and then the hardware address for DHCP clients. Since BOOTP clients cannot transmit a client identifier, a hardware address must be configured for this host type. If no manual binding has been specified for a host entry with a hardware address or client identifier, the ECN330-switch will assign an address from the first matching network pool.
- If the subnet mask is not specified for network or host address pools, the class A, B, or C natural mask is used (see page 428). The DHCP server assumes that all host addresses are available. Subsets of the address space can be excluded by using the IP Excluded Address field on the DHCP Server General configuration page.

Command Attributes

Creating a New Address Pool

- **Pool Name** – A string or integer. (Range: 1-8 characters)

Setting the Network Parameters

- **IP** – The IP address of the DHCP address pool.
- **Subnet Mask** – The bit combination that identifies the network (or subnet) and the host portion of the DHCP address pool.

Setting the Host Parameters

- **IP** – The IP address of the DHCP address pool.
- **Subnet Mask** – Specifies the network mask of the client.
- **Hardware Address** – Specifies the MAC address and protocol used on the client. (Options: Ethernet, IEEE802, FDDI; Default: Ethernet)
- **Client-Identifier** – A unique designation for the client device, either a text string (1-15 characters) or hexadecimal value.

Setting the Optional Parameters

- **Default Router** – The IP address of the primary and alternate gateway router. The IP address of the router should be on the same subnet as the client.
- **DNS Server** – The IP address of the primary and alternate DNS server. DNS servers must be configured for a DHCP client to map host names to IP addresses.
- **Netbios Server** – IP address of the primary and alternate NetBIOS Windows Internet Naming Service (WINS) name server used for Microsoft DHCP clients.
- **Netbios Type** – NetBIOS node type for Microsoft DHCP clients. (Options: Broadcast, Hybrid, Mixed, Peer to Peer; Default: Hybrid)
- **Domain Name** – The domain name of the client. (Range: 1-32 characters)
- **Bootfile** – The default boot image for a DHCP client. This file should be placed on the File Transfer Protocol (TFTP) server specified as the Next Server.
- **Next Server** – The IP address of the next server in the boot process, which is typically a File Transfer Protocol (TFTP) server.
- **Lease Time** – The duration that an IP address is assigned to a DHCP client. (Options: fixed period, Infinite; Default: 1 day)

Examples

Creating a New Address Pool

Web – Click DHCP, Server, Pool Configuration. Specify a pool name, then click Add.

Pool Configuration

Pool Name:

Pool Name	Type	IP	Mask	Configure	Delete
tps	Network	10.1.0.0	255.255.255.0	Configure	Delete

Entry Count: 1

Figure 161 DHCP Server Pool Configuration

CLI – This example adds an address pool and enters DHCP pool configuration mode.

```
Console(config)#ip dhcp pool mgr
Console(config-dhcp)#
```

Configuring a Network Address Pool

Web – Click DHCP, Server, Pool Configuration. Click the Configure button for any entry. Click the radio button for “Network.” Enter the IP address and subnet mask for the network pool. Configure the optional parameters such as gateway server and DNS server. Then click Apply.

Pool Name : tps >> [Go back to Pool Configure](#)

☒ Network ☐ Host

IP: 10.1.0.0
Subnet Mask: 255.255.255.0

IP:
Subnet Mask:
Hardware Address: Ethernet
Client-Identifier: Hex

<<Option>>

Default Router: 10.1.0.253
DNS Server: 10.2.3.4
Netbios Server: 10.1.0.33
Netbios type: Hybrid
Domain Name: example.com
Bootfile: wme.bat
Next Server: 10.1.0.21
Lease time: ☐ day hour min
☒ Infinite

Figure 162 DHCP Server Pool - Network Configuration

CLI – This example configures a network address pool.

```
Console(config)#ip dhcp pool tps
Console(config-dhcp)#network 10.1.0.0 255.255.255.0
Console(config-dhcp)#default-router 10.1.0.253
Console(config-dhcp)#dns-server 10.2.3.4
Console(config-dhcp)#netbios-name-server 10.1.0.33
Console(config-dhcp)#netbios-node-type hybrid
Console(config-dhcp)#domain-name example.com
Console(config-dhcp)#bootfile wme.bat
Console(config-dhcp)#next-server 10.1.0.21
Console(config-dhcp)#lease infinite
Console(config-dhcp)#
```

Configuring a Host Address Pool

Web – Click DHCP, Server, Pool Configuration. Click the Configure button for any entry. Click the radio button for “Host.” Enter the IP address, subnet mask, and hardware address for the client device. Configure the optional parameters such as gateway server and DNS server. Then click Apply.

Pool Name : mgr >> [Go back to Pool Configure](#)

☐ Network ☒ Host

IP:
 Subnet Mask:

IP:
 Subnet Mask:
 Hardware Address:
 Address Type:
 Client-Identifier:

<<Option>>

Default Router: Default Router2: (optional)
 DNS Server: DNS Server2: (optional)
 Netbios Server: Netbios Server2: (optional)
 Netbios type:
 Domain Name:
 Bootfile:
 Next Server:
 Lease time: ☐ day hour min
☒ Infinite

Figure 163 DHCP Server Pool - Host Configuration

CLI – This example configures a host address pool.

```
Console(config)#ip dhcp pool mgr
Console(config-dhcp)#host 10.1.0.19 255.255.255.0
Console(config-dhcp)#hardware-address 00-e0-29-94-34-28 ethernet
Console(config-dhcp)#client-identifier text bear
Console(config-dhcp)#default-router 10.1.0.253
Console(config-dhcp)#dns-server 10.2.3.4
Console(config-dhcp)#netbios-name-server 10.1.0.33
Console(config-dhcp)#netbios-node-type hybrid
Console(config-dhcp)#domain-name example.com
Console(config-dhcp)#bootfile wme.bat
Console(config-dhcp)#next-server 10.1.0.21
Console(config-dhcp)#lease infinite
Console(config-dhcp)#
```

6.18.2.3 Displaying Address Bindings

The host devices that have acquired an IP address from the ECN330-switch's DHCP server can be displayed.

Command Attributes

- **IP Address** – IP address assigned to host.
- **Mac Address** – MAC address of host.
- **Lease time** – Duration that this IP address can be used by the host.
- **Start time** – Time this address was assigned by the ECN330-switch.
- **Delete** – Clears this binding to the host. This command is normally used after modifying the address pool, or after moving DHCP service to another device.
- **Entry Count** – Number of hosts that have been given addresses by the ECN330-switch.

Note: More than one DHCP server may respond to a service request by a host. In this case, the host generally accepts the first address assigned by any DHCP server.

Web – Click DHCP, Server, IP Binding. Use the Delete button to clear an address from the DHCP server's database.

IP Binding

IP Address	Mac Address	Lease time	Start time	Delete
10.1.0.20	00-00-E8-98-73-21	2147483647	63829031	Delete

Entry Count: 1

Figure 164 DHCP Server - IP Binding

CLI – This example displays the current binding, and then clears all automatic binding.

```

Console#show ip dhcp binding

      IP                MAC                Lease Time      Start
-----
10.1.0.20 00-00-e8-98-73-21      86400 Dec 25 08:01:57 2002
Console#clear ip dhcp binding *
Console#

```

6.19 Configuring Router Redundancy

Router redundancy protocols use a virtual IP address to support a primary router and multiple backup routers. The backup routers can be configured to take over the workload if the master router fails, or can also be configured to share the traffic load. The primary goal of router redundancy is to allow a host device, which has been configured with a fixed gateway, to maintain network connectivity in case the primary gateway goes down.

The ECN330-switch supports the Virtual Router Redundancy Protocol (VRRP). VRRP requires the interface of one of the routers participating in the virtual group to be specified as the address for the master virtual router. The protocol then selects the backup routers based on the specified virtual router priority.

Router redundancy can be set up in any of the following configurations. The following examples show configuration settings for VRRP.

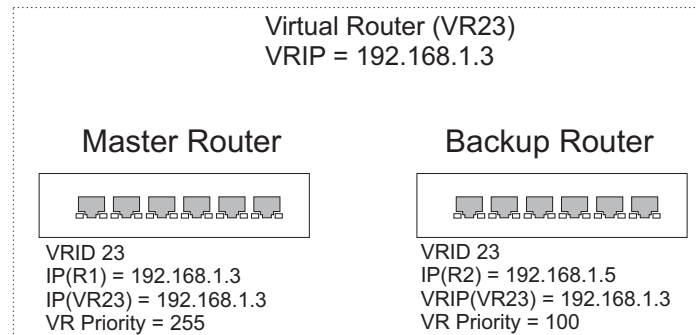


Figure 165 Master Virtual Router with Backup Routers

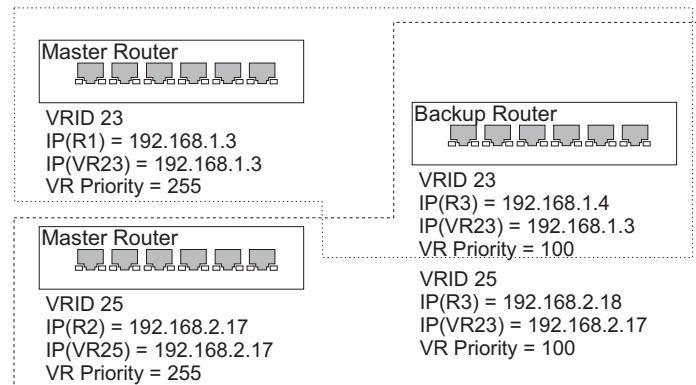


Figure 166 Several Virtual Master Routers Using Backup Routers

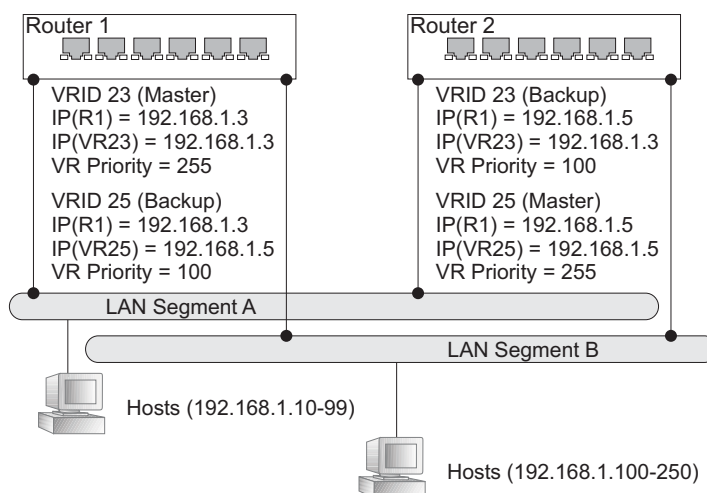


Figure 167 Several Virtual Master Routers Configured for Mutual Backup and Load Sharing

Note: Load sharing can be accomplished by assigning a subset of addresses to different host address pools using the DHCP server. (See “Configuring Address Pools” on page 380.

6.19.1 Virtual Router Redundancy Protocol

Virtual Router Redundancy Protocol (VRRP) allows a group of routers to be configured as a single virtual router. The virtual router group is configured with a single virtual IP address that can be used as the default gateway for host devices on the attached network.

6.19.1.1 Configuring VRRP Groups

To configure VRRP, select an interface on one router in the group to serve as the master virtual router. This physical interface is used as the virtual address for the router group. Now set the same virtual address and a priority on the backup routers, and configure an authentication string. The preempt feature can also be enabled, which allows a router to take over as the master router when it comes on line.

Command Usage

Address Assignment

- The IP address assigned to the virtual router must already be configured on the router that will be the Owner. In other words, the IP address for the virtual router exists on one, and only one, router in the virtual router group, and the network mask for the virtual router address is derived from the Owner. The Owner will also assume the role of the Master virtual router in the group.
- The interfaces of all routers participating in a virtual router group must be within the same IP subnet.
- VRRP creates a virtual MAC address for the master router based on a standard prefix, with the last octet equal to the group ID. When a backup router takes over as the master, it continues to forward traffic addressed to this virtual MAC address. However, the backup router cannot reply to ICMP pings sent to addresses associated with the virtual group because the IP address owner is off line.

Virtual Router Priority

- The Owner of the virtual IP address is automatically assigned the highest possible virtual router priority of 255. The backup router with the highest priority will become the master router if the current master fails. However, because the priority of the virtual IP address Owner is the highest, the original master router will always become the active master router when it recovers.
- If two or more routers are configured with the same VRRP priority, the router with the higher IP address is elected as the new master router if the current master fails.

Preempting the Acting Master

- The virtual IP Owner has the highest priority, so no other router can preempt it, and it will always resume control as the master virtual router when it comes back on line. The preempt function only allows a backup router to take over from another backup router that is temporarily acting as the group master. If preemption is enabled and this router has a higher priority than the current acting master when it comes on line, it will take over as the acting group master.

- A delay to the preempt function can be configured to give additional time to receive an advertisement message from the current master before taking control. If the router attempting to become the master has just come on line, this delay also gives it time to gather information for its routing table before actually preempting the currently active master router.

Field Attributes (VRRP Group Configuration)

- **VLAN ID** – ID of a VLAN configured with an IP interface. (Range: 1-4094; Default: 1)
- **VRID** – VRRP group identifier. (Range: 1-255)
- **State** – VRRP router role. (Values: Master, Backup)
- **Virtual Address** – Virtual IP address for this group.
- **Interval** – Interval at which the master virtual router sends advertisements communicating its state as the master.
- **Preemption** – Shows if this router is allowed to preempt the acting master.
- **Priority** – Priority of this router in the VRRP group.
- **AuthType** – Authentication mode used to verify VRRP packets from other routers.

Command Attributes (VRRP Group Configuration Detail)

- **Associated IP Table** – IP interfaces associated with this virtual router group.
- **Associated IP** – IP address of the virtual router. If this address matches a real interface on the ECN330-switch, then this interface will become the virtual master router for this VRRP group.
- **Advertisement Interval** – Interval at which the master virtual router sends advertisements communicating its state as the master. (Range: 1-255 seconds; Default: 1 second)
 - VRRP advertisements from the current master virtual router include information about its priority and current state as the master.
 - VRRP advertisements are sent to the multicast address 224.0.0.8. Using a multicast address reduces the amount of traffic that has to

be processed by network devices that are not part of the designated VRRP group.

- If the master router stops sending advertisements, backup routers will bid to become the master router based on priority. The dead interval before attempting to take over as the master is three times the hello interval plus half a second.
- **Preempt Mode** – Allows a backup router to take over as the master virtual router if it has a higher priority than the acting master virtual router (that is, another backup router that has taken over from the VRRP group address owner.) (Default: Enabled)
- **Preempt Delay** – Time to wait before issuing a claim to become the master. (Range: 0-120 seconds; 0 seconds)
- **Priority** – The priority of this router in a VRRP group. (Range: 1-254; Default: 100)
 - The priority for the VRRP group address owner is automatically set to 255.
 - The priority for backup routers is used to determine which router will take over as the acting master router if the current master fails.
- **Authentication Type** – Authentication mode used to verify VRRP packets received from other routers. (Options: None, Simple Text)
 - If simple text authentication is selected, then an authentication string must also be entered.
 - All routers in the same VRRP group must be set to the same authentication mode, and be configured with the same authentication string.
 - Plain text authentication does not provide any real security. It is supported only to prevent a misconfigured router from participating in VRRP.
- **Authentication String** – Key used to authenticate VRRP packets received from other routers. (Range: 1-8 alphanumeric characters)
 - When a VRRP packet is received from another router in the group, its authentication string is compared to the string configured on this router. If the strings match, the message is accepted. Otherwise, the packet is discarded.

Web – Click IP, VRRP, Group Configuration. Select the VLAN ID, enter the VRID group number, and click Add.

VRRP Group Configuration

VLAN ID	VRID	State	Virtual address	Interval	Preemption	Priority	AuthType	Edit	Delete
1	1	Master	192.168.1.23	1	Enabled	100	No	Edit	Delete
1	2	Initial	192.168.2.2	1	Enabled	100	No	Edit	Delete

Total VRRP group: 2

VLAN ID:

VRID:

Figure 168 VRRP Group Configuration

Click the Edit button for a group entry to open the detailed configuration window. Enter the IP address of a real interface on this router to make it the master virtual router for the group. Otherwise, enter the virtual address for an existing group to make it a backup router. Click Add IP to enter an IP address into the Associated IP Table. Then set any of the other parameters as required, and click Apply.

VRRP Group Configuration Detail

VLAN ID : 1, VRID : 3

Associated IP Table	192.168.3.254
Associated IP	

Advertisement Interval	1
Preempt Mode	☒ Enabled
Preempt Delay	0
Priority	100
Authentication Type	Simple Text
Authentication String	

Figure 169 VRRP Group Configuration Detail

CLI – This example creates VRRP group 1, sets the ECN330-switch as the master virtual router by assigning the interface address for the selected VLAN to the virtual IP address. It then sets all of the other VRRP parameters, and then displays the configured settings.

```

Console(config)#interface vlan 1
Console(config-if)#vrrp 1 ip 192.168.1.6
Console(config-if)#vrrp 1 timers advertise 5
Console(config-if)#vrrp 1 preempt delay 10
Console(config-if)#vrrp 1 priority 1
Console(config-if)#vrrp 1 authentication bluebird
Console(config-if)#end
Console#show vrrp
Vlan 1 - Group 1,
state                               Master
Virtual IP address                  192.168.1.6
Virtual MAC address                 00-00-5E-00-01-01
Advertisement interval              5 sec
Preemption                         enabled
Min delay                          10 sec
Priority                            1
Authentication                     SimpleText
Authentication key                  bluebird
Master Router                      192.168.1.6
Master priority                     255
Master Advertisement interval      5 sec
Master down interval               15
Console#

```

6.19.1.2 Displaying VRRP Global Statistics

The VRRP Global Statistics page displays counters for errors found in VRRP protocol packets.

Field Attributes

- **VRRP Packets with Invalid Checksum** – The total number of VRRP packets received with an invalid VRRP checksum value.
- **VRRP Packets with Unknown Error** – The total number of VRRP packets received with an unknown or unsupported version number.
- **VRRP Packets with Invalid VRID** – The total number of VRRP packets received with an invalid VRID for this virtual router.

Web – Click IP, VRRP, Global Statistics.

VRRP Global Statistics	
VRRP Packets with Invalid Checksum	0
VRRP Packets with Unknown Error	0
VRRP Packets with Invalid VRID	0

Figure 170 VRRP Global Statistics

CLI – This example displays counters for protocol errors for all the VRRP groups configured on the ECN330-switch.

```
Console#show vrrp router counters
  VRRP Packets with Invalid Checksum : 0
  VRRP Packets with Unknown Error   : 0
  VRRP Packets with Invalid VRID    : 0
Console#
```

6.19.1.3 Displaying VRRP Group Statistics

The VRRP Group Statistics page displays counters for VRRP protocol events and errors that have occurred on a specific VRRP interface.

Field Attributes

- **VLAN ID** – ID of a VLAN configured with an IP interface. (Range: 1-4094; Default: 1)
- **VRID** – VRRP group identifier. (Range: 1-255)
- **Times Become Master** – Number of times this router has transitioned to master.
- **Received Packets** – Number of VRRP advertisements received by this router.
- **Error Interval Packets** – Number of VRRP advertisements received for which the advertisement interval is different from the one configured for the local virtual router.
- **Authentication Failures** – Number of VRRP packets received that do not pass the authentication check.

- **Error IP TTL Packets** – Number of VRRP packets received by the virtual router with IP TTL (Time-To-Live) not equal to 255.
- **Received Priority 0 Packets** – Number of VRRP packets received by the virtual router with priority set to 0.
- **Error Packet Length Packets** – Number of packets received with a packet length less than the length of the VRRP header.
- **Invalid Type Packets** – Number of VRRP packets received by the virtual router with an invalid value in the “type” field.
- **Error Address List Packets** – Number of packets received for which the address list does not match the locally configured list for the virtual router.
- **Invalid Authentication Type Packets** – Number of packets received with an unknown authentication type.
- **Mismatch Authentication Type Packets** – Number of packets received with “Auth Type” not equal to the locally configured authentication method.
- **Sent Priority 0 Packets** – Number of VRRP packets sent by the virtual router with priority set to 0.

Web – Click IP, VRRP, Group Statistics. Select the VLAN and virtual router group.

VRRP Group Statistics		
VLAN ID	1	
VRID	1	
Times Becomed Master	0	Error Packet Length Packets
Received Packets	0	Invalid Type Packets
Error Interval Packets	0	Error Address List Packets
Authentication Failures	0	Invalid Authentication Type Packets
Error IP TTL Packets	0	Mismatch Authentication Type Packets
Received Priority 0 Packets	0	Sent Priority 0 Packets

Figure 171 VRRP Group Statistics

CLI – This example displays VRRP protocol statistics for group 1, VLAN 1.

```

Console#show vrrp 1 interface vlan 1 counters
Total Number of Times Transitioned to MASTER           : 6
Total Number of Received Advertisements Packets       : 0
Total Number of Received Error Advertisement Interval Packets : 0
Total Number of Received Authentication Failures Packets : 0
Total Number of Received Error IP TTL VRRP Packets    : 0
Total Number of Received Priority 0 VRRP Packets      : 0
Total Number of Sent Priority 0 VRRP Packets          : 5
Total Number of Received Invalid Type VRRP Packets    : 0
Total Number of Received Error Address List VRRP Packets : 0
Total Number of Received Invalid Authentication Type VRRP Packets : 0
Total Number of Received Mismatch Authentication Type VRRP Packets : 0
Total Number of Received Error Packet Length VRRP Packets : 0
Console#

```

6.20 IP Routing

6.20.1 Overview

The ECN330-switch supports IP routing and routing path management through static routing definitions (page 421) and dynamic routing such as RIP (page 424) or OSPF (page 436). When IP routing is enabled (page 425), the ECN330-switch acts as a wire-speed router, passing traffic between VLANs using different IP interfaces, and routing traffic to external IP networks. However, when the ECN330-switch is first booted, no default routing is defined. As with all traditional routers, the routing functions must first be configured to work.

6.20.1.1 Initial Configuration

In the default configuration, all ports belong to the same VLAN and the ECN330-switch provides only Layer 2 functionality. Therefore, VLANs should first be created for each unique user group or application traffic (page 284), assign all ports that belong to the same group to these VLANs (page 287), and then assign an IP interface to each VLAN (page 403). By separating the network into different VLANs, it can be partitioned into subnetworks that are disconnected at Layer 2. Network traffic within the same subnet is still switched using Layer 2 switching. And the VLANs can now be interconnected (only as required) with Layer 3 switching.

Each VLAN represents a virtual interface to Layer 3. When a network address for each virtual interface is provided, the traffic between different subnetworks is routed by Layer 3 switching.

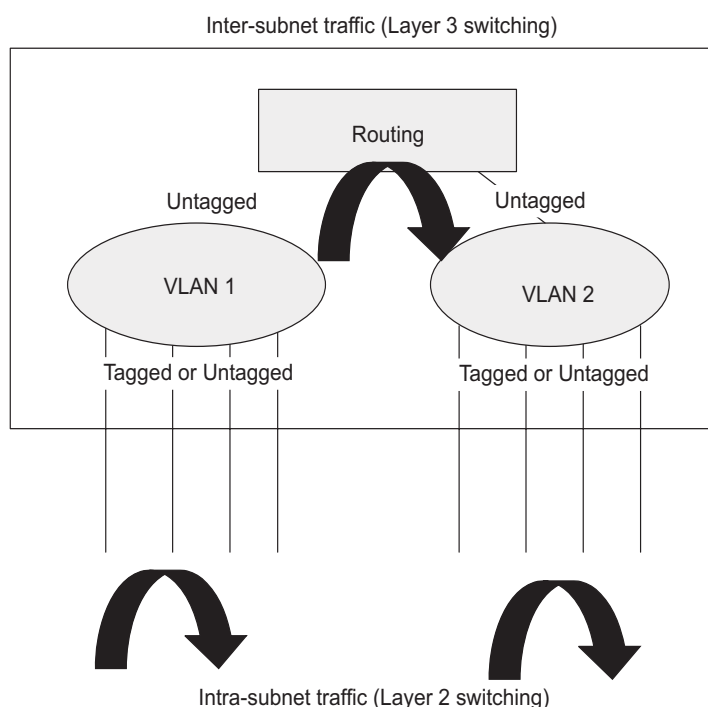


Figure 172 Virtual Interfaces and Layer 3 Routing

6.20.2

IP Switching

IP Switching (or packet forwarding) encompasses tasks required to forward packets for both Layer 2 and Layer 3, as well as traditional routing. These functions include:

- Layer 2 forwarding (switching) based on the Layer 2 destination MAC address
- Layer 3 forwarding (routing):
 - Based on the Layer 3 destination address
 - Replacing destination/source MAC addresses for each hop
 - Incrementing the hop count

- Decrementing the time-to-live
- Verifying and recalculating the Layer 3 checksum

If the destination node is on the same subnetwork as the source network, then the packet can be transmitted directly without the help of a router. However, if the MAC address is not yet known to the ECN330-switch, an Address Resolution Protocol (ARP) packet with the destination IP address is broadcast to get the destination MAC address from the destination node. The IP packet can then be sent directly with the destination MAC address.

If the destination belongs to a different subnet on the ECN330-switch, the packet can be routed directly to the destination node. However, if the packet belongs to a subnet not included on the ECN330-switch, then the packet should be sent to a router (with the MAC address of the router itself used as the destination MAC address, and the destination IP address of the destination node). The router will then forward the packet to the destination node through the correct path. The router can also use the ARP protocol to find out the MAC address of the destination node of the next router as necessary.

Note: In order to perform IP switching, the ECN330-switch should be recognized by other network nodes as an IP router, either by setting it as the default gateway or by redirection from another router through the ICMP process.

When the ECN330-switch receives an IP packet addressed to its own MAC address, the packet follows the Layer 3 routing process. The destination IP address is checked against the Layer 3 address table. If the address is not already there, the ECN330-switch broadcasts an ARP packet to all the ports on the destination VLAN to find out the destination MAC address. After the MAC address is discovered, the packet is reformatted and sent out to the destination. The reformat process includes decreasing the Time-To-Live (TTL) field of the IP header, recalculating the IP header checksum, and replacing the destination MAC address with either the MAC address of the destination node or that of the next hop router.

When another packet destined to the same node arrives, the destination MAC can be retrieved directly from the Layer 3 address table; the packet is then reformatted and sent out the destination port. IP switching can be done at wire-speed when the destination address entry is already in the Layer 3 address table.

If the ECN330-switch determines that a frame must be routed, the route is calculated only during setup. Once the route has been determined, all packets

in the current flow are simply switched or forwarded across the chosen path. This takes advantage of the high throughput and low latency of switching by enabling the traffic to bypass the routing engine once the path calculation has been performed.

6.20.2.1 Routing Path Management

Routing Path Management involves the determination and updating of all the routing information required for packet forwarding, including:

- Handling routing protocols
- Updating the routing table
- Updating the Layer 3 switching database

6.20.2.2 Routing Protocols

The ECN330-switch supports both static and dynamic routing.

- Static routing requires routing information to be stored in the ECN330-switch either manually or when a connection is set up by an application outside the ECN330-switch.
- Dynamic routing uses a routing protocol to exchange routing information, calculate routing tables, and respond to changes in the status or loading of the network.

The ECN330-switch supports RIP, RIP-2 and OSPFv2 dynamic routing protocols.

RIP and RIP-2 Dynamic Routing Protocols

The RIP protocol is the most widely used routing protocol. RIP uses a distance-vector-based approach to routing. Routes are determined on the basis of minimizing the distance vector, or hop count, which serves as a rough estimate of transmission cost. Each router broadcasts its advertisement every 30 seconds, together with any updates to its routing table. This allows all routers on the network to learn consistent tables of next hop links which lead to relevant subnets.

OSPFv2 Dynamic Routing Protocol

OSPF overcomes all the problems of RIP. It uses a link state routing protocol to generate a shortest-path tree, then builds up its routing table based on this tree. OSPF produces a more stable network because the participating routers act on network changes predictably and simultaneously, converging on the best route more quickly than RIP. Moreover, when several equal-cost routes to a destination exist, traffic can be distributed equally among them.

Non-IP Protocol Routing

The ECN330-switch supports IP routing only. Non-IP protocols such as IPX and Appletalk cannot be routed by the ECN330-switch, and will be confined within their local VLAN group unless bridged by an external router.

To coexist with a network built on multilayer switches, the subnetworks for non-IP protocols must follow the same logical boundary as that of the IP subnetworks. A separate multi-protocol router can then be used to link the subnetworks by connecting to one port from each available VLAN on the network.

6.20.3 Basic IP Interface Configuration

To allow routing between different IP subnets, IP Routing must be enabled as described in this section. Also, a VLAN for each IP subnet that will be connected directly to the ECN330-switch needs to be defined. Note that a VLAN must first be created as described under section 6.12.1.7 on page 284 before configuring the corresponding subnet. Remember that to manage the ECN330-switch in-band, the IP subnet address must be defined for at least one VLAN.

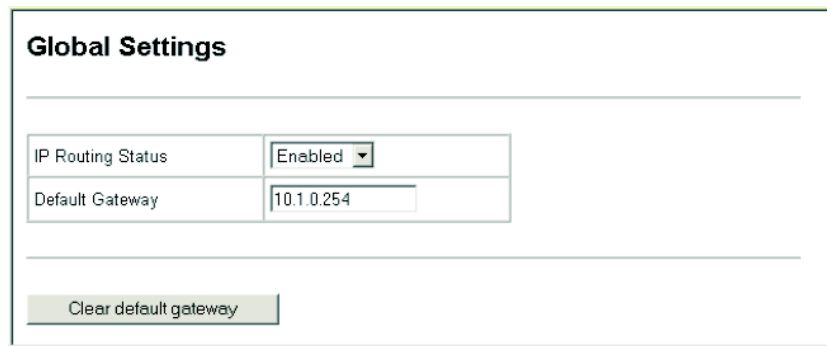
Command Attributes

- **IP Routing Status** – Configures the ECN330-switch to operate as a Layer 2 switch or as a multilayer routing switch. (Options: Disable this field to restrict operation to Layer 2 switching; enable it to allow multilayer operation at either Layer 2 or 3 as required.)
 - This command affects both static and dynamic unicast routing.
 - If IP routing is enabled, all IP packets are routed using either static routing or dynamic routing through RIP or OSPF, and other packets for all non-IP protocols (for example, NetBuei, NetWare or AppleTalk) are switched based on MAC addresses. If IP routing is

disabled, all packets are switched, with filtering and forwarding decisions based strictly on MAC addresses.

- **Default Gateway** – The routing device to which the ECN330-switch will pass packets for all unknown subnets; that is, packets that do not match any routing table entry. (Valid IP addresses consist of four numbers, 0 to 255, separated by periods.)

Web - Click IP, General, Global Settings. Set IP Routing Status to Disabled to restrict operation to Layer 2, or Enabled to allow multilayer switching, specify the default gateway which will be forwarded packets for all unknown subnets, and click Apply.



Global Settings	
IP Routing Status	Enabled
Default Gateway	10.1.0.254
<button>Clear default gateway</button>	

Figure 173 IP Global Settings

CLI - This example enables IP routing, and sets the default gateway.

```
Console(config)#ip routing
Console(config)#ip route default 10.1.0.254
```

6.20.4 Configuring IP Routing Interfaces

IP subnets connected to this router can be specified by manually assigning an IP address to each VLAN, or by using the RIP or OSPF dynamic routing protocol to identify routes that lead to other interfaces by exchanging protocol messages with other routers on the network.

Command Usage

- If this router is directly connected to end node devices (or connected to end nodes through shared media) that will be assigned to a specific subnet, then a router interface must be created for each VLAN that will support routing. The router interface consists of an IP address and subnet mask. This interface address defines both the network number to which the router interface is attached and the router's host number on that network. In other words, a router interface address defines the network and subnetwork numbers of the segment that is connected to that interface, and allows IP packets to be sent to or from the router.
- Before any network interfaces are configured on this router, first create a VLAN for each unique user group, or for each network application and its associated users. Then assign the ports associated with each of these VLANs.

Command Attributes

- **VLAN ID** – ID of configured VLAN (1-4094).
- **IP Address Mode** – Specifies whether the IP address for this interface is statically assigned, or obtained from a network address server. (Options: Static, DHCP - Dynamic Host Configuration Protocol, BOOTP - Boot Protocol; Default: Static)
 - If Static address type is selected, then also specify whether the IP address is the primary IP address on the VLAN or a secondary IP address. An interface can have only one primary IP address, but can have multiple secondary IP addresses. In other words, secondary addresses need to be specified if more than one IP subnet can be accessed through this interface.
 - If DHCP/BOOTP is enabled, IP will not function until a reply has been received from the address server. Requests will be broadcast periodically by the router for an IP address. (DHCP/BOOTP values include the IP address and subnet mask.)

- **IP Address** – Address of the VLAN interface. Valid IP addresses consist of four numbers, 0 to 255, separated by periods.
- **Subnet Mask** – This mask identifies the host address bits used for routing to specific subnets.

Web - Click IP, General, Routing Interface. Specify an IP interface for each VLAN that will support routing to other subnets. First specify a primary address, and click Set IP Configuration. To assign secondary addresses, enter these addresses one at a time, and click Set IP Configuration after entering each address.

Routing Interface

VLAN	1
IP Address Mode	Static Primary
IP Address	10.1.0.253
Subnet Mask	255.255.255.0

Set IP Configuration Remove IP Address

Restart DHCP

Figure 174 IP Routing Interface

CLI - This example sets a primary IP address for VLAN 1, and then adds a secondary IP address for a different subnet also attached to this router interface.

```
Console(config)#interface vlan 1
Console(config-if)#ip address 10.1.0.253 255.255.255.0
Console(config-if)#ip address 10.1.9.253 255.255.255.0 secondary
Console(config-if)#
```

6.20.5 Address Resolution Protocol

If IP routing is enabled (page 401), the router uses its routing tables to make routing decisions, and uses Address Resolution Protocol (ARP) to forward traffic from one hop to the next. ARP is used to map an IP address to a physical layer (that is, MAC) address. When an IP frame is received by this router (or any standards-based router), it first looks up the MAC address corresponding to the destination IP address in the ARP cache. If the address is found, the router writes the MAC address into the appropriate field in the frame header, and forwards the frame on to the next hop. IP traffic passes along the path to its final destination in this way, with each routing device mapping the destination IP address to the MAC address of the next hop toward the recipient, until the packet is delivered to the final destination.

If there is no entry for an IP address in the ARP cache, the router will broadcast an ARP request packet to all devices on the network. The ARP request contains the following fields similar to that shown in this example:

Table 22 Address Resolution Protocol

destination IP address	10.1.0.19
destination MAC address	?
source IP address	10.1.0.253
source MAC address	00-00-ab-cd-00-00

When devices receive this request, they discard it if their address does not match the destination IP address in the message. However, if it does match, they write their own hardware address into the destination MAC address field and send the message back to the source hardware address. When the source device receives a reply, it writes the destination IP address and corresponding MAC address into its cache, and forwards the IP traffic on to the next hop. As long as this entry has not timed out, the router will be able forward traffic directly to the next hop for this destination without having to broadcast another ARP request.

6.20.5.1 Proxy ARP

When a node in the attached subnetwork does not have routing or a default gateway configured, Proxy ARP can be used to forward ARP requests to a remote subnetwork. When the router receives an ARP request for a remote network and Proxy ARP is enabled, it determines if it has the best route to the remote network, and then answers the ARP request by sending its own MAC address to the requesting node. That node then sends traffic to the router, which in turn uses its own routing table to forward the traffic to the remote destination.

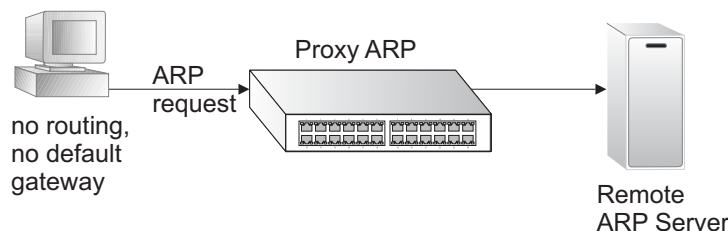


Figure 175 Proxy ARP

6.20.5.2 Basic ARP Configuration

The ARP General configuration menu can be used to specify the timeout for ARP cache entries, or to enable Proxy ARP for specific VLAN interfaces.

Command Usage

- The aging time determines how long dynamic entries remain the cache. If the timeout is too short, the router may tie up resources by repeating ARP requests for addresses recently flushed from the table.
- End stations that require Proxy ARP must view the entire network as a single network. These nodes must therefore use a smaller subnet mask than that used by the router or other relevant network devices.
- Extensive use of Proxy ARP can degrade router performance because it may lead to increased ARP traffic and increased search time for larger ARP address tables.

Command Attributes

- **Timeout** – Sets the aging time for dynamic entries in the ARP cache. (Range: 300 - 86400 seconds; Default: 1200 seconds or 20 minutes)

- **Proxy ARP** – Enables or disables Proxy ARP for specified VLAN interfaces. (Default: Disabled)

Web - Click IP, ARP, General. Set the timeout to a suitable value for the ARP cache, enable Proxy ARP for subnetworks that do not have routing or a default gateway, and click Apply.

General	
Timeout	
Set Timeout (300 - 86400 seconds)	900
Proxy ARP	
VLAN	2
Status	☒ Enabled

Figure 176 ARP General

CLI - This example sets the ARP cache timeout for 15 minutes (that is, 900 seconds), and enables Proxy ARP for VLAN 3.

```
Console(config)#arp-timeout 900
Console(config)#interface vlan 3
Console(config-if)#ip proxy-arp
Console(config-if)#
```

6.20.5.3 Configuring Static ARP Addresses

For devices that do not respond to ARP requests, traffic will be dropped because the IP address cannot be mapped to a physical address. If this occurs, an IP address can be manually mapped to the corresponding physical address in the ARP.

Command Usage

- Up to 128 static entries can be defined in the ARP cache.
- Static entries will not be aged out or deleted when power is reset. A static entry can only be removed through the configuration interface.

Command Attributes

- **IP Address** – IP address statically mapped to a physical MAC address. (Valid IP addresses consist of four numbers, 0 to 255, separated by periods.)
- **MAC Address** – MAC address statically mapped to the corresponding IP address. (Valid MAC addresses are hexadecimal numbers in the format: xx-xx-xx-xx-xx-xx.)
- **Entry Count** – The number of static entries in the ARP cache.

Web - Click IP, ARP, Static Addresses. Enter the IP address, the corresponding MAC address, and click Apply.

Figure 177 ARP Static Addresses

CLI - This example sets a static entry for the ARP cache.

```
Console(config)#arp 10.1.0.11 00-11-22-33-44-55
Console(config)#
```

6.20.5.4

Displaying Dynamically Learned ARP Entries

The ARP cache contains entries that map IP addresses to the corresponding physical address. Most of these entries will be dynamically learned through replies to broadcast messages. All of the dynamic entries in the ARP cache can be displayed, specific dynamic entries can be changed into static entries, or all dynamic entries cleared from the cache.

Command Attributes

- **IP Address** – IP address of a dynamic entry in the cache.
- **MAC Address** – MAC address mapped to the corresponding IP address.
- **Interface** – VLAN interface associated with the address entry.
- **Dynamic to Static** – Changes a selected dynamic entry to a static entry.
- **Clear All** – Deletes all dynamic entries from the ARP cache.
- **Entry Count** – The number of dynamic entries in the ARP cache.

Note: The Dynamic to Static and Clear All web interface buttons take effect immediately. There is no prompt to confirm the action.

Web - Click IP, ARP, Dynamic Addresses. Use the buttons provided to change a dynamic entry to a static entry, or to clear all dynamic entries in the cache.

The screenshot shows a web interface titled "Dynamic Addresses". It contains a table with the following data:

Current:		
IP Address	MAC Address	Interface
192.168.0.1	00-0F-3D-12-40-E1	247
192.168.0.196	00-10-B5-51-69-F7	247

Below the table, there is a "Dynamic to Static" button. At the bottom left, there is a "Clear All" button. At the bottom center, it says "Entry Count: 2".

Figure 178 ARP Dynamic Addresses

CLI - This example shows all entries in the ARP cache. it also shows how to convert a Edenic address to a static address, and then clears the remaining entries in the ARP cache.

```

Console#show arp
Arp cache timeout: 1200 (seconds)

  IP Address      MAC Address      Type      Interface
  -----
    10.1.0.11  00-11-22-33-44-55    static          2
    10.1.0.22  00-00-12-33-89-76    other           2
    192.168.0.1 00-0f-3d-12-40-e1  dynamic        247
    192.168.0.146 00-00-12-33-89-76    other        247
    192.168.0.196 00-10-b5-51-69-f7  dynamic        247
    192.168.1.250 00-00-12-33-89-76    other        248

Total entry : 6
Console#configure
Console(config)#arp 192.168.0.1 00-0f-3d-12-40-e1
Console(config)#end
Console#clear arp-cache
This operation will delete all the dynamic entries in ARP Cache.
Are you sure to continue this operation (y/n)?y
Console#

```

6.20.5.5

Displaying Local ARP Entries

The ARP cache also contains entries for local interfaces, including subnet, host, and broadcast addresses.

Command Attributes

- **IP Address** – IP address of a local entry in the cache.
- **MAC Address** – MAC address mapped to the corresponding IP address.
- **Interface** – VLAN interface associated with the address entry.
- **Entry Count** – The number of local entries in the ARP cache.

Web - Click IP, ARP, Other Addresses.

Other Addresses

Current:

IP Address, MAC Address, Interface

10.1.0.22, 00-00-12-33-89-76, 2
192.168.0.146, 00-00-12-33-89-76, 247
192.168.1.250, 00-00-12-33-89-76, 248

Entry Count: 3

Figure 179 ARP Other Addresses

CLI - This router uses the Type specification “other” to indicate local cache entries in the ARP cache.

```

Console#show arp
Arp cache timeout: 1200 (seconds)

  IP Address      MAC Address      Type      Interface
  -----
    10.1.0.11    00-11-22-33-44-55    static          2
    10.1.0.22    00-00-12-33-89-76    other           2
    192.168.0.1   00-0f-3d-12-40-e1   dynamic        247
    192.168.0.146 00-00-12-33-89-76    other        247
    192.168.0.196 00-10-b5-51-69-f7   dynamic        247
    192.168.1.250 00-00-12-33-89-76    other        248

Total entry : 6
Console#

```

6.20.5.6 Displaying ARP Statistics

The ECN330-switch can display statistics for ARP messages crossing all interfaces.

Table 23 ARP Statistics

Parameter	Description
Received Request	Number of ARP Request packets received by the router.
Received Reply	Number of ARP Reply packets received by the router.
Sent Request	Number of ARP Request packets sent by the router.
Sent Reply	Number of ARP Reply packets sent by the router.

Web - Click IP, ARP, Statistics.



The screenshot shows a web interface titled "ARP Statistics". It contains a table with the following data:

Received	
Request	31
Reply	4
Sent	
Request	53
Reply	31

Figure 180 ARP Statistics

CLI - This example provides detailed statistics on common IP-related protocols.

```

Console#show ip traffic
IP statistics:
  Rcvd:  5 total, 5 local destination
         0 checksum errors
         0 unknown protocol, 0 not a gateway
  Frags: 0 reassembled, 0 timeouts
         0 fragmented, 0 couldn't fragment
  Sent:  9 generated
         0 no route
ICMP statistics:
  Rcvd: 0 checksum errors, 0 redirects, 0 unreachable, 0 echo
        5 echo reply, 0 mask requests, 0 mask replies, 0 quench
        0 parameter, 0 timestamp
  Sent: 0 redirects, 0 unreachable, 0 echo, 0 echo reply
        0 mask requests, 0 mask replies, 0 quench, 0 timestamp
        0 time exceeded, 0 parameter problem
UDP statistics:
  Rcvd: 0 total, 0 checksum errors, 0 no port
  Sent: 0 total
TCP statistics:
  Rcvd: 0 total, 0 checksum errors
  Sent: 0 total
ARP statistics:
  Rcvd: 0 requests, 1 replies
  Sent: 1 requests, 0 replies
Console#

```

6.20.6 Displaying Statistics for IP Protocols

6.20.6.1 IP Statistics

The Internet Protocol (IP) provides a mechanism for transmitting blocks of data (often called packets or frames) from a source to a destination, where these network devices (that is, hosts) are identified by fixed length addresses. The Internet Protocol also provides for fragmentation and reassembly of long packets, if necessary, for transmission through “small packet” networks.

Table 24 IP Statistics

Parameter	Description
Packets Received	The total number of input datagrams received from interfaces, including those received in error.
Received Address Errors	The number of input datagrams discarded because the IP address in the header's destination field was not a valid address for this entity.
Received Packets Discarded	The number of input datagrams for which no problems were encountered to prevent their continued processing, but which were discarded (for example, for lack of buffer space).
Output Requests	The total number of datagrams which local IP user-protocols (including ICMP) supplied to IP in requests for transmission.
Output Packet No Route	The number of datagrams discarded because no route could be found to transmit them to their destination. Note that this includes any datagrams which a host cannot route because all of its default gateways are down.
Datagrams Forwarded	The number of input datagrams for which this entity was not their final IP destination, as a result of which an attempt was made to find a route to forward them to that final destination.
Reassembly Required	The number of IP fragments received which needed to be reassembled at this entity.
Reassembly Failures	The number of failures detected by the IP re-assembly algorithm (for whatever reason: timed out, errors, and so on).
Datagrams Failing Fragmentation	The number of datagrams that have been discarded because they needed to be fragmented at this entity but could not be, for example, because their "Don't Fragment" flag was set.

Parameter	Description
Received Header Errors	The number of input datagrams discarded due to errors in their IP headers, including bad checksums, version number mismatch, other format errors, time-to-live exceeded, errors discovered in processing their IP options, and so on
Unknown Protocols Received	The number of locally-addressed datagrams received successfully but discarded because of an unknown or unsupported protocol.
Received Packets Delivered	The total number of input datagrams successfully delivered to IP user-protocols (including ICMP).
Discarded Output Packets	The number of output IP datagrams for which no problem was encountered to prevent their transmission to their destination, but which were discarded (for example, for lack of buffer space).
Fragments Created	The number of datagram fragments that have been generated as a result of fragmentation at this entity.
Routing Discards	The number of routing entries which were chosen to be discarded even though they are valid. One possible reason for discarding such an entry could be to free-up buffer space for other routing entries.
Reassembly Successful	The number of datagrams successfully re-assembled.
Datagrams Successfully Fragmented	The number of IP datagrams that have been successfully fragmented at this entity.

Web - Click IP, Statistics, IP.

IP Statistics			
Packets Received	2367	Received Header Errors	0
Received Address Errors	0	Unknown Protocols Received	0
Received Packets Discarded	0	Received Packets Delivered	2364
Output Requests	2670	Discarded Output Packets	0
Output Packet No Route	2	Fragments Created	0
Datagrams Forwarded	3	Routing Discards	0
Reassembly Required	0	Reassembly Successful	0
Reassembly Failures	0	Datagrams Successfully Fragmented	0
Datagrams Failing Fragmentation	0		

Figure 181 IP Statistics

CLI - See the example on page 412.

6.20.6.2

ICMP Statistics

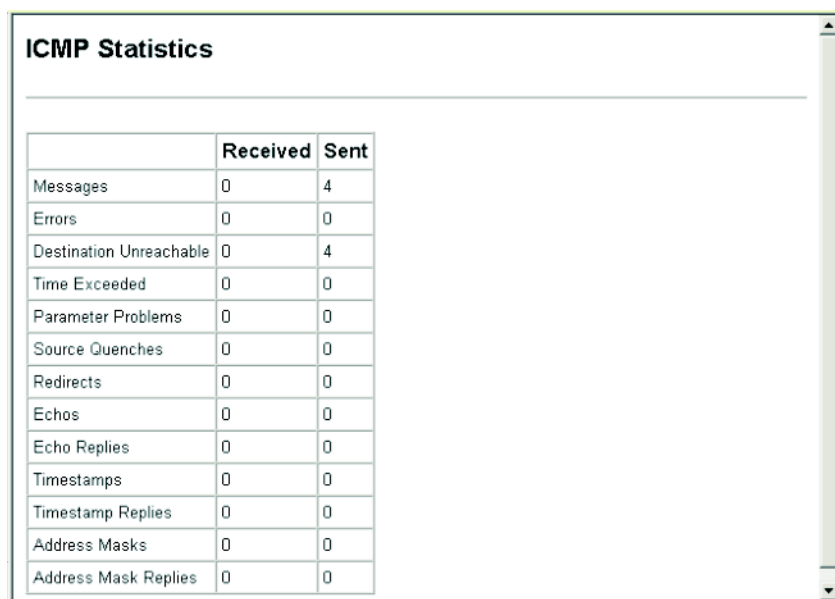
Internet Control Message Protocol (ICMP) is a network layer protocol that transmits message packets to report errors in processing IP packets. ICMP is therefore an integral part of the Internet Protocol. ICMP messages may be used to report various situations, such as when a datagram cannot reach its destination, when the gateway does not have the buffering capacity to forward a datagram, and when the gateway can direct the host to send traffic on a shorter route. ICMP is also used by routers to feed back information about more suitable routes (that is, the next hop router) to use for a specific destination.

Table 25 ICMP Statistics

Parameter	Description
Messages	The total number of ICMP messages which the entity received/sent.
Errors	The number of ICMP messages which the entity received/sent but determined as having ICMP-specific errors (bad ICMP checksums, bad length, and so on).

Parameter	Description
Destination Unreachable	The number of ICMP Destination Unreachable messages received/sent.
Time Exceeded	The number of ICMP Time Exceeded messages received/sent.
Parameter Problems	The number of ICMP Parameter Problem messages received/sent.
Source Quenches	The number of ICMP Source Quench messages received/sent.
Redirects	The number of ICMP Redirect messages received/sent.
Echos	The number of ICMP Echo (request) messages received/sent.
Echo Replies	The number of ICMP Echo Reply messages received/sent.
Timestamps	The number of ICMP Timestamp (request) messages received/sent.
Timestamp Replies	The number of ICMP Timestamp Reply messages received/sent.
Address Masks	The number of ICMP Address Mask Request messages received/sent.
Address Mask Replies	The number of ICMP Address Mask Reply messages received/sent.

Web - Click IP, Statistics, ICMP.



	Received	Sent
Messages	0	4
Errors	0	0
Destination Unreachable	0	4
Time Exceeded	0	0
Parameter Problems	0	0
Source Quenches	0	0
Redirects	0	0
Echos	0	0
Echo Replies	0	0
Timestamps	0	0
Timestamp Replies	0	0
Address Masks	0	0
Address Mask Replies	0	0

Figure 182 ICMP Statistics

CLI - See the example on page 412.

6.20.6.3

UDP Statistics

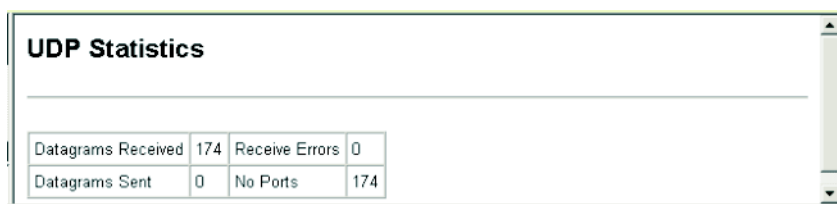
User Datagram Protocol (UDP) provides a datagram mode of packet-switched communications. It uses IP as the underlying transport mechanism, providing access to IP-like services. UDP packets are delivered just like IP packets – connection-less datagrams that may be discarded before reaching their targets. UDP is useful when TCP would be too complex, too slow, or just unnecessary.

Table 26 UDP Statistics

Parameter	Description
Datagrams Received	The total number of UDP datagrams delivered to UDP users.
Datagrams Sent	The total number of UDP datagrams sent from this entity.

Parameter	Description
Receive Errors	The number of received UDP datagrams that could not be delivered for reasons other than the lack of an application at the destination port.
No Ports	The total number of received UDP datagrams for which there was no application at the destination port.

Web - Click IP, Statistics, UDP.



UDP Statistics			
Datagrams Received	174	Receive Errors	0
Datagrams Sent	0	No Ports	174

Figure 183 UDP Statistics

CLI - See the example on page 412.

6.20.6.4

TCP Statistics

The Transmission Control Protocol (TCP) provides highly reliable host-to-host connections in packet-switched networks, and is used in conjunction with IP to support a wide variety of Internet protocols.

Table 27 TCP Statistics

Parameter	Description
Segments Received	The total number of segments received, including those received in error. This count includes segments received on currently established connections.
Segments Sent	The total number of segments sent, including those on current connections but excluding those containing only retransmitted octets.

Parameter	Description
Active Opens	The number of times TCP connections have made a direct transition to the SYN-SENT state from the CLOSED state.
Failed Connection Attempts	The number of times TCP connections have made a direct transition to the CLOSED state from either the SYN-SENT state or the SYN-RCVD state, plus the number of times TCP connections have made a direct transition to the LISTEN state from the SYN-RCVD state.
Current Connections	The number of TCP connections for which the current state is either ESTABLISHED or CLOSE-WAIT.
Receive Errors	The total number of segments received in error (for example, bad TCP checksums).
Segments Retransmitted	The total number of segments retransmitted - that is, the number of TCP segments transmitted containing one or more previously transmitted octets.
Passive Opens	The number of times TCP connections have made a direct transition to the SYN-RCVD state from the LISTEN state.
Reset Connections	The number of times TCP connections have made a direct transition to the CLOSED state from either the ESTABLISHED state or the CLOSE-WAIT state.

Web - Click IP, Statistics, TCP.

TCP Statistics			
Segments Received	3406	Receive Errors	0
Segments Sent	4162	Segments Retransmitted	0
Active Opens	0	Passive Opens	418
Failed Connection Attempts	0	Reset Connections	2
Current Connections	1		

Figure 184 TCP Statistics

CLI - See the example on page 412.

6.20.7 Configuring Static Routes

This router can dynamically configure routes to other network segments using dynamic routing protocols (that is, RIP or OSPF). However, static routes can also be manually entered in the routing table. Static routes may be required to access network segments where dynamic routing is not supported, or can be set to force the use of a specific route to a subnet, rather than using dynamic routing. Static routes do not automatically change in response to changes in network topology, so only configure a small number of stable routes to ensure network accessibility.

Command Attributes

- **Interface** – Index number of the IP interface.
- **IP Address** – IP address of the destination network, subnetwork, or host.
- **Netmask** – Network mask for the associated IP subnet. This mask identifies the host address bits used for routing to specific subnets.
- **Gateway** – IP address of the gateway used for this route.
- **Metric** – Cost for this interface. This cost is only used if a route is imported by a dynamic routing protocol such as OSPF. (Range: 1-5, default: 1)
- **Entry Count** – The number of table entries.

Web - Click IP, Routing, Static Routes.

Static Routes

Current:

Interface	IP Address	Netmask	Nexthop	Metric
1	0.0.0.0	0.0.0.0	10.1.0.254	1

<< Add Remove

Clear all static routes

Entry Count: 1

New:

IP Address	
Netmask	
Nexthop	
Metric	1

Figure 185 IP Static Routes

CLI - This example forwards all traffic for subnet 192.168.1.0 to the router 192.168.5.254, using the default metric of 1.

```
Console(config)#ip route 192.168.1.0 255.255.255.0
                  192.168.5.254
Console(config)#
```

6.20.8 Displaying the Routing Table

The ECN330-switch can display all the routes that can be accessed through the local network interfaces, through static routes, or through a dynamically learned route. If route information is available through more than one of these methods, the priority for route selection is local, static, and then dynamic. Also note that the route for a local interface is not enabled (that is, listed in the routing table) unless there is at least one active link connected to that interface.

Command Attributes

- **Interface** – Index number of the IP interface.
- **IP Address** – IP address of the destination network, subnetwork, or host. Note that the address 0.0.0.0 indicates the default gateway for this router.

- **Netmask** – Network mask for the associated IP subnet. This mask identifies the host address bits used for routing to specific subnets.
- **Next Hop** – The IP address of the next hop (or gateway) in this route.
- **Protocol** – The protocol which generated this route information. (Options: local, static, RIP, OSPF)
- **Metric** – Cost for this interface.
- **Entry Count** – The number of table entries.

Web - Click IP, Routing, Routing Table.

Routing Table

Current:

Interface, IP Address, Netmask, Next Hop, Protocol, Metric

1	0.0.0.0	0.0.0.0	10.1.0.254	static	1
1	10.1.0.0	255.255.255.0	10.1.0.253	local	1
1	10.1.1.0	255.255.255.0	10.1.0.254	RIP	2

Clear all dynamic routes

Entry Count: 3

Figure 186 IP Routing Table

CLI - This example shows routes obtained from various methods.

```
Console#show ip route
```

Ip Address	Netmask	Next Hop	Protocol	Metric	Interface
0.0.0.0	0.0.0.0	10.1.0.254	static	1	1
10.1.0.0	255.255.255.0	10.1.0.253	local	1	1
10.1.1.0	255.255.255.0	10.1.0.254	RIP	2	1

Total entries: 3

Console#

6.20.9 Configuring the Routing Information Protocol

The RIP protocol is the most widely used routing protocol. The RIP protocol uses a distance-vector-based approach to routing. Routes are determined on the basis of minimizing the distance vector, or hop count, which serves as a rough estimate of transmission cost. Each router broadcasts its advertisement every 30 seconds, together with any updates to its routing table. This allows all routers on the network to learn consistent tables of next hop links which lead to relevant subnets.

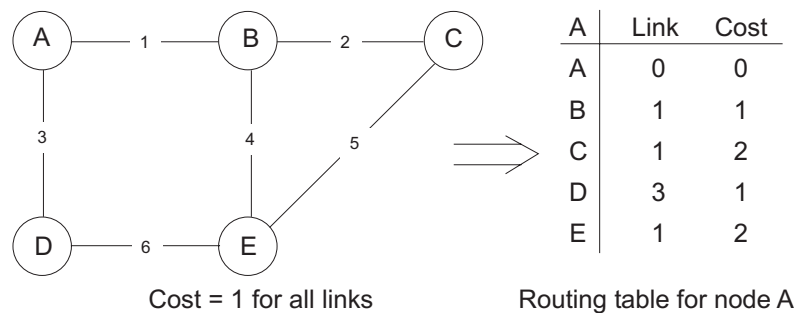


Figure 187 Configuring RIP

Command Usage

- Just as Layer 2 switches use the Spanning Tree Algorithm to prevent loops, routers also use methods for preventing loops that would cause endless retransmission of data traffic. RIP utilizes the following three methods to prevent loops from occurring:
 - Split horizon – Never propagate routes back to an interface port from which they have been acquired.
 - Poison reverse – Propagate routes back to an interface port from which they have been acquired, but set the distance-vector metrics to infinity. (This provides faster convergence.)
 - Triggered updates – Whenever a route gets changed, broadcast an update message after waiting for a short random delay, but without waiting for the periodic cycle.
- RIP-2 is a compatible upgrade to RIP. RIP-2 adds useful capabilities for plain text authentication, multiple independent RIP domains, variable length subnet masks, and multicast transmissions for route advertising (RFC 1723).

- There are several serious problems with RIP that should be considered. First of all, RIP (version 1) has no knowledge of subnets, both RIP versions can take a long time to converge on a new route after the failure of a link or router during which time routing loops may occur, and its small hop count limitation of 15 restricts its use to smaller networks. Moreover, RIP (version 1) wastes valuable network bandwidth by propagating routing information through broadcasts; it also considers too few network variables to make the best routing decision.

6.20.9.1 Configuring General Protocol Settings

RIP is used to specify how routers exchange routing information. When RIP is enabled on this router, it sends RIP messages to all devices in the network every 30 seconds (by default), and updates its own routing table when RIP messages are received from other routers. To communicate properly with other routers using RIP, the RIP version used globally by the router needs to be specified, as well as the RIP send and receive versions used on specific interfaces (page 429).

Command Usage

- When a Global RIP Version is specified, any VLAN interface not previously set to a specific Receive or Send Version (page 429) is set to the following values:
 - RIP Version 1 configures previously unset interfaces to send RIPv1 compatible protocol messages and receive either RIPv1 or RIPv2 protocol messages.
 - RIP Version 2 configures previously unset interfaces to use RIPv2 for both sending and receiving protocol messages.
- The *update* timer is the fundamental timer used to control all basic RIP processes.
 - Setting the update timer to a short interval can cause the router to spend an excessive amount of time processing updates. On the other hand, setting it to an excessively long time will make the routing protocol less sensitive to changes in the network configuration.
 - The timers must be set to the same values for all routers in the network.

Command Attributes

Global Settings

- **RIP Routing Process** – Enables RIP routing for all IP interfaces on the router. (Default: Disabled)
- **Global RIP Version** – Specifies a RIP version used globally by the router. (Default: RIP Version 1)

Timer Settings

- **Update** – Sets the rate at which updates are sent. This value will also set the timeout timer to 6 times the update time, and the garbage-collection timer to 4 times the update time. (Range: 15-60 seconds; Default: 30 seconds)
- **Timeout** – Sets the time after which there have been no update messages that a route is declared dead. The route is marked inaccessible (that is, the metric set to infinite) and advertised as unreachable. However, packets are still forwarded on this route. This parameter is automatically set to six times the value of the Update timer. (Default: 180 seconds)
- **Garbage Collection** – After the *timeout* interval expires, the router waits for an interval specified by the *garbage-collection* timer before removing this entry from the routing table. This timer allows neighbors to become aware of an invalid route prior to purging. This parameter is automatically set to four times the value of the Update timer. (Default: 120 seconds)

Web - Click Routing Protocol, RIP, General Settings. Enable or disable RIP, set the RIP version used on previously unset interfaces to RIPv1 or RIPv2, set the basic update timer, and then click Apply.

General Settings	
Global	
RIP Routing Process	☒ Enabled
Global RIP Version	RIPv2
Timer	
Update (15-60 seconds)	15
Timeout (Update*6)	90
Garbage Collection (Update*4)	60

Figure 188 RIP General Settings

CLI - This example sets the router to use RIP Version 2, and sets the basic timer to 15 seconds.

```

Console(config)#router rip
Console(config-router)#version 2
Console(config-router)#timers basic 15
Console(config-router)#end
Console#show rip globals

RIP Process: Enabled
Update Time in Seconds: 15
Number of Route Change: 0
Number of Queries: 1
Console#

```

6.20.9.2 Specifying Network Interfaces for RIP

Network interfaces that will be included in the RIP routing process must be specified.

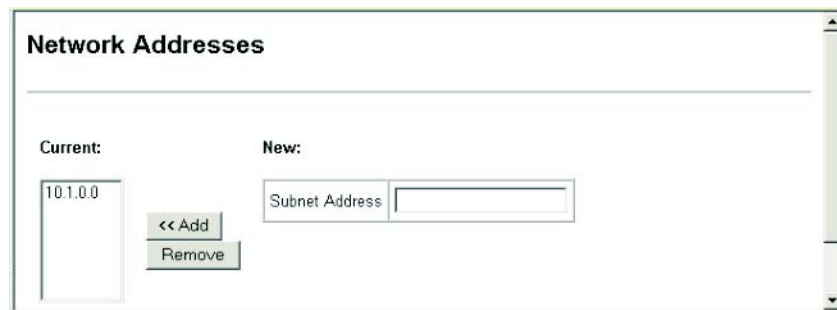
Command Usage

- RIP only sends updates to interfaces specified by this command.
- Subnet addresses are interpreted as class A, B or C, based on the first field in the specified address. In other words, if a subnet address nnn.xxx.xxx.xxx is entered, the first field (nnn) determines the class:
 - 0 - 127 is class A, and only the first field in the network address is used.
 - 128 - 191 is class B, and the first two fields in the network address are used.
 - 192 - 223 is class C, and the first three fields in the network address are used.

Command Attributes

Subnet Address – IP address of a network directly connected to this router.

Web - Click Routing Protocol, RIP, Network Addresses. Add all interfaces that will participate in RIP, and click Apply.



The screenshot shows a window titled "Network Addresses". Inside, there are two main sections: "Current:" and "New:". The "Current:" section contains a list box with the IP address "10.1.0.0". Below this list box are two buttons: "<< Add" and "Remove". The "New:" section contains a label "Subnet Address" followed by an empty text input field. The window has a standard scrollbar on the right side.

Figure 189 RIP Network Addresses

CLI - This example includes network interface 10.1.0.0 in the RIP routing process.

```

Console(config)#router-rip
Console(config-router)#network 10.1.0.0
Console(config-router)#end
Console#show ip rip status

```

	Peer	UpdateTime	Version	RcvBadPackets	RcvBadRoutes
-					
	10.1.0.253		0	0	73
	10.1.1.253		0	0	66

```

Console#

```

6.20.9.3 Configuring Network Interfaces for RIP

For each interface that participates in the RIP routing process, be sure to specify the protocol message type accepted (that is, RIP version) and the message type sent (that is, RIP version or compatibility mode), the method for preventing loopback of protocol messages, and whether or not authentication is used (authentication only applies if RIPv2 messages are being sent or received).

Command Usage

Specifying Receive and Send Protocol Types

- Setting the RIP Receive Version or Send Version for an interface overrides the global setting specified by the RIP / General Settings, Global RIP Version field.
- The Receive Version can be specified based on these options:
 - Use “RIPv1” or “RIPv2” if all routers in the local network are based on RIPv1 or RIPv2, respectively.
 - Use “RIPv1 or RIPv2” if some routers in the local network are using RIPv2, but there are still some older routers using RIPv1.
 - Use “Do Not Receive” if dynamic entries are not required to be added to the routing table for an interface. (For example, when only static routes are to be allowed for a specific interface.)

- The Send Version can be specified based on these options:
 - Use “RIPv1” or “RIPv2” if all routers in the local network are based on RIPv1 or RIPv2, respectively.
 - Use “RIPv1 Compatible” to propagate route information by broadcasting to other routers on the network using the RIPv2 advertisement list, instead of multicasting as normally required by RIPv2. (Using this mode allows RIPv1 routers to receive these protocol messages, but still allows RIPv2 routers to receive the additional information provided by RIPv2, including subnet mask, next hop and authentication information.)
 - Use “Do Not Send” to passively monitor route information advertised by other routers attached to the network.

Loopback Prevention

Just as Layer 2 switches use the Spanning Tree Algorithm to prevent loops, routers also use methods for preventing loops that would cause endless retransmission of data traffic. When protocol packets are caught in a loop, links will be congested, and protocol packets may be lost. However, the network will slowly converge to the new state. RIP utilizes the following three methods that can provide faster convergence when the network topology changes and prevent most loops from occurring:

- Split Horizon – Never propagate routes back to an interface port from which they have been acquired.
- Poison Reverse – Propagate routes back to an interface port from which they have been acquired, but set the distance-vector metrics to infinity. (This provides faster convergence.)
- Triggered Updates – Whenever a route gets changed, broadcast an update message after waiting for a short random delay, but without waiting for the periodic cycle.

Protocol Message Authentication

RIPv1 is not a secure protocol. Any device sending protocol messages from UDP port 520 will be considered a router by its neighbors. Malicious or unwanted protocol messages can be easily propagated throughout the network if no authentication is required. RIPv2 supports authentication through a simple password. When a router is configured to exchange authentication messages, it

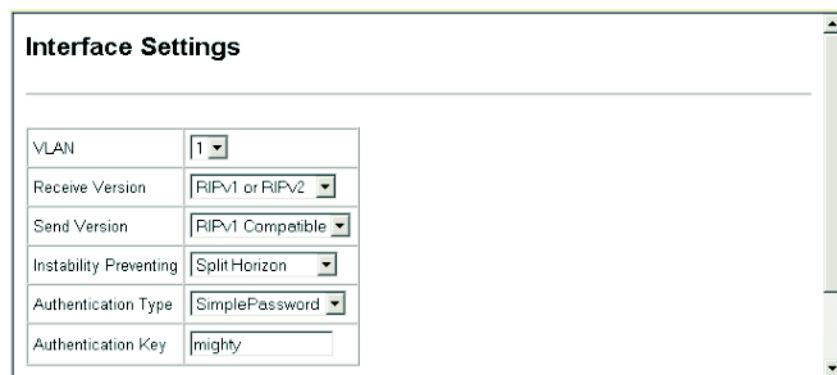
will insert the password into all transmitted protocol packets, and check all received packets to ensure that they contain the authorized password. If any incoming protocol messages do not contain the correct password, they are simply dropped.

Command Attributes

- **VLAN** – ID of configured VLAN (1-4094).
- **Receive Version** – The RIP version to receive on an interface.
 - **RIPv1**: Accepts only RIPv1 packets.
 - **RIPv2**: Accepts only RIPv2 packets.
 - **RIPv1 or RIPv2**: Accepts RIPv1 or RIPv2 packets. (Default)
 - **Do Not Receive**: Does not accept incoming RIP packets.
(The default depends on the setting specified under RIP / General Settings, Global RIP Version: RIPv1 - RIPv1 or RIPv2 packets, RIPv2 - RIPv2 packets.)
- **Send Version** – The RIP version to send on an interface.
 - **RIPv1**: Sends only RIPv1 packets.
 - **RIPv2**: Sends only RIPv2 packets.
 - **RIPv1 Compatible**: Route information is broadcast to other routers with RIPv2. (Default)
 - **Do Not Send**: Does not transmit RIP updates.
(The default depends on the setting specified under RIP / General Settings, Global RIP Version: RIPv1 - RIPv1 Compatible, RIPv2 - RIPv2 packets.)
- **Instability Preventing** – Specifies the method used to reduce the convergence time when the network topology changes, and to prevent RIP protocol messages from looping back to the source router. (Default: Split Horizon)
 - **None**: No method is used. If a loop occurs, the hop count for a route may be gradually incremented to infinity (that is, 16) before the route is deemed unreachable.
 - **Split Horizon**: This method never propagates routes back to an interface from which they have been acquired.

- **Poision Reverse:** This method propagates routes back to an interface port from which they have been acquired, but set the distance-vector metrics to infinity. (This provides faster convergence.)
- **Authentication Type** – Specifies whether or not authentication is required for exchanging protocol messages. (Default: No Authentication)
 - **No Authentication:** No authentication is required.
 - **Simple Password:** Requires the interface to exchange routing information with other routers based on an authorized password. (Note that authentication only applies to RIPv2.)
- **Authentication Key** – Specifies the key to use for authenticating RIPv2 packets. For authentication to function properly, both the sending and receiving interface must use the same password. (Range: 1-16 characters, case sensitive)

Web - Click Routing Protocol, RIP, Interface Settings. Select the RIP protocol message types that will be received and sent, the method used to provide faster convergence and prevent loopback (that is, prevent instability in the network topology), and the authentication option and corresponding password. Then click Apply.



Interface Settings	
VLAN	1
Receive Version	RIPv1 or RIPv2
Send Version	RIPv1 Compatible
Instability Preventing	Split Horizon
Authentication Type	SimplePassword
Authentication Key	mighty

Figure 190 RIP Interface Settings

CLI - This example sets the receive version to accept both RIPv1 or RIPv2 messages, the send mode to RIPv1 compatible (that is, called v2-broadcast in the CLI), sets the method of preventing instability in the network topology to Split Horizon, enables authentication through a simple password (that is, called text mode in the CLI).

```
Console(config)#interface vlan 1
Console(config-if)#ip rip receive version 1 2
Console(config-if)#ip rip send version v2-broadcast
Console(config-if)#ip split-horizon
Console(config-if)#ip rip authentication mode text
Console(config-if)#ip rip authentication key mighty
Console#
```

6.20.9.4 Displaying RIP Information and Statistics

The ECN330-switch can display basic information about the current global configuration settings for RIP, statistics about route changes and queries, information about the interfaces that are using RIP, and information about known RIP peer devices.

Table 28 RIP Information and Statistics

Parameter	Description
<i>Globals</i>	
RIP Routing Process	Indicates if RIP has been enabled or disabled.
Update Time in Seconds	The interval at which RIP advertises known route information. (Default: 30 seconds)
Number of Route Changes	Number of times routing information has changed.
Number of Queries	Number of router database queries received by this router.

Parameter	Description
<i>Interface Information</i>	
Interface	IP address of the interface.
SendMode	RIP version sent on this interface (none, RIPv1, RIPv2, rip1Compatible).
ReceiveMode	RIP version received on this interface (none, RIPv1, RIPv2, RIPv1Orv2).
InstabilityPreventing	Shows if split-horizon, poison-reverse, or no instability prevention method is in use.
AuthType	Shows if authentication is set to simple password or none.
RcvBadPackets	Number of bad RIP packets received.
RcvBadRoutes	Number of bad routes received.
SendUpdates	Number of route changes.
<i>Peer Information</i>	
PeerAddress	IP address of a neighboring RIP router.
UpdateTime	Last time a route update was received from this peer.
Version	Whether RIPv1 or RIPv2 packets were received from this peer.
RcvBadPackets	Number of bad RIP packets received from this peer.
RcvBadRoutes	Number of bad routes received from this peer.

Web - Click Routing Protocol, RIP, Statistics.

RIP Statistics	
Globals	
RIP Routing Process	Enabled
Update Time in Seconds	30
Number of Route Changes	4
Number of Queries	0
Interface Information	
Interface, SendMode, ReceiveMode, InstabilityPreventing, AuthType, RcvBadPackets, RcvBadRoutes, SendUpdates	
10.1.0.253, rip1Compatible, RIPv1Orv2, SplitHorizon, noAuthentication, 0, 0, 60	
10.1.1.253, rip1Compatible, RIPv1Orv2, SplitHorizon, noAuthentication, 0, 0, 60	
Peer Information	
PeerAddress, UpdateTime, Version, RcvBadPackets, RcvBadRoutes	
10.1.0.254, 4093, 2, 0, 14lu	
10.1.1.254, 4093, 2, 0, 14lu	

Figure 191 RIP Statistics

CLI - The information displayed by the RIP Statistics screen through the web interface can be accessed from the CLI using the following commands.

```
Console#show rip globals
```

```
RIP Process: Enabled
```

```
Update Time in Seconds: 30
```

```
Number of Route Change: 4
```

```
Number of Queries: 0
```

```
Console#show ip rip configuration
```

Interface	SendMode	ReceiveMode	Poison	Authentication
10.1.0.253	rip1Compatible	RIPv1Orv2	SplitHorizon	noAuthentication
10.1.1.253	rip1Compatible	RIPv1Orv2	SplitHorizon	noAuthentication

```
Console#show ip rip status
```

Interface	RcvBadPackets	RcvBadRoutes	SendUpdates
10.1.0.253	0	0	60
10.1.1.253	0	0	63

```
Console#show ip rip peer
```

Peer	UpdateTime	Version	RcvBadPackets	RcvBadRoutes
10.1.0.254	4610	2	0	0
10.1.1.254	4610	2	0	0

```
Console#
```

6.20.10 Configuring the Open Shortest Path First Protocol

Open Shortest Path First (OSPF) is more suited for large area networks which experience frequent changes in the links. It also handles subnets much better than RIP. OSPF protocol actively tests the status of each link to its neighbors to generate a shortest path tree, and builds a routing table based on this information. OSPF then utilizes IP multicast to propagate routing information. A separate routing area scheme is also used to further reduce the amount of routing traffic.

Note: The OSPF protocol implemented in this device is based on Version 2 (RFC 2328). It also supports Version 1 (RFC 1583) compatibility mode to ensure that the same method is used to calculate summary route costs throughout the network when older OSPF routers exist; as well as the not-so-stubby area option (RFC 1587).

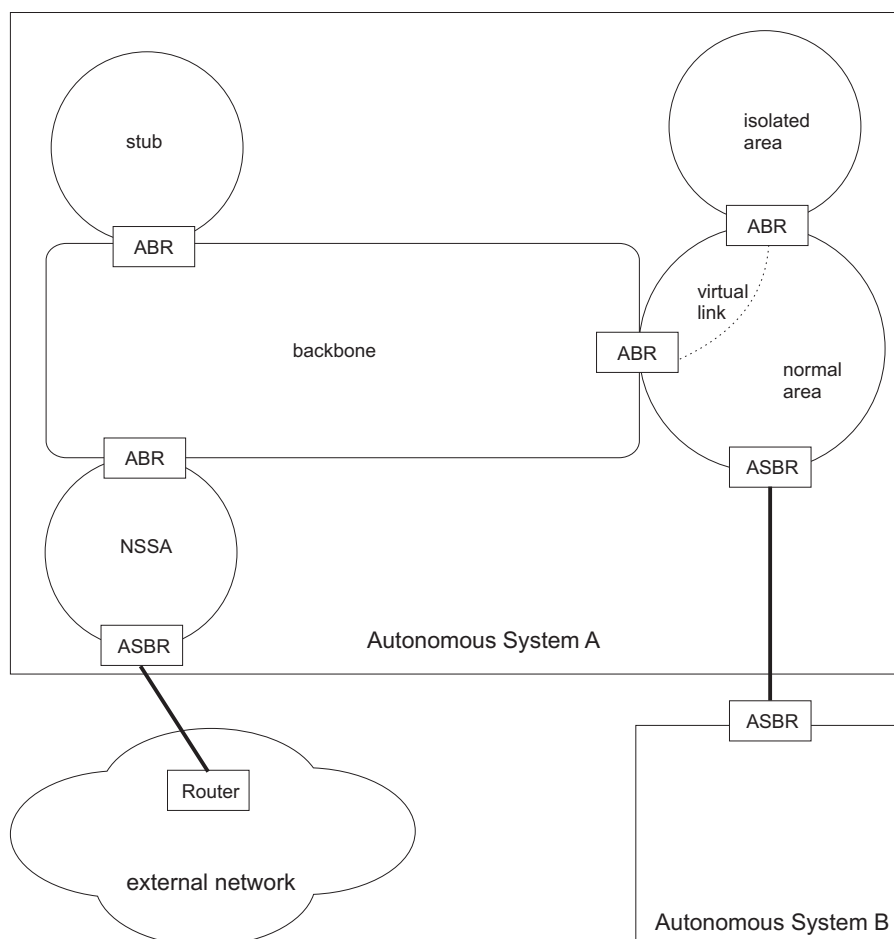


Figure 192 Configuring OSPF

Command Usage

- OSPF looks at more than just the simple hop count. When adding the shortest path to any node into the tree, the optimal path is chosen on the basis of delay, throughput and connectivity. OSPF utilizes IP multicast to reduce the amount of routing traffic required when sending or receiving routing path updates. The separate routing area scheme used by OSPF further reduces the amount of routing traffic, and thus inherently provides another level of routing protection. In addition, all routing protocol exchanges can be authenticated. Finally, the OSPF algorithms have been tailored for efficient operation in TCP/IP Internets.

- OSPFv2 is a compatible upgrade to OSPF. It involves enhancements to protocol message authentication, and the addition of a point-to-multipoint interface which allows OSPF to run over non-broadcast networks, as well as support for overlapping area ranges.
- When using OSPF, organize the network (that is, autonomous system) into normal, stub, or not-so-stubby areas; configure the ranges of subnet addresses that can be aggregated by link state advertisements; and configure virtual links for areas that do not have direct physical access to the OSPF backbone.
 - To implement OSPF for a large network, first organize the network into logical areas to limit the number of OSPF routers that actively exchange Link State Advertisements (LSAs). Then define an OSPF interface by assigning an IP interface configured on this router to one of these areas. This OSPF interface will send and receive OSPF traffic to neighboring OSPF routers.
 - The exchange of OSPF traffic can be further optimized by specifying an area range that covers a large number of subnetwork addresses. This is an important technique for limiting the amount of traffic exchanged between Area Border Routers (ABRs).
 - And finally, specify a virtual link to any OSPF area that is not physically attached to the OSPF backbone. Virtual links can also be used to provide a redundant link between contiguous areas to prevent areas from being partitioned, or to merge backbone areas.

6.20.10.1 Configuring General Protocol Settings

To implement dynamic OSPF routing, first assign VLAN groups to each IP subnet to which this router will be attached, then use the OSPF / General Configuration menu to enable OSPF, assign an Router ID to this device, and set the other basic protocol parameters.

Command Attributes

General Information

- **OSPF Routing Process** – Enables or disables OSPF routing for all IP interfaces on the router. (Default: Disabled)
- **OSPF Router ID** – Assigns a unique router ID for this device within the autonomous system. (Default: The lowest interface address)

- **Version Number** – This router only supports OSPF Version 2. (This parameter is read only.)
- **Area Border Router** – Indicates if this router connect directly to networks in two or more areas. An area border router runs a separate copy of the Shortest Path First algorithm, maintaining a separate routing database for each area. (This parameter is read only.)

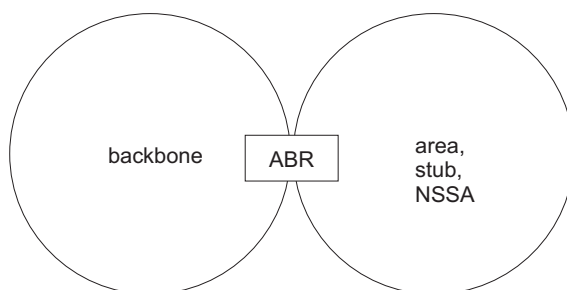


Figure 193 Area Border Router

- **AS Boundary Router** – Allows this router to exchange routing information with boundary routers in other autonomous systems to which it may be attached. If a router is enabled as an ASBR, then every other router in the autonomous system can learn about external routes from this device. (Default: Disabled)

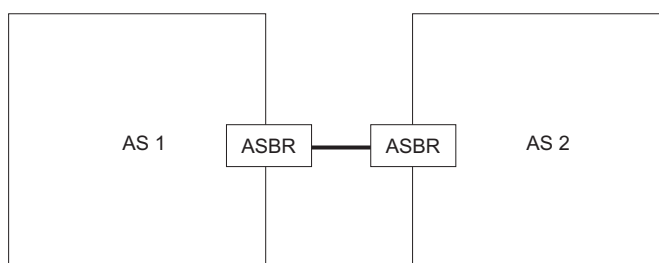


Figure 194 AS Boundary Router

- **Rfc1583 Compatible** – If one or more routers in a routing domain are using OSPF Version 1, this router should use RFC 1583 (OSPFv1) compatibility mode to ensure that all routers are using the same RFC for calculating summary route costs. Enable this field to force the router to calculate summary route costs using RFC 1583. (Default: Disabled)

- **SPF Hold Time (seconds)** – The hold time between making two consecutive shortest path first (SPF) calculations. (Range: 0-65535; Default: 10)
- **Area Numbers** – The number of OSPF areas configured on this router. (This parameter is read only.)

Default Route Information

- **Originate Default Route** – Generates a default external route into an autonomous system. Note that the **AS Boundary Router** field must be enabled, and the **Advertise Default Route** field properly configured. (Default: Disabled)
- **Advertise Default Route** – The router can advertise a default external route into the autonomous system (AS). (Options: NotAlways, Always; Default: NotAlways)
 - **Always** – The router will advertise itself as a default external route for the AS, even if a default external route does not actually exist.
 - **NotAlways** – It can only advertise a default external route into the AS if it has been configured to import external routes through RIP or static configuration, and such a route is known. (See “Redistributing External Routes” on page 460.)
- **External Metric Type** – The external link type used to advertise the default route. Type 1 route advertisements add the internal cost to the external route metric. Type 2 routes do not add the internal cost metric. When comparing Type 2 routes, the internal cost is only used as a tie-breaker if several Type 2 routes have the same cost. (Default: Type 2)
- **Default External Metric** – The Metric assigned to the default route. (Range: 1-65535; Default: 10)

Note: The AS Boundary Router and Default Route Information parameters can be configured with the **default-information originate** command (page 1058).

Web - Click Routing Protocol, OSPF, General Configuration. Enable OSPF, specify the Router ID, configure the other global parameters as required, and click Apply.

General Configuration

General Information:

OSPF Routing Process	Enabled ▾
OSPF Router ID	10.1.1.253
Version Number	Version 2
Area Border Router	Yes
AS Boundary Router	Enabled ▾
RFC1583 Compatible	Disabled ▾
SPF Hold Time (0 - 65535 seconds)	10
Area Numbers	3

Default Information:

Originate Default Route	Enabled ▾
Advertise Default Route	Always ▾
External Metric Type	Type2 ▾
Default External Metric (0 - 16777215)	10

Figure 195 OSPF General Configuration

CLI - This example configures the router with the same settings as shown in the screen capture for the web interface.

```

Console(config)#router ospf
Console(config-router)#router-id 10.1.1.253
Console(config-router)#no compatible rfc1583
Console(config-router)#default-information originate always
metric 10 metric-type 2
Console(config-router)#timers spf 10
Console(config-router)#

```

6.20.10.2 Configuring OSPF Areas

An autonomous system must be configured with a backbone area, designated by area identifier 0.0.0.0. By default, all other areas are created as normal transit areas.

Routers in a normal area may import or export routing information about individual nodes. To reduce the amount of routing traffic flooded onto the network, an area can be configured to export a single summarized route that covers a broad range of network addresses within the area (page 446). To further reduce the amount of routes passed between areas, configure an area as a stub or a not-so-stubby area (NSSA).

Normal Area – A large OSPF domain should be broken up into several areas to increase network stability and reduce the amount of routing traffic required through the use of route summaries that aggregate a range of addresses into a single route. The backbone or any normal area can pass traffic between other areas, and are therefore known as transit areas. Each router in an area has identical routing tables. These tables may include area links, summarized links, or external links that depict the topology of the autonomous system.

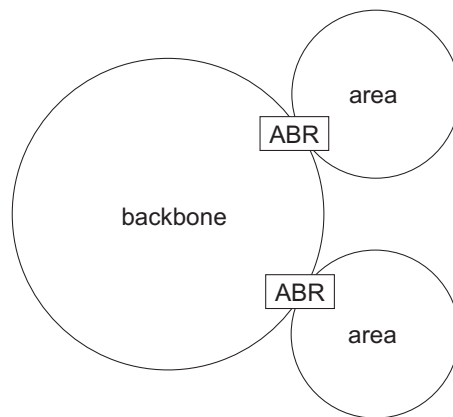


Figure 196 OSPF Areas

Stub – A stub does not accept external routing information. Instead, an area border router adjacent to a stub can be configured to send a default external route into the stub for all destinations outside the local area or the autonomous system. This route will also be advertised as a single entry point for traffic entering the stub. Using a stub can significantly reduce the amount of topology data that has to be exchanged over the network.

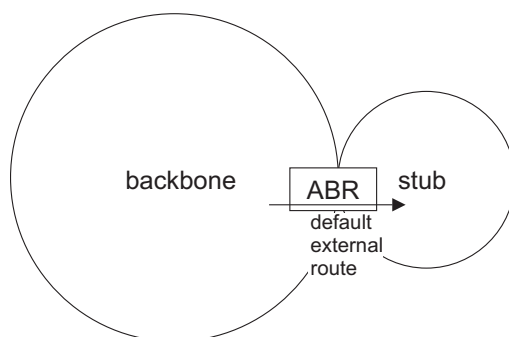


Figure 197 OSPF Stub Area

By default, a stub can only pass traffic to other areas in the autonomous system through the default external route. However, an area border router can also be configured to send Type 3 summary link advertisements into the stub.

NSSA – A not-so-stubby area (NSSA) is similar to a stub. It blocks most external routing information, and can be configured to advertise a single default route for traffic passing between the NSSA and other areas within the autonomous system (AS). However, an NSSA can also import external routes from one or more small routing domains that are not part of the AS, such as a RIP domain or locally configured static routes. This external AS routing information is generated by the NSSA's ASBR and advertised only within the NSSA. By default, these routes are not flooded onto the backbone or into any other area by area border routers. However, the NSSA's ABRs will convert NSSA external LSAs (Type 7) into external LSAs (Type-5) which are propagated into other areas within the AS.

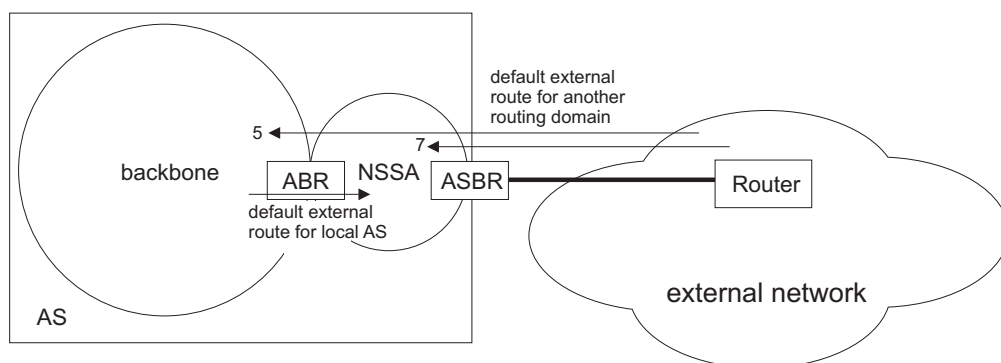


Figure 198 OSPF NSSA

- Routes that can be advertised with NSSA external LSAs include network destinations outside the AS learned through OSPF, the default route, static routes, routes derived from other routing protocols such as RIP, or directly connected networks that are not running OSPF.
- Also, note that unlike stub areas, all Type-3 summary LSAs are always imported into NSSAs to ensure that internal routes are always chosen over Type-7 NSSA external routes.

Default Cost – This specifies a cost for the default summary route sent into a stub or not-so-stubby area (NSSA) from an Area Border Router (ABR).

Command Usage

- Before creating a stub or NSSA, first specify the address range for an area using the Network Area Address Configuration screen (page 442).
- Stubs and NSSAs cannot be used as a transit area, and should therefore be placed at the edge of the routing domain.
- A stub or NSSA can have multiple ABRs or exit points. However, all of the exit points and local routers must contain the same external routing data so that the exit point does not need to be determined for each external destination.

Command Attributes

- **Area ID** – Identifier for an area, stub or NSSA.
- **Area Type** – Specifies a normal area, stub area, or not-so-stubby area (NSSA). Area ID 0.0.0.0 is set to the backbone by default. (Default: Normal area)
- **Default Cost** – Cost for the default summary route sent into a stub from an area border router (ABR). (Range: 0-16777215; Default: 1)
 - Note that if the default cost is set to “0,” the router will not advertise a default route into the attached stub.
- **Summary** – Makes an ABR send a Type-3 summary link advertisement into a stub. (Default: Summary)
 - A stub is designed to save routing table space by blocking Type-4 AS summary LSAs and Type-5 external LSAs. If the “NoSummary” option is also used to block Type-3 summary LSAs that advertise

the default route for destinations external to the local area or the AS, the stub will become completely isolated.

Note: This router supports up to 16 total areas (either normal transit areas, stubs, or NSSAs).

Web - Click Routing Protocol, OSPF, Area Configuration. Set any area to a stub or NSSA as required, specify the cost for the default summary route sent into a stub, and click Apply.

Area Configuration

Current Area Configuration:

Area ID	Area Type	Default Cost	Summary	Remove
0.0.0.0	Backbone			
0.0.0.1				☐
0.0.0.2	Stub	10	Summary	☐
0.0.0.3	NSSA			☐
Entry Count: 4				Remove

Area Configuration Settings:

Area ID	
Area Type	Normal ▾
Default Cost (0 - 16777215)	
Summary	Summary ▾
Set	

Figure 199 OSPF Area Configuration

CLI - This example configures area 0.0.0.1 as a normal area, area 0.0.0.2 as a stub, and area 0.0.0.3 as an NSSA. It also configures the router to propagate a default summary route into the stub and sets the cost for this default route to 10.

```

Console(config-router)#network 10.1.1.0 255.255.255.0
      area 0.0.0.1
Console(config-router)#area 0.0.0.2 stub summary
Console(config-router)#area 0.0.0.2 default-cost 10
Console(config-router)#area 0.0.0.3 nssa
Console(config-router)#end

Console#show ip ospf
Routing Process with ID 192.168.1.253
Supports only single TOS(TOS0) route
Number of area in this router is 3
Area 0.0.0.0 (BACKBONE)
    Number of interfaces in this area is 1
    SPF algorithm executed 40 times
Area 0.0.0.2 (STUB)
    Number of interfaces in this area is 1
    SPF algorithm executed 8 times
Area 0.0.0.3 (NSSA)
    Number of interfaces in this area is 1
    SPF algorithm executed 40 times
Console#

```

6.20.10.3

Configuring Area Ranges (Route Summarization for ABRs)

An OSPF area can include a large number of nodes. If the Area Border Router (ABR) has to advertise route information for each of these nodes, this wastes a lot of bandwidth and processor time. Instead, configure an ABR to advertise a single summary route that covers all the individual networks within its area. When using route summaries, local changes do not have to be propagated to other area routers. This allows OSPF to be easily scaled for larger networks, and provides a more stable network topology.

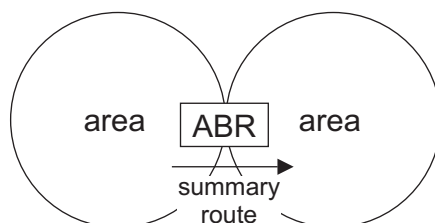


Figure 200 Route Summarization for ABRs

Command Usage

- Use the Area Range Configuration page to summarize the routes for an area. The summary route for an area is defined by an IP address and network mask. Therefore, each area needs to be structured with a contiguous set of addresses so that all routes in the area fall within an easily specified range. This router also supports Variable Length Subnet Masks (VLSMs), so an address range can be summarized on any bit boundary in a network address.
- To summarize the external LSAs imported into the autonomous system (that is, local routing domain), use the Summary Address Configuration screen (page 458).

Command Attributes

- **Area ID** – Identifies an area for which the routes are summarized. (The area ID must be in the form of an IP address.)
- **Range Network** – Base address for the routes to summarize.
- **Range Netmask** – Network mask for the summary route.
- **Advertising** – Indicates whether or not to advertise the summary route. If the summary is not sent, the routes remain hidden from the rest of the network. (Default: Advertise)

Note: This router supports up to 64 summary routes for area ranges.

Web - Click Routing Protocol, OSPF, Area Range Configuration. Specify the area identifier, the base address and network mask, select whether or not to advertise the summary route to other areas, and then click Apply.

Area Range Configuration

Current Area Range Entries:

Area ID	Range Network	Range Netmask	Advertising	Remove
0.0.0.1	10.1.1.0	255.255.255.0	Advertise ▼	☐

Entry Count: 1

Area Range Settings:

Area ID		Range Network	
Advertising	Advertise ▼	Range Netmask	

Figure 201 OSPF Range Configuration

CLI - This example summarizes all the routes for area 1. Note that the default for the **area range** command is to advertise the route summary. The configured summary route is shown in the list of information displayed for area 1.

```

Console(config-router)#area 0.0.0.1 range 10.1.1.0 255.255.255.0
Console(config-router)#end
Console#show ip ospf
Routing Process with ID 10.1.1.253
Supports only single TOS(TOS0) route
Number of area in this router is 4
Area 0.0.0.0 (BACKBONE)
    Number of interfaces in this area is 0
    SPF algorithm executed 47 times
Area 0.0.0.1
    Number of interfaces in this area is 3
    SPF algorithm executed 14 times
    Area ranges are
        255.255.255.0/24 Active
Console#

```

6.20.10.4 Configuring OSPF Interfaces

A routing interface should be specified for any local subnet that needs to communicate with other network segments located on this router or elsewhere in the network. First configure a VLAN for each subnet that will be directly connected to this router, assign IP interfaces to each VLAN (that is, one primary interface and one or more secondary interfaces), and then use the OSPF / Network Area Address Configuration page to assign an interface address range to an OSPF area.

After assigning a routing interface to an OSPF area, use the OSPF / Interface Configuration page to configure the interface-specific parameters used by OSPF to select the designated router, control the timing of link state advertisements, set the cost used to select preferred paths, and specify the method used to authenticate routing messages.

Field Attributes

OSPF Interface List

- **VLAN ID** – The VLAN to which an IP interface has been assigned.
- **Interface IP** – The IP interface associated with the selected VLAN.
- **Area ID** – The area to which this interface has been assigned.
- **Designated Router** – Designated router for this area.
- **Backup Designated Router** – Designated backup router for this area.
- **Entry Count** – The number of IP interfaces assigned to this VLAN.

Note: This router supports up 64 OSPF interfaces.

Detail Interface Configuration

- **VLAN ID** – The VLAN corresponding to the selected interface.
- **Rtr Priority** – Sets the interface priority for this router. (Range: 0-255; Default: 1)
 - A designated router (DR) and backup designated router (BDR) is elected for each OSPF area based on Router Priority. The DR forms an active adjacency to all other routers in the area to exchange

routing topology information. If for any reason the DR fails, the BDR takes over this role.

- The router with the highest priority becomes the DR and the router with the next highest priority becomes the BDR. If two or more routers are set to the same priority, the router with the higher ID will be elected. The priority can be set to zero to prevent a router from being elected as a DR or BDR.
- If a DR already exists for an area when this interface comes up, the new router will accept the current DR regardless of its own priority. The DR will not change until the next time the election process is initiated.
- **Transmit Delay** – Sets the estimated time to send a link-state update packet over an interface. (Range: 1-65535 seconds; Default: 1)
 - LSAs have their age incremented by a delay before transmission. Consider both the transmission and propagation delays for an interface when estimating this delay. Set the transmit delay according to link speed, using larger values for lower-speed links.
 - The transmit delay must be the same for all routers in an autonomous system.
 - On slow links, the router may send packets more quickly than devices can receive them. To avoid this problem, use the transmit delay to force the router to wait a specified interval between transmissions.
- **Retransmit Interval** – Sets the time between resending link-state advertisements. (Range: 1-65535 seconds; Default: 1)
 - A router will resend an LSA to a neighbor if it receives no acknowledgment. The retransmit interval should be set to a conservative value that provides an adequate flow of routing information, but does not produce unnecessary protocol traffic. Note that this value should be larger for virtual links.
 - Set this interval to a value that is greater than the round-trip delay between any two routers on the attached network to avoid unnecessary retransmissions.
- **Hello Interval** – Sets the interval between sending hello packets on an interface. (Range: 1-65535 seconds; Default: 10)

- This interval must be set to the same value for all routers on the network.
- Using a smaller Hello interval allows changes in the network topology to be discovered more quickly, but may result in more routing traffic.
- **Rtr Dead Interval** – Sets the interval at which hello packets are not seen before neighbors declare the router down. This interval must be set to the same value for all routers on the network. (Range: 1-65535 seconds; Default: 40, or 4 times the Hello Interval)
- **Cost** – Sets the cost of sending a packet on an interface, where higher values indicate slower ports. (Range: 1-65535; Default: 1)
 - This router uses a default cost of 1 for all ports. Therefore, if using ports at 100 Mbps, the cost should be reset to some value greater than 1.
 - Routes are subsequently assigned a metric equal to the sum of all metrics for each interface link in the route.
- **Authentication Type** – Specifies the authentication type used for an interface. (Options: None, Simple password, MD5; Default: None)
 - Use authentication to prevent routers from inadvertently joining an unauthorized area. Configure routers in the same area with the same password or key.
 - When using simple password authentication, a password is included in the packet. If it does not match the password configured on the receiving router, the packet is discarded. This method provides very little security as it is possible to learn the authentication key by snooping on routing protocol packets.
 - When using Message-Digest 5 (MD5) authentication, the router uses the MD5 algorithm to verify data integrity by creating a 128-bit message digest from the authentication key. Without the proper key and key-id, it is nearly impossible to produce any message that matches the pre-specified target message digest.
 - The Authentication Key and Message Digest Key-id must be used consistently throughout the autonomous system. (Note that the Message Digest Key-id field is disabled when this authentication type is selected.)

- **Authentication Key** – Assign a plain-text password used by neighboring routers to verify the authenticity of routing protocol messages. (Range: 1-8 characters for simple password or 1-16 characters for MD5 authentication; Default: no key)
 - A unique password can be assigned to each network (that is, autonomous system) to improve the security of the routing database. However, the password must be used consistently on all neighboring routers throughout a network.
- **Message Digest Key-id** – Assigns a key-id used in conjunction with the authentication key to verify the authenticity of routing protocol messages sent to neighboring routers. (Range: 1-255; Default: none)
 - Normally, only one key is used per interface to generate authentication information for outbound packets and to authenticate incoming packets. Neighbor routers must use the same key identifier and key value.
 - When changing to a new key, the router will send multiple copies of all protocol messages, one with the old key and another with the new key. Once all the neighboring routers start sending protocol messages back to this router with the new key, the router will stop using the old key. This rollover process gives the network administrator time to update all the routers on the network without affecting the network connectivity. Once all the network routers have been updated with the new key, the old key should be removed for security reasons.

Web - Click Routing Protocol, OSPF, Interface Configuration. Select the required interface from the scroll-down box, and click Detailed Settings.

Interface Configuration

OSPF Interface List of **VLAN ID** : 1
Detail Setting

Interface IP	Area ID	Designated Router	Backup DesignatedRouter
10.1.1.252	0.0.0.0	10.1.1.253	10.1.1.252

Entry Count: 1

Figure 202 OSPF Interface Configuration

Change any of the interface-specific protocol parameters, and then click Apply.

Detailed Interface Configuration	
VLAN ID	1
Rtr Priority (0 - 255)	5
Transmit Delay (0 - 3600 seconds)	6
Retransmit Interval (0 - 3600 seconds)	7
Hello Interval (1 - 65535 seconds)	5
Rtr Dead Interval (0 - 65535 seconds)	50
Cost (0 - 65535)	10
Authentication Type	MD 5
Authentication Key	aiebel
Message Digest Key-id (0 - 255)	1

Figure 203 OSPF Interface Configuration - Detailed

CLI - This example configures the interface parameters for VLAN 1.

```
Console(config)#interface vlan 1
Console(config-if)#ip ospf priority 5
Console(config-if)#ip ospf transmit-delay 6
Console(config-if)#ip ospf retransmit-interval 7
Console(config-if)#ip ospf hello-interval 5
Console(config-if)#ip ospf dead-interval 50
Console(config-if)#ip ospf cost 10
Console(config-if)#ip ospf authentication message-digest
Console(config-if)#ip ospf message-digest-key 1 md5 aiebel
Console#
```

6.20.10.5 Configuring Virtual Links

All OSPF areas must connect to the backbone. If an area does not have a direct physical connection to the backbone, a virtual link can be configured that provides a logical path to the backbone. To connect an isolated area to the backbone, the logical path can cross a single non-backbone area (that is, transit area) to reach the backbone. To define this path, an ABR must be configured that serves as an endpoint connecting the isolated area to the common transit

area, and a neighboring ABR specified as the other endpoint connecting the common transit area to the backbone itself. (Note that a virtual link cannot be configured that runs through a stub or NSSA area.)

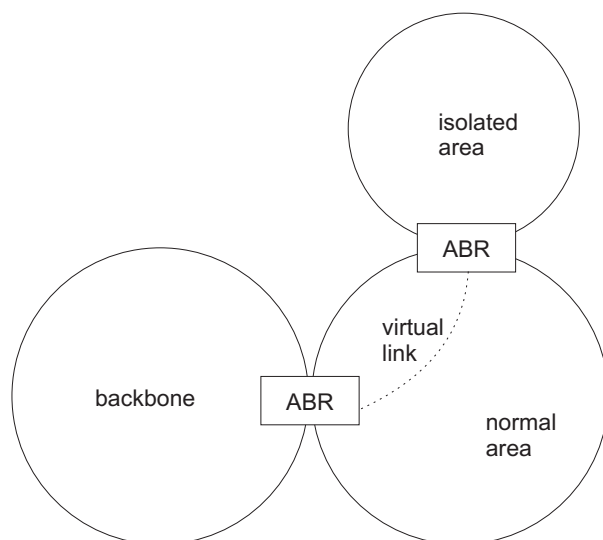


Figure 204 OSPF Virtual Link

Virtual links can also be used to create a redundant link between any area and the backbone to help prevent partitioning, or to connect two existing backbone areas into a common backbone.

Command Attributes

- **Area ID** – Identifies the transit area for the virtual link. (The area ID must be in the form of an IP address.)
- **Neighbor Router ID** – Neighbor router at other end of the virtual link. This must be an Area Border Router (ABR) that is adjacent to both the backbone and the transit area for the virtual link.
- **Events** – The number of state changes or error events on this virtual link.

The other items are described under “Configuring OSPF Interfaces,” page 449.

Note: This router supports up to 64 virtual links.

Web - Click Routing Protocol, OSPF, Virtual Link Configuration. To create a new virtual link, specify the Area ID and Neighbor Router ID, configure the link attributes, and click Add. To modify the settings for an existing link, click the Detail button for the required entry, modify the link settings, and click Set.

Virtual Link Configuration

Current Virtual Link Entries:

Area ID	Neighbor Router ID	Detail Setting	Remove
0.0.0.4	10.1.1.252	Detail	☐

Entry Count: 1

Virtual Link Settings:

Area ID	
Neighbor Router ID	
Transmit Delay (0 - 3600 seconds)	1
Retransmit Interval (0 - 3600 seconds)	5
Hello Interval (1 - 65535 seconds)	10
Rtr Dead Interval (0 - 2147483647 seconds)	40
Authentication Type	Null
Authentication Key	
Message Digest Key-id (0 - 255)	
Add	

Figure 205 OSPF Virtual Link Configuration

CLI - This example configures a virtual link from the ABR adjacent to area 0.0.0.4, through a transit area to the neighbor router 10.1.1.252 at the other end of the link which is adjacent to the backbone.

```
Console(config-router)#area 0.0.0.0 virtual-link 10.1.1.252
Console(config-router)#
```

6.20.10.6 Configuring Network Area Addresses

OSPF protocol broadcast messages (that is, Link State Advertisements or LSAs) are restricted by area to limit their impact on network performance. A large network should be split up into separate OSPF areas to increase network stability, and to reduce protocol traffic by summarizing routing information into more compact messages. Each router in an area shares the same view of the network topology, including area links, route summaries for directly connected areas, and external links to other areas.

Command Usage

- Use the Network Area Address Configuration page to specify an Area ID and the corresponding network address range. Each area identifies a logical group of OSPF routers that actively exchange LSAs to ensure that they share an identical view of the network topology.
- Each area must be connected to a backbone area. This area passes routing information between other areas in the autonomous system. The default value 0.0.0.0 is used as the Area ID for the backbone. All routers must be connected to the backbone, either directly, or through a virtual link if a direct physical connection is not possible.
- An area initially configured through the Network Area Address Configuration page is set as a normal area (or transit area) by default. A normal area can send and receive external Link State Advertisements (LSAs). If necessary, use the Area Configuration page to configure an area as a stubby area that cannot send or receive external LSAs, or a not-so-stubby area (NSSA) that can import external route information into its area (page 442).
- An area must be assigned a range of subnetwork addresses. This area and the corresponding address range forms a routing interface, and can be configured to aggregate LSAs from all of its subnetwork addresses and exchange this information with other routers in the network (page 446).

Command Attributes

- **IP Address** – Address of the interfaces to add to the area.
- **Netmask** – Network mask of the address range to add to the area.

- **Area ID** – Area to which the specified address or range is assigned. An OSPF area identifies a group of routers that share common routing information. (The area ID must be in the form of an IP address.)

Note: This router supports up to 16 total areas (either normal transit areas, stubs, or NSSAs).

Web - Click Routing Protocol, OSPF, Network Area Address Configuration. Configure a backbone area that is contiguous with all the other areas in the network, configure an area for all of the other OSPF interfaces, then click Apply.

Network Area Address Configuration

Current Network Address Entries:

IP Address	Netmask	Area ID	Remove
10.0.0.0	255.0.0.0	0.0.0.0	☐
10.1.1.0	255.255.255.0	0.0.0.1	☐
10.1.2.0	255.255.255.0	0.0.0.2	☐
10.1.3.0	255.255.255.0	0.0.0.3	☐
Entry Count: 4			Remove

Network Address Settings:

IP Address	
Netmask	
Area ID	
Set	

Figure 206 OSPF Network Area Address Configuration

CLI - This example configures the backbone area and one transit area.

```

Console(config-router)#network 10.0.0.0 255.0.0.0 area 0.0.0.0
Console(config-router)#network 10.1.1.0 255.255.255.0 area 0.0.0.1
Console(config-router)#end
Console#show ip ospf
Routing Process with ID 10.1.1.253
Supports only single TOS(TOS0) route
Number of area in this router is 4
Area 0.0.0.0 (BACKBONE)
    Number of interfaces in this area is 1
    SPF algorithm executed 8 times
Area 0.0.0.1
    Number of interfaces in this area is 1
    SPF algorithm executed 5 times
Area 0.0.0.2 (STUB)
    Number of interfaces in this area is 1
    SPF algorithm executed 13 times
Area 0.0.0.3 (NSSA)
    Number of interfaces in this area is 1
    SPF algorithm executed 12 times
Console#

```

6.20.10.7 Configuring Summary Addresses (for External AS Routes)

An Autonomous System Boundary Router (ASBR) can redistribute routes learned from other protocols into all attached autonomous systems. (See 6.20.10.8 "Redistributing External Routes" 460) To reduce the amount of external LSAs imported into the local routing domain, configure the router to advertise an aggregate route that consolidates a broad range of external addresses.

Command Usage

- If it is not clear which address ranges can be consolidated, first enable external route redistribution through the Redistribute Configuration screen, view the routes imported into the routing table, and then configure one or more summary addresses to reduce the size of the routing table and consolidate these external routes for advertising into the local domain.
- To summarize routes sent between OSPF areas, use the Area Range Configuration screen (page 446).

Command Attributes

- **IP Address** – Summary address covering a range of addresses.
- **Netmask** – Network mask for the summary route.

Note: This router supports up to 16 Type-5 summary routes.

Web - Click Routing Protocol, OSPF, Summary Address Configuration. Specify the base address and network mask, then click Add.

Summary Address Configuration

Current Summary Address Entries:

IP Address	Netmask	Remove
10.1.0.0	255.255.0.0	☐

Entry Count: 1

Summary Address Settings:

IP Address	
Netmask	
Add	

Figure 207 OSPF Summary Address Configuration

CLI - This example This example creates a summary address for all routes contained in 192.168.x.x.

```
Console(config-router)#summary-address 192.168.0.0 255.255.0.0
Console(config-router)#
```

6.20.10.8 Redistributing External Routes

The router can be configured to import external routing information from other routing protocols into the autonomous system.

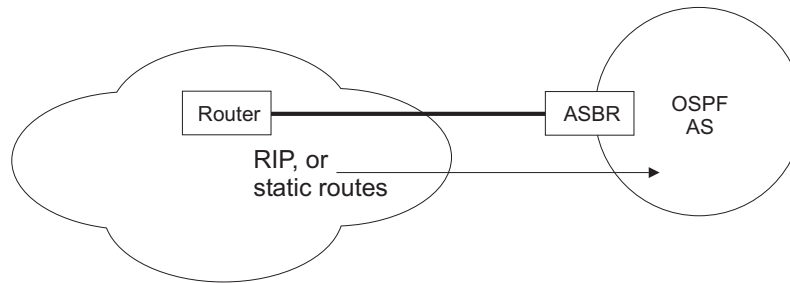


Figure 208 Redistributing External Routes

Command Usage

- This router supports redistribution for both RIP and static routes.
- When external routes are redistributed into an OSPF autonomous system (AS), the router automatically becomes an autonomous system boundary router (ASBR).
- However, if the router has been manually configured as an ASBR through the General Configuration screen, but redistribution is not enabled, the router will only generate a “default” external route into the AS if it has been configured to “always” advertise a default route even if an external route does not actually exist (page 438).
- Metric type specifies the way to advertise routes to destinations outside the autonomous system (AS) through External LSAs. Specify Type 1 to add the internal cost metric to the external route metric. In other words, the cost of the route from any router within the AS is equal to the cost associated with reaching the advertising ASBR, plus the cost of the external route. Specify Type 2 to only advertise external route metric.
- The metric value specified for redistributed routes supersedes the Default External Metric specified in the OSPF / General Configuration screen (page 438).

Command Attributes

- **Redistribute Protocol** – Specifies the external routing protocol type for which routing information is to be redistributed into the local routing domain. (Options: RIP, Static; Default: RIP)
- **Redistribute Metric Type** – Indicates the method used to calculate external route costs. (Options: Type 1, Type 2; Default: Type 1)
- **Redistribute Metric** – Metric assigned to all external routes for the specified protocol. (Range: 1-65535; Default: 10)

Web - Click Routing Protocol, OSPF, Redistribute. Specify the protocol type to import, the metric type and path cost, then click Add.

Redistribute Configuration

Current Redistribute Protocol:

Redistribute Protocol	Redistribute Metric Type	Redistribute Metric	Remove
RIP	Type1	10	☐
Entry Count: 1			Remove

Redistribute Settings:

Redistribute Protocol	RIP
Redistribute Metric Type	Type1
Redistribute Metric (0 - 16777215)	10
Set	

Figure 209 OSPF Redistribute Configuration

CLI - This example redistributes routes learned from RIP as Type 1 external routes.

```
Console(config-router)#redistribute rip metric-type 1
Console(config-router)#
```

6.20.10.9 Configuring NSSA Settings

Use the OSPF / NSSA Settings page to configure a not-so-stubby area (NSSA), and to control the use of default routes for ABRs and ASBRs, or external routes learned from other routing domains and imported through an ABR. (For a detailed description of NSSA areas, refer to “Configuring OSPF Areas” on page 442.)

Command Attributes

- **Area ID** – Identifier for an not-so-stubby area (NSSA).
- **Default Information Originate** – An NSSA ASBR originates and floods Type-7 external LSAs throughout its area for known network destination outside of the AS. However, an NSSA ASBR can also be configured to generate a Type-7 “default” route to areas outside of the AS, or an NSSA ABR to generate a Type-7 “default” route to other areas within the AS. (Default: Disabled)
- **No Redistribution** – The Redistribute Configuration page (page 460) is used to import information from other routing domains (or protocols) into the AS. However, when the router is an NSSA ABR, it can be configured to accept or not accept external routes learned from routers in other OSPF areas into the NSSA. (Default: Enabled)

Note: This router supports up to 16 areas, either normal transit areas, stubs, or NSSAs.

Web - Click Routing Protocol, OSPF, NSSA Settings. Create a new NSSA or modify the routing behavior for an existing NSSA, and click Apply.

NSSA Settings

Current NSSA Settings:

Area ID	Default Information Originate	No Redistribution	Remove
0.0.0.1	Enabled	Disabled	☐
0.0.0.2	Disabled	Enabled	☐

Entry Count: 3 Remove

NSSA Settings:

Area ID	
Default Information Originate	Enabled
No Redistribution	Enabled
Set	

Figure 210 OSPF NSSA Settings

CLI - This example configures area 0.0.0.1 as a stub and sets the cost for the default summary route to 10.

```
Console(config-router)#area 0.0.0.1 nssa
    default-information-originate
Console(config-router)#area 0.0.0.2 nssa no-redistribution
Console(config-router)#
```

6.20.10.10 Displaying Link State Database Information

OSPF routers advertise routes using Link State Advertisements (LSAs). The full collection of LSAs collected by a router interface from the attached area is known as a link state database. Routers that are connected to multiple interfaces will have a separate database for each area. Each router in the same area should have an identical database describing the topology for that area, and the shortest path to external destinations.

The full database is exchanged between neighboring routers as soon as a new router is discovered. Afterwards, any changes that occur in the routing tables are synchronized with neighboring routers through a process called reliable flooding. The router can show information about different LSAs stored in its database, which may include any of the following types:

- Router (Type 1) – All routers in an OSPF area originate Router LSAs that describe the state and cost of its active interfaces and neighbors.
- Network (Type 2) – The designated router for each area originates a Network LSA that describes all the routers that are attached to this network segment.
- Summary (Type 3) – Area border routers can generate Summary LSAs that give the cost to a subnetwork located outside the area.
- AS Summary (Type 4) – Area border routers can generate AS Summary LSAs that give the cost to an autonomous system boundary router (ASBR).
- AS External (Type 5) – An ASBR can generate an AS External LSA for each known network destination outside the AS.
- NSSA External (Type 7) – An ASBR within an NSSA generates an NSSA external link state advertisement for each known network destination outside the AS.

Command Attributes

- **Area ID** – Area defined for which LSA information is to be viewed. (This item must be entered in the form of an IP address.)
- **Link ID** – The network portion described by an LSA. The Link ID should be:
 - An IP network number for Type 3 Summary and Type 5 AS External LSAs. (When an Type 5 AS External LSA is describing a default route, its Link ID is set to the default destination 0.0.0.0.)
 - A Router ID for Router, Network, and Type 4 AS Summary LSAs.
- **Self-Originate** – Shows LSAs originated by this router.
- **LS Type** – LSA Type (Options: Type 1-5, 7). See the preceding description.

- **Adv Router** – IP address of the advertising router. If not entered, information about all advertising routers is displayed.

The following parameters are read only.

- **Age** – Age of LSA (in seconds).
- **Seq** – Sequence number of LSA (used to detect older duplicate LSAs).
- **Checksum** – Checksum of the complete contents of the LSA.

Web - Click Routing Protocol, OSPF, Link State Database Information. Specify parameters for the LSAs to display, then click Query.

Link State Database Information

Query by:

☐ Area ID: 0.0.0.0 ☐ LS Type: Type 1 : RouterLink

☐ Link ID: ☐ ADV Router:

☐ Self-Originate: 10.2.0.1

Query By : "none"

Search Results : 22 results (Total)

Type 1 : RouterLink (1) Type 2 : NetworkLink (2) Type 3 : SummaryLink (3)

Type 4 : asSummaryLink (4) Type 5 : asExternalLink (5) Type 7 : NSSAExternalLink (7)

Link State Data Router (Type 1)

Area ID	Link ID	ADV Router	Age	Seq#	Checksum
0.0.0.1	10.2.45.188	10.2.44.50	1002	0x8000001B	0xDCB7

Figure 211 OSPF Link State Database Information

CLI - The CLI provides a wider selection of display options for viewing the Link State Database. See “show ip ospf database” on page 1085.

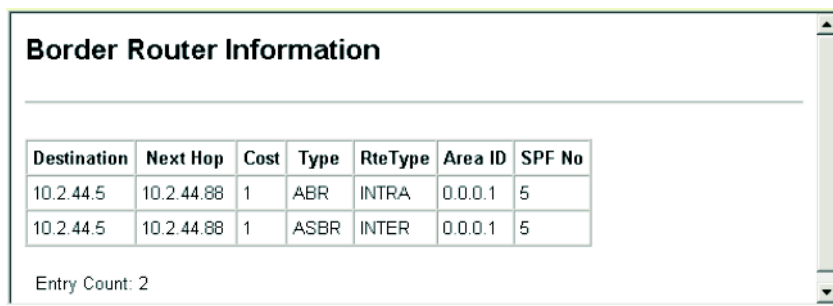
6.20.10.11 Displaying Information on Border Routers

The router can display entries in the local routing table for Area Border Routers (ABR) and Autonomous System Boundary Routers (ASBR) known by this device.

Field Attributes

- **Destination** – Identifier for the destination router.
- **Next Hop** – IP address of the next hop toward the destination.
- **Cost** – Link metric for this route.
- **Type** – Router type of the destination; either ABR, ASBR or both.
- **Rte Type** – Route type; either intra-area or interarea route (INTRA or INTER).
- **Area** – The area from which this route was learned.
- **SPF No** – The number of times the shortest path first algorithm has been executed for this route.

Web - Click Routing Protocol, OSPF, Border Router Information.



Destination	Next Hop	Cost	Type	RteType	Area ID	SPF No
10.2.44.5	10.2.44.88	1	ABR	INTRA	0.0.0.1	5
10.2.44.5	10.2.44.88	1	ASBR	INTER	0.0.0.1	5

Entry Count: 2

Figure 212 OSPF Border Router Information

CLI - This example shows one router that serves as both the ABR for the local area and the ASBR for the autonomous system.

```
Console#show ip ospf border-routers
```

Destination	Next Hop	Cost	Type	RteType	Area	SPF No
10.2.44.5	10.2.44.88	1	ABR	INTRA	0.0.0.1	5
10.2.44.5	10.2.44.88	1	ASBR	INTER	0.0.0.1	5

```
Console#
```

6.20.10.12 Displaying Information on Neighbor Routers

The router can display about neighboring routers on each interface within an OSPF area.

Field Attributes

- **ID** – Neighbor's router ID.
- **Priority** – Neighbor's router priority.
- **State** – OSPF state and identification flag.

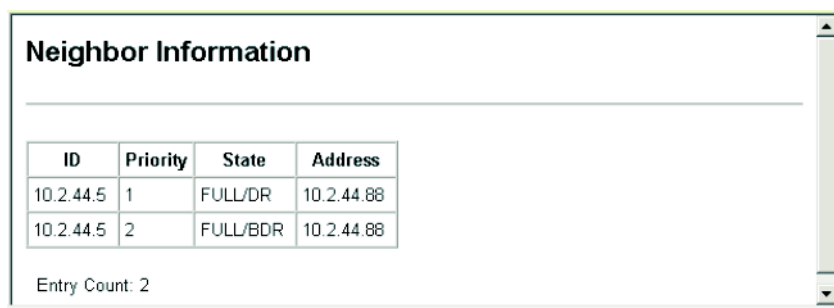
States include:

- Down – Connection down
- Attempt – Connection down, but attempting contact (non-broadcast networks)
- Init – Have received Hello packet, but communications not yet established
- Two-way – Bidirectional communications established
- ExStart – Initializing adjacency between neighbors
- Exchange – Database descriptions being exchanged
- Loading – LSA databases being exchanged
- Full – Neighboring routers now fully adjacent

Identification flags include:

- D – Dynamic neighbor
- S – Static neighbor
- DR – Designated router
- BDR – Backup designated router
- **Address** – IP address of this interface.

Web - Click Routing Protocol, OSPF, Neighbor Information.



The screenshot shows a web interface titled "Neighbor Information". Below the title is a table with four columns: ID, Priority, State, and Address. There are two rows of data. Below the table, it says "Entry Count: 2".

ID	Priority	State	Address
10.2.44.5	1	FULL/DR	10.2.44.88
10.2.44.5	2	FULL/BDR	10.2.44.88

Entry Count: 2

Figure 213 OSPF Neighbor Information

CLI - This shows a designated router and backup designated router as neighbors.

```

Console#show ip ospf neighbor

      ID                Pri          State           Address
-----
  10.2.44.5             1          FULL/DR       10.2.44.88
  10.2.44.6             2          FULL/BDR       10.2.44.88

Console#

```

6.21 Multicast Routing

This router can route multicast traffic to different subnetworks using either Distance Vector Multicast Routing Protocol (DVMRP) or Protocol-Independent Multicasting - Dense Mode or Sparse Mode (PIM-DM or PIM-SM). These protocols all rely on messages sent from IGMP-enabled Layer 2 switches and hosts to determine when hosts want to join or leave multicast groups.

DVMRP and PIM-DM flood multicast traffic downstream, and calculate the shortest-path, source-rooted delivery tree between each source and destination host group. DVMRP builds a source-rooted multicast delivery tree that allows it to prevent looping and determine the shortest path to the source of the multicast traffic. PIM-DM also builds a source-rooted multicast delivery tree for each multicast source, but uses information from the router's unicast routing table instead of maintaining its own multicast routing table, making it routing protocol independent.

PIM-SM uses the router's local unicast routing table, but does not flood multicast traffic. It only forwards multicast traffic when requested by a local or downstream host. When service is requested by a host, it can use a Reverse Path Tree (RPT) that channels the multicast traffic from each source through a single Rendezvous Point (RP) within the local PIM-SM domain, and then forwards this traffic to the Designated Router (DR) in the local network segment to which the hosts is attached. However, when the multicast load from a particular source is heavy enough to justify it, PIM-SM can be configured to construct a Shortest Path Tree (SPT) directly from the DR up to the source, bypassing the RP and thereby reducing service delays for active hosts and setup time for new hosts.

Also, note that if DVMRP and PIM are not enabled on this router or another multicast routing protocol is used on the network, the ECN330-switch ports attached to a multicast router can be manually configured to forward multicast traffic (page 358).

6.21.1 Configuring Global Settings for Multicast Routing

To use multicast routing on this router, first globally enable multicast routing as described in this section, then globally enable DVMRP (page 474) or PIM-DM (page 484) or PIM-SM (page 493), and specify the interfaces that will participate (page 479, page 485 or page 497, respectively). Note that only one multicast routing protocol can be enabled on any given interface.

Web – Click IP, Multicast Routing, General Setting. Set Multicast Forwarding Status to Enabled, and click Apply.

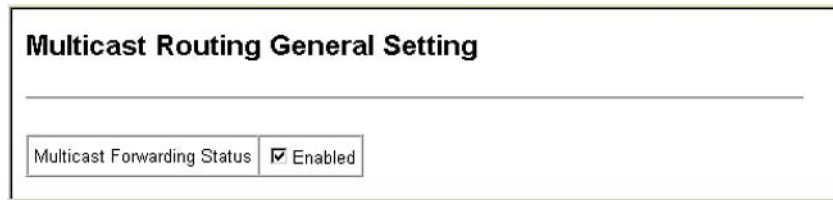


Figure 214 Multicast Routing General Settings

CLI – This example enables multicast routing globally for the router.

```
Console(config)#ip multicast-routing
Console(config)#
```

6.21.2 Displaying the Multicast Routing Table

The router can display information on each multicast route it has learned through DVMRP or PIM. The router learns multicast routes from neighboring routers, and also advertises these routes to its neighbors. The router stores entries for all paths learned by itself or from other routers, without considering actual group membership or prune messages. The routing table therefore does not indicate that the router has processed multicast traffic from any particular source listed in the table. It uses these routes to forward multicast traffic only if group members appear on directly-attached subnetworks or on subnetworks attached to downstream routers.

Field Attributes

- **Group Address** – IP group address for a multicast service.
- **Source Address** – Subnetwork containing the IP multicast source.
- **Netmask** – Network mask for the IP multicast source.
- **Interface** – Interface leading to the upstream neighbor.
- **Owner** – The associated multicast protocol (DVMRP or PIM).

- **Flags** – The flags associated with each routing entry indicate:
 - C – Source is directly connected to this subnet
 - D – PIM Dense Mode
 - F – The interface is still active and forwarding
 - J – This interface has joined the Shortest Path Tree (SPT)
 - L – Downstream interface has received IGMP report message from host in this subnet
 - P – Downstream interface has been recently pruned (terminated)
 - R – Reverse Path Tree (RPT) bit is set for Sparse Mode
 - S – PIM Sparse Mode
 - T – Shortest Path Tree (SPT) bit is set for Space Mode
- **Detail** – This button displays detailed information for the selected entry.

The following parameters are displayed in the IP Multicast Routing Entry (Detail) table.

- **Upstream Router** – The multicast router immediately upstream for this group.
- **Downstream** – Interface(s) on which multicast subscribers have been recorded.

Web – Click IP, Multicast Routing, Multicast Routing Table. Click Detail to display additional information for any entry.

IP Multicast Routing Table (Summary)						
Flags: P - Prune Up						
Group Address	Source Address	Net Mask	Interface	Owner	Flags	Detail
234.5.6.7	192.168.0.196	255.255.255.255	VLAN1	DVMRP	P	Detail
234.5.6.8	192.168.0.196	255.255.255.255	VLAN1	DVMRP	P	Detail
Entry Count: 2						

IP Multicast Routing Entry (Detail)	
IP Multicast Routing Table	
Flags: D-Dense,S-Sparse,C-Connect,L-Local,P-Prune,R- RP-bit set, F-Register flag,T- SPT-bit set,J-Join SPT, Instance state : F-Forwarding,P-Pruned	
Source Address:	192.168.0.196
RP Address:	0.0.0.0
Net Mask:	255.255.255.255
Group Address:	234.5.6.7
Owner:	DVMRP
Upstream Interface:	VLAN 1
Upstream Router:	0.0.0.0
Downstream:	(none)

Figure 215 Multicast Routing Table

CLI – This example shows that multicast forwarding is enabled. The multicast routing table displays one entry for a multicast source routed by DVMRP, and another source routed through PIM.

```

Console#show ip mroute
IP Multicast Forwarding is enabled.

IP Multicast Routing Table

Flags:  P - Prune, F - Forwarding

(234.5.6.7, 10.1.0.0, 255.255.255.0)
Owner: DVMRP
Upstream Interface: vlan2
Upstream Router: 10.1.0.0
Downstream:

(234.5.6.8, 10.1.5.19, 255.255.255.255)
Owner: PIM-DM
Upstream Interface: vlan3
Upstream Router: 10.1.5.19
Downstream:

Console#

```

6.21.3

Configuring DVMRP

The Distance-Vector Multicast Routing Protocol (DVMRP) behaves somewhat similarly to RIP. A router supporting DVMRP periodically floods its attached networks to pass information about supported multicast services along to new routers and hosts. Routers that receive a DVMRP packet send a copy out to all paths (except the path back to the origin). These routers then send a prune message back to the source to stop a data stream if the router is attached to a LAN which does not want to receive traffic from a particular multicast group. However, if a host attached to this router issues an IGMP message indicating that it wants to subscribe to the concerned multicast service, this router will use DVMRP to build up a source-rooted multicast delivery tree that allows it to prevent looping and determine the shortest path to the source of this multicast traffic.

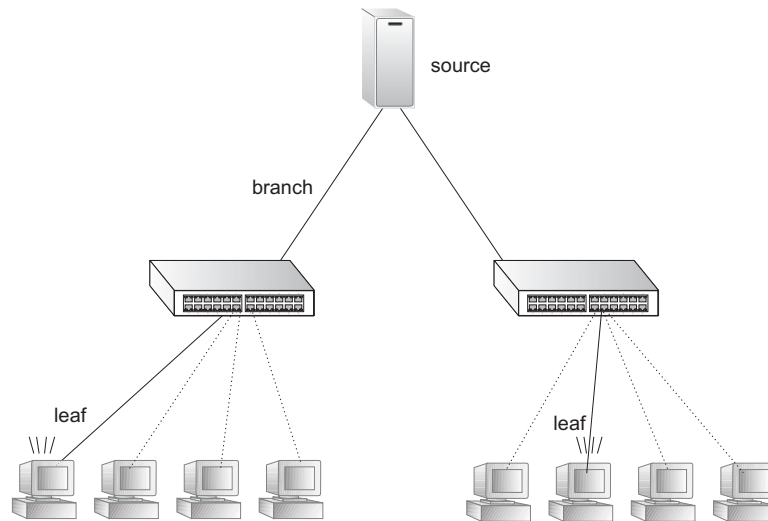


Figure 216 DVMRP Concept

When this router receives the multicast message, it checks its unicast routing table to locate the port that provides the shortest path back to the source. If that path passes through the same port on which the multicast message was received, then this router records path information for the concerned multicast group in its routing table and forwards the multicast message on to adjacent routers, except for the port through which the message arrived. This process eliminates potential loops from the tree and ensures that the shortest path (in terms of hop count) is always used.

6.21.3.1 Configuring Global DVMRP Settings

DVMRP is used to route multicast traffic to nodes which have requested a specific multicast service through IGMP. This router uses Reverse Path Forwarding (RPF) to build a shortest-path delivery tree that begins at the source and spreads out to reach group members through the network. RPF uses three different techniques to dynamically reconfigure the multicast spanning tree: broadcasting, pruning, and grafting.

Command Usage

Broadcasting periodically floods the network with traffic from any active multicast server. If IGMP snooping is disabled, multicast traffic is flooded to all ports on the router. However, if IGMP snooping is enabled, then the first packet for any source group pair is flooded to all DVMRP downstream neighbors. If a

packet is received through an interface that the router determines to be the shortest path back to the source (based on interface metrics), then the router forwards the packet on all interfaces except for the incoming interface.

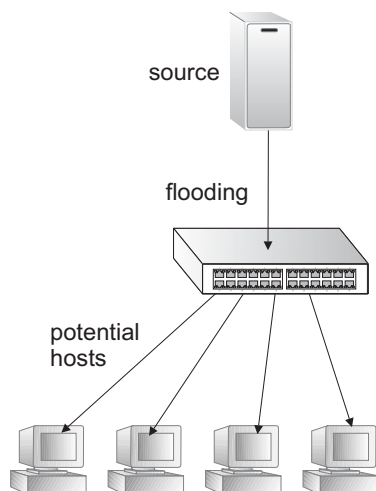


Figure 217 DVMRP Broadcasting

The router will transmit a prune message back out the receiving interface (the parent interface) to its upstream neighboring router if there are no group members on its child interfaces. A prune message tells the upstream router to stop forwarding packets for a particular source-group pair for the prune lifetime.

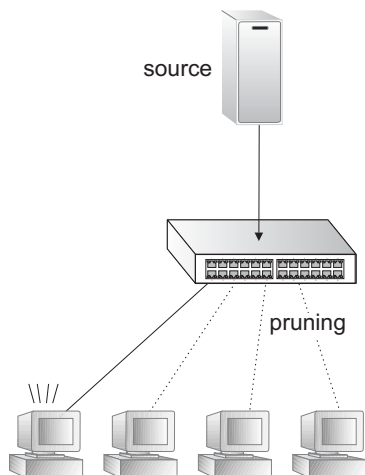


Figure 218 DVMRP Pruning

If the router that previously sent a prune message now discovers a new group member on one of its connections, it sends a graft message to the upstream router. When an upstream router receives this message, it cancels the prune message. If necessary, graft messages are propagated back toward the source until reaching the nearest live branch in the multicast tree.

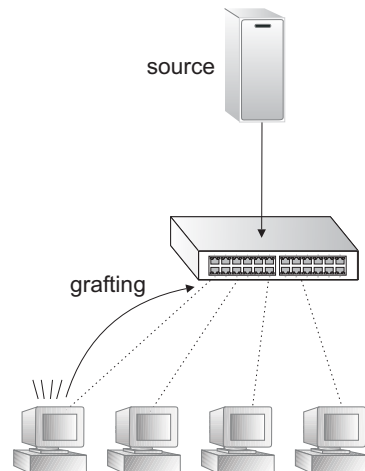


Figure 219 DVMRP Grafting

The global settings that control the prune and graft messages (that is, prune lifetime) should be configured to the same values on all routers throughout the network to allow DVMRP to function properly. However, if problems are encountered in maintaining a multicast flow, then it may be necessary to modify the protocol variables which control the exchange of topology information between DVMRP routers; such as the probe interval, neighbor timeout or report interval.

Command Attributes

- **DVMRP Protocol** – Enables/disables DVMRP globally. (Default: Disabled)
- **Probe Interval** – Sets the interval for sending neighbor probe messages to the multicast group address for all DVMRP routers. Probe messages are sent to neighboring DVMRP routers from which this device has received probes, and is used to verify whether or not these neighbors are still active members of the multicast tree. (Range: 1-65535 seconds; Default: 10 seconds)

- **Neighbor Timeout Interval** – Sets the interval to wait for messages from a DVMRP neighbor before declaring it dead. This command is used for timing out routes, and for setting the children and leaf flags. (Range: 1-65535 seconds; Default: 35 seconds)
- **Report Interval** – Specifies how often to propagate the complete set of routing tables to other neighbor DVMRP routers. (Range: 1-65535 seconds; Default: 60 seconds)
- **Flash Update Interval** – Specifies how often to send trigger updates, which reflect changes in the network topology.
- **Prune Lifetime** – Specifies how long a prune state will remain in effect for a multicast tree. (Range: 1-65535; Default: 7200 seconds)

The following parameter is configurable from the CLI only.

- **Default Gateway** – Specifies the default DVMRP gateway for IP multicast traffic. (Default: none)
 - The specified interface advertises itself as a default route to neighboring DVMRP routers. It advertises the default route out through its other interfaces. Neighboring routers on the other interfaces return Poison Reverse messages for the default route back to the router. When the router receives these messages, it records all the downstream routers for the default route.
 - When multicast traffic with an unknown source address (not found in the route table) is received on the default upstream route interface, the router forwards this traffic out through the other interfaces (with known downstream routers). However, when multicast traffic with an unknown source address is received on another interface, the router drops it because only the default upstream interface can forward multicast traffic from an unknown source.

Web – Click Routing Protocol, DVMRP, General Settings. Enable or disable DVMRP. Set the global parameters that control neighbor timeout, the exchange of routing information, or the prune lifetime, and click Apply.

DVMRP General Settings	
DVMRP Protocol	Enabled ▾
Probe Interval (seconds)	10
Neighbor Timeout Interval (seconds)	35
Report Interval (seconds)	60
Flash Update Interval (seconds)	5
Prune Lifetime (seconds)	7200

Figure 220 DVMRP General Settings

CLI – This sets the global parameters for DVMRP and displays the current settings.

```

Console(config)#router dvmrp
Console(config-router)#probe-interval 30
Console(config-router)#nbr-timeout 40
Console(config-router)#report-interval 90
Console(config-router)#flash-update-interval 10
Console(config-router)#prune-lifetime 5000
Console(config-router)#default-gateway 10.1.0.253
Console(config-router)#end
Console#show router dvmrp
Admin Status                : enable
Probe Interval               : 10
Nbr expire                   : 35
Minimum Flash Update Interval : 5
prune lifetime               : 7200
route report                  : 60
Default Gateway               :
Console#

```


6.21.3.2 Configuring DVMRP Interface Settings

To fully enable DVMRP, multicast routing needs to be enabled globally for the router (page 469), then enable DVMRP globally for the router (page 474), and also enable DVMRP for each interface that will participate in multicast routing.

Command Attributes

DVMRP Interface Information

- **Interface** – VLAN interface on this router that has enabled DVMRP.
- **Address** – IP address of this VLAN interface.
- **Metric** – The metric for this interface used to calculate distance vectors.
- **Status** – Shows that DVMRP is enabled on this interface.

DVMRP Interface Settings

- **VLAN** – Selects a VLAN interface on this router.
- **Metric** – Sets the metric for this interface used to calculate distance vectors.
- **Status** – Enables or disables DVMRP.
 - If DVMRP is enabled on any interface, Layer 3 IGMP should also be enabled on the router (page 362).
 - If DVMRP is disabled, the interface cannot propagate IP multicast routing information. However, as long as IGMP snooping is enabled, the interface will still forward multicast traffic to downstream group members within the VLAN. But if IGMP snooping is disabled, then the interface will flood incoming multicast traffic to all ports in the attached VLAN.

Web – Click Routing Protocol, DVMRP, Interface Settings. Select a VLAN from the drop-down box under DVMRP Interface Settings, modify the Metric if required, set the Status to Enabled or Disabled, and click Apply.

Interface	Address	Metric	Status
VLAN1	10.1.0.253	1	Enabled
VLAN2	10.1.1.253	1	Enabled

Entry Count: 2

DVMRP Interface Settings

VLAN:

Metric (1 - 31):

Status:

Figure 221 DVMRP Interface Settings

CLI – This example enables DVMRP and sets the metric for VLAN 1.

```

Console(config)#interface vlan 1
Console(config-if)#ip dvmrp
Console(config-if)#ip dvmrp metric 2
Console(config-if)#end
Console#show ip dvmrp interface
Vlan 1 is up
    DVMRP is enabled
    Metric is 2

Console#

```

6.21.3.3 Displaying Neighbor Information

The router can display all the neighboring DVMRP routers.

Command Attributes

- **Neighbor Address** – The IP address of the network device immediately upstream for this multicast delivery tree.
- **Interface** – The IP interface on this router that connects to the upstream neighbor.
- **Up time** – The time since this device last became a DVMRP neighbor to this router.
- **Expire** – The time remaining before this entry will be aged out.
- **Capabilities** – A hexadecimal value that indicates the neighbor's capabilities. Each time a probe message is received from a neighbor, the router compares the capabilities bits with the previous version for that neighbor to check for changes in neighbor capabilities. (Refer to draft-ietf-idmr-dvmrp-v3-11.txt section 3.2.2 for a detailed description of these bits). These bits are described below:
 - Leaf (bit 0) - Neighbor has only one interface with neighbors.
 - Prune (bit 1) - Neighbor supports pruning.
 - Generation ID (bit 2) - Neighbor sends its Generation ID in probe messages.
 - Mtrace (bit 3) - Neighbor can handle multicast trace requests.

Web – Click Routing Protocol, DVMRP, Neighbor Information.

DVMRP Neighbor Information				
Neighbor Address	Interface	Up time	Expire	Capabilities
10.1.0.254	VLAN1	79215	31	6

Entry Count: 1

Figure 222 DVMRP Neighbor Information

CLI – This example displays the only neighboring DVMRP router.

```
Console#show ip dvmrp neighbor
```

Address	Interface	Uptime	Expire	Capabilities
10.1.0.254	vlan1	79315	32	6

```
Console#
```

6.21.3.4

Displaying the Routing Table

The router learns source-routed information from neighboring DVMRP routers and also advertises learned routes to its neighbors. The router merely records path information it has learned on its own or from other routers. It does not consider group membership or prune messages. Information stored in the routing table includes subnetworks from which IP multicast traffic originates, upstream routers that have sent multicast traffic in the past or have been learned through routing messages exchanged with other routers, interfaces connected to an upstream router, or outgoing interfaces that are connected to multicast hosts.

The DVMRP routing table contains multicast route information learned through DVMRP route updates, and is used to forward IP multicast traffic. The routes listed in the table do not reflect actual multicast traffic flows. For this information, look at the IGMP Member Port Table (page 361) or the IGMP Group Membership Table (page 368).

Command Attributes

- **IP Address** – IP subnetwork that contains a multicast source, an upstream router, or an outgoing interface connected to multicast hosts.
- **Netmask** – Subnet mask that is used for the source address. This mask identifies the host address bits used for routing to specific subnets.
- **Upstream Neighbor** – IP address of the network device immediately upstream for each multicast group.
- **Interface** – The IP interface on this router that connects to the upstream neighbor.
- **Metric** – The metric for this interface used to calculate distance vectors.
- **Up time** – The time elapsed since this entry was created.
- **Expire** – The time remaining before this entry will be aged out.

Web – Click Routing Protocol, DVMRP, DVMRP Routing Table.

Ip Address	Netmask	Upstream Neighbor	Interface	Metric	Up time	Expire
10.1.0.0	255.255.255.0	10.1.0.253	VLAN1	1	84279	0
10.1.1.0	255.255.255.0	10.1.1.253	VLAN2	1	84828	0
10.1.8.0	255.255.255.0	10.1.0.254	VLAN1	2	19570	134

Entry Count: 3

Figure 223 DVMRP Routing Table

CLI – This example displays known DVMRP routes.

```
Console#show ip dvmrp route
```

Source	Mask	Upstream_nbr	Interface	Metric	UpTime	Expire
10.1.0.0	255.255.255.0	10.1.0.253	vlan1	1	84438	0
10.1.1.0	255.255.255.0	10.1.1.253	vlan2	1	84987	0
10.1.8.0	255.255.255.0	10.1.0.254	vlan1	2	19729	97

Console#

6.21.4 Configuring PIM-DM

Protocol-Independent Multicasting (PIM) provides two different modes of operation: sparse mode and dense mode. Sparse mode (SM) is designed for networks where the probability of multicast group members is low, such as the Internet. Dense mode (DM), on the other hand, is designed for networks where the probability of multicast group members is high, such as a local network. For information on configuring PIM-SM, see “Configuring PIM-SM” on page 490.

PIM-DM is a simple multicast routing protocol that uses flood and prune to build a source-routed multicast delivery tree for each multicast source-group pair. It is simpler than DVMRP because it does not maintain its own routing table. Instead, it uses the routing table provided by the unicast routing protocol enabled on the router interface. When the router receives a multicast packet for a source-group pair, PIM-DM checks the unicast routing table on the inbound interface to determine if this is the same interface used for routing unicast packets to the multicast source network. If it is not, the router drops the packet and sends a prune message back out the source interface. If it is the same interface used by the unicast protocol, then the router forwards a copy of the packet to all the other interfaces for which it has not already received a prune message for this specific source-group pair.

DVMRP holds the prune state for about two hours, while PIM-DM holds it for only about three minutes. This results in more flooding than encountered with DVMRP, but this is the only major trade-off for the lower processing overhead and simplicity of configuration for PIM-DM.

6.21.4.1 Configuring Global PIM-DM Settings

PIM-DM is used to route multicast traffic to nodes which have requested a specific multicast service through IGMP. It uses the router's unicast routing table to determine if the interface through which a packet is received provides the shortest path back to the source. This is done on a per hop basis back toward the source of the multicast delivery tree. PIM-DM uses three different techniques to dynamically reconfigure the multicast spanning tree: broadcasting, pruning, and grafting.

To use PIM-DM, it must be enabled globally for the router, as described below, and for each interface that will support multicast routing as described in the next section. Also note that IGMP must be enabled to allow the router to determine the location of group members.

Web – Click Routing Protocol, PIM-DM, General Settings. Enable or disable PIM-DM globally for the router, and click Apply.

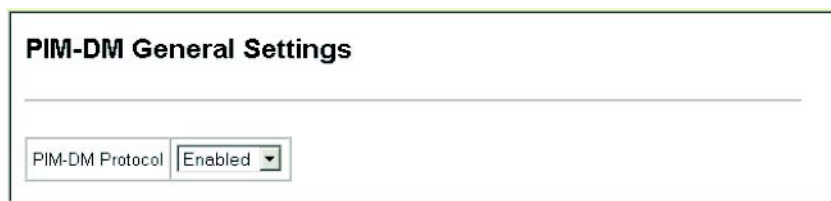


Figure 224 PIM-DM General Settings

CLI – This example enables PIM-DM globally and displays the current status.

```
Console(config)#router pim dense mode
Console#show router pim
PIM Dense-Mode Admin Status: Enabled
PIM Sparse-Mode Admin Status: Disabled
Console#
```

6.21.4.2

Configuring PIM-DM Interface Settings

To fully enable PIM-DM, multicast routing needs to be enabled globally for the router (page 469), then enable PIM-DM globally for the router (page 484), and also enable PIM-DM for each interface that will participate in multicast routing.

Command Usage

- PIM-DM functions similar to DVMRP by periodically flooding the network with traffic from any active multicast server (page 473). It also uses IGMP to determine the presence of multicast group members. The main difference, is that it uses the router's unicast routing table to determine if the interface through which a packet is received provides the shortest path back to the source.
- Dense-mode interfaces are subject to multicast flooding by default, and are only removed from the multicast routing table when the router determines that there are no group members or downstream routers, or when a prune message is received from a downstream router.
- The interface settings that control the prune and graft messages (prune holdtime) should be configured to the same values on all routers throughout the network to allow PIM to function properly.

Command Attributes

- **VLAN** – Selects a VLAN interface on this router.
- **PIM-DM Protocol Status** – Enables/disables PIM-DM.
(Default: Disabled)
- **Hello Interval** – Sets the frequency at which PIM hello messages are transmitted. Hello messages are sent to neighboring PIM routers from which this device has received probes, and are used to verify whether or not these neighbors are still active members of the multicast tree.
(Range: 1-65535 seconds; Default: 30)
- **Hello Holdtime** – Sets the interval to wait for hello messages from a neighboring PIM router before declaring it dead. Note that the hello holdtime should be 3.5 times the value of Hello Interval. (Range: 1-65535 seconds; Default: 105)
- **Trigger Hello Interval** – Configures the maximum time before transmitting a triggered PIM hello message after the router is rebooted or PIM is enabled on an interface. (Range: 1-65535 seconds; Default: 5)
 - When a router first starts or PIM is enabled on an interface, the hello-interval is set to random value between 0 and the Trigger Hello Interval. This prevents synchronization of Hello messages on multi-access links if multiple routers are powered on simultaneously.
 - Also, if a Hello message is received from a new neighbor, the receiving router will send its own Hello message after a random delay between 0 and the Trigger Hello Interval.
- **Prune Holdtime** – Configures of the hold time for the prune state. The multicast interface that first receives a multicast stream from a particular source forwards this traffic to all other PIM interfaces on the router. If there are no requesting groups on that interface, the leaf node sends a prune message upstream and enters a prune state for this multicast stream. The prune state is maintained until the prune holdtime timer expires or a graft message is received for the forwarding entry.
(Range: 1-65535 seconds; Default: 210)
- **Graft Retry Interval** – Configures the time to wait for a graft acknowledgement before resending a graft. A graft message is sent by a router to cancel a prune state. When a router receives a graft message, it must respond with an graft acknowledgement message. If this acknowledgement message is lost, the router that sent the graft

message will resend it a maximum number of times as defined by Max Graft Retries. (Range: 1-65535 seconds; Default: 3)

- **Max Graft Retries** – Configures the maximum number of times to resend a graft message if it has not been acknowledged. (Range: 1-65535; Default: 2)

Web – Click Routing Protocol, PIM-DM, Interface Settings. Select a VLAN, enable or disable PIM-DM for the selected interface, modify any of the protocol parameters as required, and click Apply.

PIM-DM Interface Settings	
VLAN	2
PIM-DM Protocol Status	Enabled
Hello Interval (seconds)	30
Hello Holdtime (seconds)	105
Trigger Hello Interval (seconds)	5
Join/Prune Holdtime (seconds)	210
Graft Retry Interval (seconds)	3
Max Graft Retries	2

Figure 225 PIM-DM Interface Settings

CLI – This example sets the PIM-DM protocol parameters for VLAN 2, and displays the current settings.

```

Console(config)#interface vlan 2
Console(config-if)#ip pim dense-mode
Console(config-if)#ip pim hello-interval 60
Console(config-if)#ip pim hello-holdtime 210
Console(config-if)#ip pim trigger-hello-interval 10
Console(config-if)#ip pim join-prune-holdtime 60
Console(config-if)#ip pim graft-retry-interval 9
Console(config-if)#ip pim max-graft-retries 5
Console(config-if)#end
Console#show ip pim interface 2
Vlan 2 is up
  PIM is enabled, mode is Dense.
  Internet address is 10.1.1.253.
  Hello time interval is 60 sec, trigger hello time interval is 10
    sec.
  Hello holdtime is 210 sec.
  Join/Prune holdtime is 60 sec.
  Graft retry interval is 9 sec, max graft retries is 5.
  DR Internet address is 10.1.1.253, neighbor count is 0.

Console#

```

6.21.4.3 Displaying Interface Information

The router can display a summary of the current interface status for PIM-DM, including the number of neighboring PIM routers, and the address of the designated PIM router.

Command Attributes

- **Interface** – A VLAN interface on this router.
- **Address** – The IP address for this interface.
- **Mode** – The PIM mode in use (that is, Dense Mode).
- **Neighbor Count** – The number of PIM neighbors detected on this interface.
- **DR Address** – The designated PIM router for this interface.

Web – Click Routing Protocol, PIM-DM, Interface Information.

PIM-DM Interface Information				
Interface	Address	Mode	Neighbor Count	DR Address
VLAN1	10.1.0.252	Dense	1	10.1.0.253
VLAN10	10.1.9.252	Dense	0	10.1.9.252

Entry Count: 2

Figure 226 PIM-DM Interface Information

CLI – This example shows the PIM-DM interface summary for VLAN 1.

```

Console#show ip pim interface 1
Vlan 1 is up
PIM is enabled, mode is Dense.
Internet address is 10.1.0.253.
Hello time interval is 30 sec, trigger hello time interval is 5
sec.
Hello holdtime is 105 sec.
Join/Prune holdtime is 210 sec.
Graft retry interval is 3 sec, max graft retries is 2.
DR Internet address is 10.1.0.253, neighbor count is 1.

Console#

```

6.21.4.4 Displaying Neighbor Information

The router can display all the neighboring PIM-DM routers.

Command Attributes

- **Neighbor Address** – IP address of the next-hop router.
- **Interface** – VLAN that is attached to this neighbor.
- **Up time** – The duration this entry has been active.
- **Expire** – The time before this entry will be removed.
- **Mode** – PIM mode used on this interface.

Web – Click Routing Protocol, PIM-DM, Neighbor Information.

PIM-DM Neighbor Information				
Neighbor Address	Interface	Up time	Expire	Mode
10.1.0.253	VLAN1	596	78	
Entry Count: 1				

Figure 227 PIM-DM Neighbor Information

CLI – This example displays the only neighboring PIM-DM router.

Console#show ip pim neighbor						
Address	VLAN	Interface	Uptime	Expire	Mode	
-----	-----	-----	-----	-----	-----	-----
10.1.0.253		1	613	91	Dense	
Console#						

6.21.5 Configuring PIM-SM

Protocol-Independent Multicasting (PIM) provides two different modes of operation: sparse mode and dense mode. Sparse mode (SM) is designed for networks where the probability of multicast group members is low, such as the Internet. Dense mode (DM), on the other hand, is designed for networks where the probability of multicast group members is high, such as a local network. For information on configuring PIM-DM, see “Configuring PIM-DM” on page 484.

PIM-SM reduces the amount of multicast traffic by forwarding it only to the ports that are attached to receivers for the group. The key components to filtering multicast traffic are listed below:

Common Domain – A common domain must be set up in which all of the multicast routers are configured with the same basic PIM-SM settings.

Bootstrap Router (BSR) – After the common domain is set, a bootstrap router is elected from this domain. Each time a PIM-SM router is booted up, or the multicast mode reconfigured to enable PIM-SM, the bootstrap router candidates start flooding bootstrap messages on all of their interfaces (using reverse path forwarding to limit the impact on the network). When neighboring routers receive

bootstrap messages, they process the message and forward it out all interfaces, except for the interface on which this message was received. If a router receives a bootstrap message with a BSR priority larger than its own, it stops advertising itself as a BSR candidate. Eventually, only the router with the highest BSR priority will continue sending bootstrap messages.

Rendezvous Point (RP) – A router may periodically send PIMv2 messages to the BSR advertising itself as a candidate RP for specified group addresses. The BSR places information about all of the candidate RPs in subsequent bootstrap messages. The BSR and all the routers receiving these messages use the same hash algorithm to elect an RP for each multicast group. If each router is properly configured, the results of the election process will be the same for each router. Each elected RP then starts to serve as the root of a shared distribution tree for one or more multicast groups.

Designated Router (DR) – A DR advertising the highest priority in its hello messages is elected for each subnet. The DR is responsible for collecting information from the subnet about multicast clients that want to join or leave a group. Join messages from the DR (receiver) for each group are sent towards the RP, and data from multicast sources is sent to the RP. Receivers can now start receiving traffic destined for the client group from the RP, or they can identify the senders and optionally set up a direct connection to the source through a shortest path tree (SPT) if the load warrants this change over.

Shared Tree – When many receivers join a group, their Join messages converge on the RP, and form a distribution tree for the group that is rooted at the RP. This is known as the Reverse Path Tree (RPT), or the shared tree since it is shared by all sources sending to that group. When a multicast source sends data destined for a group, the source's local DR takes those data packets, unicast-encapsulates them, and sends them to the RP. When the RP receives these encapsulated data packets, it decapsulates them, and forwards them onto the shared tree. These packets follow the group mapping maintained by routers along the RP Tree, are replicated wherever the RP Tree branches, and eventually reach all the receivers for that multicast group. Because all routers along the shared tree are using PIM-SM, the multicast flow is confined to the shared tree. Also, note that more than one flow can be carried over the same shared tree, but only one RP is responsible for each flow.

Shortest Path Tree (SPT) – When using the Shared Tree, multicast traffic is contained within the shared tree. However, there are several drawbacks to using the shared tree. Decapsulation of traffic at the RP into multicast packets is a resource intensive process. The protocol does not take into account the location of group members when selecting the RP, and the path from the RP to the

receiver is not always optimal. Moreover, a high degree of latency may occur for hosts wanting to join a group because the RP must wait for a register message from the DR before setting up the shared tree and establishing path back to the source. There is also a problem with bursty sources. When a source frequently times out, the shared tree has to be rebuilt each time, causing further latency in sending traffic to the receiver.

To enhance overall network performance, the ECN330-switch uses the RP only to forward the first packet from a source to the receivers. After the first packet, it calculates the shortest path between the receiver and source and uses the SPT to send all subsequent packets from the source directly to the receiver. When the first packet arrives natively through the shortest path, the RP sends a register-stop message back to the DR near the source. When this DR receives the register-stop message, it stops sending register messages to the RP. If there are no other sources using the shared tree, it is also torn down.

Setting up the SPT requires more memory than when using the shared tree, but can significantly reduce group join and data transmission delays. The ECN330-switch can also be configured to use SPT only for specific multicast groups, or to disable the change over to SPT for specific groups.

6.21.5.1 Enabling PIM-SM Globally

PIM-SM is used to route multicast traffic to nodes which have requested a specific multicast service through IGMP. The Designated Router (DR) near the receiver sends a join message the Rendezvous Point (RP) responsible for the specified multicast group. If the RP has already established a reverse path tree back to the source, it immediately starts forwarding packets to the DR; otherwise it sends a join message back toward the source and waits until traffic arrives from the source before forwarding traffic down the shared tree. However, note that if the RP does not receive a Register message back from the source requested by the host group, it will take no action.

To use PIM-SM, it must be enabled globally for the router as described below, and for each interface that will support multicast routing as described in the next section. Also note that IGMP must be enabled to allow the router to determine the location of group members.

Web – Click Routing Protocol, PIM-SM, General Settings. Enable or disable PIM-SM globally for the router, and click Apply.

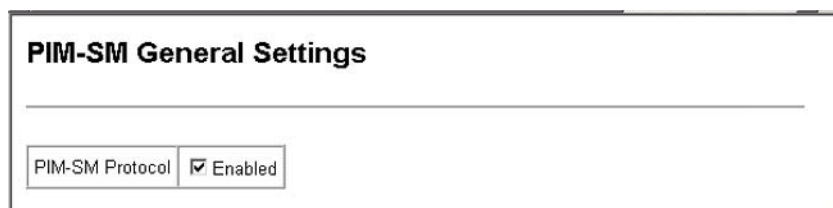


Figure 228 Enabling PIM-SM Globally

CLI – This example enables PIM-SM globally and displays the current status.

```
Console(config)#router pim sparse-mode
Console#show router pim
PIM Dense-Mode Admin Status: Disabled
PIM Sparse-Mode Admin Status: Enabled
Console#
```

6.21.5.2

Configuring Global PIM-SM Settings

PIM-SM uses global settings to determine the method used in selecting Rendezvous Point (RP) candidates. Timers for join/prune messages, register messages, and register suppression also need to be configured on each of the PIM-SM routers within the common multicast domain. Use of the Shortest Path Tree (SPT) can also be disabled for specified multicast groups.

Command Attributes

- **Ignore RP Set Priority** – Ignores the priority value for RP candidates, and only uses the hashing mechanism for RP selection. (Default: Disabled)
- **CRP Prefix** – Allows the ECN330-switch to be accepted as an RP candidate by a Cisco BSR. (Default: Disabled)
- **Register Checksum With Data** – Calculates the register checksum over the whole packet instead of just the packet header. (Default: Disabled)
- **J/P Interval** – Sets the join/prune interval. (Range: 1-65535 seconds; Default: 60 seconds)

- By default, the ECN330-switch sends join/prune messages every 60 seconds to inform other PIM-SM routers about clients who want to join or leave a multicast group.
- Use the same join/prune message interval on all PIM-SM routers in the same PIM-SM domain, otherwise the routing protocol's performance will be adversely affected.
- The multicast interface that first receives a multicast stream from a particular source forwards this traffic only to those interfaces on the router that have requests to join this group. When there are no longer any requesting groups on that interface, the leaf node sends a prune message upstream and enters a prune state for this multicast stream. The protocol maintains both the current join state and the pending RPT prune state for this (source, group) pair until the jp-interval timer expires.
- **Register Rate Limit** – Configures the rate at which register messages are sent by the Designated Router (DR) for each (source, group) entry. (Range: 1-65535: Default: 0, which means no limit)

This parameter can be used to relieve the load on the DR and RP. However, because register messages exceeding the limit are dropped, some receivers may experience data packet loss within the first few seconds in which register messages are sent from bursty sources.

- **Register Suppression** – Configures the register suppression timer on a DR or the keep alive time on an RP. This timer is used to calculate the period during which a DR stops sending register-encapsulated data to the RP after receiving a RegisterStop message. It is also used to calculate the KeepaliveTimer by the RP. (Range: 1-65535 seconds; Default: 60 seconds)
 - When the DR receives a register-stop message from the RP, it uses the register suppression time to set the register-stop timer. It then stops sending register messages and starts the register-stop timer for the specified group. Afterwards, the DR periodically sends a null-register message to the RP to determine whether or not the RP wants to start receiving normal register messages for this group.
 - When the RP receives a register message for a source for any group, it uses the register suppression time to set the keep-alive timer for that group source.

- **SPT Threshold** – Prevents the last-hop PIM-SM router from switching to Shortest Path Source Tree (SPT) mode. (Default: Disabled)
 - The default path for packets from a multicast source to a receiver is through the RP. However, the path through the RP is not always the shortest path. Therefore, the router uses the RP to forward only the first packet from a new multicast group to its receivers. Afterwards, it calculates the shortest path tree (SPT) directly between the receiver and source, and then uses the SPT to send all subsequent packets from the source to the receiver instead of using the shared tree.
 - Enable the SPT threshold to force the router to use the shared tree for all multicast groups, or just for the specified multicast groups.
- **SPT Group** – The IP address for a multicast group which must use the shared tree. If a group address is not specified, the shared tree is used for all multicast groups.
- **SPT Group Mask** – Subnet mask that is used for the group address.

Web – Click Routing Protocol, PIM-SM, Global Settings. Modify any of the protocol parameters as required, and click Apply.

PIM-SM Global Settings	
Ignore RP Set Priority	☒ Enabled
CRP Prefix	☒ Enabled
Register Checksum With Data	☒ Enabled
J/P Interval (1-65535 seconds)	80
Register Limit Rate (1-65535)	500
Register Suppression	500
SPT Threshold	☒ Enabled
SPT Group	224.1.0.0
SPT Group Mask	255.255.255.0

Figure 229 PIM-SM Global Settings

CLI – This example sets the PIM-SM global parameters.

```

Console(config)#ip pim ignore-rp-set-priority
Console(config)#ip pim crp-prefix
Console(config)#ip pim register-checksum-withdata
Console(config)#ip pim jp-interval 80
Console(config)#ip pim register-rate-limit 500
Console(config)#ip pim register-suppression 500
Console(config)#ip pim spt-threshold infinity 224.1.0.0 255.255.0.0

Console#show ip pim
PIM-DM Admin Status:      Disabled
PIM-SM Admin Status:      Enabled
Join/Prune-Interval:      80
Register-Suppression:     500
Register-Rate-Limit:      500
Register-Checksum-with Data: Enabled
Ignore RP-Set-Priority:    Enabled
CRP-Prefix:                Enabled
SPT-Threshold:             Enabled
    SPT-Threshold Group:   224.1.0.0
    SPT-Threshold Group mask: 255.255.0.0
Console#show running-config
.
.
.
!
router pim sparse-mode
    ip pim register-rate-limit 500
    ip pim rp-candidate vlan 1 224.0.0.0 255.0.0.0 priority 200
    ip pim bsr-candidate vlan 1 hash-mask-length 20 priority 200
    ip pim rp-address 10.1.1.1 224.1.0.0 255.255.0.0
    ip pim rp-address 192.168.1.1 224.0.0.0 240.0.0.0
!
.
.
.
Console#

```

6.21.5.3 Configuring PIM-SM Interface Settings

To fully enable PIM-SM, multicast routing needs to be enabled globally for the router (page 469), then enable PIM-SM globally for the router (page 492), and also enable PIM-SM for each interface that will participate in multicast routing.

Command Usage

A PIM-SM interface is used to forward multicast traffic only if a join message is received from a downstream router or if group members are directly connected to the interface. When routers want to receive a multicast flow, they periodically send join messages to the RP, and are subsequently added to the shared path for the specified flow back up to the RP. If routers want to join the source path up through the SPT, they periodically send join messages toward the source. They also send prune messages toward the RP to prune the shared path once they have connected to the source through the SPT, or if there are no longer any group members connected to the interface.

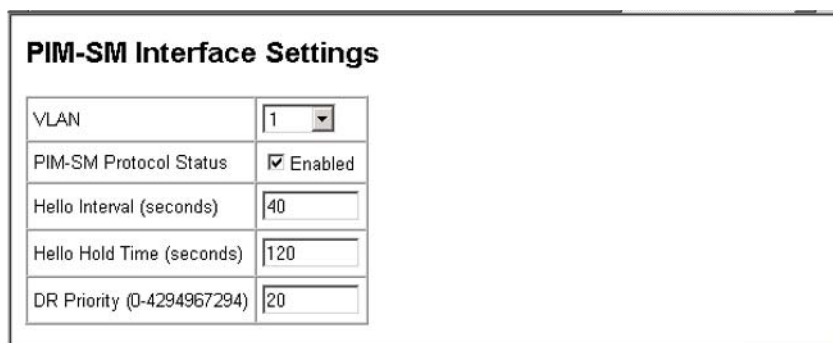
Command Attributes

- **VLAN** – VLAN interface. (Range: 1-4094; Default: VLAN 1)
- **PIM-SM Protocol Status** – Enables PIM-SM on the specified interface. (Default: Disabled)
 - PIM-SM must be enabled on each VLAN interface connected to the PIM Sparse network. Internet Group Management Protocol (IGMP) must also be enabled on each interface (see “Configuring IGMP Interface Parameters” on page 364).
- **Hello Interval (seconds)** – Sets the interval at which periodic hellos are sent out on all interfaces. (Range: 1-65535; Default: 30)
 - PIM-SM routers send periodic hello messages to inform neighboring routers of their presence, and to determine which router for each LAN segment will serve as the Designated Router (DR).
 - When a router is booted or first configured for PIM-SM, it sends an initial hello message, and then sets its Hello timer to the configured value. If a router does not hear from a neighbor for the period specified by the Hello Hold Time (set to a period of 3.5 times the Hello Interval by default), that neighbor is dropped. This hold time is included in each hello message received from a neighbor. Also note

that hello messages also contain the DR priority of the router sending the message.

- **Hello Hold Time (seconds)** – Sets the timer that detects whether a neighbor router is still alive and sending hello messages.
(Range: 1-65535; Default 3.5 times the hello interval)
 - The hello-holdtime indicates how many seconds the router holds an entry for a neighbor that has stopped sending hello messages.
 - The hello-holdtime should be included in each hello message received from a neighbor. Routers on the same subnet may therefore have different hello-holdtimes.
 - If the hello interval is set at the default value of 30 seconds, then the default hello-holdtime is 105 seconds. If the hello-holdtime has not been configured, then every time the hello interval is updated, the hello-holdtime is automatically updated. However, if the hello-holdtime has been configured, then it will not be updated when the hello interval changes.
 - If a value is set for the hello-holdtime that is less than the hello interval, the command will fail. Also, if the hello-holdtime is already configured, and the hello interval is set to a value longer than the hello-holdtime, the command will fail.
- **DR Priority (0-4294967294)** – Sets the priority advertised by a router when bidding to become the Designated Router (DR).
(Range: 0-4294967294; Default: 1)
 - More than one PIM-SM router may be connected an Ethernet or other shared-media LAN. If multicast hosts are directly connected to the LAN, then only one of these routers is elected as the DR, and acts on behalf of these hosts, sending periodic Join/Prune messages toward a group-specific RP for each group. A single DR is elected per interface (LAN or otherwise) using a simple election process.
 - The router with the highest priority configured on an interface is elected as the DR. If more than one router attached to this interface uses the same priority, then the router with the highest IP address is elected to serve as the DR.
 - If a router does not advertise a priority in its hello messages, it is assumed to have the highest priority and is elected as the DR. If more than one router is not advertising its priority, then the router with the highest IP address is elected to server as the DR.

Web – Click Routing Protocol, PIM-SM, Interface Settings. Modify any of the protocol parameters as required, and click Apply.



PIM-SM Interface Settings	
VLAN	1
PIM-SM Protocol Status	☒ Enabled
Hello Interval (seconds)	40
Hello Hold Time (seconds)	120
DR Priority (0-4294967294)	20

Figure 230 PIM-SM Interface Settings

CLI – This example sets the PIM-SM parameters for VLAN 1.

```
Console(config)#interface vlan 1
Console(config-if)#ip pim sparse-mode
Console(config-if)#ip pim hello-interval 40
Console(config-if)#ip pim hello-holdtime 120
Console(config-if)#ip pim dr-priority 20
Console(config-if)#
```

6.21.5.4 Configuring a Static Rendezvous Point

A static address can be set for the Rendezvous Point (RP) for a particular multicast group.

Command Usage

- The specified router will act as an RP for all multicast groups in the local PIM-SM domain if no group address is specified, or for the specified group or group range (indicated by the mask).
- All routers within the same PIM-SM domain must be configured with the same RP(s). Selecting an RP through the dynamic election process is therefore preferable for most situations. Using the dynamic RP election process also allows a backup RP to automatically take over if the active RP router becomes unavailable.

- Only one RP can be used for each multicast group. However, multiple RPs can be defined for different groups or group ranges using the mask. If a group is matched by more than one group mask, the router will use the RP with the longer prefix length mask. If an IP address previously used for an RP is specified again, then the older entry is replaced.
- When multiple RPs are specified for the same group and mask length, the router selects the RP with the highest priority (that is, lowest priority value). If more than one RP ties for the highest priority, the RP-election hash algorithm is used to select a candidate for that group. Ties between RPs having the same hash value and priority are broken in preference for the RP with the highest address.
- Static definitions for RP addresses may be used together with RP addresses dynamically learned through the bootstrap router (BSR).
- If the "override" parameter is used, a statically configured RP address will take precedence over those learned through the BSR.

Command Attributes

- **RP Address** – Static IP address of the router that will be an RP for the specified multicast group(s).
- **Group** – An IP multicast group address. If a group address is not specified, the RP is used for all multicast groups.
- **Address Mask** – Subnet mask that is used for the group address.
- **Override** – If there is a conflict, the static RP configured with this command prevails over a dynamically learned RP.

Web – Click Routing Protocol, PIM-SM, RP Address. Specify the static RPs to use for each multicast group, and click Apply.

RP Address

Current:

RP Address, Group , Address Mask,Override
10.1.1.1, 224.0.0.0, 255.0.0.0,
192.168.1.1, 224.0.0.0, 240.0.0.0,

New:

RP Address	
Group	
Address Mask	
Override	☐ Enabled

Figure 231 Static RP Configuration

CLI – In the following example, the address 192.168.1.1 indicates the RP to use for all multicast groups, and the address 10.1.1.1 indicates the RP to use for groups 224.0.0.0~224.255.255.255.

```

Console(config)#ip pim rp-address 192.168.1.1
Console(config)#ip pim rp-address 10.1.1.1 224.0.0.0 255.0.0.0
                  override
Console(config)#exit
Console#show ip pim rp mapping
PIM Group-to-RP Mappings:

Group(s): 224.0.0.0/4, Static
          RP:192.168.1.1,  Uptime:0:0:38

Group(s): 224.0.0.0/8, Static
          RP:10.1.1.1,   Uptime:0:0:24

Console#

```

6.21.5.5 Configuring a BSR Candidate

The ECN330-switch can be configured as a Bootstrap Router (BSR) candidate.

Command Usage

- When this router is configured as a BSR candidate, it starts sending bootstrap messages to all of its PIM-SM neighbors. The IP address of the designated VLAN is sent as the candidate's BSR address. Each neighbor receiving the bootstrap message compares the BSR address with the address from previous messages. If the current address is the same or a higher address, it accepts the bootstrap message and forwards it. Otherwise, it drops the message.
- This router will continue to be the BSR until it receives a bootstrap message from another candidate with a higher priority (or a higher IP address if the priorities are the same).
- To improve failover recovery, it is advisable to select at least two core routers in diverse locations, each to serve as both a candidate BSR and candidate RP. It is also preferable to set up one of these routers as both the primary BSR and RP.

Command Attributes

- **VLAN** – Identifier of configured VLAN interface. (Range: 1-4094; Default: VLAN 1)
- **Hash Mask Length (0-32)** – Hash mask length (in bits) used for RP selection (see “Configuring a Static Rendezvous Point” on page 499 and “Configuring an RP Candidate” on page 504). The portion of the hash specified by the mask length is ANDed with the group address. Therefore, when the hash function is executed on any BSR, all groups with the same seed hash will be mapped to the same RP. If the mask length is less than 32, then only the first portion of the hash is used, and a single RP will be defined for multiple groups. (Range: 0-32; Default: 10)
- **Priority (0-255)** – Priority used by the candidate bootstrap router in the election process. The BSR candidate with the largest priority is preferred. If the priority values are the same, the candidate with the larger IP address is elected to be the BSR. Setting the priority to zero means that this router is not eligible to server as the BSR. At least one

router in the PIM-SM domain must be set to a value greater than zero.
(Range: 0-255; Default: 0)

Web – Click Routing Protocol, PIM-SM, BSR Candidate. Specify the VLAN interface for which this router is bidding to become the BSR, the hash mask length that will subsequently be user for RP selection if this router is selected as the BSR, and the priority for BSR selection, then click Apply.

PIM-SM BSR Candidate Settings	
VLAN	1
Hash Mask Length (0-32)	20
Priority (0-255)	200

Figure 232 BSR Candidate Settings

CLI – The following example configures the router to start sending bootstrap messages out of the interface for VLAN 1 to all of its PIM-SM neighbors.

```

Console(config)#ip pim bsr-candidate vlan 1 hash-masklen 20
priority 200
Console(config)#exit
Console#show ip pim bsr-router
This system is the Bootstrap Router (BSR)
BSR address:          192.168.1.250
BSR priority:         200
BSR hash mask length: 20
Uptime:               0:0:17
Next Bootstrap Message in 0:0:48

Candidate BSR: 192.168.1.250 (Vlan1)
Candidate-BSR Priority: 200
Candidate-BSR hash mask length: 20
Console#

```

6.21.5.6 Configuring an RP Candidate

The ECN330-switch can be configured to advertise itself as a Rendezvous Point (RP) candidate to the bootstrap router (BSR).

Command Usage

- When this router is configured as an RP candidate, it periodically sends PIMv2 messages to the BSR advertising itself as a candidate RP for the specified group addresses. The IP address of the designated VLAN is sent as the candidate's RP address. The BSR places information about all of the candidate RPs in subsequent bootstrap messages. The BSR uses the RP-election hash algorithm to select an active RP for each group range. The election process is performed by the BSR only for its own use. Each PIM-SM router that receives the list of RP candidates from the BSR also elects an active RP for each group range using the same election process.
- The election process for each group is based on the following criteria:
 - Find all RPs with the most specific group range.
 - Select those with the highest priority (lowest priority value).
 - Compute hash value based on the group address, RP address, and hash mask included in the bootstrap messages.
 - If there is a tie, use the candidate RP with the highest IP address.
- This distributed election process provides faster convergence and minimal disruption when an RP fails. It also serves to provide load balancing by distributing groups across multiple RPs. Moreover, when an RP fails, the responsible RPs are re-elected on each router, and the groups automatically distributed to the remaining RPs.
- To improve failover recovery, it is advisable to select at least two core routers in diverse locations, each to serve as both a candidate BSR and candidate RP. It is also preferable to set up one of these routers as both the primary BSR and RP.

Command Attributes

- **VLAN** – Identifier of configured VLAN interface. (Range: 1-4094; Default: VLAN 1)

- **Group Address** – An IP multicast group address. If a group address is not specified, the RP is used for all multicast groups.
- **Group Mask** – Subnet mask that is used for the group address.
- **Priority (0-255)** – Priority used by the candidate RP in the election process. The RP candidate with the largest priority is preferred. If the priority values are the same, the candidate with the larger IP address is elected to be the RP. (Range: 0-255; Default: 192)

Web – Click Routing Protocol, PIM-SM, RP Candidate. Specify the VLAN interface for which this router is bidding to become the RP, the multicast group address and mask, and the priority for RP selection, then click Apply.

PIM-SM RP Candidate Settings	
VLAN	1
Group Address	224.0.0.0
Group Mask	255.0.0.0
Priority (0-255)	200

Figure 233 RP Candidate Settings

CLI – The following example configures the router to start advertising itself to the BSR as a candidate RP for the specified multicast groups.

```

Console(config)#ip pim rp-candidate vlan 1 224.0.0.0 255.0.0.0
                priority 200
Console(config)#exit
Console#show ip pim bsr-router
PIMv2 BootStrap Information:
This system is the BootStrap Router (BSR)
BSR address:          192.168.1.250
BSR priority:         200
BSR hash mask length: 20
Uptime:              0:14:49
Next Bootstrap Message in 0:0:16

Candidate BSR: 192.168.1.250 (Vlan1)
Candidate-BSR Priority: 200
Candidate-BSR hash mask length: 20

Candidate RP: 192.168.1.250 (Vlan1)
Candidate-RP Group/masklen: 224.0.0.0/8
Candidate-RP Priority: 200
Next advisement in 0:0:38
Console#

```

6.21.5.7 Displaying the Results of the RP Hash

Use the RP Hash page to display the RP elected for the specified multicast group, the source of this information, and the method of election.

Field Attributes

- **Group** – IP multicast group address.
- **RP Address** – Address of the RP responsible for the specified group.
- **RP Type** – The type can be either BSR or RP.
- **Information Source** – The device from which information about this RP entry was obtained, and the method that was used to map this RP to the specified group.

Web – Click Routing Protocol, PIM-SM, RP Hash. Enter a multicast group address, and click Query.

The screenshot shows a web interface titled "RP Hash". It has a text input field for "Group" containing "224.0.0.0" and a "Query" button. Below the button is a table with the following data:

RP Address	192.168.1.250
RP Type	BSR
Information Source	Info source: 192.168.1.250, via bootstrap

Figure 234 Displaying the Results of the RP Hash

CLI – This example displays the RP used for the specified group, and the method in which this RP was elected (that is , bootstrap or static).

```

Console#show ip pim rp-hash 224.0.1.3
      RP:      10.10.11.35
      Info source: 10.10.11.35, via bootstrap
Console#sh ip pim rp-hash 224.0.0.0
      RP:      192.168.1.19,Static
Console#

```

6.21.5.8 Displaying the BSR Router

Use the BSR Router Information page to display information about the bootstrap router (BSR).

Field Attributes

PIMV2 Bootstrap Information

- **BSR Status** – Shows if this router is the BSR.
- **BSR Address** – IP address of interface configured as the BSR.
- **BSR Priority** – Priority assigned to this interface for use in the BSR election process.

- **BSR Hash Mask Length** – The number of significant bits used in the multicast group comparison mask. This mask determines the multicast group for which this router can be a BSR.
- **BSR Up Time** – The time this BSR has been up and running.
- **BSR Next Message In Time** – The time before the BSR sends its next bootstrap message.
- **BSR Expires Time** – The time before the BSR is declared down.

Candidate BSR Information

- **Candidate BSR Address** – The address of all candidate BSRs attached to this interface.
- **Candidate BSR Priority** – Priority value used by this BSR candidate.
- **Candidate BSR Hash Mask Length** – The number of significant bits used in the multicast group comparison mask by this BSR candidate.

Candidate RP Information

- **Candidate RP Address** – The address of all candidate RPs attached to this interface.
- **Candidate RP Group Address** – The multicast group for which this candidate RP is bidding.
- **Candidate RP Group Mask Length** – The mask length for the indicated multicast group.
- **Candidate RP Priority** – Priority used by the candidate RP in the election process..
- **Candidate RP Next Advertise Time** – Time (hours:minutes:seconds) before the next candidate RP advertisement is sent. Note that this field is only displayed when the candidate RP is in service.

Web – Click Routing Protocol, PIM-SM, BSR Router Information.

BSR Router Information

PIMV2 Bootstrap Information

BSR Status	This system is the BootStrap Router (BSR)
BSR Address	192.168.1.250
BSR Priority	200
BSR Hash Mask Length	20
BSR Up Time	38
BSR Next Message In Time	27
BSR Expires Time	27

Candidate BSR Information

Candidate BSR Address	192.168.1.250 (Vlan1)
Candidate BSR Priority	200
Candidate BSR Hash Mask Length	20

Candidate RP Information

Candidate RP Address	192.168.1.250 (Vlan1)
Candidate RP Group Address	224.0.0.0
Candidate RP Group Mask	255.0.0.0
Candidate RP Group Mask Length	8
Candidate RP Priority	200
Candidate RP Next Advertise Time	60

Figure 235 Displaying BSR Information

CLI – This example displays information about the BSR

```
Console#show ip pim bsr-router
PIMv2 BootStrap Information:
This system is the BootStrap Router (BSR)
BSR address:                192.168.1.250
BSR priority:               200
BSR hash mask length:      20
Uptime:                     0:7:31
Next BootStrap Message in 0:0:34

Candidate BSR: 192.168.1.250 (Vlan1)
Candidate-BSR Priority:      200
Candidate-BSR hash mask length: 20

Candidate RP: 192.168.1.250 (Vlan1)
Candidate-RP Group/masklen: 224.0.0.0/8
Candidate-RP Priority:       200
Next advisement in          0:0:7
Console#
```

6.21.5.9

Displaying the PIM-SM Interfaces

Use the PIM-SM Interface Information page to display information about interfaces configured for PIM-SM.

Command Attributes

- **Interface** – A VLAN interface on this router.
- **Address** – The IP address for this interface.
- **Mode** – The PIM mode in use (Sparse Mode).
- **Neighbor Count** – The number of PIM neighbors detected on this interface.
- **DR Address** – The designated PIM router for this interface.

Web – Click Routing Protocol, PIM-SM, Interface Information.

PIM-SM Interface Information				
Interface	Address	Mode	Neighbor Count	DR Address
VLAN1	192.168.1.250	Sparse	0	192.168.1.250

Entry Count: 1

Figure 236 PIM-SM Interface Information

CLI – This example shows the PIM-SM interface summary for VLAN 1.

```

Console#show ip pim interface 1
Vlan 1 is up
PIM is enabled, mode is Sparse.
Internet address is 192.168.1.250.
Hello time interval is 40 sec, trigger hello time interval is 5 sec.
Hello holdtime is 120 sec.
DR priority is 20.
DR Internet address is 192.168.1.250, neighbor count is 0.

Console#

```

6.21.5.10

Displaying RP Mapping

Use the PIM-SM RP Mapping Information page to display active RPs and associated multicast routing entries.

Command Attributes

- **Group Address** – A multicast group address.
- **Mask Length** – The mask length for the listed multicast group.
- **RP Address** – IP address of the RP for the listed multicast group.
- **Info Source** – The device from which information about this RP entry was obtained.
- **Priority** – Priority used by the candidate RP in the election process.
- **Up Time** – The time this RP has been up and running.

- **Expire** – The time before the RP will be declared down.

Web – Click Routing Protocol, PIM-SM, RP Mapping Information.

PIM-SM RP Mapping Information						
Group Address	Mask Length	RP Address	Info Source	Priority	Up Time	Expire
224.0.0.0	8	192.168.1.250	192.168.1.250	200	1524	126

Static RP Mapping Information			
Group Address	Mask Length	RP Address	Up Time
224.0.0.0	4	192.168.1.1	1636
224.0.0.0	8	10.1.1.1	1600

Figure 237 PIM-SM RP Mapping Information

CLI – This example displays the elected entries in the RP map, as well as all of the static entries configured on this router.

```

Console#show ip pim rp mapping
PIM Group-to-RP Mappings:

Group(s): 224.0.0.0/8, via bootstrap
    RP: 192.168.1.250, Info source: 192.168.1.250, priority 200,
    0:36:15/0:2:15

Group(s): 224.0.0.0/4, Static
    RP:192.168.1.1,  Uptime:0:38:7

Group(s): 224.0.0.0/8, Static
    RP:10.1.1.1,  Uptime:0:37:31

Console#

```

6.21.5.11 Displaying Neighbor Information

The router can display all the neighboring PIM-SM routers.

Command Attributes

- **Neighbor Address** – IP address of the next-hop router.
- **Interface** – VLAN that is attached to this neighbor.
- **Up time** – The duration this entry has been active.
- **Expire** – The time before this entry will be removed.
- **Mode** – PIM mode used on this interface (that is, Sparse).

Web – Click Routing Protocol, PIM-SM, Neighbor Information.

PIM-SM Neighbor Information				
Neighbor Address	Interface	Up Time	Expire	Mode
192.168.0.194	VLAN1	101	94	Sparse

Entry Count: 1

Figure 238 PIM-SM Neighbor Information

CLI – This example displays the only neighboring PIM-SM router.

```

Console#show ip pim neighbor
      Address      VLAN Interface    Uptime    Expire    Mode
-----
  192.168.0.194      1      0:4:21      0:1:24  Sparse (DR)
Console#

```


7 Command Line Interface

This section describes how to use the Command Line Interface (CLI).

7.1 Using the Command Line Interface

7.1.1 Accessing the CLI

The ECN330-switch provides a command-line interface (CLI) for managing its switching features. This management interface can be accessed using a direct connection to the ECN330's console port, or through a Telnet connection. The CLI enables switch configuration through entering keywords and parameters at a command prompt, which is similar to entering commands on a UNIX system.

7.1.2 Console Connection

To access the ECN330-switch through the console port, perform these steps:

1. At the console prompt, type the user name and password. (The default user name is **admin** with corresponding password of **admin**.) When an administrator user name and password is entered, the CLI displays the `Console#` prompt and enters privileged access mode (that is, Privileged Exec). But when a guest user name and password is entered, the CLI displays the `Console>` prompt and enters normal access mode (that is, Normal Exec).
2. Enter the necessary commands to complete the desired tasks.
3. When finished, exit the session with the **quit** or **exit** command.

After connecting to the system through the console port, the login screen displays:

```
User Access Verification

Username: admin
Password:

      CLI session with the Embedded Switching/Routing Unit is opened.
      To end the CLI session, enter [Exit].

Console#
```

7.1.3 Telnet Connection

Telnet operates over the IP transport protocol. In this environment, the management station and any network device that needs to be managed over the network must have a valid IP address. Valid IP addresses consist of four numbers, 0 to 255, separated by periods. Each address consists of a network portion and host portion. For example, the IP address 10.1.0.1, consists of a network portion (10.1.0) and a host portion (1).

Note: The IP address for the ECN330-switch is obtained through DHCP by default.

To access the ECN330-switch through a Telnet session, the IP address for the ECN330-switch must be set first, and if managing the ECN330-switch from a different IP subnet, the default gateway must also be set. For example:

```
Console(config)#interface vlan 246
Console(config-if)#ip address 10.1.0.1 255.255.255.0
Console(config-if)#exit
Console(config)#ip default-gateway 10.1.0.254
```

After the ECN330-switch is configured with an IP address, a Telnet session can be opened by performing these steps.

1. From the remote host, enter the Telnet command and the IP address of the device to be accessed.

2. At the prompt, enter the user name and system password. The CLI will display the `Vty-n#` prompt for an administrator to show that it is in privileged access mode (that is, Privileged Exec), or `Vty-n>` for a guest to show that it is in normal access mode (that is, Normal Exec), where *n* indicates the number of the current Telnet session.
3. Enter the necessary commands to complete the desired tasks.
4. When finished, exit the session with the **quit** or **exit** command.

After entering the Telnet command, the login screen displays:

```
Username: admin
Password:

      CLI session with the Embedded Switching/Routing Unit is opened.
      To end the CLI session, enter [Exit].

Vty-0#
```

Note: Up to four sessions can be opened to the device through Telnet.

7.2 Entering Commands

This section describes how to enter CLI commands.

7.2.1 Keywords and Arguments

A CLI command is a series of keywords and arguments. Keywords identify a command, and arguments specify configuration parameters. For example, in the command **show interfaces status ethernet 1/5**, **show interfaces** and **status** are keywords, **ethernet** is an argument that specifies the interface type, and **1/5** specifies the unit and port.

Commands can be entered as follows:

- To enter a simple command, enter the command keyword.
- To enter multiple commands, enter each command in the required order. For example, to enter configuration mode and enable spanning tree for the ECN330-switch, type:

```
Console#configure  
Console(config)#spanning-tree
```

- To enter commands that require parameters, enter the required parameters after the command keyword. For example, to set a password for the administrator, enter:

```
Console(config)#username admin password 0 smith
```

7.2.2 Minimum Abbreviation

The CLI will accept a minimum number of characters that uniquely identify a command. For example, the command **configure** can be entered as **con**. If an entry is ambiguous, the system will prompt for further input.

7.2.3 Command Completion

If input is terminated with a Tab key, the CLI prints the remaining characters of a partial keyword up to the point of ambiguity. In the “logging history” example, typing **log** followed by a tab results in printing the command up to **logging**.

7.2.4 Getting Help on Commands

A brief description of the help system can be displayed by entering the **help** command. Command syntax can also be displayed by using the **?** character to list keywords or parameters.

7.2.4.1 Showing Commands

If a **?** is entered at the command prompt, the system displays the first level of keywords for the current command class (Normal Exec or Privileged Exec) or configuration class (Global, ACL, DHCP, Interface, Line, Router, VLAN Database, or MSTP). A list of valid keywords for a specific command can also be displayed. For example, the command **show ?** displays a list of possible show commands:

```

Console#show ?
  access-group      Access groups
  access-list       Access lists
  arp               Information of arp cache
  bridge-ext        Bridge extend information
  calendar          Date information
  class-map         Display class maps
  dns              DNS information
  dot1q-tunnel      802.1Q tunnel ports information
  dot1x            Show 802.1x content
  eaps             Display EAPS information
  garp             Garp property
  gvrp             Show GVRP information of interface
  history          Information of history
  hosts            Host information
  interfaces       Information of interfaces
  ip              IP information
  lacp            Show LACP statistic
  line            TTY line information
  logging         Show the contents of logging buffers
  mac             MAC access lists
  mac-address-table Set configuration of the address table
  mac-learning     Show status of MAC address learning
  management       Show management ip filter
  map             Map priority
  mpls            MPLS information
  policy-map       Display policy maps
  port            Characteristics of the port
  power           Show power
  protocol-vlan    Protocol-vlan information

```

public-key	Show information of public key
queue	Information of priority queue
radius-server	RADIUS server information
rip	Rip
router	Router
running-config	The system configuration of running
snmp	SNMP statistics
sntp	Sntp
spanning-tree	Specify spanning-tree
ssh	Secure shell
startup-config	The system configuration of starting up
system	Information of system
tacacs-server	Login by tacacs server
users	Display information about terminal lines
version	System hardware and software status
vlan	Switch VLAN Virtual Interface
vrrp	Show vrrp

Console#show

The command **show interfaces ?** displays the following information:

```

Console>show interfaces ?
  counters      Interface counters information
  protocol-vlan Protocol-VLAN information
  status        Interface status information
  switchport    Interface switchport information
Console>

```

7.2.5 Partial Keyword Lookup

If a partial keyword is terminated with a question mark, alternatives that match the initial letters are provided. (Remember not to leave a space between the command and question mark.) For example **s?** shows all the keywords starting with “s.”

```

Console#show s?
snmp      sntp      spanning-tree  ssh      startup-config
system
Console#show s

```

7.2.6 Negating the Effect of Commands

For many configuration commands the prefix keyword **no** can be entered to cancel the effect of a command or reset the configuration to the default value. For example, the **logging** command logs system messages to a host server. To disable logging, specify the **no logging** command. This guide describes the negation effect for all applicable commands.

7.2.7 Using Command History

The CLI maintains a history of commands that have been entered. The up arrow key can be pressed to scroll back through the history of commands. Any command displayed in the history list can be executed again, or first modified and then executed.

Using the **show history** command displays a longer list of recently executed commands.

7.2.8 Understanding Command Modes

The command set is divided into Exec and Configuration classes. Exec commands generally display information on system status or clear statistical counters. Configuration commands, on the other hand, modify interface parameters or enable certain switching functions. These classes are further divided into different modes. Available commands depend on the selected mode. A question mark **?** can always be entered at the prompt to display a list of the commands available for the current mode. The command classes and associated modes are displayed in Table 29:

Table 29 Command Classes and Modes

Class	Mode	
Exec	Normal Privileged	
Configuration	Global*	Access Control List Class Map DHCP EAPS Interface Line Multiple Spanning Tree Policy Map Router VLAN Database

* Access to Privileged Exec mode is required to access any of the configuration modes. Access to Global Configuration mode is required to access any of the other configuration modes.

7.2.9 Exec Commands

If the system is in Normal Exec command mode (or guest mode), displaying the `Console>` command prompt, only a limited number of the commands are available. All commands can only be accessed from the Privileged Exec command mode (or administrator mode). To access Privilege Exec mode, open a console session with the default user name and password **admin**. The system displays the `Console#` command prompt. Privileged Exec mode can also be entered from within Normal Exec mode, by typing the **enable** command, followed by the privileged level password **super** (see section 7.4.1 on page 532).

To enter Privileged Exec mode, enter the following commands and passwords:

```
Username: admin
Password: [system login password]

      CLI session with the Embedded Switching/Routing Unit is opened.
      To end the CLI session, enter [Exit].

Console#
```

```
Username: [Normal Exec user name]
Password: [system login password]

      CLI session with the Embedded Switching/Routing Unit is opened.
      To end the CLI session, enter [Exit].

Console>
Console>enable
Password: [privileged level password]
Console#
```

7.2.10 Configuration Commands

Configuration commands are privileged level commands used to modify ECN330-switch settings. These commands modify the running configuration only and are not saved when the ECN330-switch is rebooted. To store the running configuration in nonvolatile storage, use the **copy running-config startup-config** command.

The configuration commands are organized into different modes:

- Global Configuration - These commands modify the system level configuration, and include commands such as **hostname** and **snmp-server community**.
- Access Control List Configuration - These commands are used for packet filtering.
- Class Map Configuration - Creates a DiffServ class map for a specified traffic type.
- DHCP Configuration - These commands are used to configure the DHCP server.

- EAPS Configuration - These commands configure Automatic Ethernet Protection Switching for increased availability of Ethernet rings commonly used in service provider networks.
- Interface Configuration - These commands modify the port configuration such as **speed-duplex** and **negotiation**.
- Line Configuration - These commands modify the console port and Telnet configuration, and include commands such as **parity** and **databits**.
- Multiple Spanning Tree Configuration - These commands configure settings for the selected multiple spanning tree instance.
- Policy Map Configuration - Creates a DiffServ policy map for multiple interfaces.
- Router Configuration - These commands configure global settings for unicast and multicast routing protocols.
- VLAN Configuration - Includes the command to create VLAN groups.

To enter the Global Configuration mode, enter the command **configure** in Privileged Exec mode. The system prompt changes to `Console(config)#`, which provides access privilege to all Global Configuration commands.

```
Console#configure
Console(config)#
```

To enter the other modes, at the configuration prompt type one of the following commands. Use the **exit** or **end** command to return to the Privileged Exec mode.

Table 30 CLI Command Modes

Mode	Command	Prompt	Page
Line	line {console vty}	Console(config-line)#	570
Access Control List	access-list ip standard access-list ip extended access-list ip mask-precedence access-list mac access-list mac mask-precedence vlan access-map	Console(config-std-acl)# Console(config-ext-acl)# Console(config-ip-mask-acl)# Console(config-mac-acl)# Console(config-mac-mask-acl)# Console(config-access-map)#	692
Class Map	class map	Console(config-cmap)	923
DHCP	ip dhcp pool	Console(config-dhcp)#	983
EAPS	eaps	Console(config-eaps)#	835
Interface	interface {ethernet <port> port-channel <id> vlan <id>}	Console(config-if)#	737
MSTP	spanning-tree mst-configuration	Console(config-mstp)#	804
Policy Map	policy map	Console(config-pmap)	926
Router	router {rip ospf dvmrp pim dense-mode pim sparse-mode}	Console(config-router)#	1037
VLAN	vlan database	Console(config-vlan)#	849

For example, the following commands can be used to enter interface configuration mode, and then return to Privileged Exec mode.

```
Console(config)#interface ethernet 1/5
.
.
.
Console(config-if)#exit
Console(config)#
```

7.2.11 Command Line Processing

Commands are not case sensitive. Commands and parameters can be abbreviated as long as they contain enough letters to differentiate them from any other currently available commands or parameters. The Tab key can be used to complete partial commands, or enter a partial command followed by the ? character to display a list of possible matches. The following table shows other editing keystrokes that can be used for command-line processing:

Table 31 CLI Editing Keystrokes

Keystroke	Function
Ctrl-A	Shifts cursor to start of command line.
Ctrl-B	Shifts cursor to the left one character.
Ctrl-C	Terminates the current task and displays the command prompt.
Ctrl-E	Shifts cursor to end of command line.
Ctrl-F	Shifts cursor to the right one character.
Ctrl-K	Deletes all characters from the cursor to the end of the line.
Ctrl-L	Repeats current command line on a new line.
Ctrl-N	Enters the next command line in the history buffer.

Keystroke	Function
Ctrl-P	Shows the last command.
Ctrl-R	Repeats current command line on a new line.
Ctrl-U	Deletes the entire line.
Ctrl-W	Deletes the last word typed.
Ctrl-Z	Returns to Privileged Exec mode from configuration mode.
Esc-B	Moves the cursor back one word.
Esc-D	Deletes from the cursor to the end of the word.
Esc-F	Moves the cursor forward one word.
Delete key or backspace key	Erases a mistake when entering a command.

7.3 Command Groups

The system commands can be broken down into the functional groups as shown in Table 32.

Table 32 CLI Command Groups

Command Group	Description	Page
General	Basic commands for entering privileged access mode, restarting the system, or quitting the CLI	531
System Management	Display and setting of system information, basic modes of operation, maximum frame size, file management, console port and telnet settings, system logs, SMTP alerts, and the system clock	540
Simple Network Management Protocol	Activates authentication failure traps; configures community access strings, and trap receivers	608
User Authentication	Configures user names and passwords, logon access using local or remote authentication, management access through the web server, Telnet server and Secure Shell; as well as port security, IEEE 802.1X port access control, and restricted access based on specified IP addresses	632
Access Control List	Provides filtering for IP frames (based on address, protocol, TCP/UDP port number or TCP control code), non-IP frames (based on MAC address or Ethernet type), or for frame types within specific VLANs	690
Interface	Configures the connection parameters for all Ethernet ports, aggregated links, and VLANs	736
Link Aggregation	Statically groups multiple ports into a single logical trunk; configures Link Aggregation Control Protocol for port trunks	756
Mirror Port	Mirrors data to another port for analysis without affecting the data passing through or the performance of the monitored port	773

Command Group	Description	Page
Rate Limit	Controls the maximum rate for traffic transmitted or received on a port	776
Power over Ethernet	Controls the power available to ECN330 ports	778
Address Table	Configures the address table for filtering specified addresses, displaying current entries, clearing the table, or setting the aging time	786
Spanning Tree Algorithm	Configures Spanning Tree settings for the ECN330-switch	794
Ethernet Automatic Protection Switching	Configures EAPS for increased availability of Ethernet rings commonly used in service provider networks	824
VLANs	Configures VLAN settings, and defines port membership for VLAN groups; also enables or configures private VLANs, protocol VLANs, and QinQ tunneling	841
Layer 2 over MPLS	Configures MPLS tunnels to maintain VLAN and Layer 2 protocol settings for customer traffic crossing the service provider's network	890
Class of Service	Sets port priority for untagged frames, relative weight for each priority queue, also sets priority for TCP or UDP traffic types, IP precedence, and DSCP	897
Quality of Service	Configures Differentiated Services	921
Multicast Filtering	Configures IGMP multicast filtering, query parameters, and specifies ports attached to a multicast router	935
Domain Name Service	Configures DNS services.	963
Dynamic Host Configuration Protocol	Configures DHCP client, relay and server functions	974
Router Redundancy	Configures router redundancy to create primary and backup routers	998

Command Group	Description	Page
IP Interface	Configures IP address for the ECN330-switch interfaces; also configures ARP parameters and static entries	1015
IP Routing	Configures static and dynamic unicast routing	1028
Multicast Routing	Configures multicast routing protocols DVMRP, PIM-DM and PIM-SM	1103

The access mode shown in the following tables is indicated by these abbreviations:

ACL	(Access Control List Configuration)
CM	(Class Map Configuration)
DC	(DHCP Server Configuration)
EAPS	(EAPS Configuration)
GC	(Global Configuration)
IC	(Interface Configuration)
LC	(Line Configuration)
MST	(Multiple Spanning Tree)
NE	(Normal Exec)
PE	(Privileged Exec)
PM	(Policy Map Configuration)
RC	(Router Configuration)
VC	(VLAN Database Configuration)

7.4 General Commands

Table 33 General Commands

Command	Function	Mode	Page
enable	Activates privileged mode	NE	532
disable	Returns to normal mode from privileged mode	PE	533
configure	Activates global configuration mode	PE	534
show history	Shows the contents of the command history buffer	NE, PE	534
reload	Restarts the system	PE	535
prompt	Customizes the CLI prompt	GC	536
end	Returns to Privileged Exec mode	any config. mode	537
exit	Returns to the previous configuration mode, or exits the CLI	any	537
quit	Exits a CLI session	NE, PE	538
help	Shows how to use help	any	NA
?	Shows options for command completion (context sensitive)	any	NA

7.4.1 enable

Use this command to activate Privileged Exec mode. In privileged mode, additional commands are available, and certain commands display additional information. See section 7.2.8 on page 521.

Syntax

enable [*level*]

level - Privilege level to log into the device.

The device has two predefined privilege levels: 0: Normal Exec, 15: Privileged Exec. Enter level 15 to access Privileged Exec mode.

Default Setting

Level 15

Command Mode

Normal Exec

Command Usage

- The default password required to change the command mode from Normal Exec to Privileged Exec is **super**. (To set this password, see the **enable password** command, section 7.7.2 on page 635.)
- The # character is appended to the end of the prompt to indicate that the system is in privileged access mode.

Example

```
Console> enable
Password: [privileged level password]
Console#
```

Related Commands

disable (section 7.4.2 on page 533)

enable password (section 7.7.2 on page 635)

7.4.2 **disable**

Use this command to return to Normal Exec mode from privileged mode. In normal access mode, only basic information on the ECN330-switch's configuration or Ethernet statistics can be displayed. To gain access to all commands, the privileged mode must be used. See section 7.2.8 on page 521.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

The > character is appended to the end of the prompt to indicate that the system is in normal access mode.

Example

```
Console#disable  
Console>
```

Related Commands

enable (section 7.4.1 on page 532)

7.4.3 **configure**

Use this command to activate Global Configuration mode. This mode must be entered to modify any settings on the ECN330-switch. Also, Global Configuration mode must be entered prior to enabling some of the other configuration modes, including Interface Configuration, Line Configuration, and VLAN Database Configuration. See section 7.2.8 on page 521.

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#configure  
Console(config)#
```

Related Commands

end (section 7.4.7 on page 537)

7.4.4 **show history**

Use this command to show the contents of the command history buffer.

Default Setting

None

Command Mode

Normal Exec, Privileged Exec

Command Usage

The history buffer size is fixed at 10 Execution commands and 10 Configuration commands.

Example

In this example, the show history command lists the contents of the command history buffer:

```
Console#show history
Execution command history:
 2 config
 1 show history

Configuration command history:
 4 interface vlan 1
 3 exit
 2 interface vlan 1
 1 end

Console#
```

The **!** command repeats commands from the Execution command history buffer when in Normal Exec or Privileged Exec Mode, and commands from the Configuration command history buffer when in any of the configuration modes. In this example, the **!2** command repeats the second command in the Execution history buffer (**config**).

```
Console#!2
Console#config
Console(config)#
```

7.4.5

reload

This command restarts the system.

Note: When the system is restarted, it always runs the Power-On Self-Test. It also retains all configuration information stored in non-volatile memory by the **copy running-config startup-config** command.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

This command resets the entire system.

Example

This example shows how to reset the ECN330:

```
Console#reload
System will be restarted, continue <y/n>? y
```

7.4.6**prompt**

This command customizes the CLI prompt. Use the **no** form to revert to the default prompt.

Syntax

prompt *<string>*

no prompt

string - Any alphanumeric string to use for the command prompt.
(Maximum length: 255 characters)

Default Setting

Console

Command Mode

Global Configuration

Example

```
Console(config)#prompt  
(config)#
```

7.4.7**end**

This command returns to Privileged Exec mode.

Default Setting

None

Command Mode

Global Configuration, Interface Configuration, Line Configuration, VLAN Database Configuration, and Multiple Spanning Tree Configuration

Example

This example shows how to return to the Privileged Exec mode from the Interface Configuration mode:

```
Console(config-if)#end  
Console#
```

7.4.8**exit**

This command returns to the previous configuration mode or exit the configuration program.

Default Setting

None

Command Mode

Any

Example

This example shows how to return to the Privileged Exec mode from the Global Configuration mode, and then quit the CLI session:

```
Console(config)#exit
Console#exit

Press ENTER to start session

User Access Verification

Username:
```

7.4.9

quit

This command exits the configuration program.

Default Setting

None

Command Mode

Normal Exec, Privileged Exec

Command Usage

The **quit** and **exit** commands can both exit the configuration program.

Example

This example shows how to quit a CLI session:

```
Console#quit  
  
Press ENTER to start session  
  
User Access Verification  
  
Username:
```

7.5 System Management Commands

These commands are used to control system logs, passwords, user names, management options, and display or configure a variety of other system information.

Table 34 System Management Commands

Command Group	Function	Page
Device Designation	Configures information that uniquely identifies the ECN330-switch	541
System Status	Displays system configuration, active managers, and version information	542
System Mode	Configures the ECN330-switch to operate in normal mode, QinQ mode, or L2MPLS mode	551
System MTU	Enables support for jumbo frames; sets the maximum transfer unit size	554
System SBC Mode	Enables the SBC board; tests the SBC LED	557
File Management	Manages code image or ECN330-switch configuration files	560
Line	Sets communication parameters for the serial port, including baud rate and console time-out	569
Event Logging	Controls logging of error messages	584
SMTP Alerts	Configures SMTP email alerts	594
Time (System Clock)	Sets the system clock automatically through an NTP/SNTP server or manually	600

Device Designation Commands

This section describes commands used to configure information that uniquely identifies the ECN330-switch.

Table 35 Device Designation Commands

Command	Function	Mode	Page
hostname	Specifies the host name for the ECN330-switch	GC	541
snmp-server contact	Sets the system contact string	GC	613
snmp-server location	Sets the system location string	GC	614

7.5.1 hostname

This command specifies or modifies the host name for the ECN330-switch. Use the **no** form to restore the default host name.

Syntax

hostname <name>

no hostname

name - The name of this host. (Maximum length: 255 characters)

Default Setting

None

Command Mode

Global Configuration

Example

```
Console(config)#hostname -Copenhagen-Site1
Console(config)#
```

System Status Commands

This section describes commands used to display system information.

Table 36 System Status Commands

Command	Function	Mode	Page
show startup-config	Displays the contents of the configuration file (stored in flash memory) that is used to start up the system	PE	542
show running-config	Displays the configuration data currently in use	PE	545
show system	Displays system information	NE, PE	548
show users	Shows all active console and Telnet sessions, including user name, idle time, and IP address of Telnet client	NE, PE	549
show version	Displays version information for the system	NE, PE	550

7.5.2 show startup-config

This command displays the configuration file stored in non-volatile memory that is used to start up the system.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

- Use this command in conjunction with the **show running-config** command to compare the information in running memory to the information stored in non-volatile memory.
- This command displays settings for key command modes. Each mode group is separated by ! symbols, and includes the configuration mode command, and corresponding commands. This command displays the following information:
 - MAC address for the ECN330-switch
 - SNTP server settings
 - Queue mode
 - SNMP community strings
 - Users (names and access levels)
 - VLAN database (VLAN ID, name and state)
 - VLAN configuration settings for each interface
 - Multiple spanning tree instances (name and interfaces)
 - IP address configured for VLANs
 - Layer 4 precedence settings
 - Routing protocol configuration settings
 - Spanning tree settings
 - Any configured settings for the console port and Telnet

Example

```

Console#show startup-config
building startup-config, please wait.....
!<stackingDB>00</stackingDB>
!<stackingMac>01_00-00-12-33-89-76_03</stackingMac>
!
phymap 00-00-12-33-89-76
!
SNTP server 0.0.0.0 0.0.0.0 0.0.0.0
!
Queue Mode strict
!
snmp-server community public rw
snmp-server community private rw

username admin access-level 15
username admin password 7 21232f297a57a5a743894a0e4a801fc3
username guest access-level 0
username guest password 7 084e0343a0486ff05530df6c705c8bb4
enable password level 15 7 1b3231655cebb7a1f783eddf27d254ca
!
VLAN database
  VLAN 1 name DefaultVlan media ethernet state active
  VLAN 246 name extmgm media ethernet state active
  VLAN 247 name intmgm media ethernet state active
  VLAN 248 name dynvlan media ethernet state active
  VLAN 249 name fsavlan media ethernet state active
  VLAN 4093 name intuntag media ethernet state active
!
management vlan internal 247
management vlan dynamic 248
management vlan external 246
management vlan native 4093
management vlan fsa 249
!
spanning-tree MST configuration
!
spanning-tree mode rstp
!
interface ethernet 1/1
  switchport allowed vlan add 248 untagged
  switchport ingress-filtering
  switchport native vlan 248
  switchport allowed vlan remove 1
  switchport allowed vlan add 247,249 tagged
.
.
.

```

```
interface VLAN 1
!
interface VLAN 246
!
interface VLAN 247
  IP address DHCP
!
interface VLAN 248
!
interface VLAN 249
!
interface VLAN 4093

!
no spanning-tree
!
no map IP precedence
no map IP DSCP
!
line console
!
line VTY
!
end

Console#
```

Related Commands

show running-config (section 7.5.3 on page 545)

7.5.3 show running-config

This command displays the configuration information currently in use.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

- Use this command in conjunction with the **show startup-config** command to compare the information in running memory to the information stored in non-volatile memory.
- This command displays settings for key command modes. Each mode group is separated by ! symbols, and includes the configuration mode command, and corresponding commands. This command displays the following information:
 - MAC address for the ECN330-switch
 - SNTP server settings
 - Queue mode
 - SNMP community strings
 - Users (names, access levels, and encrypted passwords)
 - VLAN database (VLAN ID, name and state)
 - VLAN configuration settings for each interface
 - Multiple spanning tree instances (name and interfaces)
 - IP address configured for VLANs
 - Layer 4 precedence settings
 - Routing protocol configuration settings
 - Spanning tree settings
 - Any configured settings for the console port and Telnet

Example

```

Console#show running-config
building running-config, please wait.....
!<stackingDB>00</stackingDB>
!<stackingMac>01_00-00-12-33-89-76_03</stackingMac>
!
phymap 00-00-12-33-89-76
!
SNTP server 0.0.0.0 0.0.0.0 0.0.0.0
!
Queue Mode strict
!
snmp-server community public ro
snmp-server community private rw
!
username admin access-level 15
username admin password 7 21232f297a57a5a743894a0e4a801fc3
username guest access-level 0
username guest password 7 084e0343a0486ff05530df6c705c8bb4
enable password level 15 7 1b3231655cebb7a1f783eddf27d254ca
!
VLAN database
VLAN 1 name DefaultVlan media ethernet state active
VLAN 246 name extmgm media ethernet state active
VLAN 247 name intmgm media ethernet state active
VLAN 248 name dynvlan media ethernet state active
VLAN 4093 name intuntag media ethernet state active
!
management vlan internal 247
management vlan dynamic 248
management vlan external 246
management vlan native 4093
management vlan fsa 249
!
spanning-tree MST configuration
!
spanning-tree mode rstp
!
interface ethernet 1/1
switchport allowed vlan add 248 untagged
switchport ingress-filtering
switchport native vlan 248
switchport allowed vlan remove 1
switchport allowed vlan add 247,249 tagged
.
.

```

```
interface VLAN 1
!
interface VLAN 246
!
interface VLAN 247
  IP address DHCP
!
interface VLAN 248
!
interface VLAN 249
!
interface VLAN 4093
!
no spanning-tree
!
no map IP precedence
no map IP DSCP
!
line console
!
line VTY
!
end

Console#
```

Related Commands

show startup-config (section 7.5.2 on page 542)

7.5.4 show system

This command displays system information.

Default Setting

None

Command Mode

Normal Exec, Privileged Exec

Command Usage

- For a description of the items shown by this command, refer to section 6.3.1 on page 69.
- The POST results should all display `PASS`.

Example

```

Console#show system
System Description: ECN330; SW version: CXC 132 8902 V1.2;
System OID String: 1.3.6.1.4.1.193.72.1400
System Information
  System Up Time:          0 days, 1 hours, 3 minutes, and 39.29
                           seconds
  System Name:             [NONE]
  System Location:         [NONE]
  System Contact:          [NONE]
  MAC Address (Unit1):     00-00-12-33-89-76
  Web Server:              Enabled
  Web Server Port:         80
  Web Secure Server:       Enabled
  Web Secure Server Port:  443
  Telnet Server:           Enable
  Telnet Server Port:      23
  Jumbo Frame:             Disabled

  POST Result:
Console#

```

7.5.5

show users

This command shows all active console and Telnet sessions, including user name, idle time, and IP address of Telnet client.

Default Setting

None

Command Mode

Normal Exec, Privileged Exec

Command Usage

The session used to execute this command is indicated by a * symbol next to the Line (that is, session) index number.

Example

```

Console#show users
Username accounts:
  Username Privilege Public-Key
  -----
      admin         15      None
      guest          0      None
      steve          15      RSA

Online users:
  Line      Username Idle time (h:m:s) Remote IP addr.
  -----
0   console   admin         0:14:14
* 1   VTY 0    admin         0:00:00   192.168.1.19
2   SSH 1     steve         0:00:06   192.168.1.19

Web online users:
  Line      Remote IP addr Username Idle time (h:m:s).
  -----
1   HTTP    192.168.1.19   admin         0:00:00

Console#

```

7.5.6 show version

This command displays hardware and software version information for the system.

Default Setting

None

Command Mode

Normal Exec, Privileged Exec

Command Usage

See section 6.3.5 on page 75 for detailed information on the items displayed by this command.

Example

```

Console#show version
Unit1
  Serial Number:      A422000632
  Hardware Version:   R0B
  EPLD Version:       1.02
  Number of Ports:    28
  Main Power Status:  Up

Agent (Master)
  Unit ID:            1
  Loader Version:     1.1
  Boot ROM Version:   1.0
  Operation Code Version: 1.2

Console#

```

System Mode Commands

This section describes command used to configure the ECN330-switch to operate in normal mode, QinQ mode, or L2MPLS mode.

Table 37 System Mode Commands

Command	Function	Mode	Page
system mode	Configures the ECN330-switch to operate in normal mode, QinQ mode, or L2MPLS mode	PE	552
show system mode	Displays the ECN330-switch system mode	PE	553

7.5.7 system mode

This command sets the ECN330-switch to operate in QinQ or L2MPLS mode. Use the **no** form to restore the default setting of normal operating mode.

Syntax

```
system mode {qinq | l2mpls}
```

```
no system mode
```

- **qinq** – Sets the ECN330-switch to QinQ mode, and allows the dot1q tunnel port to be configured. For an explanation of QinQ see “Configuring IEEE 802.1Q Tunneling” on page 882.
- **l2mpls** – Sets the ECN330-switch to L2MPLS mode, and allows all L2MPLS commands to be configured. For an explanation of L2MPLS, see “Layer 2 over MPLS Commands” on page 890.

Default Setting

No system mode is set; the ECN330-switch functions in normal operating mode.

Command Mode

Global Configuration

Command Usage

Make sure that no dot1q-tunnel port is configured before exiting QinQ mode (see section 7.17.26 on page 884). If there are any dot1q-tunnel ports set on the ECN330-switch, the **no system mode** command will fail. If any L2MPLS VLANs or L2MPLS uplink ports are configured, the **system mode qinq** and **no system mode** commands will also fail.

Example

```
Console(config)#system mode qinq  
Console(config)#
```

Related Commands

show system mode (section 7.5.8 on page 553)

7.5.8 show system mode

This command displays the ECN330-switch system mode.

Command Mode

Privileged Exec

Command Usage

The system mode displays as QinQ, L2MPLS or Normal mode.

Example

```
Console(config)#system mode qinq
Console(config)#end
Console#show system mode

System mode is QinQ mode
Console#
```

Related Commands

system mode (section 7.5.7 on page 552)

System MTU Commands

This section describes commands used to configure the Ethernet frame size on the ECN330-switch.

Table 38 Frame Size Commands

Command	Function	Mode	Page
jumbo frame	Enables support for jumbo frames	GC	554
system mtu	Sets the maximum transfer unit	GC	555
show system mtu	Shows the maximum transfer unit size for Fast Ethernet and Gigabit Ethernet ports	GC	556

7.5.9 jumbo frame

This command enables support for jumbo frames for Gigabit Ethernet ports. Use the **no** form to disable it.

Syntax

[no] jumbo frame

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- The ECN330-switch provides more efficient throughput for large sequential data transfers by supporting jumbo frames on Gigabit Ethernet ports of up to 9216 bytes. Compared to standard Ethernet frames that run only up to 1.5 KB, using jumbo frames significantly

reduces the per-packet overhead required to process protocol encapsulation fields.

- To use jumbo frames, both the source and destination end nodes (such as a computer or server) must support this feature. Also, when the connection is operating at full duplex, all switches in the network between the two end nodes must be able to accept the extended frame size. And for half-duplex connections, all devices in the collision domain would need to support jumbo frames.

Example

```
Console(config)#jumbo frame
Console(config)#
```

Related Commands

system mtu (section 7.5.10 on page 555)

7.5.10

system mtu

This command sets the maximum transfer unit for traffic crossing the ECN330-switch. Use the **no** form to restore the default settings.

Syntax

system mtu {<*FE-size*> | **jumbo** <*GE-size*>}

no system mtu

- *FE-size* - Specifies the MTU size for Fast Ethernet ports. (Range: 1500-1546 bytes)
- *GE-size* - Specifies the jumbo frame size (MTU) for Gigabit Ethernet ports. (Range: 1500-9216 bytes)

Default Setting

1522 bytes

Command Mode

Global Configuration

Command Usage

- Gigabit Ethernet ports are not affected by the **system mtu** command. Fast Ethernet ports are not affected by the **system mtu jumbo** command.
- Use the jumbo frame command to enable for disable jumbo frames for the Gigabit Ethernet ports.

Example

```
Console(config)#system mtu 1528
Console(config)#
```

Related Commands

jumbo frame (section 7.5.9 on page 554)

show system mtu (section 7.5.11 on page 556)

7.5.11

show system mtu

This command shows the maximum transfer unit size for Fast Ethernet and Gigabit Ethernet ports.

Command Mode

Global Configuration

Example

```
Console#show system mtu
System MTU size is 1500 bytes
System Jumbo MTU size is 1500 bytes
Console#
```

System SBC Mode Commands

This section describes commands used to enable or disable the SBC and test the SBC LED.

Table 39 SBC Commands

Command	Function	Mode	Page
sbc power	Enable or disables the SBC	GC	557
sbc ctrlled	Test the SBC LED	GC	559

7.5.12 sbc power

This command enable or disables the Single Board Computer (SBC) connected to port 28. Use the **no** form to turn off the SBC.

Syntax

[no] sbc power

Default Setting

Enabled (ECN330 Mode)

Command Mode

Global Configuration

Command Usage

- Use the **sbc power** command to turn on the SBC and toggle the console interface to SBC display mode. When the SBC is enabled, the SBC provides a management proxy functionality, where management of embedded nodes including the ECN330-switch is done by the SBC which is managed by PEM. Note that when the SBC is enabled, the console interface is set to SBC display mode.

- After re-enabling the SBC, the `Factory_Default_Config.cfg` is automatically regenerated to ECN330 mode with, the startup configuration is set to use this file, and the system is restarted.
- After the system reboots, the management VLANs (247-249 and 4093) are reserved and configured. The default Internal Management VLAN (VLAN 247) is set to obtain an IP address through DHCP, allowing management access to the ECN330-switch. Information on other default settings for the management VLANs is shown under “management vlan” on page 851.
- Use the **`no sbc power`** command turns off the SBC and toggles the console interface to ECN330 display mode. When the SBC is disabled, the ECN330 runs in ECN330-switch mode.
 - After disabling the SBC, the `Factory_Default_Config.cfg` is automatically regenerated to ECN330-switch mode, the startup configuration is set to use this file, and the system is restarted.
 - After the system reboots, the management VLANs (247-249 and 4093) are not set nor reserved (as in ECN330 mode) and can now be configured. Only the default External Management VLAN (VLAN 246) is set to allow management access to the ECN330. VLAN 246 is also changed to obtain an IP address through DHCP. Ports 1-27 are configure as untagged members of VLAN 1 and tagged members of VLAN 246. Interface 28 (that is, the SBC) is shut down.
 - Also, note that if the SBC is unplugged from the system, the operating mode is automatically changed to ECN330-switch mode.
- To operate the ECN330 in Layer 2 mode, IP routing must be disabled using the **`no ip routing`** command (see section 7.26.1 on page 1029).
 - Any changes to the IP routing must be saved to flash memory to retain the setting after the system reboots using the **`copy running-config startup-config`** command (section 7.5.14 on page 561).
- The SBC power status (when disabled) and ip routing status can be displayed with the **`show startup-config`** command (section 7.5.2 on page 542) or **`show running-config`** command (section 7.5.3 on page 545)

Example

```
Console(config)#sbc power
Console(config)#
```

7.5.13

sbc ctrlld

This command tests the SBC control LED (labeled CTRL on the front panel). Use this command without specifying a mode to display the current setting.

Syntax

sbc ctrlld [*<mode>*]

- *mode* - Tests the SBC LED using the specified mode. The available options include:
 - 0 - off
 - 1 - red, no flashing
 - 2 - red, flashes one time per second
 - 3 - red, flashes two times per second
 - 4 - red, flashes five times per second
 - 5 - green, no flashing
 - 6 - green, flashes one time per second
 - 3 - green, flashes two times per second
 - 4 - green, flashes five times per second

Command Mode

Privileged Exec

Example

This example turns the SBC LED off.

```
Console#sbc ctrlld  
Console#
```

File Management Commands

Managing Firmware

Firmware can be uploaded and downloaded to or from a TFTP server. By saving runtime code to a file on a TFTP server, that file can later be downloaded to the ECN330-switch to restore operation. The ECN330-switch can also be set to use new firmware without overwriting the previous version.

When downloading runtime code, the destination file name can be specified to replace the current image, or the file can be first downloaded using a different name from the current runtime code file, and then the new file set as the startup file.

Saving or Restoring Configuration Settings

Configuration settings can be uploaded and downloaded to and from a TFTP server. The configuration file can be later downloaded to restore switch settings.

The configuration file can be downloaded under a new file name and then set as the startup file, or the current startup configuration file can be specified as the destination file to directly replace it. Note that the file "Factory_Default_Config.cfg" can be copied to the TFTP server, but cannot be used as the destination on the ECN330-switch.

Table 40 Flash and File Commands

Command	Function	Mode	Page
copy	Copies a code image or an ECN330-switch configuration to or from flash memory or a TFTP server	PE	561
delete	Deletes a file or code image	PE	565
dir	Displays a list of files in flash memory	PE	566
whichboot	Displays the files booted	PE	567
boot system	Specifies the file or image used to start up the system	GC	568

7.5.14 copy

This command moves (uploads or downloads) a code image or configuration file between the ECN330-switch's flash memory and a TFTP server. When the system code or configuration settings are saved to a file on a TFTP server, that file can later be downloaded to the ECN330-switch to restore system operation. The success of the file transfer depends on the accessibility of the TFTP server and the quality of the network connection.

Syntax

```
copy file {file | running-config | startup-config | tftp}
copy running-config {file | startup-config | tftp}
copy startup-config {file | running-config | tftp}
copy tftp {file | running-config | startup-config |
https-certificate | public-key}
```

- **file** - Keyword that copies a specified file located in the ECN330-switch's flash memory or on a TFTP server. The command prompts for the file name.
- **running-config** - Keyword that copies a file to or from the current running configuration.

- **startup-config** - The configuration used for system initialization.
- **tftp** - Keyword that copies a file to or from a TFTP server.
- **https-certificate** - Keyword used to copy an HTTPS certificate from an TFTP server to the ECN330-switch.
- **public-key** - Keyword that copies an SSH key from a TFTP server. ("Secure Shell Commands" on page 655)

Default Setting

None

Command Mode

Privileged Exec

Command Usage

- The system prompts for data required to complete the copy command.
- The destination file name should not contain slashes (\ or /), the leading letter of the file name should not be a period (.), and the maximum length for file names on the TFTP server is 127 characters or 31 characters for files on the ECN330-switch. (Valid characters: A-Z, a-z, 0-9, ".", "-", "_")
- Due to the size limit of the flash memory, the ECN330-switch supports only two operation code files.
- The maximum number of user-defined configuration files depends on available memory.
- The file "Factory_Default_Config.cfg" can be used as the source to copy the factory default configuration file, but it cannot be used as the destination.
- To replace the startup configuration, **startup-config** must be used as the destination.
- For information on specifying an https-certificate, see "Replacing the Default Secure-site Certificate" on page 134. For information on configuring the ECN330-switch to use HTTPS for a secure connection, see "ip http secure-server" on page 651.

Example

The following example shows how to download new firmware from a TFTP server:

```
Console#copy tftp file
TFTP server ip address: 10.1.0.19
Choose file type:
  1. config:  2. opcode:  3. diag:  4. loader: 2
Source file name: CXC_132_8902_V3.15.BIX
Destination file name: CXC_132_8902_V3.15.BIX
\Write to FLASH Programming.
-Write to FLASH finish.
Success.
Console#
```

The following example shows how to upload the configuration settings to a file on the TFTP server:

```
Console#copy file tftp
Choose file type:
  1. config:  2. opcode:  3. diag:  4. loader: 1
Source file name: startup
TFTP server ip address: 10.1.0.99
Destination file name: startup.01
TFTP completed.
Success.

Console#
```

The following example shows how to copy the running configuration to a startup file.

```
Console#copy running-config file
destination file name : startup
Write to FLASH Programming.
\Write to FLASH finish.
Success.

Console#
```

The following example shows how to download a configuration file:

```
Console#copy tftp startup-config
TFTP server ip address: 10.1.0.99
Source configuration file name: startup.01
Startup configuration file name [startup]:
Write to FLASH Programming.

\Write to FLASH finish.
Success.

Console#
```

This example shows how to copy a secure-site certificate from an TFTP server. It then reboots the ECN330-switch to activate the certificate:

```
Console#copy tftp https-certificate
TFTP server ip address: 10.1.0.19
Source certificate file name: SS-certificate
Source private file name: SS-private
Private password: *****

Success.
Console#reload
System will be restarted, continue <y/n>? y
```

This example shows how to copy a public-key used by SSH from an TFTP server. Note that public key authentication through SSH is only supported for users configured locally on the ECN330-switch.

```
Console#copy tftp public-key
TFTP server IP address: 192.168.1.19
Choose public key type:
  1. RSA:  2. DSA: <1-2>: 1
Source file name: steve.pub
Username: steve
TFTP Download
Success.
Write to FLASH Programming.
Success.

Console#
```

7.5.15 **delete**

This command deletes a file or image.

Syntax

```
delete <filename>
```

filename - Name of the configuration file or image name.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

- If the file type is used for system startup, then this file cannot be deleted.
- “Factory_Default_Config.cfg” cannot be deleted.

Example

This example shows how to delete the configuration file test2.cfg from flash memory.

```
Console#delete test2.cfg  
Console#
```

Related Commands

dir (section 7.5.16 on page 566)

delete public-key (section 7.7.24 on page 662)

7.5.16 **dir**

This command displays a list of files in flash memory.

Syntax

```
dir [boot-rom | config | opcode [:filename]]
```

The type of file or image to display includes:

- **boot-rom** - Boot ROM (or diagnostic) image file
- **config** - ECN330-switch configuration file
- **opcode** - Run-time operation code image file.
- *filename* - Name of the file or image. If this file exists but contains errors, information on this file cannot be shown.

Default Setting

None

Command Mode

Privileged Exec

Command Usage

- If the command **dir** is entered without any parameters, the system displays all files.
- File information is shown in Table 41:

Table 41 System File Information

Column Heading	Description
file name	The name of the file.
file type	File types: Boot-Rom, Operation Code, and Config file.
startup	Shows if this file is used when the system is started.
size	The length of the file in bytes.

Example

Console#dir			
File name	File type	Startup Size (byte)	
-----	-----	-----	
Unit1:			
CXC_132_8903_V1.1.bix	Boot-Rom Image	Y	1247116
CXC_132_8902_V3.15.bix	Operation Code	Y	5130696
Factory_Default_Config.cfg	Config File	N	6286
startup	Config File	N	6821
startup1.cfg	Config File	Y	6821

			Total free space: 25427968
Console#			

7.5.17 whichboot

This command displays which files were booted when the system powered up.

Default Setting

None

Command Mode

Privileged Exec

Example

This example shows the information displayed by the **whichboot** command. See the table under the **dir** command for a description of the file information displayed by this command.

```

Console#whichboot

```

	File name	File type	Startup	Size (byte)

Unit1:				
	CXC_132_8903_V1.1.bix	Boot-Rom Image	Y	1247116
	CXC_132_8902_V3.15.bix	Operation Code	Y	5130696
	startup1.cfg	Config File	Y	6821

```

Console#

```

7.5.18 boot system

This command specifies the file or image used to start up the system.

Syntax

boot system {boot-rom | config | opcode}: <filename>

The type of file or image to set as a default includes:

- **boot-rom*** - Boot ROM
- **config *** - Configuration file
- **opcode*** - Run-time operation code
- **filename** - Name of the configuration file or image name.

* The colon (:) is required.

Default Setting

None

Command Mode

Global Configuration

Command Usage

- A colon (:) is required after the specified file type.
- If the file contains an error, it cannot be set as the default file.

Example

```
Console(config)#boot system config: startup
Console(config)#
```

Related Commands

- dir** (section 7.5.16 on page 566)
- whichboot** (section 7.5.17 on page 567)

Line Commands

The onboard configuration program can be accessed by attaching a VT100 compatible device to the ECN330's serial port. These commands are used to set communication parameters for the serial port or Telnet (a virtual terminal).

Table 42 Line Commands

Command	Function	Mode	Page
line	Identifies a specific line for configuration and starts the line configuration mode	GC	570
login	Enables password checking at login	LC	571
password	Specifies a password on a line	LC	573
timeout login response	Sets the interval that the system waits for a login attempt	LC	
exec-timeout	Sets the interval that the command interpreter waits until user input is detected	LC	575

Command	Function	Mode	Page
password-thresh	Sets the password intrusion threshold, which limits the number of failed logon attempts	LC	576
silent-time*	Sets the amount of time the management console is inaccessible after the number of unsuccessful logon attempts exceeds the threshold set by the password-thresh command	LC	577
databits*	Sets the number of data bits per character that are interpreted and generated by hardware	LC	578
parity*	Defines the generation of a parity bit	LC	579
speed*	Sets the terminal baud rate	LC	580
stopbits*	Sets the number of the stop bits transmitted per byte	LC	581
disconnect	Terminates a line connection	PE	582
show line	Displays a terminal line's parameters	NE, PE	583

* These commands only apply to the serial port.

7.5.19 line

Use this command to identify a specific line for configuration, and to process subsequent line configuration commands.

Syntax

```
line {console | vty}
```

- **console** - Console terminal line.
- **vty** - Virtual terminal for remote console access (that is, Telnet).

Default Setting

There is no default line.

Command Mode

Global Configuration

Command Usage

Telnet is considered a virtual terminal connection and will be shown as `Vty` in screen displays such as **show users**. However, the serial communication parameters (for example, databits) do not affect Telnet connections.

Example

To enter console line mode, enter the following command:

```
Console(config)#line console
Console(config-line)#
```

Related Commands

show line (section 7.5.31 on page 583)
show users (section 7.5.5 on page 549)

7.5.20

login

Use this command to enable password checking at login. Use the **no** form to disable password checking and allow connections without a password.

Syntax

login [**local**]

no login

local - Selects local password checking. Authentication is based on the user name specified with the **username** command.

Default Setting

login local

Command Mode

Line Configuration

Command Usage

- There are three authentication modes provided by the ECN330-switch itself at login:
 - **login** selects authentication by a single global password as specified by the **password** line configuration command. When using this method, the management interface starts in Normal Exec (NE) mode.
 - **login local** selects authentication through the user name and password specified by the **username** command (the default setting). When using this method, the management interface starts in Normal Exec (NE) or Privileged Exec (PE) mode, depending on the user's privilege level (0 or 15 respectively).
 - **no login** selects no authentication. When using this method, the management interface starts in Normal Exec (NE) mode.
- This command controls login authentication by the ECN330-switch itself. To configure user names and passwords for remote authentication servers, use the RADIUS or TACACS software installed on those servers.

Example

```
Console(config-line)#login local
Console(config-line)#
```

Related Commands

username (section 7.7.1 on page 633)
password (section 7.5.21 on page 573)

7.5.21 password

Use this command to specify the password for a line. Use the **no** form to remove the password.

Syntax

```
password {0 | 7} <password>
```

```
no password
```

- {0 | 7} - 0 means plain password, 7 means encrypted password
- *password* - Character string that specifies the line password. (Maximum length: 8 characters plain text, 32 encrypted, case sensitive)

Default Setting

No password is specified.

Command Mode

Line Configuration

Command Usage

- When a connection is started on a line with password protection, the system prompts for the password. If the correct password is entered, the system shows a prompt. The **password-thresh** command can be used to set the number of times a user can enter an incorrect password before the system terminates the line connection and returns the terminal to the idle state.
- The encrypted password is required for compatibility with legacy password settings (that is, plain text or encrypted) when reading the configuration file during system bootup or when downloading the configuration file from a TFTP server. There is no need to manually configure encrypted passwords.

Example

```
Console(config-line)#password 0 secret
Console(config-line)#
```

Related Commands

login (section 7.5.20 on page 571)

password-thresh (section 7.5.24 on page 576)

7.5.22 timeout login response

This command sets the interval that the system waits for a user to log into the CLI. Use the **no** form to restore the default setting.

Syntax

timeout login response [*seconds*]

no timeout login response

seconds - Integer that specifies the timeout interval.
(Range: 0 - 300 seconds; 0: disabled)

Default Setting

CLI: Disabled (0 seconds)
Telnet: 300 seconds

Command Mode

Line Configuration

Command Usage

- If a login attempt is not detected within the timeout interval, the connection is terminated for the session.
- This command applies to both the local console and Telnet connections.
- The timeout for Telnet cannot be disabled.

- Using the command without specifying a timeout restores the default setting.

Example

To set the timeout to two minutes, enter this command:

```
Console(config-line)#timeout login response 120
Console(config-line)#
```

7.5.23

exec-timeout

Use this command to set the interval that the system waits until user input is detected. Use the **no** form to restore the default.

Syntax

exec-timeout <*seconds*>

no exec-timeout

seconds - Integer that specifies the timeout interval.
(Range: 0 - 65535 seconds; 0: no timeout)

Default Setting

Console: No timeout
Telnet: 10 minutes

Command Mode

Line Configuration

Command Usage

- If user input is detected within the timeout interval, the session is kept open; otherwise the session is terminated.
- This command applies to both the local console and Telnet connections, depending on the **line** command with which the line configuration was entered (**console** or **vtty**).

- The timeout for Telnet cannot be disabled.
- Using the command without specifying a timeout restores the default setting.

Example

To set the timeout to two minutes, enter this command:

```
Console(config-line)#exec-timeout 120
Console(config-line)#
```

7.5.24 password-thresh

Use this command to set the password intrusion threshold which limits the number of failed logon attempts. Use the **no** form to remove the threshold value.

Syntax

password-thresh *<threshold>*

no password-thresh

threshold - The number of allowed password attempts.
(Range: 1-120; 0: no threshold)

Default Setting

The default value is three attempts.

Command Mode

Line Configuration

Command Usage

- When the logon attempt threshold is reached, the system interface becomes silent for a specified amount of time before allowing the next logon attempt. (Use the **silent-time** command to set this interval.) When this threshold is reached for Telnet, the Telnet logon interface shuts down.

- This command applies to both the local console and Telnet connections, depending on the **line** command with which the line configuration was entered (**console** or **vty**).

Example

To set the password threshold to five attempts, enter this command:

```
Console(config-line)#password-thresh 5
Console(config-line)#
```

Related Commands

silent-time (section 7.5.25 on page 577)

7.5.25

silent-time

Use this command to set the amount of time the management console is inaccessible after the number of unsuccessful logon attempts exceeds the threshold set by the **password-thresh** command. Use the **no** form to remove the silent time value.

Syntax

silent-time <*seconds*>

no silent-time

seconds - The number of seconds to disable console response.
(Range: 0-65535; 0: no silent-time)

Default Setting

The default value is no silent-time.

Command Mode

Line Configuration (console only)

Command Usage

This command only applies to a console port connection, it does not apply for Telnet connections.

Example

To set the silent time to 60 seconds, enter this command:

```
Console(config-line)#silent-time 60
Console(config-line)#
```

Related Commands

password-thresh (section 7.5.24 on page 576)

7.5.26

databits

Use this command to set the number of data bits per character that are interpreted and generated by the console port. Use the **no** form to restore the default value.

Syntax

databits {7 | 8}

no databits

- **7** - Seven data bits per character.
- **8** - Eight data bits per character.

Default Setting

8 data bits per character

Command Mode

Line Configuration

Command Usage

The **databits** command can be used to mask the high bit on input from devices that generate 7 data bits with parity. If parity is being generated, specify 7 data bits per character. If no parity is required, specify 8 data bits per character.

Example

To specify 7 data bits, enter this command:

```
Console(config-line)#databits 7
Console(config-line)#
```

Related Commands

parity (section 7.5.27 on page 579)

7.5.27

parity

Use this command to define generation of a parity bit. Use the **no** form to restore the default setting.

Syntax

```
parity {none | even | odd}
```

```
no parity
```

- **none** - No parity
- **even** - Even parity
- **odd** - Odd parity

Default Setting

No parity

Command Mode

Line Configuration

Command Usage

Communication protocols provided by devices such as terminals and modems often require a specific parity bit setting.

Example

To specify no parity, enter this command:

```
Console(config-line)#parity none  
Console(config-line)#
```

7.5.28

speed

Use this command to set the terminal line's baud rate. This command sets both the transmit (to terminal) and receive (from terminal) speeds. Use the **no** form to restore the default setting.

Syntax

speed <*bps*>

no speed

bps - Baud rate in bits per second.
(Options: 9600, 19200, 38400, 57600, or 115200 bps)

Default Setting

9600 bps

Command Mode

Line Configuration

Command Usage

Set the speed to match the baud rate of the device connected to the serial port. Some baud rates available on devices connected to the port might not be supported. The system indicates if the selected speed is not supported.

Example

To specify 57600 bps, enter this command:

```
Console(config-line)#speed 57600
Console(config-line)#
```

7.5.29

stopbits

Use this command to set the number of the stop bits transmitted per byte. Use the **no** form to restore the default setting.

Syntax

stopbits {1 | 2}

- 1 - One stop bit
- 2 - Two stop bits

Default Setting

1 stop bit

Command Mode

Line Configuration

Example

To specify 2 stop bits, enter this command:

```
Console(config-line)#stopbits 2
Console(config-line)#
```

7.5.30 disconnect

This command terminates an SSH, Telnet, or console connection.

Syntax

disconnect <*session-id*>

session-id – The session identifier for an SSH, Telnet or console connection. (Range: 0-4)

Command Mode

Privileged Exec

Command Usage

Specifying session identifier “0” will disconnect the console connection.
Specifying any other identifiers for an active session will disconnect an SSH or Telnet connection.

Example

```
Console#disconnect 1
Console#
```

Related Commands

show ssh (section 7.7.29 on page 666)
show users (section 7.5.5 on page 549)

7.5.31 **show line**

Use this command to display the terminal line's parameters.

Syntax

```
show line [console | vty]
```

- **console** - Console terminal line.
- **vtty** - Virtual terminal for remote console access.

Default Setting

Shows all lines

Command Mode

Normal Exec, Privileged Exec

Example

To show all lines, enter this command:

```
Console#show line
Console Configuration:
  Password Threshold: 3 times
  Interactive Timeout: Disabled
  Login Timeout: Disabled
  Silent Time: Disabled
  Baudrate: auto
  Databits: 8
  Parity: None
  Stopbits: 1

VTY Configuration:
  Password Threshold: 3 times
  Interactive Timeout: 600 sec
  Login Timeout: 300 sec
Console#
```

Event Logging Commands

This section describes commands used to configure event logging on the ECN330-switch.

Table 43 Event Logging Commands

Command	Function	Mode	Page
logging on	Controls logging of error messages	GC	584
logging history	Limits syslog messages saved to switch memory based on severity	GC	585
logging host	Adds syslog server host IP addresses that will receive logging messages	GC	587
logging facility	Sets the facility type for remote logging of syslog messages	GC	588
logging trap	Limits syslog messages saved to a remote server based on severity	GC	589
clear logging	Clears messages from the logging buffer	PE	590
show logging	Displays the state of logging	PE	591
show log	Displays log messages	PE	593

7.5.32 logging on

This command controls logging of error messages, sending debug or error messages to a logging process. The **no** form disables the logging process.

Syntax

[no] logging on

Default Setting

None

Command Mode

Global Configuration

Command Usage

The logging process controls error messages saved to switch memory or sent to remote syslog servers. The **logging history** command controls the type of error messages that are stored in memory. The **logging trap** command controls the type of error messages that are sent to specified syslog servers.

Example

```
Console(config)#logging on
Console(config)#
```

Related Commands

logging history (section 7.5.33 on page 585)
logging trap (section 7.5.36 on page 589)
clear log (section 7.5.37 on page 590)

7.5.33 logging history

This command limits syslog messages saved to switch memory based on severity. The **no** form returns the logging of syslog messages to the default level.

Syntax

```
logging history {flash | ram} <level>
```

```
no logging history {flash | ram}
```

- **flash** - Event history stored in flash memory (permanent memory).
- **ram** - Event history stored in temporary RAM (memory flushed on power reset).
- **level** - One of the levels listed in the following table. Messages sent include the selected level down to level 0. (Range:0-7)

Table 44 Logging Levels

Level Name	Level	Description
debugging	7	Debugging messages
informational	6	Informational messages only
notifications	5	Normal but significant condition, such as cold start
warnings	4	Warning conditions (for example, return false, unexpected return)
errors	3	Error conditions (for example, invalid input, default used)
critical	2	Critical conditions (for example, memory allocation, or free memory error - resource exhausted)
alerts	1	Immediate action needed
emergencies	0	System unusable

* There are only Level 2, 5 and 6 error messages for the current firmware release.

Default Setting

Flash: errors (level 3 - 0)
RAM: warnings (level 7 - 0)

Command Mode

Global Configuration

Command Usage

The message level specified for flash memory must be a higher priority (numerically lower) than that specified for RAM.

Example

```
Console(config)#logging history ram 0  
Console(config)#
```

7.5.34 logging host

This command adds a syslog server host IP address that will receive logging messages. Use the **no** form to remove a syslog server host.

Syntax

[no] logging host <host_ip_address>

host_ip_address - The IP address of a syslog server.

Default Setting

None

Command Mode

Global Configuration

Command Usage

- Using this command more than once builds up a list of host IP addresses.
- The maximum number of host IP addresses allowed is five.

Example

```
Console(config)#logging host 10.1.0.3  
Console(config)#
```

7.5.35 logging facility

This command sets the facility type for remote logging of syslog messages. Use the **no** form to return the type to the default.

Syntax

[no] logging facility <type>

type - A number that indicates the facility used by the syslog server to dispatch log messages to an appropriate service. (Range: 16-23)

Default Setting

23

Command Mode

Global Configuration

Command Usage

The command specifies the facility type tag sent in syslog messages. (See RFC 3164.) This type has no effect on the kind of messages reported by the ECN330-switch. However, it may be used by the syslog server to sort messages or to store messages in the corresponding database.

Example

```
Console(config)#logging facility 19
Console(config)#
```

7.5.36 logging trap

This command enables the logging of system messages to a remote server, or limits the syslog messages saved to a remote server based on severity. Use this command without a specified level to enable remote logging. Use the **no** form to disable remote logging.

Syntax

```
logging trap <level>
```

```
no logging trap
```

level - One of the syslog severity levels listed in the table on page 585. Messages sent include the selected level up through level 0.

Default Setting

Disabled
Level 7 - 0

Command Mode

Global Configuration

Command Usage

- Using this command with a specified level enables remote logging and sets the minimum severity level to be saved.
- Using this command without a specified level also enables remote logging, but restores the minimum severity level to the default.

Example

```
Console(config)#logging trap 4  
Console(config)#
```

7.5.37 **clear log**

This command clears messages from the log buffer.

Syntax

```
clear log [flash | ram]
```

- **flash** - Event history stored in flash memory (permanent memory).
- **ram** - Event history stored in temporary RAM (memory flushed on power reset).

Default Setting

Flash and RAM

Command Mode

Privileged Exec

Example

```
Console#clear logging  
Console#
```

Related Commands

show log (section 7.5.39 on page 593)

7.5.38 **show logging**

This command displays the configuration settings for logging messages to local switch memory, to an SMTP event handler, or to a remote syslog server.

Syntax

```
show logging {flash | ram | sendmail | trap}
```

- **flash** - Displays settings for storing event messages in flash memory (that is, permanent memory).
- **ram** - Displays settings for storing event messages in temporary RAM (that is, memory flushed on power reset).
- **sendmail** - Displays settings for the SMTP event handler (page 599).
- **trap** - Displays settings for the trap function.

Default Setting

None

Command Mode

Privileged Exec

Example

The following example shows that system logging is enabled, the message level for flash memory is `errors` (that is, default level 3 - 0), and the message level for RAM is `debugging` (that is, default level 7 - 0).

```
Console#show logging flash
Console#show logging flash
Syslog logging:           Enabled
History logging in FLASH: level errors
Console#show logging ram
Syslog logging:           Enabled
History logging in RAM: level debugging
Console#
```

Table 45 show logging flash - Display Description

Field	Description
Syslog logging	Shows if system logging has been enabled using the logging on command.
History logging in FLASH	The message level(s) reported based on the logging history command.
History logging in RAM	The message level(s) reported based on the logging history command.

The following example displays settings for the trap function.

```

Console#show logging trap
Syslog logging: Enable
REMOTELOG status: disable
REMOTELOG facility type: local use 7
REMOTELOG level type: Debugging messages
REMOTELOG server IP address: 192.168.1.4
REMOTELOG server IP address: 0.0.0.0
REMOTELOG server IP address: 0.0.0.0
REMOTELOG server IP address: 0.0.0.0
REMOTELOG server IP address: 0.0.0.0
Console#

```

Table 46 show logging trap - Display Description

Field	Description
Syslog logging	Shows if system logging has been enabled using the logging on command.
REMOTELOG status	Shows if remote logging has been enabled through the logging trap command.
REMOTELOG facility type	The facility type for remote logging of syslog messages as specified in the logging facility command.

Field	Description
REMOTELOG level type	The severity threshold for syslog messages sent to a remote server as specified in the logging trap command.
REMOTELOG server IP address	The address of syslog servers as specified in the logging host command.

Related Commands

show logging sendmail (section 7.5.45 on page 599)

7.5.39

show log

This command displays the log messages stored in local memory.

Syntax

show log {flash | ram}

- **flash** - Event history stored in flash memory (that is, permanent memory).
- **ram** - Event history stored in temporary RAM (that is, memory flushed on power reset).

Default Setting

None

Command Mode

Privileged Exec

Example

The following example shows the event message stored in RAM.

```

Console#show log ram
[1] 00:01:30 2001-01-01
    "VLAN 1 link-up notification."
    level: 6, module: 5, function: 1, and event no.: 1
[0] 00:01:30 2001-01-01
    "Unit 1, Port 1 link-up notification."
    level: 6, module: 5, function: 1, and event no.: 1
Console#

```

SMTP Alert Commands

These commands configure SMTP event handling, and forwarding of alert messages to the specified SMTP servers and email recipients.

Table 47 SMTP Alert Commands

Command	Function	Mode	Page
logging sendmail host	SMTP servers to receive alert messages	GC	595
logging sendmail level	Severity threshold used to trigger alert messages	GC	596
logging sendmail source-email	Email address used for "From" field of alert messages	GC	597
logging sendmail destination-email	Email recipients of alert messages	GC	598
logging sendmail	Enables SMTP event handling	GC	599
show logging sendmail	Displays SMTP event handler settings	NE, PE	599

7.5.40 logging sendmail host

This command specifies SMTP servers that will be sent alert messages. Use the **no** form to remove an SMTP server.

Syntax

```
[no] logging sendmail host <ip_address>
```

ip_address - IP address of an SMTP server that will be sent alert messages for event handling.

Default Setting

None

Command Mode

Global Configuration

Command Usage

- Up to three SMTP servers can be specified for event handling. However, a separate command must be entered to specify each server.
- To send email alerts, the ECN330-switch first opens a connection, sends all the email alerts waiting in the queue one by one, and finally closes the connection.
- To open a connection, the ECN330-switch first selects the server that successfully sent mail during the last connection, or the first server configured by this command. If it fails to send mail, the ECN330-switch selects the next server in the list and tries to send mail again. If it still fails, the system will repeat the process at a periodic interval. (A trap will be triggered if the ECN330-switch cannot successfully open a connection.)

Example

```
Console(config)#logging sendmail host 192.168.1.19  
Console(config)#
```

7.5.41 logging sendmail level

This command sets the severity threshold used to trigger alert messages.

Syntax

```
logging sendmail level <level>
```

level - One of the system message levels (page 585). Messages sent include the selected level down to level 0. (Range: 0-7; Default: 7)

Default Setting

Level 7

Command Mode

Global Configuration

Command Usage

The specified level indicates an event threshold. All events at this level or higher will be sent to the configured email recipients. (For example, using Level 7 will report all events from level 7 to level 0.)

Example

This example will send email alerts for system errors from level 3 through 0.

```
Console(config)#logging sendmail level 3  
Console(config)#
```

7.5.42 logging sendmail source-email

This command sets the email address used for the “From” field in alert messages.

Syntax

```
logging sendmail source-email <email-address>
```

email-address - The source email address used in alert messages.
(Range: 1-41 characters)

Default Setting

None

Command Mode

Global Configuration

Command Usage

The source email may be a symbolic email address that identifies the ECN330-switch, or the address of an administrator responsible for the ECN330.

Example

```
Console(config)#logging sendmail source-email bill@this-company.com  
Console(config)#
```

7.5.43 logging sendmail destination-email

This command specifies the email recipients of alert messages. Use the **no** form to remove a recipient.

Syntax

```
[no] logging sendmail destination-email <email-address>
```

email-address - The source email address used in alert messages.
(Range: 1-41 characters)

Default Setting

None

Command Mode

Global Configuration

Command Usage

Up to five recipients can specified for alert messages. However, a separate command must be entered to specify each recipient.

Example

```
Console(config)#logging sendmail destination-email ted@this-  
company.com  
Console(config)#
```


7.5.44 **logging sendmail**

This command enables SMTP event handling. Use the **no** form to disable this function.

Syntax

```
[no] logging sendmail
```

Default Setting

Disabled

Command Mode

Global Configuration

Example

```
Console(config)#logging sendmail  
Console(config)#
```

7.5.45 **show logging sendmail**

This command displays the settings for the SMTP event handler.

Command Mode

Normal Exec, Privileged Exec

Example

```

Console#show logging sendmail
SMTP servers
-----
192.168.1.19
SMTP minimum severity level: 7

SMTP destination email addresses
-----
ted@this-company.com
SMTP source email address: bill@this-company.com
SMTP status: Enable

Console#

```

Time Commands

The system clock can be dynamically set by polling a set of specified time servers (NTP or SNTP). Maintaining an accurate time on the ECN330-switch enables the system log to record meaningful dates and times for event entries. If the clock is not set, the ECN330-switch will only record the time from the factory default set at the last bootup.

Table 48 Time Commands

Command	Function	Mode	Page
sntp client	Accepts time from specified time servers	GC	601
sntp server	Specifies one or more time servers	GC	602
sntp poll	Sets the interval at which the client polls for time	GC	603
show sntp	Shows current SNTP configuration settings	NE, PE	604
clock timezone	Sets the time zone for the ECN330's internal clock	GC	605
calendar set	Sets the system date and time	GC	606
show calendar	Displays the current date and time setting	GC	607

7.5.46 **sntp client**

This command enables SNTP client requests for time synchronization from NTP or SNTP time servers specified with the **sntp servers** command. Use the **no** form of this command to disable SNTP client requests.

Syntax

```
[no] sntp client
```

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- The time acquired from time servers is used to record accurate dates and times for log events. Without SNTP, the ECN330-switch only records the time starting from the factory default set at the last bootup (that is, 00:00:00, Jan. 1, 2001).
- This command enables client time requests to time servers specified through the **sntp servers** command. It issues time synchronization requests based on the interval set through the **sntp poll** command.

Example

```
Console(config)#ntp server 10.1.0.19
Console(config)#ntp poll 60
Console(config)#ntp client
Console(config)#end
Console#show ntp
Current time:  Dec 23 02:52:44 2002
Poll interval: 60
Current mode: unicast
SNTP status : Enabled
SNTP server 137.92.140.80 0.0.0.0 0.0.0.0
Current server: 137.92.140.80
Console#
```

Related Commands

ntp server (section 7.5.47 on page 602)

ntp poll (section 7.5.48 on page 603)

show ntp (section 7.5.49 on page 604)

7.5.47

ntp server

This command sets the IP address of the servers to which SNTP time requests are issued. Use this command with no arguments to clear all time servers from the current list.

Syntax

```
ntp server [ip1 [ip2 [ip3]]]
```

ip - IP address of an time server (NTP or SNTP).
(Range: 1 - 3 addresses)

Default Setting

None

Command Mode

Global Configuration

Command Usage

This command specifies time servers from which the ECN330-switch will poll for time updates when set to SNTP client mode. The client will poll the time servers in the order specified until a response is received. It issues time synchronization requests based on the interval set through the **sntp poll** command.

Example

```
Console(config)#sntp server 10.1.0.19
Console#
```

Related Commands

sntp client (section 7.5.46 on page 601)
sntp poll (section 7.5.48 on page 603)
show sntp (section 7.5.49 on page 604)

7.5.48

sntp poll

This command sets the interval between sending time requests when the ECN330-switch is set to SNTP client mode. Use the **no** form to restore to the default.

Syntax

sntp poll <*seconds*>

no sntp poll

seconds - Interval between time requests. (Range: 16-16384 seconds)

Default Setting

16 seconds

Command Mode

Global Configuration

Command Usage

This command is only applicable when the ECN330-switch is set to SNTP client mode.

Example

```
Console(config)#sntp poll 60
Console#
```

Related Commands

sntp client (section 7.5.46 on page 601)

7.5.49

show sntp

This command displays the current time and configuration settings for the SNTP client, and whether or not the local time has been properly updated.

Command Mode

Normal Exec, Privileged Exec

Command Usage

This command displays the current time, the poll interval used for sending time synchronization requests, and the current SNTP mode (that is, unicast).

Example

```
Console#show sntp
Current time: Dec 23 05:13:28 2002
Poll interval: 16
Current mode: unicast
SNTP status : Enabled
SNTP server 137.92.140.80 0.0.0.0 0.0.0.0
Current server: 137.92.140.80
Console#
```

7.5.50 clock timezone

This command sets the time zone for the ECN330's internal clock.

Syntax

```
clock timezone <name> hour <hours> minute <minutes>
{before-utc | after-utc}
```

- *name* - Name of timezone, usually an acronym. (Range: 1-29 characters)
- *hours* - Number of hours before or after UTC. (Range: 1-12 hours for **before-utc** and 1-13 hours for **after-utc**)
- *minutes* - Number of minutes before or after UTC. (Range: 0-59 minutes)
- **before-utc** - Sets the local time zone before (east) of UTC.
- **after-utc** - Sets the local time zone after (west) of UTC.

Default Setting

None

Command Mode

Global Configuration

Command Usage

This command sets the local time zone relative to the Coordinated Universal Time (UTC, formerly Greenwich Mean Time or GMT), based on the earth's prime meridian, zero degrees longitude. To display a time corresponding to the local time, the number of hours and minutes the time zone is east (before) or west (after) of UTC must be indicated.

Example

```
Console(config)#clock timezone Japan hours 8 minute 0 after-UTC
Console(config)#
```

Related Commands

show sntp (section 7.5.49 on page 604)

7.5.51 calendar set

This command sets the system clock. It may be used if there is no time server on the network, or if the ECN330-switch is not configured to receive signals from a time server.

Syntax

```
calendar set <hour> <min> <sec> {<day> <month> <year> |  
    <month> <day> <year>}
```

- *hour* - Hour in 24-hour format. (Range: 0 - 23)
- *minute* - Minute. (Range: 0 - 59)
- *sec* - Second. (Range: 0 - 59)
- *day* - Day of month. (Range: 1 - 31)
- *month* - **January | February | March | April | May |
June | July | August | September | October |
November | December**
- *year* - Year (4-digit). (Range: 2001 - 2100)

Default Setting

None

Command Mode

Privileged Exec

Example

This example shows how to set the system clock to 15:12:34, March 21st, 2003.

```
Console#calendar set 15 12 34 march 21 2003
Console#
```

7.5.52

show calendar

This command displays the system clock.

Default Setting

None

Command Mode

Normal Exec, Privileged Exec

Example

This example shows how to display the current system clock setting.

```
Console#show calendar
15:12:50 March 21 2003
Console#
```

7.6 Simple Network Management Protocol Commands

The commands in this group control access to the ECN330-switch from management stations using the Simple Network Management Protocol (SNMP). SNMP is used by the Public Ethernet Manager (PEM) to communicate with the ECN330-switch, and by the ECN330-switch to send alarms (traps) to the PEM.

SNMP Version 3 provides security features that cover message integrity, authentication, and encryption; as well as controlling user access to specific areas of the MIB tree. To use these commands, first configure an SNMP engine ID (or accept the default), specify read and write access views for the MIB tree, configure SNMP user groups with the required security model (that is, SNMP v1, v2c or v3) and security level (that is, authentication and privacy), and then assign SNMP users to these groups, along with their specific authentication and privacy passwords.

Table 49 SNMP Commands

Command	Function	Mode	Page
snmp-server	Enables the SNMP agent	GC	609
show snmp	Displays the status of SNMP communications	NE, PE	610
snmp-server community	Sets up the community access string to permit access to SNMP commands	GC	612
snmp-server contact	Sets the system contact string	GC	613
snmp-server location	Sets the system location string	GC	614
snmp-server host	Specifies the recipient of an SNMP notification operation	GC	615
snmp-server enable traps	Enables the device to send SNMP traps (SNMP notifications)	GC	618
snmp-server engine-id	Sets the SNMP engine ID	GC	619

Command	Function	Mode	Page
show snmp engine-id	Shows the SNMP engine ID	PE	621
snmp-server view	Adds an SNMP view	GC	622
show snmp view	Shows the SNMP views	PE	623
snmp-server group	Adds an SNMP group, mapping users to views	GC	625
show snmp group	Shows the SNMP groups	PE	626
snmp-server user	Adds a user to an SNMP group	GC	628
show snmp user	Shows the SNMP users	PE	630

7.6.1 snmp-server

This command enables the SNMPv3 engine and services for all management clients (that is, versions 1, 2c, 3). Use the **no** form to disable the server.

Syntax

[no] snmp-server

Default Setting

Enabled

Command Mode

Global Configuration

Example

```
Console(config)#snmp-server
Console(config)#
```

7.6.2 **show snmp**

This command can be used to check the status of SNMP communications.

Default Setting

None

Command Mode

Normal Exec, Privileged Exec

Command Usage

This command provides information on the community access strings, counter information for SNMP input and output protocol data units, and whether or not SNMP logging has been enabled with the **snmp-server enable traps** command.

Example

```
Console#show snmp

SNMP traps:
  Authentication: enable
  Link-up-down: enable

SNMP communities:
  1. private, and the privilege is read-write
  2. public, and the privilege is read-only

0 SNMP packets input
  0 Bad SNMP version errors
  0 Unknown community name
  0 Illegal operation for community name supplied
  0 Encoding errors
  0 Number of requested variables
  0 Number of altered variables
  0 Get-request PDUs
  0 Get-next PDUs
  0 Set-request PDUs
0 SNMP packets output
  0 Too big errors
  0 No such name errors
  0 Bad values errors
  0 General errors
  0 Response PDUs
  0 Trap PDUs

SNMP logging: disabled
Console#
```

7.6.3 snmp-server community

This command defines the SNMP v1 and v2c community access strings. Use the **no** form to remove the specified community string.

Syntax

```
snmp-server community <string> [ro | rw]
```

```
no snmp-server community <string>
```

- *string* - Community string that acts like a password and permits access to the SNMP protocol. (Maximum length: 32 characters, case sensitive; Maximum number of strings: 5)
- **ro** - Specifies read-only access. Authorized management stations are only able to retrieve MIB objects.
- **rw** - Specifies read/write access. Authorized management stations are able to both retrieve and modify MIB objects.

Default Setting

- **public** - Read-only access. Authorized management stations are only able to retrieve MIB objects.
- **private** - Read/write access. Authorized management stations are able to both retrieve and modify MIB objects.

Command Mode

Global Configuration

Example

```
Console(config)#snmp-server community alpha rw  
Console(config)#
```

7.6.4 snmp-server contact

This command sets the system contact string. Use the **no** form to remove the system contact information.

Syntax

```
snmp-server contact <string>
```

```
no snmp-server contact
```

string - String that describes the system contact information.
(Maximum length: 255 characters)

Default Setting

None

Command Mode

Global Configuration

Example

```
Console(config)#snmp-server contact Paul  
Console(config)#
```

Related Commands

snmp-server location (section 7.6.5 on page 614)

7.6.5 **snmp-server location**

This command sets the system location string. Use the **no** form to remove the location string.

Syntax

```
snmp-server location <text>
```

```
no snmp-server location
```

text - String that describes the system location.
(Maximum length: 255 characters)

Default Setting

None

Command Mode

Global Configuration

Example

```
Console(config)#snmp-server location Copenhagen-Site1  
Console(config)#
```

Related Commands

snmp-server contact (section 7.6.4 on page 613)

7.6.6 snmp-server host

This command specifies the recipient of SNMP traps and notifications. Use the **no** form to remove the specified host.

Syntax

```
snmp-server host <host-addr> [inform [retry <retries> |
    timeout <seconds>]] <community-string> [version {1
    | 2c | 3 {auth | noauth | priv} [udp-port <port>]]}
no snmp-server host <host-addr>
```

- **host-addr** - Internet address of the host (the targeted recipient). (Maximum host addresses: 5 trap destination IP address entries)
- **inform** - Notifications are sent as inform messages. Note that this option is only available for version 2c and 3 hosts. (Default: traps are used)
 - **retries** - The maximum number of times to resend an inform message if the recipient does not acknowledge receipt. (Range: 0-255; Default: 3)
 - **seconds** - The number of seconds to wait for an acknowledgment before resending an inform message. (Range: 0-2147483647 centiseconds; Default: 1500 centiseconds)
- **community-string** - A password-like community string sent with the notification operation to SNMP v1 and v2c hosts. Although this string can be set using the **snmp-server host** command by itself, it is recommended that the string be defined using the **snmp-server community** command prior to using the **snmp-server host** command. (Maximum length: 32 characters)
- **version** - Specifies whether to send notifications as SNMP v1, v2c, or v3 traps. (Range: 1, 2c, 3; Default: 1)
- **auth | noauth | priv** - This group uses SNMPv3 with authentication, no authentication, or with authentication and privacy.
- **port** - Host UDP port to use. (Range: 1-65535; Default: 162)

Default Setting

Host Address: None
Notification Type: Traps
SNMP Version: 1
UDP Port: 162

Command Mode

Global Configuration

Command Usage

- If an **snmp-server host** command is not entered, no notifications are sent. To configure the ECN330-switch to send SNMP notifications, enter at least one **snmp-server host** command. To enable multiple hosts, issue a separate **snmp-server host** command for each host.
- The **snmp-server host** command is used in conjunction with the **snmp-server enable traps** command. Use the **snmp-server enable traps** command to enable the sending of traps or informs and to specify which SNMP notifications are sent globally. For a host to receive notifications, at least one **snmp-server enable traps** command and the **snmp-server host** command for that host must be enabled.
- Some notification types cannot be controlled with the **snmp-server enable traps** command. For example, some notification types are always enabled.
- Notifications are issued by the ECN330-switch as trap messages by default. The recipient of a trap message does not send a response to the ECN330-switch. Traps are therefore not as reliable as inform messages, which include a request for acknowledgement of receipt. Informs can be used to ensure that critical information is received by the host. However, note that informs consume more system resources because they must be kept in memory until a response is received. Informs also add to network traffic. Consider these effects when deciding whether to issue notifications as traps or informs.
- To send an inform to a SNMPv2c host, complete these steps:
 1. Enable the SNMP agent (see section 7.6.1 on page 609).

2. Allow the ECN330-switch to send SNMP traps; that is, notifications (see section 7.6.7 on page 618).
 3. Specify the target host that will receive inform messages with the **snmp-server host** command as described in this section.
 4. Create a view with the required notification messages (see section 7.6.10 on page 622).
 5. Create a group that includes the required notify view (see section 7.6.12 on page 625).
- To send an inform to a SNMPv3 host, complete these steps:
 1. Enable the SNMP agent (see section 7.6.1 on page 609).
 2. Allow the ECN330-switch to send SNMP traps; that is, notifications (see section 7.6.7 on page 618).
 3. Specify the target host that will receive inform messages with the **snmp-server host** command as described in this section.
 4. Create a view with the required notification messages (see section 7.6.10 on page 622).
 5. Create a group that includes the required notify view (see section 7.6.12 on page 625).
 6. Specify a remote engine ID where the user resides (see section 7.6.9 on page 621).
 7. Then configure a remote user (see section 7.6.14 on page 628).
 - The ECN330-switch can send SNMP Version 1, 2c or 3 notifications to a host IP address, depending on the SNMP version that the management station supports. If the **snmp-server host** command does not specify the SNMP version, the default is to send SNMP version 1 notifications.
 - If an SNMP Version 3 host is specified, then the community string is interpreted as an SNMP user name. If the v3 “auth” or “priv” options are used, the user name must first be defined with the **snmp-server user** command. Otherwise, the authentication password and/or privacy password will not exist and the ECN330-switch will not authorize SNMP access for the host. However, if a v3 host is specified with the “noauth” option, an SNMP user account will be generated and the ECN330-switch will authorize SNMP access for the host.

Example

```
Console(config)#snmp-server host 10.1.19.23 batman
Console(config)#
```

Related Commands

snmp-server enable traps (section 7.6.7 on page 618)

7.6.7 snmp-server enable traps

This command enables the ECN330-switch to send SNMP traps or informs (that is, SNMP notifications). Use the **no** form to disable SNMP notifications.

Syntax

```
[no] snmp-server enable traps [authentication | link-up-  
down]
```

- **authentication** - Keyword to issue authentication failure traps.
- **link-up-down** - Keyword to issue link-up or link-down traps.

Default Setting

Issue authentication and link-up-down traps.

Command Mode

Global Configuration

Command Usage

- If an **snmp-server enable traps** command is not entered, no notifications controlled by this command are sent. To configure the ECN330-switch to send SNMP notifications, enter at least one **snmp-server enable traps** command. If the command is entered with no keywords, both authentication and link-up-down notifications are enabled. If the command is entered with a keyword, only the notification type related to that keyword is enabled.

- The **snmp-server enable traps** command is used in conjunction with the **snmp-server host** command. Use the **snmp-server host** command to specify which host or hosts receive SNMP notifications. To send notifications, at least one **snmp-server host** command must be configured.
- The authentication, link-up, and link-down traps are legacy notifications, and therefore when used for SNMP Version 3 hosts, they must be enabled in conjunction with the corresponding entries in the Notify View assigned by the **snmp-server group** command (see section 7.6.12 on page 625).

Example

```
Console(config)#snmp-server enable traps link-up-down
Console(config)#
```

Related Commands

snmp-server host (section 7.6.6 on page 615)

7.6.8 snmp-server engine-id

This command configures an identification string for the SNMPv3 engine. Use the **no** form to restore the default.

Syntax

```
snmp-server engine-id {local | remote {<ip-address>}}
<engineid-string>
```

```
no snmp-server engine-id {local | remote {address}}
```

- **local** - Specifies the SNMP engine on the ECN330-switch.
- **remote** - Specifies an SNMP engine on a remote device.
- *ip-address* - The Internet address of the remote device.
- *engineid-string* - String identifying the engine ID.
(Range: 10-64 hexadecimal characters)

Default Setting

A unique engine ID is automatically generated by the ECN330-switch based on its MAC address.

Command Mode

Global Configuration

Command Usage

- An SNMP engine is an independent SNMP agent that resides either on the ECN330-switch or on a remote device. This engine protects against message replay, delay, and redirection. The engine ID is also used in combination with user passwords to generate the security keys for authenticating and encrypting SNMPv3 packets.
- A remote engine ID is required when using SNMPv3 informs. (See **snmp-server host** in section 7.6.6 on page 615.) The remote engine ID is used to compute the security digest for authenticating and encrypting packets sent to a user on the remote host. SNMP passwords are localized using the engine ID of the authoritative agent. For informs, the authoritative SNMP agent is the remote agent. Therefore, the remote agent's SNMP engine ID must be configured before sending proxy requests or informs to it.
- A local engine ID is automatically generated that is unique to the ECN330-switch. This is referred to as the default engine ID. If the local engine ID is deleted or changed, all SNMP users will be cleared. All existing users will need to be reconfigured (section 7.6.14 on page 628).

Example

```
Console(config)#snmp-server engine-id local 12345
Console(config)#snmp-server engineID remote 54321 192.168.1.19
Console(config)#
```

Related Commands

snmp-server host (section 7.6.6 on page 615)

7.6.9 **show snmp engine-id**

This command shows the SNMP engine ID.

Command Mode

Privileged Exec

Example

This example shows the default engine ID.

```

Console#show snmp engine-id
Local SNMP engineID: 8000002a8000000000e8666672
Local SNMP engineBoots: 1

Remote SNMP engineID                               IP address
800000000030004e2b316c54321                        192.168.1.19
Console#

```

Table 50 show snmp engine-id - Display Description

Field	Description
Local SNMP engineID	String identifying the engine ID.
Local SNMP engineBoots	The number of times that the engine has (re-)initialized since the snmp EngineID was last configured.
Remote SNMP engineID	String identifying an engine ID on a remote device.
IP address	IP address of the device containing the corresponding remote SNMP engine.

7.6.10 **snmp-server view**

This command adds an SNMP view which controls user access to the MIB. Use the **no** form to remove an SNMP view.

Syntax

```
snmp-server view <view-name> <oid-tree> {included |  
                                excluded}
```

```
no snmp-server view <view-name>
```

- *view-name* - Name of an SNMP view. (Range: 1-32 characters)
- *oid-tree* - Object identifier of a branch within the MIB tree. Wild cards can be used to mask a specific portion of the OID string. (Refer to the examples.)
- **included** - Defines an included view.
- **excluded** - Defines an excluded view.

Default Setting

defaultview (includes access to the entire MIB tree)

Command Mode

Global Configuration

Command Usage

- Views are used in the **snmp-server group** command to restrict user access to specified portions of the MIB tree.
- The predefined view “defaultview” includes access to the entire MIB tree.

Examples

This view includes MIB-2.

```
Console(config)#snmp-server view mib-2 1.3.6.1.2.1 included
Console(config)#
```

This view includes the MIB-2 interfaces table, ifDescr. The wildcard is used to select all the index values in this table.

```
Console(config)#snmp-server view ifEntry.2 1.3.6.1.2.1.2.2.1.*.2
included
Console(config)#
```

This view includes the MIB-2 interfaces table, and the mask selects all index entries.

```
Console(config)#snmp-server view ifEntry.a 1.3.6.1.2.1.2.2.1.1.*
included
Console(config)#
```

7.6.11 show snmp view

This command shows information on the SNMP views.

Command Mode

Privileged Exec

Example

```

Console#show snmp view
View Name: mib-2
Subtree OID: 1.2.2.3.6.2.1
View Type: included
Storage Type: permanent
Row Status: active

View Name: defaultview
Subtree OID: 1
View Type: included
Storage Type: volatile
Row Status: active

Console#

```

Table 51 *show snmp view - Display Description*

Field	Description
View Name	Name of an SNMP view.
Subtree OID	A branch in the MIB tree.
View Type	Indicates if the view is included or excluded.
Storage Type	The storage type for this entry.
Row Status	The row status of this entry.

7.6.12 snmp-server group

This command adds an SNMP group, mapping SNMP users to SNMP views. Use the **no** form to remove an SNMP group.

Syntax

```
snmp-server group <groupname> {v1 | v2c | v3 {auth |  
noauth | priv}} [read <readview>] [write  
<writeview>] [notify <notifyview>]
```

```
no snmp-server group <groupname>
```

- *groupname* - Name of an SNMP group. (Range: 1-32 characters)
- **v1 | v2c | v3** - Use SNMP version 1, 2c or 3.
- **auth | noauth | priv** - This group uses SNMPv3 with authentication, no authentication, or with authentication and privacy. See “Simple Network Management Protocol” on page 106 for further information about these authentication and encryption options.
- *readview* - Defines the view for read access. (1-32 characters)
- *writeview* - Defines the view for write access. (1-32 characters)
- *notifyview* - Defines the view for notifications. (1-32 characters)

Default Setting

groupname: public (read only, no view is defined), private (read/write, maps to defaultview)

readview: Every object belonging to the Internet OID space (1.3.6.1).

writeview: Nothing is defined.

notifyview - Nothing is defined.

Command Mode

Global Configuration

Command Usage

- A group sets the access policy for the assigned users.

- When authentication is selected, the MD5 or SHA algorithm is used as specified in the **snmp-server user** command.
- When privacy is selected, the DES 56-bit algorithm is used for data encryption.
- For additional information on the notification messages supported by the ECN330-switch, see the *ECN330 Alarm Description*. Also, note that the authentication, link-up and link-down messages are legacy traps and must therefore be enabled in conjunction with the **snmp-server enable traps** command (section 7.6.7 on page 618).

Example

```
Console(config)#snmp-server group r&d v3 auth write daily
Console(config)#
```

7.6.13 show snmp group

Four default groups are provided – SNMPv1 read-only access and read/write access, and SNMPv2c read-only access and read/write access.

Command Mode

Privileged Exec

Example

```
Console#show snmp group
Group Name: r&d
Security Model: v3
Read View: defaultview
Write View: daily
Notify View: none
Storage Type: permanent
Row Status: active
```

```

Group Name: public
Security Model: v1
Read View: defaultview
Write View: none
Notify View: none
Storage Type: volatile
Row Status: active

Group Name: public
Security Model: v2c
Read View: defaultview
Write View: none
Notify View: none
Storage Type: volatile
Row Status: active

Group Name: private
Security Model: v1
Read View: defaultview
Write View: defaultview
Notify View: none
Storage Type: volatile
Row Status: active

Group Name: private
Security Model: v2c
Read View: defaultview
Write View: defaultview
Notify View: none
Storage Type: volatile
Row Status: active

Console#

```

Table 52 *show snmp group - Display Description*

Field	Description
groupname	Name of an SNMP group.
security model	The SNMP version.
readview	The associated read view.
writeview	The associated write view.

Field	Description
notifyview	The associated notify view.
storage-type	The storage type for this entry.
Row Status	The row status of this entry.

7.6.14 snmp-server user

This command adds a user to an SNMP group, restricting the user to a specific SNMP Read, Write, or Notify View. Use the **no** form to remove a user from an SNMP group.

Syntax

```
snmp-server user <username> <groupname> [remote <ip-
address>] {v1 | v2c | v3 [encrypted] [auth {md5 |
sha} <auth-password> [priv des56 <priv-password>]]}
no snmp-server user <username> {v1 | v2c | v3 | remote}
```

- **username** - Name of user connecting to the SNMP agent. (Range: 1-32 characters)
- **groupname** - Name of an SNMP group to which the user is assigned. (Range: 1-32 characters)
- **remote** - Specifies an SNMP engine on a remote device.
- **ip-address** - The Internet address of the remote device.
- **v1 | v2c | v3** - Use SNMP version 1, 2c or 3.
- **encrypted** - Accepts the password as encrypted input.
- **auth** - Uses SNMPv3 with authentication.
- **md5 | sha** - Uses MD5 or SHA authentication.
- **auth-password** - Authentication password. Enter as plain text if the **encrypted** option is not used. Otherwise, enter an encrypted password. (A minimum of eight characters is required.)
- **priv des56** - Uses SNMPv3 with privacy with DES56 encryption.

- *priv-password* - Privacy password. Enter as plain text if the **encrypted** option is not used. Otherwise, enter an encrypted password.

Default Setting

None

Command Mode

Global Configuration

Command Usage

- The SNMP engine ID is used to compute the authentication/privacy digests from the password. Therefore, configure the engine ID with the **snmp-server engine-id** command (section 7.6.8 on page 619) before using this configuration command.
- Before configuring a remote user, use the **snmp-server engine-id** command to specify the engine ID for the remote device where the user resides. Then use the **snmp-server user** command to specify the user and the IP address for the remote device where the user resides. The remote agent's SNMP engine ID is used to compute authentication/privacy digests from the user's password. If the remote engine ID is not first configured, the **snmp-server user** command specifying a remote user will fail.
- SNMP passwords are localized using the engine ID of the authoritative agent. For informs, the authoritative SNMP agent is the remote agent. Therefore, configure the remote agent's SNMP engine ID before sending proxy requests or informs to it.

Example

```
Console(config)#snmp-server user steve group r&d v3 auth md5
greenpeace priv des56 einstien
Console(config)#snmp-server user mark group r&d remote 192.168.1.19
v3 auth md5 greenpeace priv des56 einstien
Console(config)#
```

7.6.15 **show snmp user**

This command shows information on SNMP users.

Command Mode

Privileged Exec

Example

```

Console#show snmp user
EngineId: 800000ca030030f1df9ca00000
User Name: steve
Authentication Protocol: md5
Privacy Protocol: des56
Storage Type: nonvolatile
Row Status: active

SNMP remote user
EngineId: 80000000030004e2b316c54321
User Name: mark
Authentication Protocol: mdt
Privacy Protocol: des56
Storage Type: nonvolatile
Row Status: active

Console#

```

Table 53 *show snmp user - Display Description*

Field	Description
EngineId	String identifying the engine ID.
User Name	Name of user connecting to the SNMP agent.
Authenticati on Protocol	The authentication protocol used with SNMPv3.
Privacy Protocol	The privacy protocol used with SNMPv3.
Storage Type	The storage type for this entry.

Field	Description
Row Status	The row status of this entry.
SNMP remote user	A user associated with an SNMP engine on a remote device.

7.7 User Authentication Commands

The ECN330-switch can be configured to authenticate users logging into the system for management access using local or remote authentication methods. The ECN330-switch can also enable port-based authentication for network client access using IEEE 802.1X.

Table 54 Authentication Commands

Command Group	Function	Page
User Accounts	Configures the basic user names and passwords for management access	633
Authentication Sequence	Defines logon authentication method and precedence	636
RADIUS Client	Configures settings for authentication through a RADIUS server	640
TACACS+ Client	Configures settings for authentication through a TACACS+ server	646
Web Server Settings	Enables management access through a web browser	649
Telnet Server Settings	Enables management access through Telnet	654
Secure Shell Settings	Provides secure replacement for Telnet	655
Port Security	Configures secure addresses for a port	669
Port Authentication	Configures host authentication on specific ports using 802.1X	674
IP Filter	Configures IP addresses that are allowed management access	687

User Account Commands

The basic commands required for management access are listed in this section. The ECN330-switch also includes other options for password checking through the console or a Telnet connection, user authentication through a remote authentication server (page 608), and host access authentication for specific ports (page 674).

Table 55 User Access Commands

Command	Function	Mode	Page
username	Establishes a user name-based authentication system at login	GC	633
enable password	Sets a password to control access to various Privileged Exec levels	GC	635

7.7.1 username

This command adds named users, require authentication at login, specify or change a user's password (or specify that no password is required), or specify or change a user's access level. Use the **no** form to remove a user name.

Syntax

```
username <name> {access-level <level> | nopassword |  
password {0 | 7} <password>}
```

```
no username <name>
```

- **name** - The name of the user. (Maximum length: 8 characters, case sensitive. Maximum users: 16)
- **access-level <level>** - Specifies the user level.

The device has two predefined privilege levels:

0: Normal Exec, **15**: Privileged Exec. All other privilege levels are currently reserved for future use.

- **nopassword** - No password is required for this user to log in.
- **{0 | 7}** - **0** means plain password, **7** means encrypted password.

- **password** <*password*> - The authentication password for the user. (Maximum length: 8 characters, 32 encrypted, case sensitive)

Default Setting

- The default access level is Privileged Exec.
- The factory defaults are:

username	access-level	password
guest	0	guest
admin	15	admin

Command Mode

Global Configuration

Command Usage

The encrypted password is required for compatibility with legacy password settings (that is, plain text or encrypted) when reading the configuration file during system bootup or when downloading the configuration file from a TFTP server. There is no need to manually configure encrypted passwords.

Example

This example shows how to set the access level and password for a user.

```
Console(config)#username bob access-level 15
Console(config)#username bob password 0 smith
Console(config)#
```

7.7.2 enable password

After initially logging onto the system, the Privileged Exec password should be set. Remember to record it in a safe place. Use this command to control access to the Privileged Exec level from the Normal Exec level. Use the **no** form to reset the default password.

Syntax

```
enable password [level <level>] {0 | 7} <password>
```

```
no enable password [level <level>]
```

- **level** <level> - Level 15 for Privileged Exec. (Levels 0-14 are not used.)
- {0 | 7} - 0 means plain password, 7 means encrypted password.
- **password** - password for this privilege level.
(Maximum length: 8 characters plain text, 32 encrypted, case sensitive)

Default Setting

- The default is level 15.
- This default password is **super**

Command Mode

Global Configuration

Command Usage

- A null password cannot be set. A password has to be entered to change the command mode from Normal Exec to Privileged Exec with the **enable** command (see section 7.4.1 on page 532).
- The encrypted password is required for compatibility with legacy password settings (that is, plain text or encrypted) when reading the configuration file during system startup or when downloading the configuration file from a TFTP server. There is no need to manually configure encrypted passwords.

Example

```
Console(config)#enable password level 15 0 admin
Console(config)#
```

Related Commands

enable (section 7.4.1 on page 532)

authentication enable (section 7.7.4 on page 638)

Authentication Sequence

Three authentication methods can be specified to authenticate users logging into the system for management access. The commands in this section can be used to define the authentication method and sequence.

Table 56 Authentication Sequence Commands

Command	Function	Mode	Page
authentication login	Defines logon authentication method and precedence	GC	637
authentication enable	Defines the authentication method and precedence for command mode change	GC	638

7.7.3 authentication login

This command defines the login authentication method and precedence. Use the **no** form to restore the default.

Syntax

```
authentication login {[local] [radius] [tacacs]}
```

```
no authentication login
```

- **local** - Use local password only.
- **radius** - Use RADIUS server password only.
- **tacacs** - Use TACACS server password only.

Default Setting

Local

Command Mode

Global Configuration

Command Usage

- RADIUS uses UDP while TACACS+ uses TCP. UDP only offers best effort delivery, while TCP offers a connection-oriented transport. Also, note that RADIUS encrypts only the password in the access-request packet from the client to the server, while TACACS+ encrypts the entire body of the packet.
- RADIUS and TACACS+ logon authentication assigns a specific privilege level for each user name and password pair. The user name, password, and privilege level must be configured on the authentication server.
- Three authentication methods can be specified in a single command to indicate the authentication sequence. For example, by entering **authentication login radius tacacs local**, the user name and password on the RADIUS server is verified first. If the RADIUS server is not available, then authentication is attempted on the

TACACS+ server. If the TACACS+ server is not available, the local user name and password is checked.

Example

```
Console(config)#authentication login radius
Console(config)#
```

Related Commands

username (section 7.7.1 on page 633)

7.7.4 authentication enable

This command defines the authentication method and precedence to use when changing from Exec command mode to Privileged Exec command mode with the **enable** command (see page 532). Use the **no** form to restore the default.

Syntax

authentication enable {[local] [radius] [tacacs]}

no authentication enable

- **local** - Use local password only.
- **radius** - Use RADIUS server password only.
- **tacacs** - Use TACACS server password.

Default Setting

Local

Command Mode

Global Configuration

Command Usage

- RADIUS uses UDP while TACACS+ uses TCP. UDP only offers best effort delivery, while TCP offers a connection-oriented transport. Also, note that RADIUS encrypts only the password in the access-request packet from the client to the server, while TACACS+ encrypts the entire body of the packet.
- RADIUS and TACACS+ logon authentication assigns a specific privilege level for each user name and password pair. The user name, password, and privilege level must be configured on the authentication server.
- Three authentication methods can be specified in a single command to indicate the authentication sequence. For example, by entering **authentication enable radius tacacs local**, the user name and password on the RADIUS server is verified first. If the RADIUS server is not available, then authentication is attempted on the TACACS+ server. If the TACACS+ server is not available, the local user name and password is checked.

Example

```
Console(config)#authentication enable radius  
Console(config)#
```

Related Commands

enable password (section 7.7.2 on page 635) - sets the password for changing command modes

RADIUS Client

Remote Authentication Dial-in User Service (RADIUS) is a logon authentication protocol that uses software running on a central server to control access to RADIUS-aware devices on the network. An authentication server contains a database of multiple user name/password pairs with associated privilege levels for each user or group that require management access to an ECN330-switch.

Table 57 RADIUS Client Commands

Command	Function	Mode	Page
radius-server host	Specifies the RADIUS server	GC	641
radius-server port	Sets the RADIUS server network port	GC	642
radius-server key	Sets the RADIUS encryption key	GC	643
radius-server retransmit	Sets the number of retries	GC	643
radius-server timeout	Sets the interval between sending authentication requests	GC	644
show radius-server	Shows the current RADIUS settings	PE	645

7.7.5 radius-server host

This command specifies primary and backup RADIUS servers and authentication parameters that apply to each server. Use the **no** form to restore the default values.

Syntax

```
[no] radius-server <index> host {<host_ip_address> |
<host_alias>} [auth-port <auth_port>] [timeout
<timeout>] [retransmit <retransmit>] [key <key>]
```

- *index* - Allows up to five servers to be specified. These servers are queried in sequence until a server responds or the retransmit period expires.
- *host_ip_address* - IP address of server.
- *host_alias* - Symbolic name of server. (Maximum length: 20 characters)
- *port_number* - RADIUS server UDP port used for authentication messages. (Range: 1-65535)
- *timeout* - Number of seconds the ECN330-switch waits for a reply before resending a request. (Range: 1-65535)
- *retransmit* - Number of times the ECN330-switch will try to authenticate logon access via the RADIUS server. (Range: 1-30)
- *key* - Encryption key used to authenticate logon access for client. Do not use blank spaces in the string. (Maximum length: 20 characters)

Default Setting

```
auth-port: 1812
timeout: 5 seconds
retransmit: 2
```

Command Mode

Global Configuration

Example

```
Console(config)#radius-server 1 host 192.168.1.20 port 181 timeout  
10 retransmit 5 key green  
Console(config)#
```

7.7.6 radius-server port

This command sets the RADIUS server network port. Use the **no** form to restore the default.

Syntax

```
radius-server port <port_number>
```

```
no radius-server port
```

port_number - RADIUS server UDP port used for authentication messages. (Range: 1-65535)

Default Setting

1812

Command Mode

Global Configuration

Example

```
Console(config)#radius-server port 181  
Console(config)#
```

7.7.7 radius-server key

This command sets the RADIUS encryption key. Use the **no** form to restore the default.

Syntax

```
radius-server key <key_string>
```

```
no radius-server key
```

key_string - Encryption key used to authenticate logon access for client. Do not use blank spaces in the string. (Maximum length: 20 characters)

Default Setting

None

Command Mode

Global Configuration

Example

```
Console(config)#radius-server key green
Console(config)#
```

7.7.8 radius-server retransmit

This command sets the number of retries. Use the **no** form to restore the default.

Syntax

```
radius-server retransmit <number_of_retries>
```

```
no radius-server retransmit
```

number_of_retries - Number of times the ECN330-switch will try to authenticate logon access through the RADIUS server. (Range: 1 - 30)

Default Setting

2

Command Mode

Global Configuration

Example

```
Console(config)#radius-server retransmit 5
Console(config)#
```

7.7.9 radius-server timeout

This command sets the interval between the retransmitting of authentication requests to the RADIUS server. Use the **no** form to restore the default.

Syntax

```
radius-server timeout <number_of_seconds>
```

```
no radius-server timeout
```

number_of_seconds - Number of seconds the ECN330-switch waits for a reply before resending a request. (Range: 1-65535)

Default Setting

5

Command Mode

Global Configuration

Example

```
Console(config)#radius-server timeout 10
Console(config)#
```

7.7.10 **show radius-server**

This command displays the current settings for the RADIUS server.

Default Setting

None

Command Mode

Privileged Exec

Example

```
Console#show radius-server

Remote RADIUS server configuration:

Global settings:
  Communication key with RADIUS server: *****
  Server port number:                  1812
  Retransmit times:                   2
  Request timeout:                    5

Server 1:
  Server IP address:                  192.168.1.1
  Communication key with RADIUS server: *****
  Server port number: 1812
  Retransmit times: 2
  Request timeout: 5

Console#
```

TACACS+ Client

Terminal Access Controller Access Control System (TACACS+) is a logon authentication protocol that uses software running on a central server to control access to TACACS-aware devices on the network. An authentication server contains a database of multiple user name/password pairs with associated privilege levels for each user or group that require management access to an ECN330-switch.

Table 58 TACACS+ Client Commands

Command	Function	Mode	Page
tacacs-server host	Specifies the TACACS+ server	GC	646
tacacs-server port	Specifies the TACACS+ server network port	GC	647
tacacs-server key	Sets the TACACS+ encryption key	GC	648
show tacacs-server	Shows the current TACACS+ settings	GC	648

7.7.11 tacacs-server host

This command specifies the TACACS+ server. Use the **no** form to restore the default.

Syntax

```
tacacs-server host <host_ip_address>
```

```
no tacacs-server host
```

host_ip_address - IP address of a TACACS+ server.

Default Setting

None

Command Mode

Global Configuration

Example

```
Console(config)#tacacs-server host 192.168.1.25  
Console(config)#
```

7.7.12

tacacs-server port

This command specifies the TACACS+ server TCP port. Use the **no** form to restore the default.

Syntax

tacacs-server port <port_number>

no tacacs-server port

port_number - TACACS+ server TCP port used for authentication messages. (Range: 1-65535)

Default Setting

49

Command Mode

Global Configuration

Example

```
Console(config)#tacacs-server port 181  
Console(config)#
```

7.7.13 **tacacs-server key**

This command sets the TACACS+ encryption key. Use the **no** form to restore the default.

Syntax

```
tacacs-server key <key_string>
```

```
no tacacs-server key
```

key_string - Encryption key used to authenticate logon access for the client. Do not use blank spaces in the string.
(Maximum length: 20 characters)

Default Setting

None

Command Mode

Global Configuration

Example

```
Console(config)#tacacs-server key green  
Console(config)#
```

7.7.14 **show tacacs-server**

This command displays the current settings for the TACACS+ server.

Default Setting

None

Command Mode

Global Configuration

Example

```

Console#show tacacs-server
Remote TACACS server configuration:
  Server IP address:          10.11.12.13
  Communication key with TACACS server: *****
  Server port number:        49
Console#

```

Web Server Commands

This section describes commands used to configure web browser management access to the ECN330-switch.

Table 59 Web Server Commands

Command	Function	Mode	Page
ip http port	Specifies the port to be used by the web browser interface	GC	650
ip http server	Allows the ECN330-switch to be monitored or configured from a browser	GC	650
ip http secure-server	Enables HTTPS/SSL for encrypted communications	GC	651
ip http secure-port	Specifies the UDP port number for HTTPS/SSL	GC	653

7.7.15 **ip http port**

This command specifies the TCP port number used by the web browser interface. Use the **no** form to use the default port.

Syntax

```
ip http port <port-number>
```

```
no ip http port
```

port-number - The TCP port to be used by the browser interface.
(Range: 1-65535)

Default Setting

80

Command Mode

Global Configuration

Example

```
Console(config)#ip http port 769  
Console(config)#
```

Related Commands

ip http server (section 7.7.16 on page 650)

7.7.16 **ip http server**

This command allows this device to be monitored or configured from a browser. Use the **no** form to disable this function.

Syntax

```
[no] ip http server
```

Default Setting

Enabled

Command Mode

Global Configuration

Example

```
Console(config)#ip http server
Console(config)#
```

Related Commands

ip http port (section 7.7.15 on page 650)

7.7.17**ip http secure-server**

This command enables the secure hypertext transfer protocol (HTTPS) over the Secure Socket Layer (SSL), providing secure access (that is, an encrypted connection) to the ECN330-switch's web interface. Use the **no** form to disable this function.

Syntax

```
[no] ip http secure-server
```

Default Setting

Enabled

Command Mode

Global Configuration

Command Usage

- Both HTTP and HTTPS service can be enabled independently on the ECN330-switch. However, the HTTP and HTTPS servers cannot be configured to use the same UDP port.
- If HTTPS is enabled, it must be indicated in the URL that is specified in the browser: **https://device[:port_number]**
- When HTTPS is started, the connection is established in this way:
 - The client authenticates the server using the server's digital certificate.
 - The client and server negotiate a set of security protocols to use for the connection.
 - The client and server generate session keys for encrypting and decrypting data.
- The client and server establish a secure encrypted connection.

A padlock icon should appear in the status bar for Internet Explorer 5.x and Netscape Navigator 4.x or later versions.

- The following web browsers and operating systems currently support HTTPS:

Table 60 HTTPS System Support

Web Browser	Operating System
Internet Explorer 5.0 or later	Windows 98, Windows NT (with service pack 6a), Windows 2000, Windows XP
Netscape Navigator 6.2 or later	Windows 98, Windows NT (with service pack 6a), Windows 2000, Windows XP, Solaris 2.6

- To specify a secure-site certificate, see "Replacing the Default Secure-site Certificate" on page 134. Also refer to the **copy** command on page 561.

Example

```
Console(config)#ip http secure-server
Console(config)#
```

Related Commands

ip http secure-port (section 7.7.18 on page 653)
copy tftp https-certificate (section 7.5.14 on page 561)

7.7.18 ip http secure-port

This command specifies the UDP port number used for HTTPS connection to the ECN330-switch's web interface. Use the **no** form to restore the default port.

Syntax

ip http secure-port *<port_number>*

no ip http secure-port

port_number – The UDP port used for HTTPS.
 (Range: 1-65535)

Default Setting

443

Command Mode

Global Configuration

Command Usage

- The HTTP and HTTPS servers cannot be configured to use the same port.
- If the HTTPS port number is changed, clients attempting to connect to the HTTPS server must specify the port number in the URL, in this format: **https://device:port_number**

Example

```
Console(config)#ip http secure-port 1000
Console(config)#
```

Related Commands

ip http secure-server (section 7.7.17 on page 651)

Telnet Server Commands

This section describes commands used to configure Telnet management access to the ECN330-switch.

Table 61 Telnet Server Commands

Command	Function	Mode	Page
ip telnet server	Allows the ECN330-switch to be monitored or configured from Telnet; also specifies the port to be used by the Telnet interface	GC	654

7.7.19 ip telnet server

This command allows this device to be monitored or configured from Telnet. It also specifies the TCP port number used by the Telnet interface. Use the **no** form without the **port** keyword to disable this function. Use the **no** form with the **port** keyword to use the default port.

Syntax

ip telnet server **<port port-number>**

no telnet server **<port>**

- **port** - The TCP port number used by the Telnet interface.
- **port-number** - The TCP port to be used by the browser interface. (Range: 1-65535)

Default Setting

Server: Enabled

Server Port: 23

Command Mode

Global Configuration

Example

```
Console(config)#ip telnet server
Console(config)#ip telnet port 123
Console(config)#
```

Secure Shell Commands

This section describes the commands used to configure the SSH server. Note that an SSH client also needs to be installed on the management station to access the ECN330-switch for management using the SSH protocol.

Note: The ECN330-switch supports both SSH Version 1.5 and 2.0 clients.

Table 62 Secure Shell Commands

Command	Function	Mode	Page
ip ssh server	Enables the SSH server on the ECN330-switch	GC	658
ip ssh timeout	Specifies the authentication timeout for the SSH server	GC	659
ip ssh authentication-retries	Specifies the number of retries allowed by a client	GC	660
ip ssh server-key size	Sets the SSH server key size	GC	661

Command	Function	Mode	Page
copy tftp public-key	Copies the user's public key from a TFTP server to the ECN330-switch	PE	561
delete public-key	Deletes the public key for the specified user	PE	662
ip ssh crypto host-key generate	Generates the host key	PE	663
ip ssh crypto zeroize	Clear the host key from RAM	PE	664
ip ssh save host-key	Saves the host key from RAM to flash memory	PE	665
disconnect	Terminates a line connection	PE	582
show ip ssh	Displays the status of the SSH server and the configured values for authentication timeout and retries	PE	666
show ssh	Displays the status of current SSH sessions	PE	666
show public-key	Shows the public key for the specified user or for the host	PE	668
show users	Shows SSH users, including privilege level and public key type	PE	549

Configuration Guidelines

The SSH server on the ECN330-switch supports both password and public key authentication. If password authentication is specified by the SSH client, then the password can be authenticated either locally or through a RADIUS or TACACS+ remote authentication server, as specified by the **authentication login** command on page 637. If public key authentication is specified by the client, then authentication keys must be configured on both the client and the ECN330-switch as described in the following section. Note that regardless of whether public key or password authentication is used, authentication keys still have to be generated on the ECN330-switch and the SSH server enabled.

To use the SSH server, complete these steps:

1. Generate a Host Key Pair – Use the **ip ssh crypto host-key generate** command to create a host public/private key pair.
2. Provide Host Public Key to Clients – Many SSH client programs automatically import the host public key during the initial connection setup with the ECN330-switch. Otherwise, a known hosts file needs to be manually created on the management station and the host public key placed in it. An entry for a public key in the known hosts file would appear similar to the following example:

```
10.1.0.54 1024 35 15684995401867669259333946775054617325313674890836547254
15020245593199868544358361651999923329781766065830956 10825913212890233
76546801726272571413428762941301196195566782 59566410486957427888146206
519417467729848654686157177393901647793559423035774130980227370877945452408397175264635
8058176716709574804776117
```

3. Import Client's Public Key to the ECN330-switch – Use the **copy tftp public-key** command to copy a file containing the public key for all the SSH client's granted management access to the ECN330-switch. (Note that these clients must be configured locally on the ECN330-switch with the **username** command as described on page 633.) The clients are subsequently authenticated using these keys. The current firmware only accepts public key files based on standard UNIX format as shown in the following example for an RSA Version 1 key:

```
1024 35 1341081685609893921040944920155425347631641921872958921143173880
055536161631051775940838686311092912322268285192543746031009371877211996963178136627741
416898513204911720483033925432410163799759237144901193800609025394840848271781943722884
02533115952134861022902978982721353267131629432532818915045306393916643
steve@192.168.1.19
```

4. Set the Optional Parameters – Set other optional parameters, including the authentication timeout, the number of retries, and the server key size.
5. Enable SSH Service – Use the **ip ssh server** command to enable the SSH server on the ECN330-switch.
6. Configure Challenge-Response Authentication – When an SSH client attempts to contact the ECN330-switch, the SSH server uses the host key pair to negotiate a session key and encryption method. Only clients that have a private key corresponding to the public keys stored on the ECN330-switch can gain access. The following exchanges take place during this process:

A The client sends its public key to the ECN330-switch.

- B The ECN330-switch compares the client's public key to those stored in memory.
- C If a match is found, the ECN330-switch uses the public key to encrypt a random sequence of bytes, and sends this string to the client.
- D The client uses its private key to decrypt the bytes, and sends the decrypted bytes back to the ECN330-switch.
- E The ECN330-switch compares the decrypted bytes to the original bytes it sent. If the two sets match, this means that the client's private key corresponds to an authorized public key, and the client is authenticated.

Note: To use SSH with only password authentication, the host public key must still be given to the client, either during initial connection or manually entered into the known host file. However, the client's keys do not need to be configured.

7.7.20

ip ssh server

This command enables the Secure Shell (SSH) server on the ECN330-switch. Use the **no** form to disable this service.

Syntax

```
[no] ip ssh server
```

Default Setting

Disabled

Command Mode

Global Configuration

Command Usage

- The SSH server supports up to four client sessions. The maximum number of client sessions includes both current Telnet sessions and SSH sessions.
- The SSH server uses DSA or RSA for key exchange when the client first establishes a connection with the ECN330-switch, and then negotiates

with the client to select either DES (56-bit) or 3DES (168-bit) for data encryption.

- The DSA and RSA host keys must be generated before enabling the SSH server.

Example

```
Console#ip ssh crypto host-key generate dsa
Console#configure
Console(config)#ip ssh server
Console(config)#
```

Related Commands

ip ssh crypto host-key generate (section 7.7.25 on page 663)
show ssh (section 7.7.29 on page 666)

7.7.21

ip ssh timeout

This command configures the timeout for the SSH server. Use the **no** form to restore the default setting.

Syntax

ip ssh timeout <*seconds*>

no ip ssh timeout

seconds – The timeout for client response during SSH negotiation.
 (Range: 1-120)

Default Setting

10 seconds

Command Mode

Global Configuration

Command Usage

The **timeout** specifies the interval the ECN330-switch will wait for a response from the client during the SSH negotiation phase. Once an SSH session has been established, the timeout for user input is controlled by the **exec-timeout** command for vty sessions.

Example

```
Console(config)#ip ssh timeout 60
Console(config)#
```

Related Commands

exec-timeout (section 7.5.23 on page 575)
show ip ssh (section 7.7.28 on page 666)

7.7.22 ip ssh authentication-retries

This command configures the number of times the SSH server attempts to reauthenticate a user. Use the **no** form to restore the default setting.

Syntax

```
ip ssh authentication-retries <count>  
no ip ssh authentication-retries
```

count – The number of authentication attempts permitted after which the interface is reset. (Range: 1-5)

Default Setting

3

Command Mode

Global Configuration

Example

```
Console(config)#ip ssh authentication-retires 2
Console(config)#
```

Related Commands

show ip ssh (section 7.7.28 on page 666)

7.7.23

ip ssh server-key size

This command sets the SSH server key size. Use the **no** form to restore the default setting.

Syntax

ip ssh server-key size <key-size>

no ip ssh server-key size

key-size – The size of server key. (Range: 512-896 bits)

Default Setting

768 bits

Command Mode

Global Configuration

Command Usage

- The server key is a private key that is never shared outside the ECN330-switch.
- The host key is shared with the SSH client, and is fixed at 1024 bits.

Example

```
Console(config)#ip ssh server-key size 512
Console(config)#
```

7.7.24

delete public-key

This command deletes the specified user's public key.

Syntax

```
delete public-key <username> [dsa | rsa]
```

- **username** – Name of an SSH user. (Range: 1-8 characters)
- **dsa** – DSA public key type.
- **rsa** – RSA public key type.

Default Setting

Deletes both the DSA and RSA key.

Command Mode

Privileged Exec

Example

```
Console#delete public-key admin dsa
Console#
```


7.7.25 **ip ssh crypto host-key generate**

This command generates the host key pair (that is, public and private).

Syntax

```
ip ssh crypto host-key generate [dsa | rsa]
```

- **dsa** – DSA (Version 2) key type.
- **rsa** – RSA (Version 1) key type.

Default Setting

Generates both the DSA and RSA key pairs.

Command Mode

Privileged Exec

Command Usage

- This command stores the host key pair in memory (that is, RAM). Use the **ip ssh save host-key** command to save the host key pair to flash memory.
- Some SSH client programs automatically add the public key to the known hosts file as part of the configuration process. Otherwise, a known hosts file must be manually created and the host public key placed in it.
- The SSH server uses this host key to negotiate a session key and encryption method with the client trying to connect to it.

Example

```
Console#ip ssh crypto host-key generate dsa  
Console#
```

Related Commands

ip ssh crypto zeroize (section 7.7.26 on page 664)
ip ssh save host-key (section 7.7.27 on page 665)

7.7.26 ip ssh crypto zeroize

This command clears the host key from memory (that is RAM).

Syntax

```
ip ssh crypto zeroize [dsa | rsa]
```

- **dsa** – DSA key type.
- **rsa** – RSA key type.

Default Setting

Clears both the DSA and RSA key.

Command Mode

Privileged Exec

Command Usage

- This command clears the host key from volatile memory (RAM). Use the **no ip ssh save host-key** command to clear the host key from flash memory.
- The SSH server must be disabled before this command can be executed.

Example

```
Console#ip ssh crypto zeroize dsa
Console#
```

Related Commands

ip ssh crypto host-key generate (section 7.7.25 on page 663)
ip ssh save host-key (section 7.7.27 on page 665)
no ip ssh server (section 7.7.20 on page 658)

7.7.27 ip ssh save host-key

This command saves the host key from RAM to flash memory.

Syntax

```
ip ssh save host-key [dsa | rsa]
```

- **dsa** – DSA key type.
- **rsa** – RSA key type.

Default Setting

Saves both the DSA and RSA key.

Command Mode

Privileged Exec

Example

```
Console#ip ssh save host-key dsa
Console#
```

Related Commands

ip ssh crypto host-key generate (section 7.7.25 on page 663)

7.7.28 **show ip ssh**

This command displays the connection settings used when authenticating client access to the Secure Shell (SSH) server.

Command Mode

Privileged Exec

Example

```
Console#show ip ssh
SSH Enabled - version 1.99
Negotiation timeout: 120 secs; Authentication retries: 3
Server key size: 768 bits
Console#
```

7.7.29 **show ssh**

This command displays the current Secure Shell (SSH) server connections.

Command Mode

Privileged Exec

Example

```
Console#show ssh
Connection Version State      Username Encryption
0           2.0    Session-Started    admin    ctos aes128-cbc-hmac-md5
                               stoc aes128-cbc-hmac-md5
Console#
```

Table 63 *show ssh - Display Description*

Field	Description
Session	The session number. (Range: 0-3)
Version	The Secure Shell version number.
State	The authentication negotiation state. (Values: Negotiation-Started, Authentication-Started, Session-Started)
Username	The user name of the client.
Encryption	The encryption method is automatically negotiated between the client and server. Options for SSHv1.5 include: DES, 3DES Options for SSHv2.0 can include different algorithms for the client-to-server (ctos) and server-to-client (stoc): aes128-cbc-hmac-sha1 aes192-cbc-hmac-sha1 aes256-cbc-hmac-sha1 3des-cbc-hmac-sha1 blowfish-cbc-hmac-sha1 aes128-cbc-hmac-md5 aes192-cbc-hmac-md5 aes256-cbc-hmac-md5 3des-cbc-hmac-md5 blowfish-cbc-hmac-md5

Field	Description
Encryption (continued)	Terminology: DES – Data Encryption Standard (56-bit key) 3DES – Triple-DES (Uses three iterations of DES, 112-bit key) aes – Advanced Encryption Standard (160 or 224-bit key) blowfish – Blowfish (32-448 bit key) cbc – cypher-block chaining sha1 – Secure Hash Algorithm 1 (160-bit hashes) md5 – Message Digest algorithm number 5 (128-bit hashes)

7.7.30 **show public-key**

This command shows the public key for the specified user or for the host.

Syntax

```
show public-key [user [username] | host]
```

username – Name of an SSH user. (Range: 1-8 characters)

Default Setting

Shows all public keys.

Command Mode

Privileged Exec

Command Usage

- If no parameters are entered, all keys are displayed. If the user keyword is entered, but no user name is specified, then the public keys for all users are displayed.

- When an RSA key is displayed, the first field indicates the size of the host key (for example, 1024), the second field is the encoded public exponent (for example, 35), and the last string is the encoded modulus. When a DSA key is displayed, the first field indicates that the encryption method used by SSH is based on the Digital Signature Standard (DSS), and the last string is the encoded modulus.

Example

```

Console#show public-key host
Host:
RSA:
1024 35
  156849954018676692593339467750546173253136748908365472541502024559319986854435836
  165199992332978176606583095861082591321289023376546801726272571413428762941301196
  195566782595664104869574278881462065194174677298486546861571773939016477935594230
  357741309802273708779454524083971752646358058176716709574804776117
DSA:
ssh-dss AAAB3NzaC1kc3MAAACBAPWKZTPbsRIB8ydEXcxM3dyV/yrDbKStIlnzD/Dg0h2HxcYV44sXZ2JXh
amLK6P8bvuiyacWbUW/a4PAtp1KMSdqsKeh3hKoA3vRRSy1N2XFfAKx15fwFfvJlPdOkFgzLGMinvSNYQ
wiQXbKTBH0Z4mUZpE85PWxDZMacNBPjBrRAAAAFQChb4vsdfQGNIjwbvwrNLaQ77isiwAAAIEAsy5YWDc
99ebYHNRj5kh47wY4i8cZvH+/p9cnrfwFTMU01VFDly3IR 2G395NLy5Qd7ZDxfA9mCOFT/yyEfbobMJZ
i8oGCstSNOxrZZVnMqWrTYfdrKX7YKBw/Kjw6Bm iFq70+jAhf1Dg45loAc27s6TLdtnylwRq/ow2eTCD
5nekAAACBAJ8rMccXTxHLFAczWS7EjOyDbsloBfPuSAb4oAsyjKXKVYNLQkTLZfcFRu41bS2KV5LAWecs
igF/+DjKGWtPNIQqabKgYCw2o/dVzX4Gg+yqdTlYmGA7fHGm8ARGeiG4ssFKy4Z6DmYPXFum1Yg0fhLwu
HpOSKdxT3kk475S7w0W
Console#

```

Port Security Commands

These commands can be used to enable port security on a port. When using port security, the ECN330-switch stops learning new MAC addresses on the specified port when it has reached a configured maximum number. Only incoming traffic with source addresses already stored in the dynamic or static address table for this port will be authorized to access the network. The port will drop any incoming frames with a source MAC address that is unknown or has been previously learned from another port. If a device with an unauthorized MAC address attempts to use the ECN330 port, the intrusion will be detected and the ECN330-switch can automatically take action by disabling the port and sending a trap message.

Table 64 Port Security Commands

Command	Function	Mode	Page
port security	Configures a secure port	IC	670
mac-address-table static	Maps a static address to a port in a VLAN	GC	787
show mac-address-table	Displays entries in the bridge-forwarding database	PE	789
mac-learning	Enables MAC address learning on the selected port	IC	672
show mac-learning	Displays the status of MAC address learning status for all ports.	PE	673

7.7.31 port security

This command enables or configures port security. Use the **no** form without any keywords to disable port security. Use the **no** form with the appropriate keyword to restore the default settings for a response to security violation or for the maximum number of allowed addresses.

Syntax

```
port security [action {shutdown | trap | trap-and-
               shutdown} | max-mac-count <address-count>]
```

```
no port security [action | max-mac-count]
```

- **action** - Response to take when port security is violated.
 - **shutdown** - Disable port only.
 - **trap** - Issue SNMP trap message only.
 - **trap-and-shutdown** - Issue SNMP trap message and disable port.
- **max-mac-count**
 - **address-count** - The maximum number of MAC addresses that can be learned on a port. (Range: 0 - 1024, where 0 means disabled)

Default Setting

Status: Disabled
Action: None
Maximum Addresses: 0

Command Mode

Interface Configuration (Ethernet)

Command Usage

- If port security is enabled, the ECN330-switch stops learning new MAC addresses on the specified port when it has reached a configured maximum number. Only incoming traffic with source addresses already stored in the dynamic or static address table will be accepted.
- First use the **port security max-mac-count** command to set the number of addresses, and then use the **port security** command to enable security on the port.
- Use the **no port security max-mac-count** command to disable port security and reset the maximum number of addresses to the default.
- Secure addresses can also be manually added with the **mac-address-table static** command.
- A secure port has the following restrictions:
 - Cannot use port monitoring.
 - Cannot be a multi-VLAN port.
 - Cannot be connected to a network interconnection device.
 - Cannot be a trunk port.
- If a port is disabled due to a security violation, it must be manually re-enabled using the **no shutdown** command.

Example

The following example enables port security for port 5, and sets the response to a security violation to issue a trap message:

```
Console(config)#interface ethernet 1/5  
Console(config-if)#port security action trap
```

Related Commands

shutdown (section 7.9.8 on page 746)
mac-address-table static (section 7.14.1 on page 787)
show mac-address-table (section 7.14.3 on page 789)

7.7.32 mac-learning

This command enables MAC address learning on the selected port. Use the **no** form to disable MAC address learning.

Syntax

[no] mac-learning

Default Setting

Enabled

Command Mode

Interface Configuration (Ethernet)

Command Usage

- The **port security** command (section 7.7.31 on page 670) stops the ECN330-switch from learning new MAC addresses on the specified port when it has reached a configured maximum number. Only incoming traffic with source addresses already stored in the dynamic or static address table will be accepted.

- The **no mac-learning** command immediately stops the ECN330-switch from learning new MAC addresses on the specified port, and all MAC addresses that have learned on this port will be flushed.
- The **mac-learning** commands cannot be used if any of the following conditions exist:
 - Security has been enabled on a port with the **port security** command (section 7.7.31 on page 670).
 - 802.1x Port Authentication has been globally enabled on the ECN330-switch with the **dot1x system-auth-control** command (section 7.7.34 on page 675).
 - GVRP has been enabled on a port with the **switchport gvrp** command (section 7.17.1.3 on page 844).

Example

The following example disables MAC address learning for port 2:

```
Console(config)#interface ethernet 1/2
Console(config-if)#no mac-learning
Console(config-if)#
```

Related Commands

show mac-learning (section 7.7.33 on page 673)
show interfaces status (section 7.9.11 on page 749)

7.7.33

show mac-learning

This command displays the status of MAC address learning status for all ports..

Command Mode

Privileged Exec

Example

```

Console#show mac-learning
Port    MAC-Learng-stuatus
1/1      Enable
1/2      Disable
1/3      Enable
1/4      Enable
1/5      Enable
.
.
.

```

802.1X Port Authentication

The ECN330-switch supports IEEE 802.1X (dot1x) port-based access control that prevents unauthorized access to the network by requiring users to first submit credentials for authentication. Client authentication is controlled centrally by a RADIUS server using EAP (Extensible Authentication Protocol).

Table 65 802.1X Port Authentication Commands

Command	Function	Mode	Page
dot1x system-auth-control	Enables dot1x globally on the ECN330-switch.	GC	675
dot1x default	Resets all dot1x parameters to their default values.	GC	676
dot1x max-req	Sets the maximum number of times that the ECN330-switch retransmits an EAP request/identity packet to the client before it times out the authentication session	IC	676
dot1x port-control	Sets dot1x mode for a port interface	IC	677
dot1x operation-mode	Allows single or multiple hosts on a port	IC	678

Command	Function	Mode	Page
dot1x re-authenticate	Forces a re-authentication on specific ports	PE	679
dot1x re-authentication	Enables re-authentication for all ports	IC	680
dot1x timeout quiet-period	Sets the time that an ECN330 port waits after the Max Request Count has been exceeded before attempting to acquire a new client	IC	681
dot1x timeout re-authperiod	Sets the time period after which a connected client must be re-authenticated	IC	682
dot1x timeout tx-period	Sets the time period during an authentication session that the ECN330-switch waits before re-transmitting an EAP packet	IC	682
show dot1x	Shows all dot1x related information	PE	683

7.7.34 dot1x system-auth-control

This command enables IEEE 802.1X port authentication globally on the ECN330-switch. Use the **no** form to restore the default.

Syntax

```
[no] dot1x system-auth-control
```

Default Setting

Disabled

Command Mode

Global Configuration

Example

```
Console(config)#dot1x system-auth-control  
Console(config)#
```

7.7.35 dot1x default

This command sets all configurable dot1x global and port settings to their default values.

Command Mode

Global Configuration

Example

```
Console(config)#dot1x default  
Console(config)#
```

7.7.36 dot1x max-req

This command sets the maximum number of times the ECN330 port will retransmit an Extensible Authentication Protocol (EAP) request/identity packet to the client before it times out the authentication session. Use the **no** form to restore the default.

Syntax

```
dot1x max-req <count>
```

```
no dot1x max-req
```

count – The maximum number of requests (Range: 1-10)

Default

2

Command Mode

Interface Configuration

Example

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x max-req 2
Console(config-if)#
```

7.7.37 dot1x port-control

This command sets the dot1x mode on a port interface. Use the **no** form to restore the default.

Syntax

```
dot1x port-control {auto | force-authorized | force-unauthorized}
```

```
no dot1x port-control
```

- **auto** – Requires a dot1x-aware connected client to be authorized by the RADIUS server. Clients that are not dot1x-aware will be denied access.
- **force-authorized** – Configures the port to grant access to all clients, either dot1x-aware or otherwise.
- **force-unauthorized** – Configures the port to deny access to all clients, either dot1x-aware or otherwise.

Default

force-authorized

Command Mode

Interface Configuration

Example

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x port-control auto
Console(config-if)#
```

7.7.38 dot1x operation-mode

This command allows single or multiple hosts (clients) to connect to an 802.1X-authorized port. Use the **no** form with no keywords to restore the default to single host. Use the **no** form with the **multi-host max-count** keywords to restore the default maximum count.

Syntax

```
dot1x operation-mode {single-host | multi-host [max-
count <count>]}
```

```
no dot1x operation-mode [multi-host max-count]
```

- **single-host** – Allows only a single host to connect to this port.
- **multi-host** – Allows multiple host to connect to this port.
- **max-count** – Keyword for the maximum number of hosts.
- **count** – The maximum number of hosts that can connect to a port. (Range: 1-1024; Default: 5)

Default

Single-host

Command Mode

Interface Configuration

Command Usage

- The **max-count** parameter specified by this command is only effective if the dot1x mode is set to **auto** by the **dot1x port-control** command (page 677).

- In “multi-host” mode, only one host connected to a port needs to pass authentication for all other hosts to be granted network access. Similarly, a port can become unauthorized for all hosts if one attached host fails re-authentication or sends an EAPOL logoff message.

Example

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x operation-mode multi-host max-count 10
Console(config-if)#
```

7.7.39

dot1x re-authenticate

This command forces re-authentication on all ports or a specific interface.

Syntax

dot1x re-authenticate [*interface*]

interface

- **ethernet** <*unit*>/<*port*>
 - *unit* - This is device 1.
 - *port* - Physical port number on the ECN330 (Range: 1-28).

Command Mode

Privileged Exec

Command Usage

The re-authentication process verifies the connected client’s user ID and password on the RADIUS server. During re-authentication, the client remains connected the network and the process is handled transparently by the dot1x client software. Only if re-authentication fails is the port blocked. Re-authentication can be used to detect if a new device is plugged into an ECN330 port.

Example

```
Console#dot1x re-authenticate
Console#
```

7.7.40 dot1x re-authentication

This command enables periodic re-authentication for a specified port. Use the **no** form to disable re-authentication.

Syntax

```
[no] dot1x re-authentication
```

Command Mode

Interface Configuration

Command Usage

- The re-authentication process verifies the connected client's user ID and password on the RADIUS server. During re-authentication, the client remains connected the network and the process is handled transparently by the dot1x client software. Only if re-authentication fails is the port blocked. Re-authentication can be used to detect if a new device is plugged into an ECN330 port.
- The connected client is re-authenticated after the interval specified by the **dot1x timeout re-authperiod** command. The default is 3600 seconds.

Example

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x re-authentication
Console(config-if)#
```

Related Commands

`dot1x timeout re-authperiod` (section 7.7.42 on page 682)

7.7.41 `dot1x timeout quiet-period`

This command sets the time that an ECN330 port waits after the Max Request Count has been exceeded before attempting to acquire a new client. Use the **no** form of this command to reset the default.

Syntax

`dot1x timeout quiet-period <seconds>`

`no dot1x timeout quiet-period`

seconds - The number of seconds. (Range: 1-65535)

Default

60 seconds

Command Mode

Interface Configuration

Example

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x timeout quiet-period 350
Console(config-if)#
```

7.7.42 dot1x timeout re-authperiod

This command sets the time period after which a connected client must be re-authenticated. Use the **no** form of this command to reset the default.

Syntax

```
dot1x timeout re-authperiod <seconds>
```

```
no dot1x timeout re-authperiod
```

seconds - The number of seconds. (Range: 1-65535)

Default

3600 seconds

Command Mode

Interface Configuration

Example

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x timeout re-authperiod 300
Console(config-if)#
```

7.7.43 dot1x timeout tx-period

This command sets the time that an interface on the ECN330 waits during an authentication session before re-transmitting an EAP packet. Use the **no** form to reset to the default value.

Syntax

```
dot1x timeout tx-period <seconds>
```

```
no dot1x timeout tx-period
```

seconds - The number of seconds. (Range: 1-65535)

Default

30 seconds

Command Mode

Interface Configuration

Example

```
Console(config)#interface eth 1/2
Console(config-if)#dot1x timeout tx-period 300
Console(config-if)#
```

7.7.44**show dot1x**

This command shows general port authentication related settings on the ECN330-switch or a specific interface.

Syntax

```
show dot1x [statistics] [interface <interface>]
```

- **statistics** - Displays dot1x status for each port.
- **interface**
 - **ethernet <unit>/<port>**
 - **unit** - This is device 1.
 - **port** - Physical port number on the ECN330 (Range: 1-28).

Command Mode

Privileged Exec

Command Usage

This command displays the following information:

- **Global 802.1X Parameters** – Shows whether or not 802.1X port authentication is globally enabled on the ECN330-switch.
- **802.1X Port Summary** – Displays the current status of port access control parameters for each interface, including the following items:
 - **Status** – Administrative state for port access control. Displays `enabled` if the dot1x port mode is set to **Auto** or **Force-Unauthorized**. Displays `disabled` if the port mode is set to **Force-Authorized**.
 - **Operation Mode** – Allows single or multiple hosts, see section 7.7.38 on page 678).
 - **Mode** – Dot1x port control mode (configurable, see section 7.7.37 on page 677).
 - **Authorized** – Authorization status (displays `yes` or `n/a`—not authorized).
- **802.1X Port Details** – Displays detailed port access control settings and the current status for each interface as described in the preceding pages. The following items are displayed:
 - **reauth-enabled** – Re-authentication (configurable, see section 7.7.40 on page 680)
 - **reauth-period** – Re-authentication period (configurable, see section 7.7.42 on page 682)
 - **quiet-period** – The timeout before a port attempts to acquire a new client (configurable, see section 7.7.41 on page 681)
 - **tx-period** – The timeout before the ECN330-switch retransmits an EAP packet (configurable, see section 7.7.43 on page 682)
 - **supplicant-timeout** – Supplicant timeout (a fixed setting).
 - **server-timeout** – Server timeout (a fixed setting).
 - **reauth-max** – Maximum number of reauthentication attempts (a fixed setting).
 - **max-req** – The maximum number of retransmitted EAP request packets (configurable, see section 7.7.36 on page 676)

- `Status` – Current authorization status of the client (authorized or unauthorized).
- `Operation Mode` – Shows if single or multiple hosts (clients) can connect to an 802.1X-authorized port.
- `Max Count` – The maximum number of hosts allowed to access this port (configurable, see section 7.7.38 on page 678).
- `Port-control` – Shows the current configured status of the port-control mode as Auto, ForceUnauthorized, or ForceAuthorized (configurable, see section 7.7.37 on page 677).
- `Supplicant` – The MAC address of a currently authorized client. Zeros are displayed if no client is authorized.
- `Current Identifier` – The integer (0-255) used by the Authenticator to identify the current authentication session; that is, the current unit among multiple hosts..
- `Authenticator State Machine`
 - `State` – Current status of authentication (including initialize, disconnected, connecting, authenticating, authenticated, aborting, held, force_authorized, force_unauthorized).
 - `Reauth Count` – The current number of times the connecting state has been re-entered.
- `Backend State Machine (current status)`
 - `State` – Current state (including request, response, success, fail, timeout, idle, initialize).
 - `Request Count` – Number of EAP Request packets sent to the Supplicant without receiving a response.
 - `Identifier(Server)` – Identifier carried in the most recent EAP Success, Failure or Request packet received from the Authentication Server.
- `Reauthentication State Machine (current status)`
 - `State` – Current state (including initialize, reauthenticate).

Example

```

Console#show dot1x
Global 802.1X Parameters
  system-auth-control: enable

802.1X Port Summary

Port Name   Status      Operation Mode   Mode              Authorized
1/1         disabled   Single-Host      ForceAuthorized   n/a
1/2         disabled   Single-Host      ForceAuthorized   n/a
.
1/27        disabled   Single-Host      ForceAuthorized   yes
1/28        enabled    Single-Host      Auto              yes

802.1X Port Details

802.1X is disabled on port 1
.
802.1X is enabled on port 28
reauth-enabled:      Enable
reauth-period:       3600
quiet-period:        60
tx-period:           30
supplicant-timeout:  30
server-timeout:      10
reauth-max:          2
max-req:             2
Status               Authorized
Operation mode       Multi-Host
Max count            5
Port-control         Auto
Supplicant            00-e0-29-94-34-65
Current Identifier    3

Authenticator State Machine
State                Authenticated
Reauth Count         0

Backend State Machine
State                Idle
Request Count        0
Identifier(Server)    2

Reauthentication State Machine
State                Initialize

Console#

```


IP Filter Commands

This section describes commands used to configure IP management access to the ECN330-switch.

Table 66 IP Filter Commands

Command	Function	Mode	Page
management	Configures IP addresses that are allowed management access	GC	687
show management	Displays the client IP addresses that are allowed management access to the ECN330-switch	PE	689

7.7.45 management

This command specifies the client IP addresses that are allowed management access to the ECN330-switch through various protocols. Use the **no** form to restore the default setting.

Syntax

```
[no] management {all-client | http-client | snmp-client  
| telnet-client} <start-address> [end-address]
```

- **all-client** - Adds IP address(es) to the SNMP, web and Telnet groups.
- **http-client** - Adds IP address(es) to the web group.
- **snmp-client** - Adds IP address(es) to the SNMP group.
- **telnet-client** - Adds IP address(es) to the Telnet group.
- **start-address** - A single IP address, or the starting address of a range.
- **end-address** - The end address of a range.

Default Setting

All addresses

Command Mode

Global Configuration

Command Usage

- If anyone tries to access a management interface on the ECN330-switch from an invalid address, the ECN330-switch will reject the connection, enter an event message in the system log, and send a trap message to the trap manager.
- IP address can be configured for SNMP, web and Telnet access respectively. Each of these groups can include up to five different sets of addresses, either individual addresses or address ranges.
- When entering addresses for the same group (that is, SNMP, web or Telnet), the ECN330-switch will not accept overlapping address ranges. When entering addresses for different groups, the ECN330-switch will accept overlapping address ranges.
- An individual address cannot be deleted from a specified range. The entire range must be deleted and the addresses reentered.
- An address range can be deleted just by specifying the start address, or by specifying both the start address and end address.

Example

This example restricts management access to the indicated addresses.

```
Console(config)#management all-client 192.168.1.19
Console(config)#management all-client 192.168.1.25 192.168.1.30
Console#
```

7.7.46 **show management**

This command displays the client IP addresses that are allowed management access to the ECN330-switch through various protocols.

Syntax

```
show management {all-client | http-client | snmp-client  
| telnet-client}
```

- **all-client** - Adds IP address(es) to the SNMP, web and Telnet groups.
- **http-client** - Adds IP address(es) to the web group.
- **snmp-client** - Adds IP address(es) to the SNMP group.
- **telnet-client** - Adds IP address(es) to the Telnet group.

Command Mode

Privileged Exec

Example

```
Console#show management all-client
Management Ip Filter
  Http-Client:
    Start ip address      End ip address
    -----
    1. 192.168.1.19        192.168.1.19
    2. 192.168.1.25        192.168.1.30

  Snmp-Client:
    Start ip address      End ip address
    -----
    1. 192.168.1.19        192.168.1.19
    2. 192.168.1.25        192.168.1.30

  Telnet-Client:
    Start ip address      End ip address
    -----
    1. 192.168.1.19        192.168.1.19
    2. 192.168.1.25        192.168.1.30

Console#
```

7.8 Access Control List Commands

Access Control Lists (ACL) provide packet filtering for IP frames (based on address, protocol, Layer 4 protocol port number or TCP control code), any frames (based on MAC address or Ethernet type), or for frame types within a specified VLAN. To filter packets, first create an access list, add the required rules, specify a mask to modify the precedence in which the rules are checked, and then bind the list to a specific port. This section describes the Access Control List commands.

Table 67 Access Control List Commands

Command Groups	Function	Page
IP ACLs	Configures ACLs based on IP addresses, TCP/UDP port number, protocol type, and TCP control code	691
MAC ACLs	Configures ACLs based on hardware addresses, packet format, and Ethernet type	707
VLAN ACLs	Configures ACLs for filtering VLAN ingress traffic based on the frame types matched within specific IP or MAC ACLs	719
ACL Information	Displays ACLs and associated rules; shows ACLs assigned to each port	733

IP ACLs

The commands in this section configure ACLs based on IP addresses, TCP/UDP port number, protocol type, and TCP control code. To configure IP ACLs, first create an access list containing the required permit or deny rules, set a precedence mask to control the filter sequence, and then bind the access list to one or more ports

Table 68 IP ACL Commands

Command	Function	Mode	Page
access-list ip	Creates an IP ACL and enters configuration mode for standard or extended IP ACLs	GC	692
permit, deny	Filters packets matching a specified source IP address	STD-ACL	693
permit, deny	Filters packets meeting the specified criteria, including source and destination IP address, TCP/UDP port number, protocol type, and TCP control code	EXT-ACL	694
show ip access-list	Displays the rules for configured IP ACLs	PE	697
access-list ip mask-precedence	Changes to the mode for configuring access control masks	GC	698
mask	Sets a precedence mask for the ACL rules	IP-Mask	699
show access-list ip mask-precedence	Shows the ingress or egress rule masks for IP ACLs	PE	705
ip access-group	Adds a port to an IP ACL	IC	705
show ip access-group	Shows port assignments for IP ACLs	PE	705

7.8.1 access-list ip

This command adds an IP access list and enters configuration mode for standard or extended IP ACLs. Use the **no** form to remove the specified ACL.

Syntax

```
[no] access-list ip {standard | extended} <acl_name>
```

- **standard** – Specifies an ACL that filters packets based on the source IP address.
- **extended** – Specifies an ACL that filters packets based on the source or destination IP address, and other more specific criteria.
- **acl_name** – Name of the ACL. (Maximum length: 16 characters)

Default Setting

None

Command Mode

Global Configuration

Command Usage

- An egress ACL must contain all deny rules.
- When a new ACL is created or configuration mode entered for an existing ACL, use the **permit** or **deny** command to add new rules to the bottom of the list. To create an ACL, add at least one rule to the list.
- To remove a rule, use the **no permit** or **no deny** command followed by the exact text of a previously configured rule.
- An ACL can contain up to 32 rules.

Example

```
Console(config)#access-list ip standard david
Console(config-std-acl)#
```

Related Commands

permit, deny (section 7.8.2 on page 693)
ip access-group (section 7.8.8 on page 705)
show ip access-list (section 7.8.4 on page 697)

7.8.2 permit, deny (Standard ACL)

This command adds a rule to a Standard IP ACL. The rule sets a filter condition for packets emanating from the specified source. Use the **no** form to remove a rule.

Syntax

```
[no] {permit | deny} {any | <source> <bitmask> | host
    <source>}
```

- **any** – Any source IP address.
- **source** – Source IP address.
- **bitmask** – Decimal number representing the address bits to match.
- **host** – Keyword followed by a specific IP address.

Default Setting

None

Command Mode

Standard ACL

Command Usage

- New rules are appended to the end of the list.
- Address bitmasks are similar to a subnet mask, containing four integers from 0 to 255, each separated by a period. The binary mask uses 1 bits to indicate “match” and 0 bits to indicate “ignore.” The bitmask is bitwise ANDed with the specified source IP address, and then compared with

the address for each IP packet entering the port(s) to which this ACL has been assigned.

Example

This example configures one permit rule for the specific address 10.1.1.21 and another rule for the address range 168.92.16.x – 168.92.31.x using a bitmask.

```
Console(config-std-acl)#permit host 10.1.1.21
Console(config-std-acl)#permit 168.92.16.0 255.255.240.0
Console(config-std-acl)#
```

Related Commands

access-list ip (section 7.8.1 on page 692)

7.8.3 permit, deny (Extended ACL)

This command adds a rule to an Extended IP ACL. The rule sets a filter condition for packets with specific source or destination IP addresses, protocol types, source or destination protocol ports, or TCP control codes. Use the **no** form to remove a rule.

Syntax

```
[no] {permit | deny} [<protocol-number> | udp]
    {any | <source> <address-bitmask> | host <source>}
    {any | <destination> <address-bitmask> |
    host <destination>} [precedence <precedence>]
    [tos <tos>] [dscp <dscp>] [source-port <sport>
    [bitmask]] [destination-port <dport> [port-
    bitmask]]
```

```
[no] {permit | deny} tcp
    {any | <source> <address-bitmask> | host <source>}
    {any | <destination> <address-bitmask> |
    host <destination>} [precedence <precedence>]
    [tos <tos>] [dscp <dscp>] [source-port <sport>
    [bitmask]] [destination-port <dport> [port-
    bitmask]] [control-flag <control-flags> <flag-
    bitmask>]
```


- *protocol-number* – A specific protocol number. (Range: 0-255)
- *source* – Source IP address.
- *destination* – Destination IP address.
- *address-bitmask* – Decimal number representing the address bits to match.
- *host* – Keyword followed by a specific IP address.
- *precedence* – IP precedence level. (Range: 0-7)
- *tos* – Type of Service level. (Range: 0-15)
- *dscp* – DSCP priority level. (Range: 0-63)
- *sport* – Protocol source port number. Includes TCP, UDP or other protocol types. (Range: 0-65535)
- *dport* – Protocol destination port number. Includes TCP, UDP or other protocol types. (Range: 0-65535)
- *port-bitmask* – Decimal number representing the port bits to match. (Range: 0-65535)
- *control-flags* – Decimal number (representing a bit string) that specifies flag bits in byte 14 of the TCP header. (Range: 0-63)
- *flag-bitmask* – Decimal number representing the code bits to match.

Default Setting

None

Command Mode

Extended ACL

Command Usage

- All new rules are appended to the end of the list.
- Address bitmasks are similar to a subnet mask, containing four integers from 0 to 255, each separated by a period. The binary mask uses 1 bits to indicate “match” and 0 bits to indicate “ignore.” The bitmask is bitwise

ANDed with the specified source IP address, and then compared with the address for each IP packet entering the port(s) to which this ACL has been assigned.

- Both Precedence and ToS can be specified in the same rule. However, if DSCP is used, then neither Precedence nor ToS can be specified.
- The control-code bitmask is a decimal number (representing an equivalent bit mask) that is applied to the control code. Enter a decimal number, where the equivalent binary bit “1” means to match a bit and “0” means to ignore a bit. The following bits may be specified:
 - 1 (fin) – Finish
 - 2 (syn) – Synchronize
 - 4 (rst) – Reset
 - 8 (psh) – Push
 - 16 (ack) – Acknowledgement
 - 32 (urg) – Urgent pointer

For example, use the code value and mask below to catch packets with the following flags set:

- SYN flag valid, use “control-code 2 2”
- Both SYN and ACK valid, use “control-code 18 18”
- SYN valid and ACK invalid, use “control-code 2 18”

Example

This example accepts any incoming packets if the source address is within subnet 10.7.1.x. For example, if the rule is matched; that is, the rule (10.7.1.0 & 255.255.255.0) equals the masked address (10.7.1.2 & 255.255.255.0), the packet passes through.

```
Console(config-ext-acl)#permit 10.7.1.1 255.255.255.0 any
Console(config-ext-acl)#
```

This allows TCP packets from class C addresses 192.168.1.0 to any destination address when set for destination TCP port 80 (that is, HTTP).

```
Console(config-ext-acl)#permit 192.168.1.0 255.255.255.0 any
destination-port 80
Console(config-ext-acl)#
```

This permits all TCP packets from class C addresses 192.168.1.0 with the TCP control code set to “SYN.”

```
Console(config-ext-acl)#permit tcp 192.168.1.0 255.255.255.0 any
control-flag 2 2
Console(config-ext-acl)#
```

Related Commands

access-list ip (section 7.8.1 on page 692)

7.8.4 show ip access-list

This command displays the rules for configured IP ACLs.

Syntax

- ```
show ip access-list {standard | extended} [acl_name]
```
- **standard** – Specifies a standard IP ACL.
  - **extended** – Specifies an extended IP ACL.
  - **acl\_name** – Name of the ACL. (Maximum length: 16 characters)

### Command Mode

Privileged Exec

## Example

```
Console#show ip access-list standard
IP standard access-list david:
 permit host 10.1.1.21
 permit 168.92.0.0 255.255.15.0
Console#
```

## Related Commands

**permit**, **deny** (section 7.8.2 on page 693)  
**ip access-group** (section 7.8.8 on page 705)

### 7.8.5 access-list ip mask-precedence

This command changes to the IP Mask mode used to configure access control masks. Use the **no** form to delete the mask table.

#### Syntax

```
[no] access-list ip mask-precedence {in | out}
```

- **in** – Ingress mask for ingress ACLs.
- **out** – Egress mask for egress ACLs.

#### Default Setting

Default system mask: Filter inbound packets according to specified IP ACLs.

#### Command Mode

Global Configuration

#### Command Usage

- A mask can only be used by all ingress ACLs or all egress ACLs.
- The precedence of the ACL rules applied to a packet is not determined by order of the rules, but instead by the order of the masks; that is, the

first mask that matches a rule will determine the rule that is applied to a packet.

- A mask must be configured for an ACL rule it is bound to a port or the queue or frame priorities associated with the rule set.

### Example

```
Console(config)#access-list ip mask-precedence in
Console(config-ip-mask-acl)#
```

### Related Commands

- mask** (IP ACL) (section 7.8.6 on page 699)
- ip access-group** (section 7.8.8 on page 705)

## 7.8.6

### mask (IP ACL)

This command defines a mask for IP ACLs. This mask defines the fields to check in the IP header. Use the **no** form to remove a mask.

#### Syntax

```
[no] mask [protocol]
 {any | host | <source-bitmask>}
 {any | host | <destination-bitmask>}
 [precedence] [tos] [dscp]
 [source-port [port-bitmask]]
 [destination-port [port-bitmask]]
 [control-flag [flag-bitmask]]
```

- **protocol** – Check the protocol field.
- **any** – Any address will be matched.
- **host** – The address must be for a host device, not a subnetwork.
- **source-bitmask** – Source address of rule must match this bitmask.
- **destination-bitmask** – Destination address of rule must match this bitmask.

- **precedence** – Check the IP precedence field.
- **tos** – Check the TOS field.
- **dscp** – Check the DSCP field.
- **source-port** – Check the protocol source port field.
- **destination-port** – Check the protocol destination port field.
- **port-bitmask** – Protocol port of rule must match this bitmask.  
(Range: 0-65535)
- **control-flag** – Check the field for control flags.
- **flag-bitmask** – Control flags of rule must match this bitmask.  
(Range: 0-63)

### Default Setting

None

### Command Mode

IP Mask

### Command Usage

- Packets crossing a port are checked against all the rules in the ACL until a match is found. The order in which these packets are checked is determined by the mask, and not the order in which the ACL rules were entered.
- First create the required ACLs and ingress or egress masks before mapping an ACL to an interface.
- If **dscp** is entered, **tos** or **precedence** cannot be entered. Both **tos** and **precedence** can be entered without **dscp**.
- Masks that include an entry for a Layer 4 protocol source port or destination port can only be applied to packets with a header length of exactly five bytes.

## Example

This example creates an IP ingress mask with two rules. Each rule is checked in order of precedence to look for a match in the ACL entries. The first entry matching a mask is applied to the inbound packet.

```
Console(config)#access-list ip mask-precedence in
Console(config-ip-mask-acl)#mask host any
Console(config-ip-mask-acl)#mask 255.255.255.0 any
Console(config-ip-mask-acl)#
```

This shows that the entries in the mask override the precedence in which the rules are entered into the ACL. In the following example, packets with the source address 10.1.1.1 are dropped because the “deny 10.1.1.1 255.255.255.255” rule has the higher precedence according the “mask host any” entry.

```
Console(config)#access-list ip standard A2
Console(config-std-acl)#permit 10.1.1.0 255.255.255.0
Console(config-std-acl)#deny 10.1.1.1 255.255.255.255
Console(config-std-acl)#exit
Console(config)#access-list ip mask-precedence in
Console(config-ip-mask-acl)#mask host any
Console(config-ip-mask-acl)#mask 255.255.255.0 any
Console(config-ip-mask-acl)#
```

This shows how to create a standard ACL with an ingress mask to deny access to the IP host 171.69.198.102, and permit access to any others.

```
Console(config)#access-list ip standard A2
Console(config-std-acl)#permit any
Console(config-std-acl)#deny host 171.69.198.102
Console(config-std-acl)#end
Console#show access-list
IP standard access-list A2:
 deny host 171.69.198.102
 permit any
Console#configure
Console(config)#access-list ip mask-precedence in
Console(config-ip-mask-acl)#mask host any
Console(config-ip-mask-acl)#exit
Console(config)#interface ethernet 1/1
Console(config-if)#ip access-group A2 in
Console(config-if)#end
Console#show access-list
IP standard access-list A2:
 deny host 171.69.198.102
 permit any
Console#
```



This shows how to create an extended ACL with an egress mask to drop packets leaving network 171.69.198.0 when the Layer 4 source port is 23.

```
Console(config)#access-list ip extended A3
Console(config-ext-acl)#deny host 171.69.198.5 any
Console(config-ext-acl)#deny 171.69.198.0 255.255.255.0 any source-
 port 23
Console(config-ext-acl)#end
Console#show access-list
IP extended access-list A3:
 deny host 171.69.198.5 any
 deny 171.69.198.0 255.255.255.0 any source-port 23
Console#config
Console(config)#access-list ip mask-precedence out
Console(config-ip-mask-acl)#mask 255.255.255.0 any source-port
Console(config-ip-mask-acl)#exit
Console(config)#interface ethernet 1/15
Console(config-if)#ip access-group A3 out
Console(config-if)#end
Console#show access-list
IP extended access-list A3:
 deny 171.69.198.0 255.255.255.0 any source-port 23
 deny host 171.69.198.5 any
IP egress mask ACL:
 mask 255.255.255.0 any source-port
Console#
```

This is a more comprehensive example. It denies any TCP packets in which the SYN bit is ON, and permits all other packets. It then sets the ingress mask to check the deny rule first, and finally binds port 1 to this ACL. Note that once the ACL is bound to an interface (that is, the ACL is active), the order in which the rules are displayed is determined by the associated mask.

```
Switch(config)#access-list ip extended 6
Switch(config-ext-acl)#permit any any
Switch(config-ext-acl)#deny tcp any any control-flag 2 2
Switch(config-ext-acl)#end
Console#show access-list
IP extended access-list A6:
 permit any any
 deny tcp any any control-flag 2 2
Console#configure
Switch(config)#access-list ip mask-precedence in
Switch(config-ip-mask-acl)#mask protocol any any control-flag 2
Switch(config-ip-mask-acl)#end
Console#sh access-list
IP extended access-list A6:
 permit any any
 deny tcp any any control-flag 2 2
IP ingress mask ACL:
 mask protocol any any control-flag 2
Console#configure
Console(config)#interface ethernet 1/1
Console(config-if)#ip access-group A6 in
Console(config-if)#end
Console#show access-list
IP extended access-list A6:
 deny tcp any any control-flag 2 2
 permit any any
IP ingress mask ACL:
 mask protocol any any control-flag 2
Console#
```

### 7.8.7 **show access-list ip mask-precedence**

This command shows the ingress or egress rule masks for IP ACLs.

#### **Syntax**

```
show access-list ip mask-precedence [in | out]
```

- **in** – Ingress mask precedence for ingress ACLs.
- **out** – Egress mask precedence for egress ACLs.

#### **Command Mode**

Privileged Exec

#### **Example**

```
Console#show access-list ip mask-precedence
IP ingress mask ACL:
 mask host any
 mask 255.255.255.0 any
Console#
```

#### **Related Commands**

**mask** (IP ACL) (section 7.8.6 on page 699)

### 7.8.8 **ip access-group**

This command binds a port to an IP ACL. Use the **no** form to remove the port.

#### **Syntax**

```
[no] ip access-group <acl_name> {in | out}
```

- **acl\_name** – Name of the ACL. (Maximum length: 16 characters)
- **in** – Indicates that this list applies to ingress packets.
- **out** – Indicates that this list applies to egress packets.

### Default Setting

None

### Command Mode

Interface Configuration (Ethernet)

### Command Usage

- A port can only be bound to one ACL.
- If a port is already bound to an ACL and it is bound to a different ACL, the ECN330-switch will replace the old binding with the new one.
- A mask must be configured for an ACL rule before it can be bound to a port.

### Example

```
Console(config)#int eth 1/2
Console(config-if)#ip access-group standard david in
Console(config-if)#
```

### Related Commands

**show ip access-list** (section 7.8.4 on page 697)

## 7.8.9 show ip access-group

This command shows the ports assigned to IP ACLs.

### Command Mode

Privileged Exec

## Example

```
Console#show ip access-group
Interface ethernet 1/2
 IP standard access-list david
Console#
```

## Related Commands

**ip access-group** (section 7.8.8 on page 705)

## MAC ACLs

The commands in this section configure ACLs based on hardware addresses, packet format, and Ethernet type. To configure MAC ACLs, first create an access list containing the required permit or deny rules, set a precedence mask to control the filter sequence, and then bind the access list to one or more ports

*Table 69 MAC ACL Commands*

| Command                                     | Function                                                                                              | Mode     | Page |
|---------------------------------------------|-------------------------------------------------------------------------------------------------------|----------|------|
| <b>access-list mac</b>                      | Creates a MAC ACL and enters configuration mode                                                       | GC       | 708  |
| <b>permit, deny</b>                         | Filters packets matching a specified source and destination address, packet format, and Ethernet type | MAC-ACL  | 709  |
| <b>show mac access-list</b>                 | Displays the rules for configured MAC ACLs                                                            | PE       | 711  |
| <b>access-list mac mask-precedence</b>      | Changes to the mode for configuring access control masks                                              | GC       | 712  |
| <b>mask</b>                                 | Sets a precedence mask for the ACL rules                                                              | MAC-Mask | 713  |
| <b>show access-list mac mask-precedence</b> | Shows the ingress or egress rule masks for MAC ACLs                                                   | PE       | 716  |

| Command                      | Function                            | Mode | Page |
|------------------------------|-------------------------------------|------|------|
| <b>mac access-group</b>      | Adds a port to a MAC ACL            | IC   | 717  |
| <b>show mac access-group</b> | Shows port assignments for MAC ACLs | PE   | 718  |

### 7.8.10 access-list mac

This command adds a MAC access list and enters MAC ACL configuration mode. Use the **no** form to remove the specified ACL.

#### Syntax

```
[no] access-list mac <acl_name>
```

*acl\_name* – Name of the ACL. (Maximum length: 16 characters)

#### Default Setting

None

#### Command Mode

Global Configuration

#### Command Usage

- An egress ACL must contain all deny rules.
- When a new ACL is created or configuration mode for an existing ACL entered, use the **permit** or **deny** command to add new rules to the bottom of the list. To create an ACL, add at least one rule to the list.
- To remove a rule, use the **no permit** or **no deny** command followed by the exact text of a previously configured rule.
- An ACL can contain up to 32 rules.

## Example

```
Console(config)#access-list mac jerry
Console(config-mac-acl)#
```

## Related Commands

**permit, deny** (section 7.8.11 on page 709)  
**mac access-group** (section 7.8.16 on page 717)  
**show mac access-list** (section 7.8.12 on page 711)

### 7.8.11 permit, deny (MAC ACL)

This command adds a rule to a MAC ACL. The rule filters packets matching a specified MAC source or destination address (that is, physical layer address), or Ethernet protocol type. Use the **no** form to remove a rule.

#### Syntax

```
[no] {permit | deny}
 {any | host <source> | <source> <address-bitmask>}
 {any | host <destination> | <destination> <address-
 bitmask>}
 [vid <vid> <vid-bitmask>] [ethertype <protocol>
 [protocol-bitmask]]
```

**Note:** The default is for Ethernet II packets.

```
[no] {permit | deny} tagged-eth2
 {any | host <source> | <source> <address-bitmask>}
 {any | host <destination> | <destination> <address-
 bitmask>}
 [vid <vid> <vid-bitmask>] [ethertype <protocol>
 [protocol-bitmask]]

[no] {permit | deny} untagged-eth2
 {any | host <source> | <source> <address-bitmask>}
 {any | host <destination> | <destination> <address-
 bitmask>}
 [ethertype <protocol> [protocol-bitmask]]
```

```
[no] {permit | deny} tagged-802.3
 {any | host <source> | <source> <address-bitmask>}
 {any | host <destination> | <destination> <address-
 bitmask>}
 [vid <vid> <vid-bitmask>]
```

```
[no] {permit | deny} untagged-802.3
 {any | host <source> | <source> <address-bitmask>}
 {any | host <destination> | <destination> <address-
 bitmask>}
```

- **tagged-eth2** – Tagged Ethernet II packets.
- **untagged-eth2** – Untagged Ethernet II packets.
- **tagged-802.3** – Tagged Ethernet 802.3 packets.
- **untagged-802.3** – Untagged Ethernet 802.3 packets.
- **any** – Any MAC source or destination address.
- **host** – A specific MAC address.
- **source** – Source MAC address.
- **destination** – Destination MAC address range with bitmask.
- **address-bitmask** – Bitmask for MAC address (in hexadecimal format).
- **vid** – VLAN ID. (Range: 1-4094)
- **vid-bitmask** – VLAN bitmask. (Range: 1-4094)
- **protocol** – A specific Ethernet protocol number. (Range: 600-fff hex.)
- **protocol-bitmask** – Protocol bitmask. (Range: 600-fff hex.)

**Note:** For all bitmasks, “1” means care and “0” means ignore.

### Default Setting

None

### Command Mode

MAC ACL



## Command Usage

- New rules are added to the end of the list.
- The **ethertype** option can only be used to filter Ethernet II formatted packets.
- A detailed listing of Ethernet protocol types can be found in RFC 1060. A few of the more common types include the following:
  - 0800 - IP
  - 0806 - ARP
  - 8137 - IPX

## Example

This rule permits packets from any source MAC address to the destination address 00-e0-29-94-34-de where the Ethernet type is 0800.

```
Console(config-mac-acl)#permit any host 00-e0-29-94-34-de ethertype
0800
Console(config-mac-acl)#
```

## Related Commands

**access-list mac** (section 7.8.10 on page 708)

## 7.8.12 show mac access-list

This command displays the rules for configured MAC ACLs.

### Syntax

```
show mac access-list [acl_name]
```

*acl\_name* – Name of the ACL. (Maximum length: 16 characters)

### Command Mode

Privileged Exec

## Example

```
Console#show mac access-list
MAC access-list jerry:
 permit any 00-e0-29-94-34-de ethertype 0800
Console#
```

## Related Commands

**permit**, **deny** (section 7.8.11 on page 709)  
**mac access-group** (section 7.8.16 on page 717)

### 7.8.13 access-list mac mask-precedence

This command changes to MAC Mask mode used to configure access control masks. Use the **no** form to delete the mask table.

#### Syntax

```
[no] access-list ip mask-precedence {in | out}
```

- **in** – Ingress mask for ingress ACLs.
- **out** – Egress mask for egress ACLs.

#### Default Setting

Default system mask: Filter inbound packets according to specified MAC ACLs.

#### Command Mode

Global Configuration

#### Command Usage

- A mask must be configured for an ACL rule before it can be bound to a port or the queue or frame priorities associated with the rule set.
- A mask can only be used by all ingress ACLs or all egress ACLs.

- The precedence of the ACL rules applied to a packet is not determined by order of the rules, but instead by the order of the masks; that is, the first mask that matches a rule will determine the rule that is applied to a packet.

### Example

```
Console(config)#access-list mac mask-precedence in
Console(config-mac-mask-acl)#
```

### Related Commands

- mask** (MAC ACL) (section 7.8.14 on page 713)
- mac access-group** (section 7.8.16 on page 717)

## 7.8.14

### mask (MAC ACL)

This command defines a mask for MAC ACLs. This mask defines the fields to check in the packet header. Use the **no** form to remove a mask.

### Syntax

```
[no] mask [pktformat]
 {any | host | <source-bitmask>}
 {any | host | <destination-bitmask>}
 [vid [vid-bitmask]] [ethertype [ethertype-bitmask]]
```

- **pktformat** – Check the packet format field. (If this keyword must be used in the mask, the packet format must be specified in ACL rule to match.)
- **any** – Any address will be matched.
- **host** – The address must be for a single node.
- **source-bitmask** – Source address of rule must match this bitmask.
- **destination-bitmask** – Destination address of rule must match this bitmask.
- **vid** – Check the VLAN ID field.

- *vid-bitmask* – VLAN ID of rule must match this bitmask.
- **ethertype** – Check the Ethernet type field.
- *ethertype-bitmask* – Ethernet type of rule must match this bitmask.

### Default Setting

None

### Command Mode

MAC Mask

### Command Usage

- Up to seven masks can be assigned to an ingress or egress ACL.
- Packets crossing a port are checked against all the rules in the ACL until a match is found. The order in which these packets are checked is determined by the mask, and not the order in which the ACL rules were entered.
- First create the required ACLs and inbound or outbound masks before mapping an ACL to an interface.

## Example

This example shows how to create an Ingress MAC ACL and bind it to a port. Notice that the order of the rules have been changed by the mask.

```
Console(config)#access-list mac M4
Console(config-mac-acl)#permit any any
Console(config-mac-acl)#deny tagged-eth2 00-11-11-11-11-11 ff-ff-ff-
 ff-ff-ff any vid 3
Console(config-mac-acl)#end
Console#show access-list
MAC access-list M4:
 permit any any
 deny tagged-eth2 host 00-11-11-11-11-11 any vid 3
Console(config)#access-list mac mask-precedence in
Console(config-mac-mask-acl)#mask pktformat ff-ff-ff-ff-ff-ff any
 vid
Console(config-mac-mask-acl)#exit
Console(config)#interface ethernet 1/12
Console(config-if)#mac access-group M4 in
Console(config-if)#end
Console#show access-list
MAC access-list M4:
 deny tagged-eth2 host 00-11-11-11-11-11 any vid 3
 permit any any
MAC ingress mask ACL:
 mask pktformat host any vid
Console#
```

This example creates an Egress MAC ACL.

```

Console(config)#access-list mac M5
Console(config-mac-acl)#deny tagged-802.3 host 00-11-11-11-11-11 any
Console(config-mac-acl)#deny tagged-eth2 00-11-11-11-11-11 ff-ff-ff-
 ff-ff-ff any vid 3 ethertype 0806
Console(config-mac-acl)#end
Console#show access-list
MAC access-list M5:
 deny tagged-802.3 host 00-11-11-11-11-11 any
 deny tagged-eth2 host 00-11-11-11-11-11 any vid 3 ethertype 0806
Console(config)#access-list mac mask-precedence out
Console(config-mac-mask-acl)#mask pktformat ff-ff-ff-ff-ff-ff any
 vid
Console(config-mac-mask-acl)#exit
Console(config)#interface ethernet 1/5
Console(config-if)#mac access-group M5 out
Console(config-if)#end
Console#show access-list
MAC access-list M5:
 deny tagged-eth2 host 00-11-11-11-11-11 any vid 3 ethertype 0806
 deny tagged-802.3 host 00-11-11-11-11-11 any
MAC ingress mask ACL:
 mask pktformat host any vid ethertype
Console#

```

### 7.8.15 **show access-list mac mask-precedence**

This command shows the ingress or egress rule masks for MAC ACLs.

#### **Syntax**

```
show access-list mac mask-precedence [in | out]
```

- **in** – Ingress mask precedence for ingress ACLs.
- **out** – Egress mask precedence for egress ACLs.

#### **Command Mode**

Privileged Exec

## Example

```
Console#show access-list mac mask-precedence
MAC egress mask ACL:
 mask pktformat host any vid ethertype
Console#
```

## Related Commands

**mask** (MAC ACL) (section 7.8.14 on page 713)

## 7.8.16

### mac access-group

This command binds a port to a MAC ACL. Use the **no** form to remove the port.

#### Syntax

```
[no] mac access-group <acl_name> {in | out}
```

- *acl\_name* – Name of the ACL. (Maximum length: 16 characters)
- **in** – Indicates that this list applies to ingress packets.
- **out** – Indicates that this list applies to egress packets.

#### Default Setting

None

#### Command Mode

Interface Configuration (Ethernet)

#### Command Usage

- A port can only be bound to one ACL.
- If a port is already bound to an ACL and it is then bound to a different ACL, the ECN330-switch will replace the old binding with the new one.
- A mask must be configured for an ACL rule before it can be bound to a port.

## Example

```
Console(config)#interface ethernet 1/2
Console(config-if)#mac access-group jerry in
Console(config-if)#
```

## Related Commands

**show mac access-list** (section 7.8.12 on page 711)

## 7.8.17 show mac access-group

This command shows the ports assigned to MAC ACLs.

## Command Mode

Privileged Exec

## Example

```
Console#show mac access-group
Interface ethernet 1/5
 MAC access-list M5 out
Console#
```

## Related Commands

**mac access-group** (section 7.8.16 on page 717)



## VLAN ACLs

The commands in this section configure VLAN access maps based on existing IP or MAC ACLs. To configure VLAN ACLs, first create an access map, specify the IP or MAC ACLs to use, set the action to drop or forward packets that match an ACL rule, set a precedence mask to control the filter sequence, and then bind the access map to one or more VLANs.

*Table 70 VLAN ACL Commands*

| Command                                 | Function                                                                            | Mode       | Page |
|-----------------------------------------|-------------------------------------------------------------------------------------|------------|------|
| <b>vlan access-map</b>                  | Creates a VLAN ACL and enters access map configuration mode                         | GC         | 720  |
| <b>match</b>                            | Sets the match criteria for one IP ACL or one MAC ACL                               | Access Map | 722  |
| <b>action</b>                           | Sets the action for a VLAN access map entry to forward or drop matching packets     | Access Map | 723  |
| <b>show vlan filter access-map</b>      | Displays information about a particular VLAN access map or for all VLAN access maps | PE         | 725  |
| <b>access-list mask-precedence vlan</b> | Changes to the mode for configuring VLAN access control masks                       | GC         | 726  |
| <b>mask</b>                             | Sets a precedence mask for the IP ACL rules                                         | IP-Mask    | 727  |
| <b>mask</b>                             | Sets a precedence mask for the MAC ACL rules                                        | MAC-Mask   | 729  |
| <b>vlan filter</b>                      | Binds a VLAN access map to one or more VLANs                                        | GC         | 731  |
| <b>show vlan filter</b>                 | Displays information about the specified VLAN access map or all VLAN access maps    | PE         | 732  |

*Configuration Guidelines*

Follow these steps to create and bind an access map to an interface:

1. Create the required VLAN access map using the **vlan access-map** command (section 7.8.18 on page 720), entering access-map configuration mode.
2. Use the **match** command (section 7.8.19 on page 722) to specify the IP or MAC ACL to specify the match criteria for the access map.
3. Use **action** command (section 7.8.20 on page 723) to drop or forward traffic when a match is found.
4. Select a VLAN IP or VLAN MAC ACL mask using the **access-list ip/mac mask-precedence** command (section 7.8.22 on page 726).
5. Configure the required mask with the IP **mask** command (section 7.8.23 on page 727) or MAC **mask** command (section 7.8.24 on page 729).
6. Map the VLAN access map to an interface using the **vlan filter** command (section 7.8.25 on page 731).

## 7.8.18 **vlan access-map**

This command creates a VLAN ACL for packet filtering and enters access map configuration mode. Use the **no** form to remove the specified ACL.

### Syntax

```
[no] vlan access-map <access-map_name>
```

*access-map\_name* – Name of the access map.  
(Maximum length: 16 characters)

### Default Setting

None

### Command Mode

Global Configuration

## Command Usage

- Use this command to create a new access-map or modify an existing access-map.
- Specify one **match** and **action** command for each access map. If an access map is created without specifying either a **match** or **action** command, or only specifying the **match** command without an **action** command, the system default will assume a forward action for this entry.
- Use the **vlan filter** command to bind a VLAN map to one or more VLANs.

## Example

The following command creates a VLAN access-map called vlanMAP1, sets the match criteria for an IP ACL called acl1, and sets the action for forward matching packets.

```
Console(config)#vlan access-map vlanMAP1
Console(config-access-map)#match ip address ipACL1
Console(config-access-map)#action forward
Console(config-access-map)#
```

## Related Commands

**match** (section 7.8.19 on page 722)  
**action** (section 7.8.20 on page 723)  
**show vlan access map** (section 7.8.21 on page 725)  
**vlan filter** (section 7.8.25 on page 731)

## 7.8.19 match

This command sets the match criteria for one or more IP or MAC access lists. Use the **no** form to remove the match parameters.

### Syntax

```
match {ip address <acl-name> | mac address <acl-name>}
```

- **ip address** – Configures the access map to match packets against an IP address access list.
- **mac address** – Configures the access map to match packets against a MAC address access list.
- **acl-name** – Name of access list against which to match packets.

### Default Setting

No match parameters are set

### Command Mode

Access Map Configuration

### Command Usage

- Use the **match** command to specify match criteria for the VLAN map. If the packets match, they will be forwarded or dropped, depending on the specified action.
- If more than one **match** command is entered for same access-map entry, all of the **match** commands share the same **action** command.
- If the action is drop matching packets, first define the access map, including configuring any access control list (ACL) names used in the match clauses before binding the map to a VLAN, or all packets could be dropped.

## Example

The following command creates a VLAN access-map called vlanMAP1, sets the match criteria for an IP ACL called ipACL1 and a MAC ACL called macACL1, sets the action for forward matching packets, and then binds the VLAN ACL to VLANs 2 and 3.

```
Console(config)#vlan access-map vlanMAP1
Console(config-access-map)#match ip address ipACL1
Console(config-access-map)#match mac address macACL1
Console(config-access-map)#action forward
Console(config-access-map)#exit
Console(config)#vlan filter vlanMAP1 vlan-lists 2-3
Console(config)#
```

## Related Commands

**vlan access-map** (section 7.8.18 on page 720)  
**action** (section 7.8.20 on page 723)  
**show vlan access map** (section 7.8.21 on page 725)  
**vlan filter** (section 7.8.25 on page 731)

## 7.8.20

### action

This command sets the action for a VLAN access map entry to forward or drop matching packets for a VLAN access map entry. Use the **no** form to restore the default setting.

#### Syntax

**action {drop | forward}**

- **drop** – Drops the packet when the specified conditions are matched.
- **forward** – Forwards the packet when the specified conditions are matched.

#### Default Setting

Forward matching packets

## Command Mode

### Access Map Configuration

## Command Usage

- For each VLAN access-map entry, use only one **action** command to specify whether to drop or forward matching packets. If more than one **action** command is entered, only the later one is used.
- If an access map is created without specifying a **match** or **action** command, or only specifying the **match** command without an **action** command, the system default will assume a forward action for this entry.

## Example

The following command creates a VLAN access-map called vlanMAP1, sets the match criteria for an IP ACL called ipACL1, sets the action for forward matching packets, and then binds the VLAN ACL to VLANs 2 and 3.

```
Console(config)#vlan access-map vlanMAP1
Console(config-access-map)#match ip address ipACL1
Console(config-access-map)#action forward
Console(config-access-map)#exit
Console(config)#vlan filter vlanMAP1 vlan-lists 2-3
Console(config)#
```

## Related Commands

**vlan access-map** (section 7.8.18 on page 720)  
**match** (section 7.8.19 on page 722)  
**show vlan access map** (section 7.8.21 on page 725)  
**vlan filter** (section 7.8.25 on page 731)

## 7.8.21 **show vlan filter access-map**

This command shows information about a specified VLAN access map or information for all VLAN access maps.

### **Command Mode**

Privileged Exec

### **Command Usage**

Use the **show ip access-list** or **show ip mac access-list** command to display the ACLs used by the access map.

### **Example**

```
Console#show vlan filter access-map vlanMAP1
VLAN Access-map: vlanMAP1
 Applied VLAN Lists: 10
 Match IP ACL: ipACL1
 Match MAC ACL: macACL1
 Action: forward
Console#
```

### **Related Commands**

**vlan access-map** (section 7.8.18 on page 720)  
**match** (section 7.8.19 on page 722)  
**action** (section 7.8.20 on page 723)

## 7.8.22 **access-list mask-precedence vlan**

This command changes to the mode for configuring VLAN access control masks. Use the **no** form to delete the mask table.

### **Syntax**

```
[no] access-list {ip | mac} mask-precedence vlan
```

- **ip** – Defines IP address mask precedence.
- **mac** – Define MAC address mask precedence.

### **Default Setting**

None

### **Command Mode**

Global Configuration

### **Command Usage**

- First create the required mask before binding ACL rules to an interface with the **vlan filter** command. Otherwise, any attempt to bind the VLAN access map to an interface will fail.
- If conflicting rules are created, the ECN330-switch will use the mask priority to determine which rule to apply.
- When an ACL port binding is removed, the ECN330-switch removes the mask settings from ASIC but keeps this information in RAM. When creating a VLAN mask, the ECN330-switch first checks whether there are enough available masks based on the current mask information stored in RAM. If there are not enough available masks, the ECN330-switch responds with an error such as "There are 4 user masks available, 3 used for port ACL, 1 used for VLAN ACL, no mask available now." If this kind of message appears, remove a port ACL mask by using the "**no access-list ip/mac mask-precedence**" command. Enough masks should then be made available to create a VLAN ACL.



## Example

```
Console(config)#access-list ip mask-precedence vlan
Console(config-ip-mask-acl)#
```

## Related Commands

**vlan access-map** (section 7.8.18 on page 720)  
**mask** (IP Mask) (section 7.8.23 on page 727)  
**mask** (MAC Mask) (section 7.8.24 on page 729)

### 7.8.23

#### mask (IP Mask)

This command sets a precedence mask for packet filtering used in IP ACL rules. This mask defines the fields to check in the IP header. Use the **no** form to remove a mask.

#### Syntax

```
[no] mask [protocol]
 {any | host | <source-bitmask>}
 {any | host | <destination-bitmask>}
 [precedence] [tos] [dscp]
 [source-port [port-bitmask]]
 [destination-port [port-bitmask]]
 [control-flag [flag-bitmask]]
```

- **protocol** – Check the protocol field.
- **any** – Any address will be matched.
- **host** – The address must be for a host device, not a subnetwork.
- **source-bitmask** – Source address of rule must match this bitmask.
- **destination-bitmask** – Destination address of rule must match this bitmask.
- **precedence** – Check the IP precedence field.
- **tos** – Check the TOS field.
- **dscp** – Check the DSCP field.

- **source-port** – Check the protocol source port field.
- **destination-port** – Check the protocol destination port field.
- **port-bitmask** – Protocol port of rule must match this bitmask.  
(Range: 0-65535)
- **control-flag** – Check the field for control flags.
- **flag-bitmask** – Control flags of rule must match this bitmask.  
(Range: 0-63)

### Default Setting

None

### Command Mode

IP Mask

### Command Usage

- Packets crossing a port are checked against all the rules in the ACL until a match is found. The order in which these packets are checked is determined by the mask, not just the order in which the ACL rules were entered.
- If **dscp** is entered, **tos** or **precedence** cannot be entered. Both **tos** and **precedence** can be entered without **dscp**.
- Masks that include an entry for a Layer 4 protocol source port or destination port can only be applied to packets with a header length of exactly five bytes.
- The VLAN ID field is not specified in the IP or MAC mask commands used for VLAN ACLs. The ECN330-switch automatically appends the VID field for these masks when the VLAN ACL is bound to an interface.

## Example

The following example creates a mask that checks the protocol field in the IP header, ignores the source and destination IP addresses, then checks the destination port.

```
Console(config-ip-mask-acl)#mask protocol any any destination-port 80
Console(config-ip-mask-acl)#
```

The following example creates a mask that checks the protocol field in the IP header, ignores the source and destination IP addresses, then checks the destination port, and both the syn and ack bits in the control flag.

```
Console(config-ip-mask-acl)#mask protocol any any destination-port 80
control-flag 18
Console(config-ip-mask-acl)#
```

## Related Commands

**vlan access-map** (section 7.8.18 on page 720)

**access-list mask-precedence vlan** (section 7.8.22 on page 726)

## 7.8.24

### mask (MAC Mask)

This command sets a precedence mask for packet filtering used in MAC ACL rules. This mask defines the fields to check in the packet header. Use the **no** form to remove a mask.

## Syntax

```
[no] mask [pktformat]
 {any | host | <source-bitmask>}
 {any | host | <destination-bitmask>}
 [ethertype [ethertype-bitmask]]
```

- **pktformat** – Check the packet format field. (If this keyword must be used in the mask, the packet format must be specified in ACL rule to match.)
- **any** – Any address will be matched.

- **host** – The address must be for a single node.
- **source-bitmask** – Source address of rule must match this bitmask.
- **destination-bitmask** – Destination address of rule must match this bitmask.
- **ethertype** – Check the Ethernet type field.
- **ethertype-bitmask** – Ethernet type of rule must match this bitmask.

### Default Setting

None

### Command Mode

MAC Mask

### Command Usage

- Packets crossing a port are checked against all the rules in the ACL until a match is found. The order in which these packets are checked is determined by the mask, not just the order in which the ACL rules were entered.
- The VLAN ID field is not specified in the IP or MAC mask commands used for VLAN ACLs. The ECN330-switch automatically appends the VID field for these masks when the VLAN ACL is bound to an interface.

### Example

The following example creates a mask that checks packet format, ignores the source MAC address, checks the destination MAC address in MAC header, and checks the Ethernet type field if the packet type is Ethernet II.

```
Console(config-mac-mask-acl)#mask pktformat any host ethertype
Console(config-mac-mask-acl)#
```

## Related Commands

**vlan access-map** (section 7.8.18 on page 720)

**access-list mask-precedence vlan** (section 7.8.22 on page 726)

## 7.8.25

### vlan filter

This command binds a VLAN access map to one or more VLANs. Use the **no** form to remove the map.

#### Syntax

```
[no] vlan filter <access-map_name> vlan-list <list>
```

- *access-map\_name* – Name of the VLAN map entry.  
(Maximum length: 16 characters)
- *list* – A list of one or more VLANs. (Range: 1-4094)

#### Default Setting

None

#### Command Mode

Global Configuration

#### Command Usage

- A mask must be configured for any access map before it can be bound to a VLAN.
- Only one VLAN access map can be bound to a VLAN. If more than one access map is bound to the same VLAN, the later one will be rejected.
- The VLAN access map must be bound to one or more VLANs before it takes effect. When specifying a list of VLANs, use a dash “-” or comma “,” to list consecutive or non-consecutive VLANs. Do not include any spaces in the list. For example, “1-4,5,10-11” indicates VLAN 1 to 4, VLAN 5 and VLAN 10 to 11.

- When an IP or MAC access list is bound to a port interface, and a VLAN map is subsequently bound to a VLAN containing that port, the priority is determined by the mask applied to the corresponding rules.

### Example

The following example binds vlanMAP1 to VLAN 1 and 3 to 4.

```
Console(config)#vlan filter vlanMAP1 vlan-lists 1,3-4
Console(config)#
```

### Related Commands

**vlan access-map** (section 7.8.18 on page 720)

**show vlan access-map** (section 7.8.21 on page 725)

## 7.8.26

### show vlan filter

This command displays information about the specified VLAN access map or all VLAN access maps.

### Syntax

```
show vlan filter {access-map <access-map_name> |
 vlan <vlan-id>}
```

- *access-map\_name* – Name of the VLAN map entry. (Maximum length: 16 characters)
- *vlan-id* – VLAN identifier. (Range: 1-4094)

### Command Mode

Privileged Exec

### Command Usage

- Entering **show vlan filter access-map** followed by a specific map name only displays filter information for the specified access map.

- Entering **show vlan filter vlan** followed by a specified vlan only displays filter information about the specified VLAN.

### Example

```

Console#show vlan filter access-map vlanMAP1
VLAN Access-map: vlanMAP1
 Applied VLAN Lists: 1, 2
 Match IP ACL: ipACL1
 Match MAC ACL: macACL1
 Action: forward
Console#show vlan filter vlan 1
VLAN ID: 1
Access-map: vlanMAP1
 Match IP VLANACL: ipACL1
 Match MAC VLANACL: macACL1
 Action: forward
Console#

```

### Related Commands

**vlan access-map** (section 7.8.18 on page 720)

**show vlan filter access-map** (section 7.8.21 on page 725)

**vlan filter** (section 7.8.25 on page 731)

## ACL Information

This section describes commands used to display ACL information.

*Table 71 ACL Information Commands*

| Command                            | Function                                                                            | Mode | Page |
|------------------------------------|-------------------------------------------------------------------------------------|------|------|
| <b>show access-list</b>            | Show all ACLs and associated rules                                                  | PE   | 734  |
| <b>show access-group</b>           | Shows the ACLs assigned to each port                                                | PE   | 735  |
| <b>show vlan filter</b>            | Displays information about the specified VLAN access map or all VLAN access maps    | PE   | 732  |
| <b>show vlan filter access-map</b> | Displays information about a particular VLAN access map or for all VLAN access maps | PE   | 725  |

## 7.8.27 **show access-list**

This command shows all ACLs and associated rules, as well as all the user-defined masks.

### **Command Mode**

Privileged Exec

### **Command Usage**

Once the ACL is bound to an interface (that is, the ACL is active), the order in which the rules are displayed is determined by the associated mask.

### **Example**

```
Console#show access-list
IP standard access-list david:
 permit host 10.1.1.21
 permit 168.92.0.0 255.255.15.0
IP extended access-list bob:
 permit 10.7.1.1 255.255.255.0 any
 permit 192.168.1.0 255.255.255.0 any destination-port 80 80
 permit 192.168.1.0 255.255.255.0 any protocol tcp control-code 2 2
MAC access-list jerry:
 permit any host 00-30-29-94-34-de ethertype 800 800
IP extended access-list A6:
 deny tcp any any control-flag 2 2
 permit any any
IP ingress mask ACL:
 mask protocol any any control-flag 2
Console#
```



## 7.8.28 **show access-group**

This command shows the port assignments of ACLs.

### **Command Mode**

Privileged Executive

### **Example**

```
Console#show access-group
Interface ethernet 1/2
 IP standard access-list david
 MAC access-list jerry
Console#
```

## 7.9 Interface Commands

These commands are used to display or set communication parameters for an Ethernet port, aggregated link, or VLAN.

Table 72 Interface Commands

| Command                                         | Function                                                                                        | Mode      | Page |
|-------------------------------------------------|-------------------------------------------------------------------------------------------------|-----------|------|
| <b>interface</b>                                | Configures an interface type and enters interface configuration mode                            | GC        | 737  |
| <b>description</b>                              | Adds a description to an interface configuration                                                | IC        | 738  |
| <b>speed-duplex</b>                             | Configures the speed and duplex operation of a given interface when autonegotiation is disabled | IC        | 739  |
| <b>negotiation</b>                              | Enables autonegotiation of a given interface                                                    | IC        | 740  |
| <b>capabilities</b>                             | Advertises the capabilities of a given interface for use in autonegotiation                     | IC        | 741  |
| <b>flowcontrol</b>                              | Enables flow control on a given interface                                                       | IC        | 743  |
| <b>media-type</b>                               | Force port type selected for combination ports                                                  | IC        | 745  |
| <b>shutdown</b>                                 | Disables an interface                                                                           | IC        | 746  |
| <b>switchport<br/>broadcast<br/>packet-rate</b> | Configures broadcast storm control                                                              | IC        | 747  |
| <b>clear<br/>counters</b>                       | Clears the statistics on a given interface                                                      | PE        | 748  |
| <b>show<br/>interfaces<br/>status</b>           | Displays status for the specified interface                                                     | NE,<br>PE | 749  |

| Command                                   | Function                                                           | Mode      | Page |
|-------------------------------------------|--------------------------------------------------------------------|-----------|------|
| <b>show<br/>interfaces<br/>counters</b>   | Displays statistics for the specified interfaces                   | NE,<br>PE | 751  |
| <b>show<br/>interfaces<br/>switchport</b> | Displays the administrative and operational status of an interface | NE,<br>PE | 753  |

### 7.9.1 interface

This command configures an interface type and enter interface configuration mode. Use the **no** form to remove a trunk.

#### Syntax

```
interface <interface>
```

```
no interface port-channel <channel-id>
```

```
interface
```

- **ethernet** <unit>/<port>
  - *unit* - This is device 1.
  - *port* - Physical port number on the ECN330 (Range: 1-28).
- **port-channel** <channel-id> - The assigned number of an aggregated link (Range: 1-13)
- **vlan** <vlan-id> (Range: 1-4094)

#### Default Setting

None

#### Command Mode

Global Configuration

## Example

To specify port 4, enter the following command:

```
Console(config)#interface ethernet 1/4
Console(config-if)#
```

## 7.9.2

### description

This command adds a description to an interface. Use the **no** form to remove the description.

#### Syntax

**description** *<string>*

**no description**

*string* - A comment or description that identifies what is attached to this interface. (Range: 1-64 characters)

#### Default Setting

None

#### Command Mode

Interface Configuration (Ethernet, Port Channel)

## Example

The following example adds a description to port 4.

```
Console(config)#interface ethernet 1/4
Console(config-if)#description RD-SW#3
Console(config-if)#
```

### 7.9.3 speed-duplex

This command configures the speed and duplex mode of a given interface when autonegotiation is disabled. Use the **no** form to restore the default.

#### Syntax

```
speed-duplex {1000full | 100full | 100half | 10full | 10half}
```

```
no speed-duplex
```

- **1000full** - Forces 1000 Mbps full-duplex operation
- **100full** - Forces 100 Mbps full-duplex operation
- **100half** - Forces 100 Mbps half-duplex operation
- **10full** - Forces 10 Mbps full-duplex operation
- **10half** - Forces 10 Mbps half-duplex operation

#### Default Setting

- Auto-negotiation is enabled by default.
- Auto-negotiation cannot be disabled for Gigabit Ethernet ports, which only operate at 1000full (1 Gbps full-duplex).
- When auto-negotiation is disabled for Fast Ethernet ports, the default speed-duplex setting is: 100full (100 Mbps full-duplex).

#### Command Mode

Interface Configuration (Ethernet, Port Channel)

#### Command Usage

- The 1000BASE-T standard does not support forced mode. Auto-negotiation must always be used to establish a connection over any 1000BASE-T port or trunk.
- To force operation to the speed and duplex mode specified in a **speed-duplex** command for Fast Ethernet ports, use the **no negotiation** command to disable auto-negotiation on the selected interface.

- When using the **negotiation** command to enable auto-negotiation, the optimal settings will be determined by the **capabilities** command. To set the speed or duplex mode under auto-negotiation, the required mode must be specified in the capabilities list for an interface.

### Example

The following example configures port 5 to 100 Mbps, half-duplex operation.

```
Console(config)#interface ethernet 1/5
Console(config-if)#speed-duplex 100half
Console(config-if)#no negotiation
Console(config-if)#
```

### Related Commands

**negotiation** (section 7.9.4 on page 740)  
**capabilities** (section 7.9.5 on page 741)

## 7.9.4 negotiation

This command enables auto-negotiation for a given interface. Use the **no** form to disable auto-negotiation.

### Syntax

**[no] negotiation**

### Default Setting

Enabled

### Command Mode

Interface Configuration (Ethernet, Port Channel)

### Command Usage

- Auto-negotiation is enabled by default.

- Auto-negotiation cannot be disabled for Gigabit Ethernet ports, which only operate at 1000full (1 Gbps full-duplex).
- When auto-negotiation is enabled, the ECN330-switch negotiates the best settings for a link based on the available capabilities advertised by the interface. An interface's advertised capabilities can be configured using the **capabilities** command. When auto-negotiation is disabled for Fast Ethernet ports, link attributes must be manually specified using the **speed-duplex** and **flowcontrol** commands.
- If auto-negotiation is disabled for Fast Ethernet ports, auto-MDI/MDI-X pin signal configuration will also be disabled for the RJ45 ports.

### Example

The following example configures port 11 to use auto-negotiation.

```
Console(config)#interface ethernet 1/11
Console(config-if)#negotiation
Console(config-if)#
```

### Related Commands

**negotiation** (section 7.9.4 on page 740)  
**speed-duplex** (section 7.9.3 on page 739)

## 7.9.5 capabilities

This command advertises the port capabilities of a given interface during auto-negotiation. Use the **no** form with parameters to remove an advertised capability, or the **no** form without parameters to restore the default values.

### Syntax

```
[no] capabilities {1000full | 100full | 100half | 10full

| 10half | flowcontrol | symmetric}
```

- **1000full** - Supports 1000 Mbps full-duplex operation
- **100full** - Supports 100 Mbps full-duplex operation
- **100half** - Supports 100 Mbps half-duplex operation

- **10full** - Supports 10 Mbps full-duplex operation
- **10half** - Supports 10 Mbps half-duplex operation
- **flowcontrol** - Supports flow control
- **symmetric** (Gigabit only) - When specified, the port transmits and receives pause frames; when not specified, the port will auto-negotiate to determine the sender and receiver for asymmetric pause frames. (The current switch ASIC only supports symmetric pause frames.)

### Default Setting

- 100BASE-TX: 10half, 10full, 100half, 100full
- 1000BASE-T: 10half, 10full, 100half, 100full, 1000full
- 1000BASE-X (SFP): 1000full

### Command Mode

Interface Configuration (Ethernet, Port Channel)

### Command Usage

- Auto-negotiation is enabled by default.
- Auto-negotiation cannot be disabled for Gigabit Ethernet ports, which only operate at 1000full (1 Gbps full-duplex).
- When auto-negotiation is enabled with the **negotiation** command, the ECN330-switch will negotiate the best settings for a link based on the **capabilities** command. When auto-negotiation is disabled for Fast Ethernet ports, the link attributes must be manually specify with the **speed-duplex** and **flowcontrol** commands.



## Example

The following example configures Ethernet port 5 capabilities to 100half, 100full and flow control.

```
Console(config)#interface ethernet 1/5
Console(config-if)#capabilities 100half
Console(config-if)#capabilities 100full
Console(config-if)#capabilities flowcontrol
Console(config-if)#
```

## Related Commands

**negotiation** (section 7.9.4 on page 740)  
**speed-duplex** (section 7.9.3 on page 739)  
**flowcontrol** (section 7.9.6 on page 743)

## 7.9.6

### flowcontrol

This command enables flow control. Use the **no** form to disable flow control.

#### Syntax

```
[no] flowcontrol
```

#### Default Setting

Flow control enabled

#### Command Mode

Interface Configuration (Ethernet, Port Channel)

#### Command Usage

- Flow control can eliminate frame loss by “blocking” traffic from end stations or segments connected directly to the ECN330-switch when its buffers fill. When enabled, back pressure is used for half-duplex operation and IEEE 802.3-2002 (formally IEEE 802.3x) for full-duplex operation.

- To force flow control on or off (with the **flowcontrol** or **no flowcontrol** command), use the **no negotiation** command to disable auto-negotiation on the selected interface. Note that auto-negotiation cannot be disabled for Gigabit Ethernet ports, which only operate at 1000full (1 Gbps full-duplex).
- When using the **negotiation** command to enable auto-negotiation, the optimal settings will be determined by the **capabilities** command. To enable flow control under auto-negotiation, “flowcontrol” must be included in the capabilities list for any port.
- Avoid using flow control on a port connected to a hub unless it is actually required to solve a problem. Otherwise back pressure jamming signals may degrade overall performance for the segment attached to the hub.

### Example

The following example enables flow control on port 5.

```
Console(config)#interface ethernet 1/5
Console(config-if)#flowcontrol
Console(config-if)#no negotiation
Console(config-if)#
```

### Related Commands

**negotiation** (section 7.9.4 on page 740)

**capabilities** (flowcontrol, symmetric) (section 7.9.5 on page 741)

## 7.9.7 media-type

This command forces the port type selected for combination ports 25 - 27. Use the **no** form to restore the default mode.

### Syntax

**media-type** <mode>

**no media-type**

*mode*

- **copper-forced** - Always uses the built-in RJ45 port.
- **sfp-forced** - Always uses the SFP port (even if module not installed).
- **sfp-preferred-auto** - Uses SFP port if both combination types are functioning and the SFP port has a valid link.

### Default Setting

sfp-preferred-auto

### Command Mode

Interface Configuration (Ethernet - Port 25=26)

### Example

This forces the ECN330-switch to use the built-in RJ45 port for the combination port 12.

```
Console(config)#interface ethernet 1/12
Console(config-if)#media-type copper-forced
Console(config-if)#
```

## 7.9.8 shutdown

This command disables an interface. To restart a disabled interface, use the **no** form.

### Syntax

```
[no] shutdown
```

### Default Setting

All interfaces are enabled.

### Command Mode

Interface Configuration (Ethernet, Port Channel)

### Command Usage

This command allows a port to be disabled due to abnormal behavior (for example, excessive collisions), and then reenabled after the problem has been resolved. A port can also be disabled for security reasons.

### Example

The following example disables port 5.

```
Console(config)#interface ethernet 1/5
Console(config-if)#shutdown
Console(config-if)#
```

## 7.9.9 switchport broadcast packet-rate

This command configures broadcast storm control. Use the **no** form to disable broadcast storm control.

### Syntax

```
switchport broadcast packet-rate <rate>
```

```
no switchport broadcast
```

*rate* - Threshold level as a rate; that is, packets per second.  
(Range: 500 - 262143)

### Default Setting

Enabled for all ports  
Packet-rate limit: 500 packets per second

### Command Mode

Interface Configuration (Ethernet)

### Command Usage

- When broadcast traffic exceeds the specified threshold, packets above that threshold are dropped.
- Broadcast control does not effect IP multicast traffic.

### Example

The following shows how to configure broadcast storm control at 600 packets per second on port 5 (sets the broadcast packet rate to 600 on all ports):

```
Console(config)#interface ethernet 1/5
Console(config-if)#switchport broadcast packet-rate 600
Console(config-if)#
```

## 7.9.10 clear counters

This command clears statistics on an interface.

### Syntax

```
clear counters <interface>
```

*interface*

- **ethernet** <unit>/<port>
  - *unit* - This is device 1.
  - *port* - Physical port number on the ECN330 (Range: 1-28).
- **port-channel** <channel-id> - The assigned number of an aggregated link (Range: 1-13)

### Default Setting

None

### Command Mode

Privileged Exec

### Command Usage

Statistics are only initialized for a power reset. This command sets the base value for displayed statistics to zero for the current management session. However, by logging out and back into the management interface, the statistics displayed show the absolute values accumulated since the last power reset.

### Example

The following example clears statistics on Ethernet port 1/1.

```
Console#clear counters ethernet 1/1
Console#
```

## 7.9.11 **show interfaces status**

This command displays the status for an interface.

### **Syntax**

```
show interfaces status [interface]
```

*interface*

- **ethernet** <*unit*>/<*port*>
  - *unit* - This is device 1.
  - *port* - Physical port number on the ECN330 (Range: 1-28).
- **port-channel** <*channel-id*> - The assigned number of an aggregated link (Range: 1-13)
- **vlan** <*vlan-id*> (Range: 1-4094)

### **Default Setting**

Shows the status for all interfaces.

### **Command Mode**

Normal Exec, Privileged Exec

### **Command Usage**

- If no interface is specified, information on all interfaces is displayed.
- For a description of the items displayed by this command, see “Displaying Connection Status” on page 184.

## Example

```
Console#show interfaces status ethernet 1/9
Information of Eth 1/9
Basic information:
 Port Type: 100TX
 Mac address: 00-30-F1-8F-D5-59
Configuration:
 Name:
 Port Admin: Up
 Speed-duplex: Auto
 Capabilities: 10half, 10full, 100half, 100full
 Broadcast Storm: Enabled
 Broadcast Storm Limit: 500 packets/second
 Flow Control: Disabled
 LACP: Disabled
 Port Security: Disabled
 Max MAC Count: 0
 Port Security Action: None
 Port MAC Learning: Enabled
 Media Type: None
Current status:
 Link status: Up
 Port operation status: Up
 Operation speed-duplex: 100full
 Flow control type: None
Console#show interfaces status vlan 1
Information of VLAN 1
 MAC address: 00-30-F1-8F-D5-50
Console#
```



## 7.9.12 **show interfaces counters**

This command displays interface statistics.

### **Syntax**

```
show interfaces counters [interface]
interface
• ethernet <unit>/<port>
 • unit - This is device 1.
 • port - Physical port number on the ECN330 (Range: 1-28).
• port-channel <channel-id> - The assigned number of an
 aggregated link (Range: 1-13)
```

### **Default Setting**

Shows the counters for all interfaces.

### **Command Mode**

Normal Exec, Privileged Exec

### **Command Usage**

- If no interface is specified, information on all interfaces is displayed.
- For a description of the items displayed by this command, see “Showing Port Statistics” on page 213.

## Example

```
Console#show interfaces counters ethernet 1/7
Ethernet 1/7
Iftable stats:
 Octets input: 30658, Octets output: 196550
 Unicast input: 6, Unicast output: 5
 Discard input: 0, Discard output: 0
 Error input: 0, Error output: 0
 Unknown protos input: 0, QLen output: 0
Extended iftable stats:
 Multi-cast input: 0, Multi-cast output: 3064
 Broadcast input: 262, Broadcast output: 1
Ether-like stats:
 Alignment errors: 0, FCS errors: 0
 Single Collision frames: 0, Multiple collision frames: 0
 SQE Test errors: 0, Deferred transmissions: 0
 Late collisions: 0, Excessive collisions: 0
 Internal mac transmit errors: 0, Internal mac receive errors: 0
 Frame too longs: 0, Carrier sense errors: 0
 Symbol errors: 0
RMON stats:
 Drop events: 0, Octets: 227208, Packets: 3338
 Broadcast pkts: 263, Multi-cast pkts: 3064
 Undersize pkts: 0, Oversize pkts: 0
 Fragments: 0, Jabbers: 0
 CRC align errors: 0, Collisions: 0
 Packet size <= 64 octets: 3150, Packet size 65 to 127 octets: 139
 Packet size 128 to 255 octets: 49, Packet size 256 to 511 octets: 0
 Packet size 512 to 1023 octets: 0, Packet size 1024 to 1518 octets: 0
Console#
```

### 7.9.13 **show interfaces switchport**

This command displays the administrative and operational status of the specified interfaces.

#### **Syntax**

```
show interfaces switchport [interface]
```

*interface*

- **ethernet** <*unit*>/<*port*>
  - *unit* - This is device 1.
  - *port* - Physical port number on the ECN330 (Range: 1-28).
- **port-channel** <*channel-id*> - The assigned number of an aggregated link (Range: 1-13)

#### **Default Setting**

Shows all interfaces.

#### **Command Mode**

Normal Exec, Privileged Exec

#### **Command Usage**

If no interface is specified, information on all interfaces is displayed.

## Example

This example shows the configuration setting for port 3.

```

Console#show interfaces switchport ethernet 1/3
Broadcast threshold: Enabled, 500 packets/second
LACP status: Disabled
Ingress rate limit: disable,1000M bits per second
Egress rate limit: disable,1000M bits per second
VLAN membership mode: Hybrid
Ingress rule: Disabled
Acceptable frame type: All frames
Native VLAN: 1
Priority for untagged traffic: 0
Gvrp status: Disabled
Allowed Vlan: 1(u),
Forbidden Vlan:
Private-VLAN Mode: NONE
Private-VLAN host-association: NONE
Private-VLAN Mapping: NONE
Console#

```

**Table 73** *Interface Parameters*

| Field                     | Description                                                                                                                            |
|---------------------------|----------------------------------------------------------------------------------------------------------------------------------------|
| Broadcast threshold       | Shows if broadcast storm suppression is enabled or disabled; if enabled it also shows the threshold level (section 7.9.9 on page 747). |
| Lacp status               | Shows if Link Aggregation Control Protocol has been enabled or disabled (section 7.10.2 on page 759).                                  |
| Ingress/Egress rate limit | Shows if rate limiting is enabled or disabled, and the current rate limit (section 7.12 on page 776).                                  |
| VLAN membership mode      | Indicates membership mode as Trunk or Hybrid (section 7.17.6 on page 857).                                                             |
| Ingress rule              | Shows if ingress filtering is enabled or disabled (section 7.17.8 on page 859).                                                        |

| Field                         | Description                                                                                                                     |
|-------------------------------|---------------------------------------------------------------------------------------------------------------------------------|
| Acceptable frame type         | Shows if acceptable VLAN frames include all types or tagged frames only (section 7.17.7 on page 858).                           |
| Native VLAN                   | Indicates the default Port VLAN ID (section 7.17.9 on page 860).                                                                |
| Priority for untagged traffic | Indicates the default priority for untagged frames (section 7.19.2 on page 900).                                                |
| Gvrp status                   | Shows if GARP VLAN Registration Protocol is enabled or disabled (section 7.17.1.3 on page 844).                                 |
| Allowed Vlan                  | Shows the VLANs this interface has joined, where (u) indicates untagged and (t) indicates tagged (section 7.17.10 on page 861). |
| Forbidden Vlan                | Shows the VLANs this interface can not dynamically join through GVRP (section 7.17.11 on page 863).                             |
| Private-VLAN Mode             | Shows the private VLAN mode as host, promiscuous, or none (section 7.17.18 on page 873).                                        |
| Private-VLAN host-association | Shows the secondary (or community) VLAN with which this port is associated (section 7.17.20 on page 875).                       |
| Private-VLAN Mapping          | Shows the primary VLAN mapping for a promiscuous port (section 7.17.19 on page 874).                                            |

## 7.10 Link Aggregation Commands

Ports can be statically grouped into an aggregate link (that is, trunk) to increase the bandwidth of a network connection or to ensure fault recovery. Or the Link Aggregation Control Protocol (LACP) can be used to automatically negotiate a trunk link between the ECN330-switch and another network device. For static trunks, the switches have to comply with the Cisco EtherChannel standard. For dynamic trunks, the switches have to comply with LACP. The ECN330-switch supports up to 13 trunks. For example, a trunk consisting of two 1000 Mbps ports can support an aggregate bandwidth of 4 Gbps when operating at full duplex.

Table 74 Link Aggregation Commands

| Command                              | Function                                                                 | Mode              | Page |
|--------------------------------------|--------------------------------------------------------------------------|-------------------|------|
| <i>Manual Configuration Commands</i> |                                                                          |                   |      |
| <b>interface port-channel</b>        | Configures a trunk and enters interface configuration mode for the trunk | GC                | 737  |
| <b>channel-group</b>                 | Adds a port to a trunk                                                   | IC (Ethernet)     | 758  |
| <i>Dynamic Configuration Command</i> |                                                                          |                   |      |
| <b>lacp</b>                          | Configures LACP for the current interface                                | IC (Ethernet)     | 759  |
| <b>lacp system-priority</b>          | Configures a port's LACP system priority                                 | IC (Ethernet)     | 761  |
| <b>lacp admin-key</b>                | Configures a port's administration key                                   | IC (Ethernet)     | 762  |
| <b>lacp admin-key</b>                | Configures an port channel's administration key                          | IC (Port Channel) | 763  |
| <b>lacp port-priority</b>            | Configures a port's LACP port priority                                   | IC (Ethernet)     | 764  |

| Command                                            | Function                | Mode   | Page |
|----------------------------------------------------|-------------------------|--------|------|
| <i>Trunk Status Display Command</i>                |                         |        |      |
| <b>show interfaces<br/>status<br/>port-channel</b> | Shows trunk information | NE, PE | 749  |
| <b>show lacp</b>                                   | Shows LACP information  | PE     | 766  |

## Guidelines for Creating Trunks

### *General Guidelines –*

- Finish configuring port trunks before connecting the corresponding network cables between switches to avoid creating a loop.
- A trunk can have up to eight ports.
- The ports at both ends of a connection must be configured as trunk ports.
- All ports in a trunk must be configured in an identical manner, including communication mode (that is, speed, duplex mode and flow control), VLAN assignments, and CoS settings.
- Any of the Gigabit ports on the front panel can be trunked together, including ports of different media types.
- All the ports in a trunk have to be treated as a whole when moved from/to, added or deleted from a VLAN through the specified port-channel.
- STP, VLAN, and IGMP settings can only be made for the entire trunk through the specified port-channel.

### *Dynamically Creating a Port Channel –*

- Ports assigned to a common port channel must meet the following criteria:
- Ports must have the same LACP system priority.
- Ports must have the same port admin key (Ethernet Interface).

- If the port channel admin key (lacp admin key - Port Channel) is not set when a channel group is formed (that is, it has the null value of 0), this key is set to the same value as the port admin key (lacp admin key - Ethernet Interface) used by the interfaces that joined the group.
- However, if the port channel admin key is set, then the port admin key must be set to the same value for a port to be allowed to join a channel group.
- If a link goes down, LACP port priority is used to select the backup link.

### 7.10.1 **channel-group**

This command adds a port to a trunk. Use the **no** form to remove a port from a trunk.

#### **Syntax**

**channel-group** <*channel-id*>

**no channel-group**

*channel-id* - Trunk index (Range: 1-13)

#### **Default Setting**

The current port will be added to this trunk.

#### **Command Mode**

Interface Configuration (Ethernet)

#### **Command Usage**

- When configuring static trunks, the switches must comply with the Cisco EtherChannel standard.
- Use **no channel-group** to remove a port group from a trunk.
- Use **no interfaces port-channel** to remove a trunk from the ECN330-switch.



## Example

The following example creates trunk 1 and then adds port 11:

```
Console(config)#interface port-channel 1
Console(config-if)#exit
Console(config)#interface ethernet 1/11
Console(config-if)#channel-group 1
Console(config-if)#
```

### 7.10.2

## lACP

This command enables 802.3ad Link Aggregation Control Protocol (LACP) for the current interface. Use the **no** form to disable it.

### Syntax

**[no] lACP**

### Default Setting

Disabled

### Command Mode

Interface Configuration (Ethernet)

### Command Usage

- The ports on both ends of an LACP trunk must be configured for full duplex, either by forced mode or auto-negotiation.
- A trunk formed with another switch using LACP will automatically be assigned the next available port-channel ID.
- If the target switch has also enabled LACP on the connected ports, the trunk will be activated automatically.
- If more than eight ports attached to the same target switch have LACP enabled, the additional ports will be placed in standby mode, and will only be enabled if one of the active links fails.

## Example

The following shows LACP enabled on ports 10 - 12. Because LACP has also been enabled on the ports at the other end of the links, the **show interfaces status port-channel 1** command shows that Trunk1 has been established.

```
Console(config)#interface ethernet 1/10
Console(config-if)#lacp
Console(config-if)#exit
Console(config)#interface ethernet 1/11
Console(config-if)#lacp
Console(config-if)#exit
Console(config)#interface ethernet 1/12
Console(config-if)#lacp
Console(config-if)#exit
Console(config)#exit
Console#show interfaces status port-channel 1
Information of Trunk 1
Basic information:
 Port Type: 100TX
 Mac address: 00-00-e8-00-00-0b
Configuration:
 Name:
 Port Admin: Up
 Speed-duplex: Auto
 Capabilities: 10half, 10full, 100half, 100full
 Flow Control: Disabled
 Port Security: Disabled
 Max MAC Count: 0
Current status:
 Created by: LACP
 Link status: Up
 Operation speed-duplex: 100full
 Flow control type: None
 Member Ports: Eth1/10, Eth1/11, Eth1/12,
Console#
```

### 7.10.3 lacp system-priority

This command configures a port's LACP system priority. Use the **no** form to restore the default setting.

#### Syntax

```
lacp {actor | partner} system-priority <priority>
```

```
no lacp {actor | partner} system-priority
```

- **actor** - The local side an aggregate link.
- **partner** - The remote side of an aggregate link.
- **priority** - This priority is used to determine link aggregation group (LAG) membership, and to identify this device to other switches during LAG negotiations. (Range: 0-65535)

#### Default Setting

32768

#### Command Mode

Interface Configuration (Ethernet)

#### Command Usage

- Port must be configured with the same system priority to join the same LAG.
- System priority is combined with the ECN330-switch's MAC address to form the LAG identifier. This identifier is used to indicate a specific LAG during LACP negotiations with other systems.
- Once the remote side of a link has been established, LACP operational settings are already in use on that side. Configuring LACP settings for the partner only applies to its administrative state, not its operational state, and will only take effect the next time an aggregate link is established with the partner.

## Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#lacp actor system-priority 3
Console(config-if)#
```

### 7.10.4 lacp admin-key (Ethernet Interface)

This command configures a port's LACP administration key. Use the **no** form to restore the default setting.

#### Syntax

```
lacp {actor | partner} admin-key <key>
```

```
[no] lacp {actor | partner} admin-key
```

- **actor** - The local side an aggregate link.
- **partner** - The remote side of an aggregate link.
- *key* - The port admin key must be set to the same value for ports that belong to the same link aggregation group (LAG). (Range: 0-65535)

#### Default Setting

0

#### Command Mode

Interface Configuration (Ethernet)

#### Command Usage

- Ports are only allowed to join the same LAG if (1) the LACP system priority matches, (2) the LACP port admin key matches, and (3) the LACP port channel key matches (if configured).
- If the port channel admin key (**lacp admin key** - Port Channel) is not set when a channel group is formed (that is, it has the null value of 0),

this key is set to the same value as the port admin key (**lacp admin-key** - Ethernet Interface) used by the interfaces that joined the group.

- Once the remote side of a link has been established, LACP operational settings are already in use on that side. Configuring LACP settings for the partner only applies to its administrative state, not its operational state, and will only take effect the next time an aggregate link is established with the partner.

### Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#lacp actor admin-key 120
Console(config-if)#
```

## 7.10.5 lacp admin-key (Port Channel)

This command configures a port channel's LACP administration key string. Use the **no** form to restore the default setting.

### Syntax

**lacp admin-key <key>**

**[no] lacp admin-key**

**key** - The port channel admin key is used to identify a specific link aggregation group (LAG) during local LACP setup on the ECN330-switch. (Range: 0-65535)

### Default Setting

0

### Command Mode

Interface Configuration (Port Channel)

## Command Usage

- Ports are only allowed to join the same LAG if (1) the LACP system priority matches, (2) the LACP port admin key matches, and (3) the LACP port channel key matches (if configured).
- If the port channel admin key (**lacp admin key** - Port Channel) is not set when a channel group is formed (that is, it has the null value of 0), this key is set to the same value as the port admin key (**lacp admin key** - Ethernet Interface) used by the interfaces that joined the group. Note that when the LAG is no longer used, the port channel admin key is reset to 0.

## Example

```
Console(config)#interface port-channel 1
Console(config-if)#lacp admin-key 3
Console(config-if)#
```

### 7.10.6

## lacp port-priority

This command configures LACP port priority. Use the **no** form to restore the default setting.

## Syntax

```
lacp {actor | partner} port-priority <priority>
```

```
no lacp {actor | partner} port-priority
```

- **actor** - The local side an aggregate link.
- **partner** - The remote side of an aggregate link.
- **priority** - LACP port priority is used to select a backup link.  
(Range: 0-65535)

## Default Setting

32768

## Command Mode

Interface Configuration (Ethernet)

## Command Usage

- Setting a lower value indicates a higher effective priority.
- If an active port link goes down, the backup port with the highest priority is selected to replace the downed link. However, if two or more ports have the same LACP port priority, the port with the lowest physical port number will be selected as the backup port.
- Once the remote side of a link has been established, LACP operational settings are already in use on that side. Configuring LACP settings for the partner only applies to its administrative state, not its operational state, and will only take effect the next time an aggregate link is established with the partner.

## Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#lacp actor port-priority 128
```

## 7.10.7 **show lacp**

This command displays LACP information.

### **Syntax**

```
show lacp [<port-channel>] {counters | internal |
 neighbors | sys-id}
```

- *port-channel* - Local identifier for a link aggregation group.  
(Range: 1-13)
- **counters** - Statistics for LACP protocol messages.
- **internal** - Configuration settings and operational state for local side.
- **neighbors** - Configuration settings and operational state for remote side.
- **sys-id** - Summary of system priority and MAC address for all channel groups.

### **Default Setting**

Port Channel: all

### **Command Mode**

Privileged Exec



## Example

```

Console#show lacp 1 counters
Port channel: 1

Eth 1/ 2

LACPDUs Sent: 10
LACPDUs Receive: 5
Marker Sent: 0
Marker Receive: 0
LACPDUs Unknown Pkts: 0
LACPDUs Illegal Pkts: 0
.
.
.

```

*Table 75 show lacp counters - display description*

| Field                | Description                                                                                                                                                                                                                          |
|----------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| LACPDUs Sent         | Number of valid LACPDUs transmitted from this channel group.                                                                                                                                                                         |
| LACPDUs Received     | Number of valid LACPDUs received on this channel group.                                                                                                                                                                              |
| Marker Sent          | Number of valid Marker PDUs transmitted from this channel group.                                                                                                                                                                     |
| Marker Received      | Number of valid Marker PDUs received by this channel group.                                                                                                                                                                          |
| LACPDUs Unknown Pkts | Number of frames received that either (1) Carry the Slow Protocols Ethernet Type value, but contain an unknown PDU, or (2) are addressed to the Slow Protocols group MAC Address, but do not carry the Slow Protocols Ethernet Type. |
| LACPDUs Illegal Pkts | Number of frames that carry the Slow Protocols Ethernet Type value, but contain a badly formed PDU or an illegal value of Protocol Subtype.                                                                                          |

```

Console#show lacp 1 internal
Port channel: 1

Oper Key: 3
Admin Key: 0
Eth 1/ 2

LACPDUs Internal: 30 sec
LACP System Priority: 32768
LACP Port Priority: 32768
Admin Key: 3
Oper Key: 3
Admin State: default, aggregation, long timeout, LACP-activity
Oper State: distributing, collecting, synchronization,
 aggregation, long timeout, LACP-activity
.
.
.

```

**Table 76** *show lacp internal - display description*

| Field                | Description                                                        |
|----------------------|--------------------------------------------------------------------|
| Oper Key             | Current operational value of the key for the aggregation port.     |
| Admin Key            | Current administrative value of the key for the aggregation port.  |
| LACPDUs Internal     | Number of seconds before invalidating received LACPDU information. |
| LACP System Priority | LACP system priority assigned to this port channel.                |

| Field                      | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|----------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| LACP Port Priority         | LACP port priority assigned to this interface within the channel group.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Admin State,<br>Oper State | <p>Administrative or operational values of the actor's state parameters:</p> <ul style="list-style-type: none"> <li>Expired – The actor's receive machine is in the expired state;</li> <li>Defaulted – The actor's receive machine is using defaulted operational partner information, administratively configured for the partner.</li> <li>Distributing – If false, distribution of outgoing frames on this link is disabled; that is, distribution is currently disabled and is not expected to be enabled in the absence of administrative changes or changes in received protocol information.</li> <li>Collecting – Collection of incoming frames on this link is enabled; that is, collection is currently enabled and is not expected to be disabled in the absence of administrative changes or changes in received protocol information.</li> <li>Synchronization – The System considers this link to be IN_SYNC; that is, it has been allocated to the correct Link Aggregation Group, the group has been associated with a compatible Aggregator, and the identity of the Link Aggregation Group is consistent with the System ID and operational Key information transmitted.</li> <li>Aggregation – The system considers this link to be aggregatable; that is, a potential candidate for aggregation.</li> <li>Long timeout – Periodic transmission of LACPDU's uses a slow transmission rate.</li> <li>LACP-Activity – Activity control value with regard to this link. (0: Passive; 1: Active)</li> </ul> |

```

Console#show lacp 1 neighbors
Port channel 1 neighbors

Eth 1/1

Partner Admin System ID: 32768, 00-00-00-00-00-00
Partner Oper System ID: 32768, 00-01-F4-78-AE-C0
Partner Admin Port Number: 2
Partner Oper Port Number: 2
Port Admin Priority: 32768
Port Oper Priority: 32768
Admin Key: 0
Oper Key: 3
Admin State: defaulted, distributing, collecting,
 synchronization, long timeout,
Oper State: distributing, collecting,
 synchronization, aggregation,
 long timeout, LACP-activity
.
.
.

```

**Table 77** *show lacp neighbors - display description*

| Field                     | Description                                                                               |
|---------------------------|-------------------------------------------------------------------------------------------|
| Partner Admin System ID   | LAG partner's system ID assigned by the user.                                             |
| Partner Oper System ID    | LAG partner's system ID assigned by the LACP protocol.                                    |
| Partner Admin Port Number | Current administrative value of the port number for the protocol Partner.                 |
| Partner Oper Port Number  | Operational port number assigned to this aggregation port by the port's protocol partner. |
| Port Admin Priority       | Current administrative value of the port priority for the protocol partner.               |
| Port Oper Priority        | Priority value assigned to this aggregation port by the partner.                          |

| Field       | Description                                                                     |
|-------------|---------------------------------------------------------------------------------|
| Admin Key   | Current administrative value of the Key for the protocol partner.               |
| Oper Key    | Current operational value of the Key for the protocol partner.                  |
| Admin State | Administrative values of the partner's state parameters. (See preceding table.) |
| Oper State  | Operational values of the partner's state parameters. (See preceding table.)    |

```

Console#show lacp sysid
Port Channel System Priority System MAC Address

 1 32768 00-30-F1-8F-2C-A7
 2 32768 00-30-F1-8F-2C-A7
 3 32768 00-30-F1-8F-2C-A7
 4 32768 00-30-F1-8F-2C-A7
 5 32768 00-30-F1-8F-2C-A7
 6 32768 00-30-F1-8F-2C-A7
 7 32768 00-30-F1-D4-73-A0
 8 32768 00-30-F1-D4-73-A0
 9 32768 00-30-F1-D4-73-A0
 10 32768 00-30-F1-D4-73-A0
 11 32768 00-30-F1-D4-73-A0
 12 32768 00-30-F1-D4-73-A0
.
.
.

```

*Table 78 show lacp sysid - display description*

| Field               | Description                                               |
|---------------------|-----------------------------------------------------------|
| Channel group       | A link aggregation group configured on the ECN330-switch. |
| System Priority*    | LACP system priority for this channel group.              |
| System MAC Address* | System MAC address.                                       |

\* The LACP system priority and system MAC address are concatenated to form the LAG system ID.

## 7.11 Mirror Port Commands

This section describes how to mirror traffic from a source port to a target port.

Table 79 Mirror Port Commands

| Command                  | Function                                  | Mode | Page |
|--------------------------|-------------------------------------------|------|------|
| <b>port monitor</b>      | Configures a mirror session               | IC   | 773  |
| <b>show port monitor</b> | Shows the configuration for a mirror port | PE   | 774  |

### 7.11.1 port monitor

This command configures a mirror session. Use the **no** form to clear a mirror session.

#### Syntax

```
port monitor <interface> [rx | tx | both]
```

```
no port monitor <interface>
```

- *interface* - **ethernet** <unit>/<port> (source port)
  - *unit* - ECN330-switch (unit 1).
  - *port* - Physical port number on the ECN330.
- **rx** - Mirror received packets.
- **tx** - Mirror transmitted packets.
- **both** - Mirror both received and transmitted packets.

#### Default Setting

No mirror session is defined. When enabled, the default mirroring is for both received and transmitted packets.

## Command Mode

Interface Configuration (Ethernet, destination port)

## Command Usage

- Traffic can be mirrored from any source port to a destination port for real-time analysis. A logic analyzer or RMON probe can then be attached to the destination port to study the traffic crossing the source port in a completely unobtrusive manner.
- The destination port is set by specifying an Ethernet interface.
- The mirror port and monitor port speeds should match, otherwise traffic may be dropped from the monitor port.
- Multiple mirror sessions can be created, but all sessions must share the same destination port. However, avoid sending too much traffic to the destination port from multiple source ports.

## Example

The following example configures the ECN330-switch to mirror all packets from port 6 to port 11:

```
Console(config)#interface ethernet 1/11
Console(config-if)#port monitor ethernet 1/6 both
Console(config-if)#
```

### 7.11.2 show port monitor

This command displays mirror information.

## Syntax

```
show port monitor [interface]
 interface - ethernet <unit>/<port> (source port)
```

- *unit* - ECN330-switch (unit 1).
- *port* - Physical port number on the ECN330.



## Default Setting

Shows all sessions.

## Command Mode

Privileged Exec

## Command Usage

This command displays the currently configured source port, destination port, and mirror mode (that is, RX, TX, or RX/TX).

## Example

The following shows mirroring configured from port 6 to port 11:

```
Console(config)#interface ethernet 1/11
Console(config-if)#port monitor ethernet 1/6
Console(config-if)#end
Console#show port monitor
Port Mirroring

Destination port(listen port):Eth1/11
Source port(monitored port) :Eth1/6
Mode :RX/TX
Console#
```

## 7.12 Rate Limit Commands

This function allows the network manager to control the maximum rate for traffic transmitted or received on an interface. Rate limiting is configured on interfaces at the edge of a network to limit traffic into or out of the network. Traffic that falls within the rate limit is transmitted, while packets that exceed the acceptable amount of traffic are dropped.

Rate limiting can be applied to individual ports or trunks. When an interface is configured with this feature, the traffic rate will be monitored by the hardware to verify conformity. Non-conforming traffic is dropped, conforming traffic is forwarded without any changes.

Table 80 Rate Limit Commands

| Command           | Function                                                     | Mode | Page |
|-------------------|--------------------------------------------------------------|------|------|
| <b>rate-limit</b> | Configures the maximum input or output rate for an interface | IC   | 776  |

### 7.12.1 rate-limit

This command defines the rate limit for a specific interface. Use the command without specifying a rate to restore the default rate. Use the **no** form to restore the default status of disabled.

#### Syntax

```
rate-limit {input [rate [vlan <vlan-id>]] |
 output [rate]}
```

```
no rate-limit {input | output}
```

- **input** – Input rate limit
- **output** – Output rate limit
- **rate** – Maximum value in Mbps. (Range: Fast Ethernet - 1 to 100 Mbps, Gigabit Ethernet - 1 to 1000 Mbps in multiples of 64 Kbps)
- **vlan-id** - VLAN ID (Range: 1-4094)

## Default Setting

Fast Ethernet: 100 Mbps  
Gigabit Ethernet: 1000 Mbps

## Command Usage

- Use the command without specifying a rate to restore the default rate.
- Use the **no** form to restore the default status of disabled.
- Use the **vlan** option to configure the input rate limit for a port within the specified VLAN.

## Command Mode

Interface Configuration (Ethernet, Port Channel)

## Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#rate-limit input 64000
Console(config-if)#rate-limit input 6400 vlan 1
Console(config-if)#
```

## 7.13 Power over Ethernet Commands

The commands in this group control the power that can be delivered to EDA devices through the ECN330's ports.

The ECN330-switch's power management enables total ECN330 power and individual port power to be controlled within a configured power budget. Port power can be automatically turned on and off for connected EDA devices and a per-port power priority can be set so that the ECN330 never exceeds its allocated power budget. When a device is connected to a ECN330 port, its power requirements are detected by the ECN330-switch before power is supplied. If the power required by a device exceeds the power budget of the port or the whole ECN330, power is not supplied.

Ports can be set to one of three power priority levels, critical, high, or low. To control power supply within the ECN330's budget, ports set at critical or high priority have power enabled in preference to those ports set at low priority. For example, when a device is connected to a port set to critical priority, the ECN330 supplies the required power, if necessary by dropping power to ports set for a lower priority. If power is dropped to some low-priority ports and later the power demands on the ECN330 fall back within its budget, the dropped power is automatically restored.

*Table 81 Power Management Commands*

| Command                                           | Function                                                  | Mode | Page |
|---------------------------------------------------|-----------------------------------------------------------|------|------|
| <b>power mainpower<br/>maximum<br/>allocation</b> | Sets the maximum power available to all ECN330 ports      | GC   | 779  |
| <b>power inline</b>                               | Turns power on and off for specific ports                 | IC   | 780  |
| <b>power inline<br/>maximum<br/>allocation</b>    | Sets the maximum power available to specific ECN330 ports | IC   | 781  |
| <b>power inline<br/>priority</b>                  | Sets the priority for power supplied to specific ports    | IC   | 782  |

| Command                         | Function                                                                       | Mode | Page |
|---------------------------------|--------------------------------------------------------------------------------|------|------|
| <b>show power inline status</b> | Displays the current status of power management on specific ports or all ports | PE   | 783  |
| <b>show power mainpower</b>     | Displays the current status of power management for the ECN330-switch          | PE   | 785  |

### 7.13.1 power mainpower maximum allocation

This command defines the maximum power budget for the ECN330 (power available to all ECN330 ports). Use the **no** form to restore the default setting.

#### Syntax

```
power mainpower maximum allocation <watts >
```

```
no power mainpower maximum allocation
```

*watts* - The maximum power budget for the ECN330. (Range: 36 - 800 watts)

#### Default Setting

555 watts

#### Command Mode

Global Configuration

#### Command Usage

- Setting a maximum power budget for the ECN330 enables power to be centrally managed preventing overload conditions at the power source.
- If the power demand from devices connected to the ECN330 exceeds the power budget setting, the ECN330-switch uses port power priority settings to limit the supplied power.

## Example

```
Console(config)#power mainpower maximum allocation 400
Console(config)#
```

## Related Commands

**power inline priority** (section 7.13.4 on page 782)

### 7.13.2 power inline

This command automatically detects if a PoE-compliant device is connected to the specified port, and turns power on or off accordingly. It can also be used to force a port into test mode. Use the **no** form to turn off power for a port.

#### Syntax

```
power inline [auto | test]
```

```
no power inline
```

- **auto** - The ECN330-switch automatically detects if an EDA device is connected to the port and turns power on or off accordingly.
- **test** - Forces the port into a test mode. In test mode the port continuously attempts to detect if an EDA device is connected to the port, but does not supply power.

#### Default Setting

auto

#### Command Mode

Interface Configuration

#### Command Usage

- Using the command without an argument enables port power in **auto** mode (the same as the **power inline auto** command).

- In the default **auto** mode, power is automatically supplied when a device is detected on the port, providing that the power demanded does not exceed ECN330's power budget.

### Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#power inline auto
Console(config-if)#exit
Console(config)#interface ethernet 1/2
Console(config-if)#no power inline
Console(config-if)#
```

## 7.13.3 power inline maximum allocation

This command limits the power allocated to specific ports. Use the **no** form to restore the default setting.

### Syntax

**power inline maximum allocation <milliwatts>**

**no power inline maximum allocation**

- *milliwatts* - The maximum power budget for the port.  
(Range: 3000 - 24700 milliwatts).

**Note:** The maximum power allocation that configured is 24700 milliwatts. However, the maximum guaranteed power that can be delivered to any port is only 23100 milliwatts.

### Default Setting

24700 milliwatts

### Command Mode

Interface Configuration

## Command Usage

If a device is connected to an ECN330 port and the ECN330-switch detects that it requires more than the maximum power allocated to the port, no power is supplied to the device (the port power remains off).

## Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#power inline maximum allocation 16000
Console(config-if)#
```

### 7.13.4 power inline priority

This command sets the power priority for specific ports. Use the **no** form to restore the default setting.

#### Syntax

**power inline priority <priority>**

**no power inline priority**

*priority* - The power priority for the port.  
Options: 1 (critical), 2 (high), or 3 (low).

#### Default Setting

3 (low)

#### Command Mode

Interface Configuration



## Command Usage

- If the power demand from devices connected to the ECN330 exceeds the power budget setting, the ECN330-switch uses port power priority settings to control the supplied power. For example:
  - A device connected to a low-priority port that causes the ECN330 to exceed its budget is not supplied power.
  - A device connected to a critical or high-priority port that causes the ECN330 to exceed its budget is supplied power, but the ECN330-switch drops power to one or more lower-priority ports.
- Power is dropped from low-priority ports in sequence starting from port number 1.

## Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#power inline priority 3
Console(config-if)#
```

## Related Commands

**power mainpower maximum allocation** (section 7.13.1 on page 779)

### 7.13.5 show power inline status

This command displays the current power status for all ports or for specific ports.

## Syntax

**show power inline status** [*interface*]

*interface*

**ethernet** *unit/port*

- *unit* - This is device 1.
- *port* - Physical port number on the ECN330 (Range: 1-24).

**Command Mode**

Privileged Exec

**Example**

```

Console#show power inline status
Interface Admin Oper Power(mWatt) Power(used) Priority

Eth 1/ 1 enable off 23100 0 low
Eth 1/ 2 enable off 23100 0 low
Eth 1/ 3 enable on 23100 7505 low
Eth 1/ 4 enable off 23100 0 low
Eth 1/ 5 enable off 23100 0 low
Eth 1/ 6 enable off 23100 0 low
Eth 1/ 7 enable on 23100 8597 low
.
.
.
Eth 1/23 enable off 23100 0 low
Eth 1/24 enable off 23100 0 low
Console#

```

**Table 82** *show power inline status - Display Description*

| Field         | Description                                                                             |
|---------------|-----------------------------------------------------------------------------------------|
| Admin         | The power mode set on the port (configurable, see section 7.13.2 on page 780).          |
| Oper          | The current operating power status (displays on or off).                                |
| Power (mWatt) | The available power budget for the port (configurable, see section 7.13.3 on page 781). |
| Power (used)  | The current power consumption on the port in milliwatts.                                |
| Priority      | The port's power priority setting (configurable, see section 8.7.4 on page 119).        |

### 7.13.6 **show power mainpower**

Use this command to display the current power status for the ECN330.

#### **Command Mode**

Privileged Exec

#### **Example**

```
Console#show power mainpower
Unit 1 Mainpower Status
Maximum Available Power : 555 watts
System Operation Status : on
Mainpower Consumption : 15 watts
Thermal Temperature : 41 (in Celsius)
Software Version : Version 0x1B6F, Build 0x07
Console#
```

**Table 83** *show power mainpower - Display Description*

| Field                   | Description                                                                                                                                           |
|-------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|
| Maximum Available Power | The available power budget for the ECN330 (configurable, see section 7.13.1 on page 779).                                                             |
| System Operation Status | The current operating power status for the ECN330 (displays on or off).                                                                               |
| Mainpower Consumption   | The current power consumption on the ECN330 in watts.                                                                                                 |
| Thermal Temperature     | The current internal temperature of the ECN330. Note that the ECN330 automatically shuts down if the measured temperature exceeds 80 degrees Celsius. |

## 7.14 Address Table Commands

These commands are used to configure the address table for filtering specified addresses, displaying current entries, clearing the table, or setting the aging time.

*Table 84 Address Table Commands*

| Command                                  | Function                                                               | Mode | Page |
|------------------------------------------|------------------------------------------------------------------------|------|------|
| <b>mac-address-table static</b>          | Maps a static address to a port in a VLAN                              | GC   | 787  |
| <b>clear mac-address-table dynamic</b>   | Removes any learned entries from the forwarding database               | PE   | 788  |
| <b>show mac-address-table</b>            | Displays entries in the bridge-forwarding database                     | PE   | 789  |
| <b>mac-address-table aging-time</b>      | Sets the aging time of the address table                               | GC   | 791  |
| <b>mac-address-table threshold</b>       | Sends a trap message when address entries exceed a specified threshold | GC   | 792  |
| <b>show mac-address-table aging-time</b> | Shows the aging time for the address table                             | PE   | 793  |

### 7.14.1 **mac-address-table static**

This command maps a static address to a destination port in a VLAN. Use the **no** form to remove an address.

#### **Syntax**

```
mac-address-table static <mac-address> interface
 <interface> vlan <vlan-id> [action]

no mac-address-table static <mac-address> vlan <vlan-id>
```

- *mac-address* - MAC address.
- *interface*
  - **ethernet** <unit>/<port>
    - *unit* - This is device 1.
    - *port* - Physical port number on the ECN330 (Range: 1-28).
  - **port-channel** <channel-id> - The assigned number of an aggregated link (Range: 1-13)
- *vlan-id* - VLAN ID (Range: 1-4094)
- *action* -
  - **delete-on-reset** - Assignment lasts until the ECN330-switch is reset.
  - **permanent** - Assignment is permanent.

#### **Default Setting**

No static addresses are defined. The default mode is **permanent**.

#### **Command Mode**

Global Configuration

## Command Usage

The static address for a host device can be assigned to a specific port within a specific VLAN. Use this command to add static addresses to the MAC Address Table. Static addresses have the following characteristics:

- Static addresses will not be removed from the address table when a given interface link is down.
- Static addresses are bound to the assigned interface and will not be moved. When a static address is seen on another interface, the address will be ignored and will not be written to the address table.
- A static address cannot be learned on another port until the address is removed with the **no** form of this command.

## Example

```
Console(config)#mac-address-table static 00-e0-29-94-34-de interface
ethernet 1/1 vlan 1 delete-on-reset
Console(config)#
```

### 7.14.2 clear mac-address-table dynamic

This command removes any learned entries from the forwarding database and clears the transmit and receive counts for any static or system configured entries.

## Default Setting

None

## Command Mode

Privileged Exec

## Example

```
Console#clear mac-address-table dynamic
Console#
```

### 7.14.3 **show mac-address-table**

This command shows the classes of entries in the bridge-forwarding database.

#### **Syntax**

```
show mac-address-table [address <mac-address>] [mask]
[interface <interface>] [vlan <vlan-id>]
[sort {address | vlan | interface}]
```

- *mac-address* - MAC address.
- *mask* - Bits to match in the address.
- *interface*
  - **ethernet** <*unit*>/<*port*>
    - *unit* - This is device 1.
    - *port* - Physical port number on the ECN330 (Range: 1-28).
  - **port-channel** <*channel-id*> - The assigned number of an aggregated link (Range: 1-13)
- *vlan-id* - VLAN ID (Range: 1-4094)
- **sort** - Sort by address, vlan or interface.

#### **Default Setting**

None

#### **Command Mode**

Privileged Exec

#### **Command Usage**

- The MAC Address Table contains the MAC addresses associated with each interface. Note that the Type field may include the following types:
  - *Learned* - Dynamic address entries
  - *Permanent* - Static entry

- `Delete-on-reset` - Static entry to be deleted when system is reset
- The mask should be hexadecimal numbers (representing an equivalent bit mask) in the form **xx-xx-xx-xx-xx-xx** that is applied to the specified MAC address. Enter hexadecimal numbers, where an equivalent binary bit “0” means to match a bit and “1” means to ignore a bit. For example, a mask of **00-00-00-00-00-00** means an exact match, and a mask of **FF-FF-FF-FF-FF-FF** means “any.”
- The maximum number of address entries is 8191.

### Example

The following example displays the MAC addresses of all Ericsson IP DSLAMs and FE-E1s switches connected to the ECN330-switch. All Ericsson nodes can be identified by the MAC address starting 00-80-37-xx-xx-xx. Using the bit mask **00-00-00-FF-FF-FF** on the MAC address **00-80-37-00-00-00** displays only the Ericsson devices.

```

Console#show mac-address-table address 00-80-37-00-00-00 00-00-00-
FF-FF-FF
Interface Mac Address Vlan Type

Eth 1/ 1 00-80-37-04-30-D1 1 Learned
Eth 1/ 2 00-80-37-14-64-0E 1 Learned
Eth 1/ 3 00-80-37-03-34-8E 1 Learned
Eth 1/ 4 00-80-37-07-1A-51 1 Learned
Eth 1/ 5 00-80-37-12-96-4C 1 Learned
Console#

```



### 7.14.4 **mac-address-table aging-time**

This command sets the aging time for entries in the address table. Use the **no** form to restore the default aging time.

#### **Syntax**

```
mac-address-table aging-time <seconds>
```

```
no mac-address-table aging-time
```

*seconds* - Time in number of seconds (10-1000000; 0 to disable aging).

#### **Default Setting**

300 seconds

#### **Command Mode**

Global Configuration

#### **Command Usage**

The aging time is used to age out dynamically learned forwarding information.

#### **Example**

```
Console(config)#mac-address-table aging-time 100
Console(config)#
```

### 7.14.5 mac-address-table threshold

This command sends a trap message when address entries exceed a specified threshold. Use the **no** form to restore the default aging time.

#### Syntax

```
[no] mac-address-table threshold {enable |
falling-threshold | rising-threshold}
```

- **enable** - Sends a trap when entries in the MAC address table exceed the rising threshold. Note that once this trap has been sent, the next trigger time for this trap is after the MAC address entries fall below the falling threshold, and then exceed the rising threshold again. (Default: Disabled)
- **falling-threshold** - Falling threshold for the address table. (Default: 0; Range 0-16384)
- **rising-threshold** - Rising threshold for the address table. (Default: 1024; Range 0-16384)

#### Default Setting

Disabled

#### Command Mode

Global Configuration

#### Example

```
Console(config)#mac-address-table threshold enable
Console(config)#mac-address-table threshold falling-threshold 100
Console(config)#mac-address-table threshold rising-threshold 1024
Console(config)#
```

### 7.14.6 **show mac-address-table aging-time**

This command shows the aging time for entries in the address table.

#### **Default Setting**

None

#### **Command Mode**

Privileged Exec

#### **Example**

```
Console#show mac-address-table aging-time
Aging time: 300 sec.
Console#
```

## 7.15 Spanning Tree Algorithm Commands

This section includes commands that configure the Spanning Tree Algorithm (STA) globally for the ECN330-switch, and commands that configure STA for the selected interface.

*Table 85 Spanning Tree Commands*

| Command                                 | Function                                            | Mode | Page |
|-----------------------------------------|-----------------------------------------------------|------|------|
| <b>spanning-tree</b>                    | Enables the spanning tree protocol                  | GC   | 796  |
| <b>spanning-tree mode</b>               | Configures STP, RSTP, or MSTP mode                  | GC   | 797  |
| <b>spanning-tree forward-time</b>       | Configures the spanning tree bridge forward time    | GC   | 799  |
| <b>spanning-tree hello-time</b>         | Configures the spanning tree bridge hello time      | GC   | 800  |
| <b>spanning-tree max-age</b>            | Configures the spanning tree bridge maximum age     | GC   | 801  |
| <b>spanning-tree priority</b>           | Configures the spanning tree bridge priority        | GC   | 802  |
| <b>spanning-tree pathcost method</b>    | Configures the path cost method for RSTP/MSTP       | GC   | 803  |
| <b>spanning-tree transmission-limit</b> | Configures the transmission limit for RSTP/MSTP     | GC   | 804  |
| <b>spanning-tree mst-configuration</b>  | Changes to MSTP configuration mode                  | GC   | 804  |
| <b>mst vlan</b>                         | Adds VLANs to a spanning tree instance              | MST  | 805  |
| <b>mst priority</b>                     | Configures the priority of a spanning tree instance | MST  | 806  |

| Command                                 | Function                                                                               | Mode | Page |
|-----------------------------------------|----------------------------------------------------------------------------------------|------|------|
| <b>name</b>                             | Configures the name for the multiple spanning tree                                     | MST  | 807  |
| <b>revision</b>                         | Configures the revision number for the multiple spanning tree                          | MST  | 808  |
| <b>max-hops</b>                         | Configures the maximum number of hops allowed in the region before a BPDU is discarded | MST  | 809  |
| <b>spanning-tree spanning-disabled</b>  | Disables spanning tree for an interface                                                | IC   | 810  |
| <b>spanning-tree cost</b>               | Configures the spanning tree path cost of an interface                                 | IC   | 811  |
| <b>spanning-tree port-priority</b>      | Configures the spanning tree priority of an interface                                  | IC   | 812  |
| <b>spanning-tree edge-port</b>          | Enables fast forwarding for edge ports                                                 | IC   | 813  |
| <b>spanning-tree portfast</b>           | Sets an interface to fast forwarding                                                   | IC   | 814  |
| <b>spanning-tree link-type</b>          | Configures the link type for RSTP                                                      | IC   | 816  |
| <b>spanning-tree mst cost</b>           | Configures the path cost of an instance in the MST                                     | IC   | 817  |
| <b>spanning-tree mst port-priority</b>  | Configures the priority of an instance in the MST                                      | IC   | 818  |
| <b>spanning-tree protocol-migration</b> | Re-checks the appropriate BPDU format                                                  | PE   | 820  |

| Command                                     | Function                                                                         | Mode | Page |
|---------------------------------------------|----------------------------------------------------------------------------------|------|------|
| <b>show spanning-tree</b>                   | Shows spanning tree configuration for the overall bridge or a selected interface | PE   | 821  |
| <b>show spanning-tree mst configuration</b> | Shows the multiple spanning tree configuration                                   | PE   | 823  |

### 7.15.1 spanning-tree

This command enables the Spanning Tree Algorithm globally for the ECN330-switch. Use the **no** form to disable it.

#### Syntax

**[no] spanning-tree**

#### Default Setting

Spanning tree is disabled.

#### Command Mode

Global Configuration

#### Command Usage

The Spanning Tree Algorithm (STA) can be used to detect and disable network loops, and to provide backup links between switches, bridges or routers. This allows the ECN330-switch to interact with other bridging devices (that is, an STA-compliant switch, bridge or router) in the network to ensure that only one route exists between any two stations on the network, and provide backup links which automatically take over when a primary link goes down.

## Example

This example shows how to enable the Spanning Tree Algorithm for the ECN330-switch:

```
Console(config)#spanning-tree
Console(config)#
```

## 7.15.2 spanning-tree mode

This command selects the spanning tree mode for the ECN330-switch. Use the **no** form to restore the default.

### Syntax

**spanning-tree mode {stp | rstp | mstp}**

**no spanning-tree mode**

- **stp** - Spanning Tree Protocol (IEEE 802.1D)
- **rstp** - Rapid Spanning Tree Protocol (IEEE 802.1w)
- **mstp** - Multiple Spanning Tree Protocol (IEEE 802.1s)

### Default Setting

RSTP

### Command Mode

Global Configuration

### Command Usage

- **Spanning Tree Protocol**  
Uses RSTP for the internal state machine, but sends only 802.1D BPDUs.
- This creates one spanning tree instance for the entire network. If multiple VLANs are implemented on a network, the path between specific VLAN members may be inadvertently disabled to prevent

network loops, thus isolating group members. When operating multiple VLANs, it is recommended to select the MSTP option.

- **Rapid Spanning Tree Protocol**

RSTP supports connections to either STP or RSTP nodes by monitoring the incoming protocol messages and dynamically adjusting the type of protocol messages the RSTP node transmits, as described below:

- **STP Mode** – If the ECN330-switch receives an 802.1D BPDU after a port's migration delay timer expires, the ECN330-switch assumes it is connected to an 802.1D bridge and starts using only 802.1D BPDUs.
- **RSTP Mode** – If RSTP is using 802.1D BPDUs on a port and receives an RSTP BPDU after the migration delay expires, RSTP restarts the migration delay timer and begins using RSTP BPDUs on that port.

- **Multiple Spanning Tree Protocol**

- To allow multiple spanning trees to operate over the network, a related set of bridges with the same MSTP configuration must be configured, allowing them to participate in a specific set of spanning tree instances.
- A spanning tree instance can exist only on bridges that have compatible VLAN instance assignments.
- Be careful when switching between spanning tree modes. Changing modes stops all spanning-tree instances for the previous mode and restarts the system in the new mode, temporarily disrupting user traffic.

### Example

The following example configures the ECN330-switch to use the Rapid Spanning Tree Protocol.

```
Console(config)#spanning-tree mode rstp
Console(config)#
```



### 7.15.3 spanning-tree forward-time

This command configures the spanning tree bridge forward time globally for the ECN330-switch. Use the **no** form to restore the default.

#### Syntax

**spanning-tree forward-time** <*seconds*>

**no spanning-tree forward-time**

*seconds* - Time in seconds. (Range: 4 - 30 seconds)

The minimum value is calculated as  $(\text{max-age} / 2) + 1$ , though never less than 4.

#### Default Setting

15 seconds

#### Command Mode

Global Configuration

#### Command Usage

This command sets the maximum time (in seconds) the root device will wait before changing states (that is, discarding to learning to forwarding). This delay is required because every device must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to the discarding state; otherwise, temporary data loops might result.

#### Example

```
Console(config)#spanning-tree forward-time 20
Console(config)#
```

#### Related Commands

**spanning-tree hello-time** (section 7.15.4 on page 800)

**spanning-tree max-age** (section 7.15.5 on page 801)

## 7.15.4 spanning-tree hello-time

This command configures the spanning tree bridge hello time globally for the ECN330-switch. Use the **no** form to restore the default.

### Syntax

**spanning-tree hello-time** <*time*>

**no spanning-tree hello-time**

*time* - Time in seconds, (Range: 1 - 10 seconds).

The minimum value is calculated as (max-age / 2) - 1, though never greater than 10.

### Default Setting

2 seconds

### Command Mode

Global Configuration

### Command Usage

This command sets the time interval (in seconds) at which the root device transmits a configuration message.

### Example

```
Console(config)#spanning-tree hello-time 5
Console(config)#
```

### Related Commands

**spanning-tree forward-time** (section 7.15.3 on page 799)

**spanning-tree max-age** (section 7.15.5 on page 801)

## 7.15.5 spanning-tree max-age

This command configures the spanning tree bridge maximum age globally for the ECN330-switch. Use the **no** form to restore the default.

### Syntax

**spanning-tree max-age <seconds>**

**no spanning-tree max-age**

*seconds* - Time in seconds. (Range: 6-40 seconds)

The minimum value is 2 x (hello-time + 1), though never less than 6.

The maximum value is 2 x (forward-time - 1), though never greater than 40.

### Default Setting

20 seconds

### Command Mode

Global Configuration

### Command Usage

This command sets the maximum time (in seconds) a device can wait without receiving a configuration message before attempting to reconfigure. All device ports (except for designated ports) should receive configuration messages at regular intervals. Any port that ages out STA information (provided in the last configuration message) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the device ports attached to the network.

### Example

```
Console(config)#spanning-tree max-age 40
Console(config)#
```

## Related Commands

**spanning-tree forward-time** (section 7.15.3 on page 799)

**spanning-tree hello-time** (section 7.15.4 on page 800)

## 7.15.6 spanning-tree priority

This command configures the spanning tree priority globally for the ECN330-switch. Use the **no** form to restore the default.

### Syntax

**spanning-tree priority** <priority>

**no spanning-tree priority**

*priority* - Priority of the bridge. (Range: 0 - 65535)  
(Range – 0-61440, in steps of 4096; Options: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440)

### Default Setting

32768

### Command Mode

Global Configuration

### Command Usage

Bridge priority is used in selecting the root device, root port, and designated port. The device with the highest priority (highest number) becomes the STA root device. However, if all devices have the same priority, the device with the lowest MAC address will then become the root device.

### Example

```
Console(config)#spanning-tree priority 16384
Console(config)#
```

## 7.15.7 spanning-tree pathcost method

This command configures the path cost method used for Rapid Spanning Tree and Multiple Spanning Tree. Use the **no** form to restore the default.

### Syntax

```
spanning-tree pathcost method {long | short}
```

```
no spanning-tree pathcost method
```

- **long** - Specifies 32-bit based values that range from 1-200,000,000.
- **short** - Specifies 16-bit based values that range from 1-65535.

### Default Setting

Long method

### Command Mode

Global Configuration

### Command Usage

The path cost method is used to determine the best path between devices. Therefore, lower values should be assigned to ports attached to faster media, and higher values assigned to ports with slower media (attached with the **spanning-tree cost** command). Note that path cost (section 7.15.16 on page 811) takes precedence over port priority (section 7.15.17 on page 812).

### Example

```
Console(config)#spanning-tree pathcost method long
Console(config)#
```

### 7.15.8 spanning-tree transmission-limit

This command configures the minimum interval between the transmission of consecutive RSTP/MSTP BPDUs. Use the **no** form to restore the default.

#### Syntax

```
spanning-tree transmission-limit <count>
```

```
no spanning-tree transmission-limit
```

*count* -The transmission limit in seconds. (Range: 1-10)

#### Default Setting

3

#### Command Mode

Global Configuration

#### Command Usage

This command limits the maximum transmission rate for BPDUs.

#### Example

```
Console(config)#spanning-tree transmission-limit 4
Console(config)#
```

### 7.15.9 spanning-tree mst-configuration

This command changes to Multiple Spanning Tree (MST) configuration mode.

#### Default Setting

- No VLANs are mapped to any MST instance.
- The region name is set the ECN330-switch's MAC address.

## Command Mode

Global Configuration

## Example

```
Console(config)#spanning-tree mst-configuration
Console(config-mstp)#
```

## Related Commands

**mst vlan** (section 7.15.10 on page 805)  
**name** (section 7.15.12 on page 807)  
**revision** (section 7.15.13 on page 808)  
**max-hops** (section 7.15.14 on page 809)

### 7.15.10 mst vlan

This command adds VLANs to a spanning tree instance. Use the **no** form to remove the specified VLANs. Using the **no** form without any VLAN parameters to remove all VLANs.

## Syntax

```
[no] mst <instance_id> vlan <vlan-range>
```

- *instance\_id* - Instance identifier of the spanning tree. (Range: 0-4094)
- *vlan-range* - Range of VLANs. (Range: 1-4094)

## Default Setting

none

## Command Mode

MST Configuration

## Command Usage

- Use this command to group VLANs into spanning tree instances. MSTP generates a unique spanning tree for each instance. This provides multiple pathways across the network, thereby balancing the traffic load, preventing wide-scale disruption when a bridge node in a single instance fails, and allowing for faster convergence of a new topology for the failed instance.
- By default all VLANs are assigned to the Internal Spanning Tree (MSTI 0) that connects all bridges and LANs within the MST region. The ECN330-switch supports up to 4094 instances. Try to group VLANs which cover the same general area of the network. However, remember that all bridges within the same MSTI Region (section 7.15.12 on page 807) must be configured with the same set of instances, and the same instance (on each bridge) with the same set of VLANs. Also, note that RSTP treats each MSTI region as a single node, connecting all regions to the Common Spanning Tree.

## Example

```
Console(config-mstp)#mst 1 vlan 2-5
Console(config-mstp)#
```

### 7.15.11

## mst priority

This command configures the priority of a spanning tree instance. Use the **no** form to restore the default.

## Syntax

```
mst <instance_id> priority <priority>
```

```
no mst <instance_id> priority
```

- *instance\_id* - Instance identifier of the spanning tree.  
(Range: 0-4094)
- *priority* - Priority of the a spanning tree instance.  
(Range: 0-61440 in steps of 4096; Options: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440)



**Default Setting**

32768

**Command Mode**

MST Configuration

**Command Usage**

- MST priority is used in selecting the root bridge and alternate bridge of the specified instance. The device with the highest priority (that is, lowest numerical value) becomes the MSTI root device. However, if all devices have the same priority, the device with the lowest MAC address will then become the root device.
- The ECN330-switch can be set to act as the MSTI root device by specifying a priority of 0, or as the MSTI alternate device by specifying a priority of 16384.

**Example**

```
Console(config-mstp)#mst 1 priority 4096
Console(config-mstp)#
```

**7.15.12****name**

This command configures the name for the multiple spanning tree region in which the ECN330-switch is located. Use the **no** form to clear the name.

**Syntax**

**name** <*name*>

*name* - Name of the spanning tree.

**Default Setting**

ECN330-switch's MAC address

## Command Mode

MST Configuration

## Command Usage

The MST region name and revision number (section 7.15.13 on page 808) are used to designate a unique MST region. A bridge (that is, spanning-tree compliant device such as the ECN330-switch) can only belong to one MST region. And all bridges in the same region must be configured with the same MST instances.

## Example

```
Console(config-mstp)#name R&D
Console(config-mstp)#
```

## Related Commands

**revision** (section 7.15.13 on page 808)

### 7.15.13

## revision

This command configures the revision number for this multiple spanning tree configuration of the ECN330-switch. Use the **no** form to restore the default.

## Syntax

**revision** *<number>*

*number* - Revision number of the spanning tree. (Range: 0-65535)

## Default Setting

0

## Command Mode

MST Configuration

## Command Usage

The MST region name (section 7.15.12 on page 807) and revision number are used to designate a unique MST region. A bridge (that is, spanning-tree compliant device such as the ECN330-switch) can only belong to one MST region. And all bridges in the same region must be configured with the same MST instances.

## Example

```
Console(config-mstp)#revision 1
Console(config-mstp)#
```

## Related Commands

**name** (section 7.15.12 on page 807)

### 7.15.14 max-hops

This command configures the maximum number of hops in the region before a BPDU is discarded. Use the **no** form to restore the default.

## Syntax

**max-hops** *<hop-number>*

*hop-number* - Maximum hop number for multiple spanning tree.  
(Range: 1-40)

## Default Setting

20

## Command Mode

MST Configuration

## Command Usage

An MSTI region is treated as a single node by the STP and RSTP protocols. Therefore, the message age for BPDUs inside an MSTI region is never changed. However, each spanning tree instance within a region, and the internal spanning tree (IST) that connects these instances use a hop count to specify the maximum number of bridges that will propagate a BPDU. Each bridge decrements the hop count by one before passing on the BPDU. When the hop count reaches zero, the message is dropped.

## Example

```
Console(config-mstp)#max-hops 30
Console(config-mstp)#
```

### 7.15.15 spanning-tree spanning-disabled

This command disables the spanning tree algorithm for the specified interface. Use the **no** form to reenable the spanning tree algorithm for the specified interface.

#### Syntax

```
[no] spanning-tree spanning-disabled
```

#### Default Setting

Enabled

#### Command Mode

Interface Configuration (Ethernet, Port Channel)

## Example

This example disables the spanning tree algorithm for port 5.

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree spanning-disabled
Console(config-if)#
```

## 7.15.16 spanning-tree cost

This command configures the spanning tree path cost for the specified interface. Use the **no** form to restore the default.

### Syntax

**spanning-tree cost <cost>**

**no spanning-tree cost**

*cost* - The path cost for the port.  
(Range: 1-200,000,000)

The recommended range is:

- Ethernet: 200,000-20,000,000
- Fast Ethernet: 20,000-2,000,000
- Gigabit Ethernet: 2,000-200,000

### Default Setting

By default, the system automatically detects the speed and duplex mode used on each port, and configures the path cost according to the values shown below.

- Ethernet – half duplex: 2,000,000; full duplex: 1,000,000; trunk: 500,000
- Fast Ethernet – half duplex: 200,000; full duplex: 100,000; trunk: 50,000
- Gigabit Ethernet – full duplex: 10,000; trunk: 5,000

## Command Mode

Interface Configuration (Ethernet, Port Channel)

## Command Usage

- This command is used by the Spanning Tree Algorithm to determine the best path between devices. Therefore, lower values should be assigned to ports attached to faster media, and higher values assigned to ports with slower media.
- Use the **no spanning-tree cost** command to specify auto-configuration mode.
- Path cost takes precedence over port priority.
- When **spanning-tree pathcost method** (section 7.15.7 on page 803) is set to **short**, the maximum value for path cost is 65,535.

## Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree cost 50
Console(config-if)#
```

## 7.15.17 spanning-tree port-priority

This command configures the priority for the specified interface. Use the **no** form to restore the default.

### Syntax

**spanning-tree port-priority** <priority>

**no spanning-tree port-priority**

*priority* - The priority for a port. (Range: 0-240, in steps of 16)

### Default Setting

128

## Command Mode

Interface Configuration (Ethernet, Port Channel)

## Command Usage

- This command defines the priority for the use of a port in the Spanning Tree Algorithm. If the path cost for all ports on an ECN330-switch are the same, the port with the highest priority (that is, lowest value) will be configured as an active link in the spanning tree.
- Where more than one port is assigned the highest priority, the port with the lowest numeric identifier will be enabled.

## Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree port-priority 0
Console(config-if)#
```

## Related Commands

**spanning-tree cost** (section 7.15.16 on page 811)

## 7.15.18 spanning-tree edge-port

This command specifies an interface as an edge port. Use the **no** form to restore the default.

## Syntax

**[no] spanning-tree edge-port**

## Default Setting

Disabled

## Command Mode

Interface Configuration (Ethernet, Port Channel)

## Command Usage

- This option can be enabled if an interface is attached to a LAN segment that is at the end of a bridged LAN or to an end node. Since end nodes cannot cause forwarding loops, they can pass directly through to the spanning tree forwarding state. Specifying Edge Ports provides quicker convergence for devices such as workstations or servers, retains the current forwarding database to reduce the amount of frame flooding required to rebuild address tables during reconfiguration events, does not cause the spanning tree to initiate reconfiguration when the interface changes state, and also overcomes other STA-related timeout problems. However, remember that Edge Port should only be enabled for ports connected to an end-node device.
- This command has the same effect as **spanning-tree portfast**.

## Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree edge-port
Console(config-if)#
```

## Related Commands

**spanning-tree portfast** (section 7.15.19 on page 814)

### 7.15.19 spanning-tree portfast

This command sets an interface to fast forwarding. Use the **no** form to disable fast forwarding.

#### Syntax

**[no] spanning-tree portfast**

#### Default Setting

Disabled



## Command Mode

Interface Configuration (Ethernet, Port Channel)

## Command Usage

- This command is used to enable or disable the fast spanning-tree mode for the selected port. In this mode, ports skip the Discarding and Learning states, and proceed straight to Forwarding.
- Since end-nodes cannot cause forwarding loops, they can be passed through the spanning tree state changes more quickly than allowed by standard convergence time. Fast forwarding can achieve quicker convergence for end-node workstations and servers, and also overcome other STA related timeout problems. (Remember that fast forwarding should only be enabled for ports connected to a LAN segment that is at the end of a bridged LAN or for an end-node device.)
- This command is the same as **spanning-tree edge-port**, and is only included for backward compatibility with earlier products. Note that this command may be removed in future software versions.

## Example

```
Console(config)#interface ethernet 1/5
Console(config-if)#spanning-tree portfast
Console(config-if)#
```

## Related Commands

**spanning-tree edge-port** (section 7.15.18 on page 813)

## 7.15.20 spanning-tree link-type

This command configures the link type for Rapid Spanning Tree and Multiple Spanning Tree. Use the **no** form to restore the default.

### Syntax

```
spanning-tree link-type {auto | point-to-point | shared}
```

```
no spanning-tree link-type
```

- **auto** - Automatically derived from the duplex mode setting.
- **point-to-point** - Point-to-point link.
- **shared** - Shared medium.

### Default Setting

auto

### Command Mode

Interface Configuration (Ethernet, Port Channel)

### Command Usage

- Specify a point-to-point link if the interface can only be connected to exactly one other bridge, or a shared link if it can be connected to two or more bridges.
- When automatic detection is selected, the ECN330-switch derives the link type from the duplex mode. A full-duplex interface is considered a point-to-point link, while a half-duplex interface is assumed to be on a shared link.
- RSTP only works on point-to-point links between two bridges. If a port is designated as a shared link, RSTP is forbidden. Since MSTP is an extension of RSTP, this same restriction applies.

## Example

```
Console(config)#interface ethernet ethernet 1/5
Console(config-if)#spanning-tree link-type point-to-point
```

### 7.15.21 spanning-tree mst cost

This command configures the path cost on a spanning instance in the Multiple Spanning Tree. Use the **no** form to restore the default.

#### Syntax

**spanning-tree mst <instance\_id> cost <cost>**

**no spanning-tree mst <instance\_id> cost**

- *instance\_id* - Instance identifier of the spanning tree.  
(Range: 0-4094, no leading zeroes)
- *cost* - Path cost for an interface.  
(Range: 1-200,000,000)  
The recommended range is -
  - Ethernet: 200,000-20,000,000
  - Fast Ethernet: 20,000-2,000,000
  - Gigabit Ethernet: 2,000-200,000

#### Default Setting

By default, the system automatically detects the speed and duplex mode used on each port, and configures the path cost according to the values shown below.

- Ethernet – half duplex: 2,000,000; full duplex: 1,000,000; trunk: 500,000
- Fast Ethernet – half duplex: 200,000; full duplex: 100,000; trunk: 50,000
- Gigabit Ethernet – full duplex: 10,000; trunk: 5,000

#### Command Mode

Interface Configuration (Ethernet, Port Channel)

## Command Usage

- Each spanning-tree instance is associated with a unique set of VLAN IDs.
- This command is used by the multiple spanning-tree algorithm to determine the best path between devices. Therefore, lower values should be assigned to interfaces attached to faster media, and higher values assigned to interfaces with slower media.
- Use the **no spanning-tree mst cost** command to specify auto-configuration mode.
- Path cost takes precedence over interface priority.

## Example

```
Console(config)#interface ethernet ethernet 1/5
Console(config-if)#spanning-tree mst 1 cost 50
Console(config-if)#
```

## Related Commands

**spanning-tree mst port-priority** (section 7.15.22 on page 818)

### 7.15.22 spanning-tree mst port-priority

This command configures the interface priority on a spanning instance in the Multiple Spanning Tree. Use the **no** form to restore the default.

## Syntax

**spanning-tree mst <instance\_id> port-priority <priority>**

**no spanning-tree mst <instance\_id> port-priority**

- *instance\_id* - Instance identifier of the spanning tree.  
(Range: 0-4094, no leading zeroes)
- *priority* - Priority for an interface. (Range: 0-240 in steps of 16)

## Default Setting

128

## Command Mode

Interface Configuration (Ethernet, Port Channel)

## Command Usage

- This command defines the priority for the use of an interface in the multiple spanning-tree. If the path cost for all interfaces on an ECN330-switch are the same, the interface with the highest priority (that is, lowest value) will be configured as an active link in the spanning tree.
- Where more than one interface is assigned the highest priority, the interface with lowest numeric identifier will be enabled.

## Example

```
Console(config)#interface ethernet ethernet 1/5
Console(config-if)#spanning-tree mst 1 port-priority 0
Console(config-if)#
```

## Related Commands

**spanning-tree mst cost** (section 7.15.21 on page 817)

### 7.15.23 spanning-tree protocol-migration

This command re-checks the appropriate BPDU format to send on the selected interface.

#### Syntax

**spanning-tree protocol-migration** <interface>

*interface*

- **ethernet** <unit>/<port>
  - *unit* - This is device 1.
  - *port* - Physical port number on the ECN330 (Range: 1-28).
- **port-channel** <channel-id> - The assigned number of an aggregated link (Range: 1-13)

#### Command Mode

Privileged Exec

#### Command Usage

If at any time the ECN330-switch detects STP BPDUs, including Configuration or Topology Change Notification BPDUs, it will automatically set the selected interface to forced STP-compatible mode. However, the **spanning-tree protocol-migration** command can be used at any time to manually re-check the appropriate BPDU format to send on the selected interfaces (RSTP or STP-compatible).

#### Example

```
Console#spanning-tree protocol-migration ethernet 1/7
Console#
```

## 7.15.24 **show spanning-tree**

This command shows the configuration for the common spanning tree (CST) or for an instance within the multiple spanning tree (MST).

### Syntax

```
show spanning-tree [interface] mst <instance_id>
```

- *interface*
  - **ethernet** <*unit*>/<*port*>
    - *unit* - This is device 1.
    - *port* - Physical port number on the ECN330 (Range: 1-28).
  - **port-channel** <*channel-id*> - The assigned number of an aggregated link (Range: 1-13)
- *instance\_id* - Instance identifier of the multiple spanning tree. (Range: 0-4094, no leading zeroes)

### Default Setting

None

### Command Mode

Privileged Exec

### Command Usage

- Use the **show spanning-tree** command with no parameters to display the spanning tree configuration for the ECN330-switch, for the Common Spanning Tree (CST), and for every interface in the tree.
- Use the **show spanning-tree** <*interface*> command to display the spanning tree configuration for an interface within the Common Spanning Tree (CST).
- Use the **show spanning-tree mst** <*instance\_id*> command to display the spanning tree configuration for an instance within the Multiple Spanning Tree (MST).

- For a description of the items displayed under `Spanning-tree` information, see “Configuring Global Settings” on page 238. For a description of the items displayed for specific interfaces, see “Displaying Interface Settings” on page 243.

### Example

```

Console#show spanning-tree
Spanning-tree information

Spanning tree mode :MSTP
Spanning tree enable/disable :enable
Instance :0
Vlans configuration :1-4094
Priority :32768
Bridge Hello Time (sec.) :2
Bridge Max Age (sec.) :20
Bridge Forward Delay (sec.) :15
Root Hello Time (sec.) :2
Root Max Age (sec.) :20
Root Forward Delay (sec.) :15
Max hops :20
Remaining hops :20
Designated Root :32768.0.0000ABCD0000
Current root port :1
Current root cost :200000
Number of topology changes :1
Last topology changes time (sec.):22
Transmission limit :3
Path Cost Method :long

Eth 1/ 1 information

Admin status : enable
Role : root
State : forwarding
External path cost : 100000
Internal path cost : 100000
Priority : 128
Designated cost : 200000
Designated port : 128.24
Designated root : 32768.0.0000ABCD0000
Designated bridge : 32768.0.0030F1552000

```



```

Fast forwarding : disable
Forward transitions : 1
Admin edge port : enable
Oper edge port : disable
Admin Link type : auto
Oper Link type : point-to-point
Spanning Tree Status : enable
.
.
Console#

```

### 7.15.25 **show spanning-tree mst configuration**

This command shows the configuration of the multiple spanning tree.

#### **Command Mode**

Privileged Exec

#### **Example**

```

Console#show spanning-tree mst configuration
Mstp Configuration Information

Configuration name:00 30 f1 8f d5 50
Revision level:0

Instance VLANs

 1 2
Console#

```

## 7.16 Ethernet Automatic Protection Switching Commands

This section describes commands used to configure EAPS.

Table 86 EAPS Commands

| Command             | Function                                                | Mode | Page |
|---------------------|---------------------------------------------------------|------|------|
| <b>eaps domain</b>  | Creates an EAPS domain                                  | GC   | 826  |
| <b>mode</b>         | Configures master node or transit node                  | EAPS | 827  |
| <b>hellotime</b>    | Sets the interval at which to send health-check packets | EAPS | 828  |
| <b>failtime</b>     | Sets the time to wait for a health-check packet         | EAPS | 829  |
| <b>port</b>         | Sets port type on ring as primary or secondary          | EAPS | 830  |
| <b>control-vlan</b> | Adds a Control VLAN to an EAPS domain                   | EAPS | 831  |
| <b>protect-vlan</b> | Adds a Protected VLAN to an EAPS domain                 | EAPS | 833  |
| <b>enable</b>       | Activates an EAPS domain                                | EAPS | 834  |
| <b>eaps</b>         | Enables EAPS on the ECN330-switch                       | GC   | 835  |
| <b>show eaps</b>    | Displays status information for configured EAPS domains | PE   | 836  |

### Configuration Guidelines for EAPS

1. Create or delete an EAPS domain: Create or delete a domain using the **eaps domain** command (section 7.16.1 on page 826). The domain name is used as the index for this domain in the EAPS database. When deleting an EAPS Domain, first release the Control VLAN (CVLAN) and Protected VLANs configured on this domain (as described in step 5 and 6 below). If a port on the domain ring has not been added to another domain ring, this port will be reset to operate as a normal port. The database of this domain will then be cleared.
2. Define the EAPS mode of the ECN330-switch: After creating an EAPS domain, define the EAPS mode for this node using the **mode** command

(section 7.16.2 on page 827). Only one node can be defined as the master node on a domain ring, all the other ports should be defined as transit nodes.

3. Configure EAPS polling timers: Set the values of the polling timers the master node uses for the EAPS health-check packet that is circulated around the ring for an EAPS domain using the **hellotime** (section 7.16.3 on page 828) and **failtime** (section 7.16.4 on page 829) commands. The hello-timer is the periodic time at which the master sends a health-check packet, and the fail-time is the time the master waits to receive back a health-check packet from the other direction in the ring.
4. Configure the primary and secondary ports: Each node on the ring connects to it through two ring ports. Use the **port primary** command (section 7.16.5 on page 830) to configure one port as the primary port; and the **port secondary** command to configure the other as the secondary port.
5. Configure the EAPS Control VLAN (CVLAN): Use the **control vlan** command (section 7.16.6 on page 831) to create the VLAN used to pass ring integrity commands. The CVLAN is automatically assigned a QoS profile of Qp8 (with the QoS High priority setting). The CVLAN must NOT be configured with an IP address. In addition, only ring ports may be added to the CVLAN. No other ports can be members of this VLAN. Also, the ring ports of the CVLAN must be tagged. Failure to observe these restrictions can result in a loop in the network.

Note that the CVLAN must be cleared prior to deleting an EAPS Domain. Use the **no control vlan** command to release the CVLAN.

6. Configuring EAPS Protected VLANs (PVLAN): Use the **protect vlan** command (section 7.16.7 on page 833) to create the protected VLANs that carry normal traffic and are protected by the EAPS ring integrity mechanism. One EAPS domain can be assigned 10 VLANs – 1 control VLAN and 9 protected VLANs. The ring ports of a protected VLAN must be tagged. The protected VLANs will be blocked on the secondary port.

Note that the protected VLANs must be cleared prior to deleting an EAPS Domain. Use the **no protect vlan** command to release the Protected VLANs.

7. Enable or disable EAPS: Before enabling a domain as described in the next step, first use the **eaps** command (section 7.16.9 on page 835) to globally enable the EAPS function on the ECN330-switch. If EAPS has not yet been enabled or has been disabled with the **no eaps** command, no EAPS domains will work.

8. Enable or disable an EAPS domain: Before an EAPS domain can work, it must be enabled using the **enable** command (section 7.16.8 on page 834). When configuration is completed and the domain is enabled, it will start running on the ring. To stop a domain running on an ring, it can be disabled on any node using the **disable** command.
9. Unconfigure an EAPS ring port: Use the **no port primary** or **no port secondary** command (section 7.16.5 on page 830) to unconfigure an EAPS primary or secondary ring port for an EAPS domain.
10. Display EAPS status information: Use the **show eaps** command (section 7.16.10 on page 836) to display general EAPS status information or more detailed EAPS status information. The output displayed depends on whether the node is a transit node or a master node.

### 7.16.1 eaps domain

This command creates an EAPS domain and enters EAPS configuration mode for the specified domain. Use the **no** form to delete an EAPS domain.

#### Syntax

**[no] eaps domain <name>**

*name* - Name of a specific EAPS domain. (Range: 1-32 characters)

#### Default Setting

None

#### Command Mode

Global Configuration

#### Example

```
Console(config)#eaps domain r&d
Console(config-eaps)#
```

## Related Commands

**show eaps** (section 7.16.10 on page 836)

### 7.16.2 mode

This command configures the ECN330-switch as a master node or transit node on the ring. Use the **no** form to delete an EAPS domain.

#### Syntax

**mode {master | transit}**

- **master** - Configures the ECN330-switch as the master node of the EAPS domain. This node actively monitors ring integrity and sends health check and state change messages to transit nodes. Only one master node can be set for a domain.
- **transit** - Configures the ECN330-switch as a transit node in the EAPS domain. Transit nodes receive master control messages, detect ring topology changes, and send status messages to the master node.

#### Default Setting

None

#### Command Mode

EAPS Domain Configuration

#### Command Usage

- The master node is the control node of the EAPS domain.
- The transit node will receive control messages from the master node to synchronize the hello and fail timers. All other configuration parameters for a transit node should be configured to be the same as that the EAPS domain's master node.

## Example

```
Console(config-eaps)#mode master
Console(config-eaps)#
```

## Related Commands

**port** (section 7.16.5 on page 830)

### 7.16.3

## hellotime

This command sets the interval at which the master node sends health-check packets on the domain ring.

## Syntax

**hellotime** <*seconds*>

*seconds* - The interval at which the master node sends health-check packets. (Range: 1-3 seconds)

## Default Setting

1 second

## Command Mode

EAPS Domain Configuration

## Command Usage

The hello time should be set on the master node. Once set, the master node will send a health-check packet at the interval specified by this timer to all transit nodes. The transit nodes check for a health-check packet at the interval specified by the **failtime** command (section 7.16.4 on page 829).

## Example

```
Console(config-eaps)#hellotime 2
Console(config-eaps)#
```

## Related Commands

**failtime** (section 7.16.4 on page 829)

### 7.16.4

## failtime

This command sets the time the master node waits for a health-check packet before declaring a break in the ring.

## Syntax

**failtime** <*seconds*>

*seconds* - The interval at which the master node sends health-check packets. (Range: 3-9 seconds)

## Default Setting

3 seconds

## Command Mode

EAPS Domain Configuration

## Command Usage

- The fail time should be set on the master node. Once set, the master node will send the newly configured fail time to all transit nodes, forcing each node to update its fail timer. The transit nodes then check for a health-check packet at the interval specified by the fail time, and report a link down event to the master node if a health-check packet is not received during this interval.

- On transit nodes, the default value for the fail time can be used until receiving a control message from the master node to update their timers.

### Example

```
Console(config-eaps)#failtime 3
Console(config-eaps)#
```

### Related Commands

**hellotime** (section 7.16.3 on page 828)

## 7.16.5 port

This command sets the port type attached to the ring as primary or secondary. Each node must connect to the ring through two ports as part of the protection switching scheme – one port as the primary port and another as the secondary port. Use the **no** form to remove a primary or secondary port from the ring.

### Syntax

**port {primary | secondary} <port-number>**

**no port {primary | secondary}**

- **primary** - This port is open on the Protected VLAN and is used for passing both control messages and data traffic. The master node sends control messages from this port.
- **secondary** - This port is blocked on the Protected VLAN and is used only to receive control messages on the master node.
- **port-number** - Range: 1-27

### Default Setting

None



## Command Mode

### EAPS Domain Configuration

## Command Usage

- If the ring is complete, the master node prevents a loop by logically blocking all data traffic in the transmit and receive directions on its secondary port. If the master node subsequently detects a break in the ring, it unblocks its secondary port and allows data traffic to be transmitted and received through it.
- The primary port and secondary port must be removed from an EAPS domain with the **no port** command, before specifying a new primary or secondary port.

## Example

```
Console(config-eaps)#port primary 25
Console(config-eaps)#port secondary 26
Console(config-eaps)#
```

## 7.16.6

### control-vlan

This command adds a Control VLAN to an EAPS domain. The Control VLAN is used only to send and receive EAPS ring maintenance messages. Use the **no** form to clear the Control VLAN.

## Syntax

```
[no] control-vlan <vlan-id>
```

*vlan-id* - VLAN ID (Range: 1-4094, no leading zeroes)

## Default Setting

None

## Command Mode

### EAPS Domain Configuration

## Command Usage

- Only one Control VLAN can be configured in an EAPS domain. First create the VLAN to be used as the Control VLAN (**vlan**, section 7.17.3 on page 850), add the primary and secondary ring ports as tagged members to this VLAN (**switchport allowed vlan**, section 7.17.10 on page 861), and then use the **control-vlan** command to add the Control VLAN to the EAPS domain.
- The Control VLAN must not be configured with an IP address. In addition, only ring ports may be added to the Control VLAN. No other ports can be members of this VLAN. Also, the ring ports of the CVLAN must be tagged. Failure to observe these restrictions can result in a loop in the network.
- Once the domain has been activated with the **enable** command (section 7.16.8 on page 834), the configuration of the Control VLAN cannot be modified. Use the **no enable** command to stop the EAPS domain before making any configuration changes to this domain.

## Example

```
Console(config-eaps)#control-vlan 2
Console(config-eaps)#
```

## Related Commands

**protect-vlan** (section 7.16.7 on page 833)

## 7.16.7 protect-vlan

This command adds a Protected VLAN to an EAPS domain. Protected VLANs are used to send and receive data traffic on the EAPS ring. Use the **no** form to clear the Protected VLANs.

### Syntax

```
[no] protect-vlan <vlan-id>
```

*vlan-id* - VLAN ID (Range: 1-4094, no leading zeroes)

### Default Setting

None

### Command Mode

EAPS Domain Configuration

### Command Usage

- Up to nine Protected VLANs can be configured in an EAPS domain. First create the VLANs to be used as Protected VLANs (**vlan**, section 7.17.3 on page 850), add the primary and secondary ring ports as tagged members to this VLAN (**switchport allowed vlan**, section 7.17.10 on page 861), and then use the **protect-vlan** command to add the Protected VLAN to the EAPS domain.
- Once the domain has been activated with the **enable** command (section 7.16.8 on page 834), the configuration of the Protected VLAN cannot be modified. Use the **no enable** command to stop the EAPS domain before making any configuration changes to this domain.

### Example

```
Console(config-eaps)#protect-vlan 246
Console(config-eaps)#protect-vlan 247
Console(config-eaps)#protect-vlan 248
Console(config-eaps)#
```

## Related Commands

**control-vlan** (section 7.16.6 on page 831)

### 7.16.8 **enable**

This command enables an EAPS domain. Use the **no** form to disable the EAPS domain.

#### Syntax

**[no] enable**

#### Default Setting

Disabled

#### Command Mode

EAPS Domain Configuration

#### Command Usage

An EAPS domain containing one Control VLAN and one or more Protected VLANs must be enabled with the **enable** command, and the EAPS function enabled on the ECN330-switch with the **eaps** command (section 7.16.9 on page 835) before these domains start running on the ring. Once enabled, the master node and transit node state machines will start, and the domain will enter the active state.

#### Example

```
Console(config-eaps)#enable
Console(config-eaps)#
```

## Related Commands

**eaps** (section 7.16.9 on page 835)

## 7.16.9 eaps

This command enables EAPS on the ECN330-switch. Use the **no** form to disable EAPS.

### Syntax

**[no] eaps**

### Default Setting

Disabled

### Command Mode

Global Configuration

### Command Usage

An EAPS domain containing one Control VLAN and one or more Protected VLANs must be enabled with the **enable** command (section 7.16.8 on page 834), and the EAPS function enabled on the ECN330-switch with the **eaps** command before these domains start running on the ring. Once enabled, the master node and transit node state machines will start, and the domain will enter the active state.

### Example

```
Console(config)#eaps
Console(config)#
```

### Related Commands

**enable** (section 7.16.8 on page 834)

## 7.16.10 **show eaps**

This command displays status information for configured EAPS domains.

### Syntax

```
show eaps [<domain-name>]
```

*domain-name* - Name of a specific EAPS domain. (Range: 1-32 characters)

### Default Setting

None

### Command Mode

Privileged Exec

### Command Usage

- Enter the **show eaps** command without any argument to display a summary of status information for all configured EAPS domains.
- Enter the **show eaps** command followed by a domain name to display detailed status information for the specified domain.

### Example

This example displays a summary of all the EAPS domains configured on the ECN330-switch.

```
Console#show eaps
EAPS Enabled: Yes
Number of EAPS instances: 1
Domain r&d:
State Mode En PriPort SecPort CVID Vcount
Init M Y 25 26 2 1

Console#
```

Table 87 *show eaps - summary display description*

| Field                    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|--------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| EAPS Enabled             | Shows whether EAPS is enabled on the ECN330-switch.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Number of EAPS instances | Shows the number of EAPS instances configured on the ECN330-switch.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Domain                   | Displays the name of each domain followed by a brief list of status information                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| State                    | <p>Shows the following EAPS states:</p> <p><i>Master Node</i></p> <p><b>Idle</b> – The EAPS domain has been enabled, but the configuration is not complete.</p> <p><b>Init</b> – The EAPS domain has started but has not yet determined the status of the ring.</p> <p><b>Complete</b> – The ring is in the COMPLETE state for this EAPS domain.</p> <p><b>Failed</b> – There is a break in the ring for this EAPS domain.</p> <p><i>Transit Node</i></p> <p><b>Idle</b> – The EAPS domain has been enabled, but the configuration is not complete.</p> <p><b>Link-Up</b> – The EAPS domain is running, and both of its ports are up and in the FORWARDING state.</p> <p><b>Link-Down</b> – This EAPS domain is running, but one or both of its ports are down.</p> <p><b>Preforwarding</b> – This EAPS domain is running, and both of its ports are up, but the new link port is in a temporary BLOCKED state.</p> |
| Mode                     | Shows if the ECN330-switch is a master or transit node.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| En                       | Shows if the specified domain is enabled.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |

| Field   | Description                                         |
|---------|-----------------------------------------------------|
| PriPort | Shows the primary port.                             |
| SecPort | Shows the secondary port.                           |
| CVID    | Shows the Control VLAN ID.                          |
| Vcount  | Shows the number of Protected VLANs in this domain. |

This example displays detailed information for the specified EAPS domain.

```

Console#show eaps r&d
EAPS Enabled: Yes
Number of EAPS instances: 1
EAPSD-Bridge links: 2
 Name: r&d
 State: Init
 Enabled: Yes Mode: Master
 Primary port :25 Port status: Down
 secondary port :26 Port status: Down
 Hello Timer intervals: 2
 Fail Timer interval: 3
 Preforwarding Timer interval: 6
 EAPS Domain has following Control Vlan:
 Vlan Name VID
 [EAPS]2
 EAPS Domain has following Protected Vlan:
 Vlan Name VID
 [protect-vlan]3
 [V4]4
Console#

```



Table 88 *show eaps - detailed display description*

| Field                        | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| EAPS Enabled                 | Shows whether EAPS is enabled on the ECN330-switch.                                                                                                                                                                                                                                                                                                                                                                                                         |
| Number of EAPS instances     | Shows the number of EAPS instances configured on the ECN330-switch.                                                                                                                                                                                                                                                                                                                                                                                         |
| EAPSD-Bridge links           | The number of Protected VLANs configured on the EAPS domain.                                                                                                                                                                                                                                                                                                                                                                                                |
| Name                         | Displays the name of each domain followed by a brief list of status information                                                                                                                                                                                                                                                                                                                                                                             |
| State                        | See Table 87 on page 837.                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Enabled                      | Shows if the specified domain is enabled.                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Primary port                 | Shows the primary port.                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Secondary port               | Shows the secondary port.                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Hello Timer interval         | The interval at which the master node sends health-check packets on the domain ring.                                                                                                                                                                                                                                                                                                                                                                        |
| Fail Timer interval          | The time the master node waits for a health-check packet before declaring a break in the ring.                                                                                                                                                                                                                                                                                                                                                              |
| Preforwarding Timer interval | <p>This EAPS domain is running, and both ports on the transit node are up, but the new link port is in a temporary BLOCKED state.</p> <p>This delay is used by a transit node after receiving a message from the master node to bring the link up. This delay is used to ensure that the ring is stable and no more state change messages are being sent from the master node before changing the primary port on the transit node to forwarding state.</p> |
| Control Vlan                 | Shows the name and VLAN ID of the Control VLAN.                                                                                                                                                                                                                                                                                                                                                                                                             |
| Protected Vlan               | Shows the name and VLAN ID of Protected VLANs.                                                                                                                                                                                                                                                                                                                                                                                                              |

| Field  | Description                                             |
|--------|---------------------------------------------------------|
| Mode   | Shows if the ECN330-switch is a master or transit node. |
| CVID   | Shows the Control VLAN ID.                              |
| Vcount | Shows the number of Protected VLANs in this domain.     |

## 7.17 VLAN Commands

A VLAN is a group of ports that can be located anywhere in the network, but communicate as though they belong to the same physical segment. This section describes commands used to create VLAN groups, add port members, specify how VLAN tagging is used, and enable automatic VLAN registration for the selected interface.

*Table 89 VLAN Commands*

| Command Groups               | Function                                                                                                                              | Page |
|------------------------------|---------------------------------------------------------------------------------------------------------------------------------------|------|
| GVRP and Bridge Extension    | Configures GVRP settings that permit automatic VLAN learning; shows the configuration for bridge extension MIB                        | 842  |
| Editing VLAN Groups          | Sets up VLAN groups, including name, VID and state                                                                                    | 848  |
| Configuring VLAN Interfaces  | Configures VLAN interface parameters, including ingress and egress tagging mode, ingress filtering, PVID, and GVRP                    | 855  |
| Displaying VLAN Information  | Displays VLAN groups, status, port members, and MAC addresses                                                                         | 865  |
| Configuring Private VLANs    | Configures private VLANs, including uplink and downlink ports                                                                         | 868  |
| Configuring Protocol VLANs   | Configures protocol-based VLANs based on frame type and protocol                                                                      | 877  |
| Configuring 802.1Q Tunneling | Configures IEEE 802.1Q tunneling (QinQ) to segregate and preserve customer VLAN IDs for traffic crossing the service provider network | 882  |

### 7.17.1 GVRP and Bridge Extension Commands

GARP VLAN Registration Protocol defines a way for switches to exchange VLAN information in order to automatically register VLAN members on interfaces across the network. This section describes how to enable GVRP for individual interfaces and globally for the , as well as how to display default configuration settings for the Bridge Extension MIB.

---

---

#### Caution!

GVRP is included for future use only. It is recommended not to use GVRP in the EDA system.

---

---

Table 90 GVRP and Bridge Extension Commands

| Command                          | Function                                           | Mode   | Page |
|----------------------------------|----------------------------------------------------|--------|------|
| <b>bridge-ext gvrp</b>           | Enables GVRP globally for the ECN330-switch        | GC     | 843  |
| <b>show bridge-ext</b>           | Shows the global bridge extension configuration    | PE     | 843  |
| <b>switchport gvrp</b>           | Enables GVRP for an interface                      | IC     | 844  |
| <b>switchport forbidden vlan</b> | Configures forbidden VLANs for an interface        | IC     | 863  |
| <b>show gvrp configuration</b>   | Displays GVRP configuration for selected interface | NE, PE | 845  |
| <b>garp timer</b>                | Sets the GARP timer for the selected function      | IC     | 846  |
| <b>show garp timer</b>           | Shows the GARP timer for the selected function     | NE, PE | 847  |

### 7.17.1.1 **bridge-ext gvrp**

This command enables GVRP globally for the ECN330-switch. Use the **no** form to disable it.

#### **Syntax**

```
[no] bridge-ext gvrp
```

#### **Default Setting**

Disabled

#### **Command Mode**

Global Configuration

#### **Command Usage**

GVRP defines a way for switches to exchange VLAN information in order to register VLAN members on ports across the network. This function should be enabled to permit automatic VLAN registration, and to support VLANs which extend beyond the local switch.

#### **Example**

```
Console(config)#bridge-ext gvrp
Console(config)#
```

### 7.17.1.2 **show bridge-ext**

This command shows the configuration for bridge extension commands.

#### **Default Setting**

None

#### **Command Mode**

Privileged Exec

## Command Usage

See “Displaying Basic VLAN Information” on page 277 and “Displaying Bridge Extension Capabilities” on page 77 for a description of the displayed items.]

## Example

```
Console#show bridge-ext
 Max Support VLAN Numbers: 4094
 Max Support VLAN ID: 4094
 Extended Multicast Filtering Services: No
 Static Entry Individual Port: Yes
 VLAN Learning: IVL
 Configurable PVID Tagging: Yes
 Local VLAN Capable: No
 Traffic Classes: Enabled
 Global GVRP Status: Disabled
 GMRP: Disabled
Console#
```

### 7.17.1.3

## switchport gvrp

This command enables GVRP for a port. Use the **no** form to disable it.

## Syntax

```
[no] switchport gvrp
```

## Default Setting

Disabled

## Command Mode

Interface Configuration (Ethernet, Port Channel)

## Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport gvrp
Console(config-if)#
```

### 7.17.1.4 show gvrp configuration

This command shows if GVRP is enabled.

## Syntax

**show gvrp configuration** [*interface*]

*interface*

- **ethernet** *<unit>/<port>*
  - *unit* - This is device 1.
  - *port* - Physical port number on the ECN330 (Range: 1-28).
- **port-channel** *<channel-id>* - The assigned number of an aggregated link (Range: 1-13)

## Default Setting

Shows both global and interface-specific configuration.

## Command Mode

Normal Exec, Privileged Exec

## Example

```
Console#show gvrp configuration ethernet 1/7
Eth 1/ 7:
 Gvrp configuration: Disabled
Console#
```

### 7.17.1.5 **garp timer**

This command sets the values for the join, leave and leaveall timers. Use the **no** form to restore the timers' default values.

#### **Syntax**

```
garp timer {join | leave | leaveall} <timer_value>
```

```
no garp timer {join | leave | leaveall}
```

- **{join | leave | leaveall}** - Which timer to set.
- **timer\_value** - Value of timer.  
Ranges:  
join: 20-1000 centiseconds  
leave: 60-3000 centiseconds  
leaveall: 500-18000 centiseconds

#### **Default Setting**

- join: 20 centiseconds
- leave: 60 centiseconds
- leaveall: 1000 centiseconds

#### **Command Mode**

Interface Configuration (Ethernet, Port Channel)

#### **Command Usage**

- Group Address Registration Protocol is used by GVRP and GMRP to register or deregister client attributes for client services within a bridged LAN. The default values for the GARP timers are independent of the media access method or data rate. These values should not be changed unless there are difficulties with GMRP or GVRP registration or deregistration.
- Timer values are applied to GVRP for all the ports on all VLANs.



- Timer values must meet the following restrictions:
  - `leave`  $\geq$  (2 x `join`)
  - `leaveall`  $>$  `leave`

**Note:** Set GVRP timers on all Layer 2 devices connected in the same network to the same values. Otherwise, GVRP may not operate successfully.

### Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#garp timer join 100
Console(config-if)#
```

### Related Commands

**show garp timer** (section 7.17.1.6 on page 847)

#### 7.17.1.6

### show garp timer

This command shows the GARP timers for the selected interface.

### Syntax

**show garp timer** [*interface*]

*interface*

- **ethernet** *<unit>/<port>*
  - *unit* - This is device 1.
  - *port* - Physical port number on the ECN330 (Range: 1-28).
- **port-channel** *<channel-id>* - The assigned number of an aggregated link (Range: 1-13)

### Default Setting

Shows all GARP timers.

**Command Mode**

Normal Exec, Privileged Exec

**Example**

```
Console#show garp timer ethernet 1/1
Eth 1/ 1 GARP timer status:
 Join timer: 20 centiseconds
 Leave timer: 60 centiseconds
 Leaveall timer: 1000 centiseconds

Console#
```

**Related Commands**

**garp timer** (section 7.17.1.5 on page 846)

**Editing VLAN Groups**

This section describes commands used to configure VLANs on the ECN330-switch.

*Table 91    Commands for Editing VLAN Groups*

| Command                | Function                                                   | Mode | Page |
|------------------------|------------------------------------------------------------|------|------|
| <b>vlan database</b>   | Enters VLAN database mode to add, change, and delete VLANs | GC   | 849  |
| <b>vlan</b>            | Configures a VLAN, including VID, name and state           | VC   | 850  |
| <b>management vlan</b> | Configures the management VLANs                            | GC   | 851  |

## 7.17.2 **vlan database**

This command enters VLAN database mode. All commands in this mode will take effect immediately.

### **Default Setting**

None

### **Command Mode**

Global Configuration

### **Command Usage**

- Use the VLAN database command mode to add, modify, and delete VLANs. After finishing configuration changes, the VLAN settings can be displayed by entering the **show vlan** command.
- Use the **interface vlan** command mode to define the port membership mode and add or remove ports from a VLAN. The results of these commands are written to the running-configuration file, and this file can be displayed by entering the **show running-config** command.

### **Example**

```
Console(config)#vlan database
Console(config-vlan)#
```

### **Related Commands**

**show vlan** (section 7.17.13 on page 866)

### 7.17.3 **vlan**

This command configures a VLAN. Use the **no** form to restore the default settings or delete a VLAN.

#### **Syntax**

```
vlan <vlan-id> [name <vlan-name>] media ethernet [state
{active | suspend}]
```

```
no vlan <vlan-id> [name | state]
```

- **vlan-id** - ID of configured VLAN. (Range: 1-4094, no leading zeroes)
- **name** - Keyword to be followed by the VLAN name.
  - **vlan-name** - ASCII string from 1 to 32 characters.
- **media ethernet** - Ethernet media type.
- **state** - Keyword to be followed by the VLAN state.
  - **active** - VLAN is operational.
  - **suspend** - VLAN is suspended. Suspended VLANs do not pass packets.

#### **Default Setting**

By default only VLAN 1, 246-248, and 4093 exist and are active.

#### **Command Mode**

VLAN Database Configuration

#### **Command Usage**

- **no vlan** <vlan-id> deletes the VLAN.
- **no vlan** <vlan-id> **name** removes the VLAN name.
- **no vlan** <vlan-id> **state** returns the VLAN to the default state (that is, active).
- Up to 4094 VLANs can be configured on the ECN330-switch.

## Example

The following examples adds a VLAN, using VLAN ID 105 and name RD5 (the VLAN is activated by default), suspends the VLAN with ID 120, and deletes the VLAN with ID 95.

```
Console(config)#vlan database
Console(config-vlan)#vlan 105 name RD5 media ethernet
Console(config-vlan)#vlan 120 media ethernet state suspend
Console(config-vlan)#no vlan 95
Console(config-vlan)#
```

## Related Commands

**show vlan** (section 7.17.13 on page 866)

### 7.17.4 management vlan

This command configures the management VLANs for secure management access to the ECN330-switch. Use the **no** form to restore the default settings.

## Syntax

```
management vlan {internal | dynamic | external | native
| fsa} <vlan-id>
```

```
no management vlan {internal | dynamic | external |
unnamed}
```

- **internal** – Internal Management VLAN is the gateway for the embedded nodes (such as ECN330-switch, IP DSLAM, ESN108). By default, it is configured through DHCP with an internal IP address for the ECN330-switch.

Downlink ports(1-24) are configured automatically with the Internal Management VLAN ID (default 247).

- **dynamic** – Dynamic Management VLAN (DMV) ensures that embedded nodes will be automatically reconfigured if their configured management VLAN is not the same as the internal VLAN in the EAN (for example, if an IP DSLAM that was connected directly to the EDA network using VLAN id 247, is connected as an embedded node using VLAN id 248).

Any untagged traffic entering a downlink port is tagged with the Untagged VLAN ID (default 248). The embedded nodes can use untagged frames to get information about the used management VLAN.

For more information about the DMV, please refer the *Management VLAN Configuration Guide*. Note that the ECN330-switch does not have to be configured for the DMV. It automatically supports the DMV for all embedded nodes.

- **external** – External Management VLAN provides management access through the Gigabit Ethernet ports using tagged frames. This interface represents the EANA to the outside network. By default, it must be manually configured with an IP address for the ECN330-switch, using the same management VLAN as that used by the EDA network.

Uplink ports (25 - 27) are configured automatically with the External Management VLAN ID (default 246). Any untagged traffic entering an uplink port is tagged with VLAN ID 1 and silently dropped.

- **native** – Native Management VLAN is used internally to terminate untagged traffic passed from or to the SBC (for example, when using a QinQ tunnel).
- **fsa** – FSA Management VLAN provides management access through the Fast Ethernet ports using tagged frames.
- **vlan-id** – ID of configured VLAN. (Range: 1-4094, no leading zeroes)

### Default Setting

- **internal** – VID: 247; Members: 1-24, 28 tagged
- **dynamic** – VID: 248; Members: 1-24 untagged, 28 tagged
- **native** – VID: 4093; Members: 28 untagged
- **external** – VID: 246; Members: 25-28 tagged
- **fsa** – VID: 249; Members: 1-24, 28 tagged

### Command Mode

#### Global Configuration

## Command Usage

- Management VLANs can be defined for secure management access to the ECN330-switch. Only IP addresses assigned to these management VLANs can be used to manage the ECN330-switch.

The default management VLANs assigned to the switch are described under “Enabling the SBC to Access Advanced Management Tools” on page 74.

- The management VLAN applies to management access through the web, Telnet, SSH, and SNMP.
- There may be one or more management VLANs on the ECN330-switch, depending on whether the switch is set the ECN330 mode or ECN330-switch mode (see section 7.5.12 on page 557).
- When a management VLAN is defined, IP addresses assigned to other non-management VLAN interfaces cannot be used for management access. When no management VLAN is defined, the ECN330-switch can be managed through any IP address assigned to any VLAN interface.
- Management VLANs operate as an isolated VLAN. Data traffic is not routed to or from other VLANs, routing protocols cannot be enabled on these interfaces, nor is the management IP interface advertised by routing protocols to other routers.
- A management VLAN cannot be deleted when a IP address is assigned to the interface.
- To change one of the management VLANs, first use the **vlan** command (section 7.17.3 on page 850) to set up a new VLAN without naming it, use the **switchport allowed vlan** command (section 7.17.10 on page 861) to add the required port members as tagged or untagged, use the **management vlan** command to remove the current management VLAN, and then configure the newly created VLAN as the new management VLAN.

## Example

This example shows how to change a management VLAN. First set up a new VLAN with the required port members (without naming the VLAN), remove the current FSA management VLAN, and then configure the newly configured VLAN as the new FSA management VLAN.

```
Console#configure
Console(config)#vlan database
Console(config-vlan)#vlan 349 media ethernet state active
Console(config)#exit
Console(config)#interface ethernet 1/1
Console(config-if)#switchport allowed vlan add 349 tagged
.
.
.
Console(config)#exit
Console(config)#interface ethernet 1/24
Console(config-if)#switchport allowed vlan add 349 tagged
Console(config)#exit
Console(config)#interface ethernet 1/28
Console(config-if)#switchport allowed vlan add 349 tagged
Console(config)#exit
Console(config)#no management vlan fsa
Console(config)#management vlan fsa 349
Console#show management vlan
Current Internal Management VLAN: 247
Current Dynamic Management VLAN: 248
Current External Management VLAN: 246
Current Native Management VLAN: 4093
Current FSA Management VLAN: 349
Console#
```

## Related Commands

**show management vlan** (section 7.17.15 on page 868)



## Configuring VLAN Interfaces

This section describes commands used to configure VLAN interfaces on the ECN330-switch.

*Table 92 Commands for Configuring VLAN Interfaces*

| Command                                  | Function                                                 | Mode | Page |
|------------------------------------------|----------------------------------------------------------|------|------|
| <b>interface vlan</b>                    | Enters interface configuration mode for a specified VLAN | IC   | 856  |
| <b>switchport mode</b>                   | Configures VLAN membership mode for an interface         | IC   | 857  |
| <b>switchport acceptable-frame-types</b> | Configures frame types to be accepted by an interface    | IC   | 858  |
| <b>switchport ingress-filtering</b>      | Enables ingress filtering on an interface                | IC   | 859  |
| <b>switchport native vlan</b>            | Configures the PVID (native VLAN) of an interface        | IC   | 860  |
| <b>switchport allowed vlan</b>           | Configures the VLANs associated with an interface        | IC   | 861  |
| <b>switchport gvrp</b>                   | Enables GVRP for an interface                            | IC   | 844  |
| <b>switchport forbidden vlan</b>         | Configures forbidden VLANs for an interface              | IC   | 863  |
| <b>mac-address</b>                       | Configures the MAC address of a VLAN                     | IC   | 864  |

## 7.17.5 interface vlan

This command enters interface configuration mode for VLANs, which is used to configure a physical interface.

### Syntax

```
interface vlan <vlan-id>
```

*vlan-id* - ID of the configured VLAN. (Range: 1-4094, no leading zeroes)

### Default Setting

None

### Command Mode

Global Configuration

### Example

The following example shows how to set the interface configuration mode to VLAN 1, and then assign an IP address to the VLAN:

```
Console(config)#interface vlan 246
Console(config-if)#ip address 192.168.1.254 255.255.255.0
Console(config-if)#
```

### Related Commands

**shutdown** (section 7.9.8 on page 746)

## 7.17.6 switchport mode

This command configures the VLAN membership mode for a port. Use the **no** form to restore the default.

### Syntax

```
switchport mode {hybrid | trunk | private-vlan |
dot1q-tunnel}
```

```
no switchport mode
```

- **hybrid** - Specifies a hybrid VLAN interface. The port may transmit tagged or untagged frames.
- **trunk** - Specifies a port as an end-point for a VLAN trunk. A trunk is a direct link between two switches, so the port transmits tagged frames that identify the source VLAN. However, note that frames belonging to the port's default VLAN (that is, associated with the PVID) are also transmitted as tagged frames.
- **private-vlan** - For an explanation of this command see section 7.17.18 on page 873.
- **dot1q-tunnel** - For an explanation of this command see section on page 882.

### Default Setting

All ports are in hybrid mode.

### Command Mode

Interface Configuration (Ethernet, Port Channel)

### Example

The following shows how to set the configuration mode to port 1, and then set the switchport mode to hybrid:

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport mode hybrid
Console(config-if)#
```

## Related Commands

**switchport acceptable-frame-types** (section 7.17.7 on page 858)

### 7.17.7 switchport acceptable-frame-types

This command configures the acceptable frame types for a port. Use the **no** form to restore the default.

#### Syntax

```
switchport acceptable-frame-types {all | tagged}
```

```
no switchport acceptable-frame-types
```

- **all** - The port accepts all frames, tagged or untagged.
- **tagged** - The port only passes tagged frames.

#### Default Setting

All frame types

#### Command Mode

Interface Configuration (Ethernet, Port Channel)

#### Command Usage

When set to receive all frame types, any received frames that are untagged are assigned to the default VLAN.

#### Example

The following example shows how to restrict the traffic passed on port 1 to tagged frames:

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport acceptable-frame-types tagged
Console(config-if)#
```

## Related Commands

**switchport mode** (section 7.17.6 on page 857)

### 7.17.8 switchport ingress-filtering

This command enables ingress filtering for an interface. Use the **no** form to restore the default.

#### Syntax

**[no] switchport ingress-filtering**

#### Default Setting

Enabled

#### Command Mode

Interface Configuration (Ethernet, Port Channel)

#### Command Usage

- Ingress filtering only affects tagged frames.
- If ingress filtering is disabled and a port receives frames tagged for VLANs for which it is not a member, these frames will be flooded to all other ports (except for those VLANs explicitly forbidden on this port).
- If ingress filtering is enabled and a port receives frames tagged for VLANs for which it is not a member, these frames will be discarded.
- Ingress filtering does not affect VLAN independent BPDU frames, such as GVRP or STA. However, they do affect VLAN dependent BPDU frames, such as GMRP.

## Example

The following example shows how to set the interface to port 1 and then enable ingress filtering:

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport ingress-filtering
Console(config-if)#
```

### 7.17.9 switchport native vlan

This command configures the Port VLAN ID (PVID, that is, the default VLAN ID) for a port. Use the **no** form to restore the default.

#### Syntax

```
switchport native vlan <vlan-id>
```

```
no switchport native vlan
```

*vlan-id* - Default VLAN ID for a port. (Range: 1-4094, no leading zeroes)

#### Default Setting

VLAN 1

#### Command Mode

Interface Configuration (Ethernet, Port Channel)

#### Command Usage

- If an interface is not a member of VLAN 1 and its PVID is assigned to this VLAN, the interface will automatically be added to VLAN 1 as an untagged member. For all other VLANs, an interface must first be configured as an untagged member before its PVID can be assigned to that group.

- If acceptable frame types is set to **a11** or switchport mode is set to **hybrid**, the PVID will be inserted into all untagged frames entering the ingress port.

### Example

The following example shows how to set the PVID for port 1 to VLAN 3:

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport native vlan 3
Console(config-if)#
```

## 7.17.10 switchport allowed vlan

This command configures VLAN groups on the selected interface. Use the **no** form to restore the default.

### Syntax

```
switchport allowed vlan {add <vlan-list> [tagged |
 untagged] | remove <vlan-list>}
```

```
no switchport allowed vlan
```

- **add <vlan-list>** - List of VLAN identifiers to add.
- **remove <vlan-list>** - List of VLAN identifiers to remove.
- **vlan-list** - Separate nonconsecutive VLAN identifiers with a comma and no spaces; use a hyphen to designate a range of IDs. Do not enter leading zeros. (Range: 1-4094).

### Default Setting

All ports are assigned to VLAN 247 (untagged) and 248 (tagged) by default. The default frame type is untagged.

### Command Mode

Interface Configuration (Ethernet, Port Channel)

## Command Usage

- A port, or a trunk with switchport mode set to **hybrid**, must be assigned to at least one VLAN as untagged.
- If a trunk has switchport mode set to **trunk** (that is, 1Q Trunk), an interface can only be assigned to VLAN groups as a tagged member.
- Frames are always tagged within the ECN330-switch. The tagged or untagged parameter used when adding a VLAN to an interface tells the ECN330-switch whether to keep or remove the tag from a frame on egress.
- If none of the intermediate network devices nor the host at the other end of the connection supports VLANs, the interface should be added to these VLANs as an untagged member. Otherwise, it is only necessary to add at most one VLAN as untagged, and this should correspond to the native VLAN for the interface.
- If a VLAN on the forbidden list for an interface is manually added to that interface, the VLAN is automatically removed from the forbidden list for that interface.

## Example

The following example shows how to add VLANs 1, 2, 5 and 6 to the allowed list as tagged VLANs for port 1:

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport allowed vlan add 1,2,5,6 tagged
Console(config-if)#
```



### 7.17.11 **switchport forbidden vlan**

This command configures forbidden VLANs. Use the **no** form to remove the list of forbidden VLANs.

#### **Syntax**

```
switchport forbidden vlan {add <vlan-list> | remove
 <vlan-list>}
```

```
no switchport forbidden vlan
```

- **add <vlan-list>** - List of VLAN identifiers to add.
- **remove <vlan-list>** - List of VLAN identifiers to remove.
- **vlan-list** - Separate nonconsecutive VLAN identifiers with a comma and no spaces; use a hyphen to designate a range of IDs. Do not enter leading zeros. (Range: 1-4094).

#### **Default Setting**

No VLANs are included in the forbidden list.

#### **Command Mode**

Interface Configuration (Ethernet, Port Channel)

#### **Command Usage**

- This command prevents a VLAN from being automatically added to the specified interface through GVRP.
- If a VLAN has been added to the set of allowed VLANs for an interface, it cannot be added to the set of forbidden VLANs for that same interface.

## Example

The following example shows how to prevent port 1 from being added to VLAN 3:

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport forbidden vlan add 3
Console(config-if)#
```

### 7.17.12 mac-address

This command configures the MAC address of a VLAN. Use the **no** form to reset the MAC address to the default setting.

#### Syntax

**mac-address** <mac-address>

**no mac-address**

- *mac-address* - MAC address of the selected VLAN.  
(Format examples: 00-01-02-03-0d-0e or 000102030d0e)

#### Default Setting

MAC address of the ECN330-switch.

#### Command Mode

Interface Configuration (VLAN)

#### Command Usage

- It may be necessary to configure a unique MAC address for a VLAN to ensure proper operation of service provider applications, or to simplify troubleshooting.
- After configuring a MAC address for a VLAN, all Layer 3 traffic originating from this VLAN will use the specified MAC address.

- MAC addresses used for VLANs have the following restrictions:
  - Cannot be a broadcast MAC address.
  - Cannot be a multicast MAC address.
  - Cannot be a MAC address or all zeroes.

### Example

The following example sets the MAC address for VLAN 3:

```
Console(config)#interface vlan 3
Console(config-if)#mac-address 00-01-02-03-0d-0e
Console(config-if)#
```

### Related Commands

**show vlan mac-address** (section 7.17.14 on page 867)

## Displaying VLAN Information

This section describes commands used to display VLAN information.

*Table 93 Commands for Displaying VLAN Information*

| Command                            | Function                                                           | Mode   | Page |
|------------------------------------|--------------------------------------------------------------------|--------|------|
| <b>show vlan</b>                   | Shows VLAN information                                             | NE, PE | 866  |
| <b>show vlan mac-address</b>       | Displays the MAC address for VLANs                                 | PE     | 867  |
| <b>show management vlan</b>        | Displays the current management VLAN settings                      | PE     | 868  |
| <b>show interfaces status vlan</b> | Displays status for the specified VLAN interface                   | NE, PE | 749  |
| <b>show interfaces switchport</b>  | Displays the administrative and operational status of an interface | NE, PE | 753  |

### 7.17.13 **show vlan**

This command shows VLAN information.

#### **Syntax**

```
show vlan [id <vlan-id> | name <vlan-name>]
```

- **id** - Keyword to be followed by the VLAN ID.
- **vlan-id** - ID of the configured VLAN. (Range: 1-4094, no leading zeroes)
- **name** - Keyword to be followed by the VLAN name.
- **vlan-name** - ASCII string from 1 to 32 characters.

#### **Default Setting**

Shows all VLANs.

#### **Command Mode**

Normal Exec, Privileged Exec

#### **Example**

The following example shows how to display information for VLAN 1:

```
Console#show vlan id 1
VLAN Type Name Status Ports/Channel groups

 1 Static DefaultVlan Active Eth1/ 1 Eth1/ 2 Eth1/ 3 Eth1/ 4 Eth1/ 5
 Eth1/ 6 Eth1/ 7 Eth1/ 8 Eth1/ 9 Eth1/10
 Eth1/11 Eth1/12
Console#
```

## 7.17.14 show vlan mac-address

This command displays the MAC address for VLANs.

### Syntax

```
show vlan [id <vlan-id> | name <vlan-name>]
```

- **id** - Keyword to be followed by the VLAN ID.
- **vlan-id** - ID of the configured VLAN. (Range: 1-4094, no leading zeroes)
- **name** - Keyword to be followed by the VLAN name.
- **vlan-name** - ASCII string from 1 to 32 characters.

### Default Setting

Shows the MAC address for all configured VLANs.

### Command Mode

Privileged Exec

### Example

The following example shows how to display the MAC address for all VLANs:

```
Console#show vlan mac-address
VLAN MAC Address Status Type Name

1 00-01-02-03-0D-0E Active Static DefaultVlan
246 00-00-12-33-89-76 Active Static extmgm
247 00-00-12-33-89-76 Active Static intmgm
248 00-00-12-33-89-76 Active Static dynvlan
249 00-00-12-33-89-76 Active Static fsavlan
4093 00-00-12-33-89-76 Active Static intuntag
Console#
```

### 7.17.15 **show management vlan**

This command displays the current management VLAN settings.

#### **Command Mode**

Privileged Exec

#### **Example**

```
Console#show management vlan
Current Internal Management VLAN: 247
Current Dynamic Management VLAN: 248
Current External Management VLAN: 246
Current Native Management VLAN: 4093
Current FSA Management VLAN: 249
Console#
```

## Configuring Private VLANs

This section describes commands used to configure private VLANs.

*Table 94 Private VLAN Commands*

| Command                                  | Function                                               | Mode | Page |
|------------------------------------------|--------------------------------------------------------|------|------|
| <i>Edit Private VLAN Groups</i>          |                                                        |      |      |
| <b>private-vlan</b>                      | Adds or deletes primary or isolated VLANs              | VC   | 870  |
| <b>private-vlan association</b>          | Associates an isolated VLAN with a primary VLAN        | VC   | 871  |
| <i>Configure Private VLAN Interfaces</i> |                                                        |      |      |
| <b>switchport mode private-vlan</b>      | Sets an interface to promiscuous mode or isolated mode | IC   | 873  |
| <b>switchport private-vlan mapping</b>   | Maps an interface to a primary VLAN                    | IC   | 874  |

| Command                                                 | Function                                      | Mode   | Page |
|---------------------------------------------------------|-----------------------------------------------|--------|------|
| <b>switchport<br/>private-vlan<br/>host-association</b> | Associates an interface with an isolated VLAN | IC     | 875  |
| <i>Display Private VLAN Information</i>                 |                                               |        |      |
| <b>show vlan<br/>private-vlan</b>                       | Shows private VLAN information                | NE, PE | 876  |

To configure primary/secondary associated groups, follow these steps:

1. Use the **private-vlan** command (section 7.17.16 on page 870) to designate the primary VLAN that will be used to channel traffic outside of the isolated VLAN(s), and one or more isolated VLANs.
2. Use the **private-vlan association** command (section 7.17.17 on page 871) to map the isolated VLAN(s) to a primary VLAN.
3. Use the **switchport mode private-vlan** command (section 7.17.18 on page 873) to configure one or more promiscuous port (that is, having access to all ports in the primary VLAN and all ports in the associated isolated VLANs), and one or more isolated ports.

Note that a promiscuous port can join a normal VLAN, but at most be mapped to one primary VLAN. Because private VLAN ports can belong to a normal VLAN and private VLAN concurrently, the native VLAN of a private port will not automatically change to the private VLAN when executing the **switchport private-vlan mapping** or **switchport private-vlan host-association** commands described in the following steps.

4. Use the **switchport private-vlan mapping** command (section 7.17.19 on page 874) to assign a promiscuous port to a primary VLAN.
5. Use the **switchport private-vlan host-association** command (section 7.17.20 on page 875) to assign an isolated port to an isolated VLAN.
6. Private VLANs can support tagged or untagged members. Use the **switchport allowed vlan** command (section 7.17.10 on page 861) to specify tagged or untagged members.
7. Use the **show vlan private-vlan** command (section 7.17.21 on page 876) to verify the configuration settings.

## 7.17.16 private-vlan

This command creates a primary or isolated private VLAN. Use the **no** form to remove the specified private VLAN.

### Syntax

```
private-vlan <vlan-id> {primary | isolated}
```

```
no private-vlan <vlan-id>
```

- **vlan-id** – ID of private VLAN. (Range: 1-4094, no leading zeroes).
- **primary** – Specifies a primary VLAN which contains one or more promiscuous ports, and serves to channel traffic between associated isolated VLANs and other locations.
- **isolated** – Specifies an isolated VLAN. Ports assigned to an isolated VLAN cannot directly communicate with other isolated port members, and can only communicate with promiscuous ports in the associated primary VLAN.

### Default Setting

None

### Command Mode

VLAN Configuration

### Command Usage

- Private VLANs restrict traffic to ports within isolated VLANs, and channel traffic passing outside the isolated VLAN through promiscuous ports in the associated primary VLAN. When using isolated VLANs, they must be mapped to an associated “primary” VLAN that contains promiscuous ports.
- Port membership for private VLANs is static. Once a port has been assigned to a private VLAN, it cannot be dynamically moved to another VLAN via GVRP.



- Private VLAN ports cannot be set to trunked mode. (See the **switchport mode** command, section 7.17.6 on page 857.)

### Example

```
Console(config)#vlan database
Console(config-vlan)#private-vlan 2 primary
Console(config-vlan)#private-vlan 3 isolated
Console(config-vlan)#private-vlan 4 isolated
Console(config)#
```

### Related Commands

**private vlan association** (section 7.17.17 on page 871)

## 7.17.17 private vlan association

This command associates a primary VLAN with an isolated VLAN. Use the **no** form to remove all associations for the specified primary VLAN.

### Syntax

```
private-vlan <primary-vlan-id> association {<isolated-
vlan-id> | add <isolated-vlan-id> | remove
<isolated-vlan-id>}
```

```
no private-vlan <primary-vlan-id> association
```

- *primary-vlan-id* – ID of primary VLAN. (Range: 1-4094, no leading zeroes).
- *isolated-vlan-id* – ID of isolated VLAN. (Range: 1-4094, no leading zeroes).

### Default Setting

None

### Command Mode

VLAN Configuration

## Command Usage

- Isolated VLANs provide security for group members. The associated primary VLAN provides a common interface for access to other network resources within the primary VLAN (for example, servers configured with promiscuous ports) and to resources outside of the primary VLAN (via promiscuous ports).
- When an isolated VLAN is associated with a primary VLAN (see **private vlan association**, section 7.17.17 on page 871), the ports associated with the isolated VLAN (see **switchport private-vlan host-association**, section 7.17.20 on page 875) automatically join the primary VLAN, and the ports mapped to the primary VLAN (see **switchport private-vlan mapping**, section 7.17.19 on page 874) automatically join the isolated VLAN. Even though these ports are added to both the primary and isolated VLANs for software processing, this does not affect the basic relationship between isolated and promiscuous ports described in the previous sections.

## Example

```
Console(config-vlan)#private-vlan 2 association 3
Console(config-vlan)#private-vlan 2 association 4
Console(config)#
```

## Related Commands

**private-vlan** (section 7.17.16 on page 870)

### 7.17.18 **switchport mode private-vlan**

This command sets the private VLAN mode for an interface. Use the **no** form to restore the default setting.

#### **Syntax**

```
switchport mode private-vlan {promiscuous | isolated}
```

```
no switchport mode private-vlan
```

- **promiscuous** – This port type can communicate with all other promiscuous ports in the same primary VLAN, as well as with all the ports in the associated isolated VLANs.
- **isolated** – This port type can subsequently be assigned to an isolated VLAN.

#### **Default Setting**

Normal VLAN

#### **Command Mode**

Interface Configuration (Ethernet, Port Channel)

#### **Command Usage**

- To assign a promiscuous port to a primary VLAN, use the **switchport private-vlan mapping** command (section 7.17.19 on page 874). To assign an isolated port to an isolated VLAN, use the **private-vlan host association** command (section 7.17.20 on page 875).
- Use the **no switchport mode private-vlan** command to restore a interface to normal mode.

## Example

```
Console(config)#interface ethernet 1/2
Console(config-if)#switchport mode private-vlan promiscuous
Console(config-if)#exit
Console(config)#interface ethernet 1/3
Console(config-if)#switchport mode private-vlan isolated
Console(config-if)#exit
Console(config)#interface ethernet 1/4
Console(config-if)#switchport mode private-vlan isolated
Console(config-if)#
```

### 7.17.19 switchport private-vlan mapping

This command maps an promiscuous interface to a primary VLAN. Use the **no** form to remove this mapping.

#### Syntax

**switchport private-vlan mapping** *<primary-vlan-id>*

**no switchport private-vlan mapping**

*primary-vlan-id* – ID of primary VLAN. (Range: 1-4094, no leading zeroes).

#### Default Setting

None

#### Command Mode

Interface Configuration (Ethernet, Port Channel)

#### Command Usage

- The interface mapped to a primary VLAN must first be configured as a promiscuous port using the **switchport mode private-vlan** (section 7.17.18 on page 873).

- Promiscuous ports assigned to a primary VLAN can communicate with any other promiscuous ports in the same VLAN, and with the group members within any associated isolated VLANs.

### Example

```
Console(config)#interface ethernet 1/2
Console(config-if)#switchport private-vlan mapping 2
Console(config-if)#
```

## 7.17.20 switchport private-vlan host-association

This command associates an isolated interface with an isolated VLAN. Use the **no** form to remove this association.

### Syntax

```
switchport private-vlan host-association
 <isolated-vlan-id>
```

```
no switchport private-vlan host-association
```

*isolated-vlan-id* – ID of secondary (that is, community) VLAN.  
(Range: 1-4094, no leading zeroes).

### Default Setting

None

### Command Mode

Interface Configuration (Ethernet, Port Channel)

### Command Usage

- The interface mapped to an isolated VLAN must first be configured as an isolated port using the **switchport mode private-vlan** (section 7.17.18 on page 873).

- Ports assigned to an isolated VLAN cannot pass traffic between group members, and can only communicate with resources outside of the group via promiscuous ports in the associated primary VLAN.

### Example

```
Console(config)#interface ethernet 1/3
Console(config-if)#switchport private-vlan host-association 3
Console(config-if)#
```

## 7.17.21 show vlan private-vlan

This command shows the private VLAN configuration settings on the ECN330-switch.

### Syntax

```
show vlan private-vlan [primary | isolated]
```

- **primary** – Displays all primary VLANs, along with any assigned promiscuous interfaces.
- **isolated** – Displays all isolated VLANs, along with the associated primary VLAN, and any assigned isolated interfaces.

### Default Setting

None

### Command Mode

Privileged Executive

### Example

```

Console#show vlan private-vlan
Primary Secondary Type Interfaces

 2 Primary Eth1/ 2 Eth1/ 3
 2 3 Isolated Eth1/ 4
 2 4 Isolated Eth1/ 5
Console#

```

## Configuring Protocol-based VLANs

The network devices required to support multiple protocols cannot be easily grouped into a common VLAN. This may require non-standard devices to pass traffic between different VLANs in order to encompass all the devices participating in a specific protocol. This kind of configuration deprives users of the basic benefits of VLANs, including security and easy accessibility.

To avoid these problems, configure the ECN330-switch with protocol-based VLANs that divide the physical network into logical VLAN groups for each required protocol. When a frame is received at a port, its VLAN membership can then be determined based on the protocol type in use by the inbound packets.

Table 95 Protocol-based VLAN Commands

| Command                                                     | Function                                                                   | Mode | Page |
|-------------------------------------------------------------|----------------------------------------------------------------------------|------|------|
| <b>protocol-vlan<br/>protocol-group</b>                     | Create a protocol group, specifying the supported protocols                | GC   | 878  |
| <b>protocol-vlan<br/>protocol-group</b>                     | Maps a protocol group to a VLAN                                            | IC   | 879  |
| <b>show protocol-<br/>vlan protocol-<br/>group</b>          | Shows the configuration of protocol groups                                 | PE   | 880  |
| <b>show interfaces<br/>protocol-vlan<br/>protocol-group</b> | Shows the interfaces mapped to a protocol group and the corresponding VLAN | PE   | 881  |

To configure protocol-based VLANs, follow these steps:

1. First configure VLAN groups for the required protocols (page 850). Although not mandatory, it is suggested to configure a separate VLAN for each major protocol running on the network. Do not add port members at this time.
2. Create a protocol group for each of the protocols assigned to a VLAN using the **protocol-vlan protocol-group** command (General Configuration mode).
3. Then map the protocol for each interface to the appropriate VLAN using the **protocol-vlan protocol-group** command (Interface Configuration mode).

### 7.17.22 protocol-vlan protocol-group (Configuring Groups)

This command creates a protocol group, or to add specific protocols to a group. Use the **no** form to remove a protocol group.

#### Syntax

```
protocol-vlan protocol-group <group-id> [{add | remove}
 frame-type <frame> protocol-type <protocol>]
```

```
no protocol-vlan protocol-group <group-id>
```

- *group-id* - Group identifier of this protocol group. (Range: 1-2147483647)
- *frame* - Frame type used by this protocol. (Options: ethernet, rfc\_1042, llc\_other)

**Note:** SNAP frame types are not supported due to hardware limitations.

- *protocol* - Protocol type. The only option for the llc\_other frame type is ipx\_raw. The options for all other frames types include: ip, arp, rarp.

#### Default Setting

No protocol groups are configured.



## Command Mode

Global Configuration

### Example

The following creates protocol group 1, and specifies Ethernet frames with IP and ARP protocol types:

```
Console(config)#protocol-vlan protocol-group 1 add frame-type
 ethernet protocol-type ip
Console(config)#protocol-vlan protocol-group 1 add frame-type
 ethernet protocol-type arp
Console(config)#
```

## 7.17.23 protocol-vlan protocol-group (Configuring Interfaces)

This command maps a protocol group to a VLAN for the current interface. Use the **no** form to remove the protocol mapping for this interface.

### Syntax

**protocol-vlan protocol-group <group-id> vlan <vlan-id>**

**no protocol-vlan protocol-group <group-id> vlan**

- **group-id** - Group identifier of this protocol group. (Range: 1-2147483647)
- **vlan-id** - VLAN to which matching protocol traffic is forwarded. (Range: 1-4094)

### Default Setting

No protocol groups are mapped for any interface.

## Command Mode

Interface Configuration (Ethernet, Port Channel)

## Command Usage

- When creating a protocol-based VLAN, only assign interfaces through this command. If interfaces are assigned using any of the other VLAN commands (such as **vlan** on page 850), these interfaces will admit traffic of any protocol type into the associated VLAN.
- When a frame enters a port that has been assigned to a protocol VLAN, it is processed in the following manner:
  - If the frame is tagged, it will be processed according to the standard rules applied to tagged frames.
  - If the frame is untagged and the protocol type matches, the frame is forwarded to the appropriate VLAN.
  - If the frame is untagged but the protocol type does not match, the frame is forwarded to the default VLAN for this interface.

## Example

The following example maps the traffic entering Port 1 which matches the protocol type specified in protocol group 1 to VLAN 2.

```
Console(config)#interface ethernet 1/1
Console(config-if)#protocol-vlan protocol-group 1 vlan 2
Console(config-if)#
```

### 7.17.24 show protocol-vlan protocol-group

This command shows the frame and protocol type associated with protocol groups.

## Syntax

**show protocol-vlan protocol-group [group-id]**

*group-id* - Group identifier for a protocol group. (Range: 1-2147483647)

## Default Setting

All protocol groups are displayed.

## Command Mode

Privileged Exec

## Example

This shows protocol group 1 configured for IP over Ethernet:

```

Console#show protocol-vlan protocol-group

ProtocolGroup ID Frame Type Protocol Type

 1 ethernet 08 00
Console#

```

## 7.17.25

## show interfaces protocol-vlan protocol-group

This command shows the mapping from protocol groups to VLANs for the selected interfaces.

## Syntax

**show interfaces protocol-vlan protocol-group** [*interface*]

*interface*

- **ethernet** *unit/port*
  - *unit* - This is device 1.
  - *port* - Port number.
- **port-channel** <*channel-id*> (Range: 1-13)

## Default Setting

The mapping for all interfaces is displayed.

## Command Mode

Privileged Exec

## Example

This shows that traffic entering Port 1 that matches the specifications for protocol group 1 will be mapped to VLAN 2:

```

Console#show interfaces protocol-vlan protocol-group

 Port ProtocolGroup ID VLAN ID

 Eth 1/1 1 vlan2
Console#

```

## Configuring IEEE 802.1Q Tunneling

This section describes commands used to configure QinQ tunneling.

*Table 96 IEEE 802.1Q Tunneling Commands*

| Command                             | Function                                                                                                   | Mode | Page |
|-------------------------------------|------------------------------------------------------------------------------------------------------------|------|------|
| <b>system mode</b>                  | Configures the ECN330-switch to operate in normal mode, QinQ mode, or L2MPLS mode                          | PE   | 552  |
| <b>show system mode</b>             | Displays the ECN330-switch system mode                                                                     | PE   | 553  |
| <b>switchport mode dot1q-tunnel</b> | Configures an interface as a QinQ tunnel port                                                              | IC   | 884  |
| <b>show dot1q-tunnel</b>            | Displays information about QinQ tunnel ports                                                               | PE   | 885  |
| <b>switchport dot1q-ethertype</b>   | Sets the Tag Protocol Identifier (TPID) value of a tunnel port                                             | IC   | 885  |
| <b>address-monitor qinq</b>         | Forwards traffic for the internal management VLANs (VIDs 247-249) between the QinQ tunnel port and the SBC | IC   | 887  |

| Command                | Function                                                                          | Mode | Page |
|------------------------|-----------------------------------------------------------------------------------|------|------|
| <b>switchport mtu</b>  | Sets the maximum transfer unit for an interface                                   | IC   | 889  |
| <b>system mtu</b>      | Sets the maximum transfer unit for the ECN330-switch                              | GC   | 555  |
| <b>show system mtu</b> | Shows the maximum transfer unit size for Fast Ethernet and Gigabit Ethernet ports | GC   | 555  |

### *General Configuration Guidelines for QinQ*

1. Configure the ECN330-switch to QinQ mode (**system mode**, section 7.5.7 on page 552).
2. Create a SPVLAN (**vlan**, section 7.17.3 on page 850).
3. Configure the QinQ tunnel port to dot1Q tunnel port mode (**switchport mode dot1q-tunnel**, section 7.17.26 on page 884).
4. Set the Tag Protocol Identifier (TPID) value of the tunnel port. This step is required if the attached client is using a nonstandard 2-byte ethertype to identify 802.1Q tagged frames. The standard ethertype value is 0x8100. (See **switchport dot1q-ethertype**, section 7.17.28 on page 885.)
5. Configure the QinQ tunnel port to join the SPVLAN as an untagged member (**switchport allowed vlan**, section 7.17.10 on page 861).
6. Configure the SPVLAN ID as the native VID on the QinQ tunnel port (**switchport native vlan**, section 7.17.9 on page 860).
7. Configure system MTU to 1526 if jumbo frames are not enabled (**Related Commands**, section on page 555).
8. Configure the QinQ uplink port to join the SPVLAN as a tagged member (**switchport allowed vlan**, section 7.17.10 on page 861).

## 7.17.26 **switchport mode dot1q-tunnel**

This command configures an interface as a QinQ tunnel port. Use the **no** form to restore the default setting.

### **Syntax**

```
switchport mode dot1q-tunnel
```

```
no switchport mode
```

**dot1q-tunnel** – Sets the port as an 802.1Q tunnel port.

### **Default Setting**

All ports are in hybrid mode.

### **Command Mode**

Interface Configuration (Ethernet, Port Channel)

### **Command Usage**

Use the **switchport mode** command to set the ECN330-switch to QinQ mode before entering this command.

### **Example**

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport mode dot1q-tunnel
Console(config-if)#
```

### **Related Commands**

**show dot1q-tunnel** (section 7.17.27 on page 885)

**show interfaces switchport** (section 7.9.13 on page 753)

## 7.17.27 **show dot1q-tunnel**

This command displays information about QinQ tunnel ports.

### Command Mode

Privileged Exec

### Example

```

Console(config)#system mode qinq
Console(config)#interface ethernet 1/1
Console(config-if)#switchport mode dot1q-tunnel
Console(config-if)#end
Console#show dot1q-tunnel

Dot1q-Tunnel Port List

eth 1/1

Total 1 Dot1q-Tunnel Ports, 0 Dot1q-Tunnel Port-Channel
Console#

```

### Related Commands

**switchport mode dot1q-tunnel** (section 7.17.26 on page 884)

## 7.17.28 **switchport dot1q-ethertype**

This command sets the Tag Protocol Identifier (TPID) value of a tunnel port. Use the no form. Use the **no** form to restore the default setting.

### Syntax

**switchport dot1q-ethertype <tpid>**

**no switchport dot1q-ethertype**

*tpid* – Sets the ethertype value for 802.1Q encapsulation. This identifier is used to select a nonstandard 2-byte ethertype to identify 802.1Q tagged frames. The standard ethertype value is 0x8100. (Range: 0-ffff hexadecimal)

## Default Setting

No dot1q-ethertype is set.

## Command Mode

Interface Configuration (Ethernet, Port Channel)

## Command Usage

- Use the **switchport dot1q-ethertype** command to set a custom 802.1Q ethertype value on the selected interface. This feature allows the ECN330-switch to interoperate with third-party switches that do not use the standard 0x8100 ethertype to identify 802.1Q-tagged frames. For example, 0x1234 is set as the custom 802.1Q ethertype on a trunk port, incoming frames containing that ethertype are assigned to the VLAN contained in the tag following the ethertype field, as they would be with a standard 802.1Q trunk. Frames arriving on the port containing any other ethertype are looked upon as untagged frames, and assigned to the native VLAN of that port.
- All members of a VLAN should be set to the same ethertype.

## Example

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport dot1q-ethertype 9100
Console(config-if)#
```

## Related Commands

**show interfaces switchport** (section 7.9.13 on page 753)



## 7.17.29 address-monitor qinq

This command forwards traffic for the internal management VLANs (VIDs 247-249) between the QinQ tunnel port and the SBC connected to port 28. Use the **no** form to disable this feature.

### Default Setting

Enabled for any interface configured as a QinQ tunnel port.

### Command Mode

Interface Configuration (Ethernet, Port Channel)

### Command Usage

- Address monitoring must be enabled on a QinQ tunnel port to properly forward traffic for the internal management VLANs (VIDs 247-249) between the QinQ tunnel port and the SBC connected to port 28.
- Before enabling address monitoring, the ECN330-switch must first be set to QinQ mode with the **system mode** command (section 7.5.7 on page 552), and the access port set to a QinQ tunnel port with the **switchport mode dot1q-tunnel** command (section 7.17.26 on page 884).
- When address monitoring for the QinQ tunnel port is enabled, and incoming traffic is tagged for the internal management VLAN (247) or the FSA VLAN (249), an outer VLAN tag of 4093 is inserted and the packet redirected to port 28. The outer tag is removed at port 28 and the SBC processes the packet. When a packet for VLAN 247 or 249 is sent from port 28 to the tunnel port, a single inner tag is used and the packet is sent as in any normal forwarding operation.
- When address monitoring for the QinQ tunnel port is enabled, and the tunnel port is a member of the dynamic management VLAN (248) and an incoming untagged packet enters this port, the ECN330-switch inserts an inner dummy tag, an outer tag of 248, and the packet is redirected to port 28. The outer VLAN tag is retained because port 28 is tagged member of 248, and the SBC processes the packet. When a packet for VLAN 248 is sent from port 28 to the tunnel port, a single inner tag is used and the packet is sent as in any normal forwarding

operation. However, note that the tag will be stripped from the packet by the tunnel port because it is an untagged member of VLAN 248.

- When a tunnel port changes to QinQ Tunnel mode from normal mode, address monitoring is automatically enabled on this port, and all dynamic MAC address entries are deleted. If a new address entry is subsequently learned at the tunnel port, a static address entry for any internal management VLAN is added to the address table. If multiple internal management VLANs are configured, multiple entries are added to the address table.
- When a tunnel port changes to normal mode from QinQ Tunnel mode, address monitoring is automatically disabled on this port, and all static internal management VLAN address entries are deleted.
- If the internal management VLAN ID is changed, all dynamic MAC address and static internal management VLAN address entries are deleted.
- When the PVID of a tunnel port is changed, all dynamic MAC address and static internal management VLAN address entries are deleted.

### Example

```
Console(config)#system mode qinq
Console(config)#interface ethernet 1/2
Console(config-if)#switchport mode dot1q-tunnel
Console(config-if)#address-monitor qinq
Console(config-if)#
```

### Related Commands

**system mode** (section 7.5.7 on page 552)

**switchport mode dot1q-tunnel** (section 7.17.26 on page 884)

**management vlan** (section 7.17.4 on page 851)

### 7.17.30 **switchport mtu**

This command sets the maximum transfer unit (MTU) for an interface. Use the **no** form to restore the default setting.

#### **Syntax**

```
switchport mtu <mtu-size>
```

```
no switchport mtu
```

*mtu-size* – Specifies the MTU size for the specified port.  
(Range: 1500-9216 bytes)

#### **Default Setting**

1522 bytes

#### **Command Mode**

Interface Configuration (Ethernet, Port Channel)

#### **Command Usage**

- The **switchport mtu** command takes precedence over the **system mtu** command (section on page 555).
- If the MTU of a port is specified, then setting the system MTU will not change the port MTU.

#### **Example**

```
Console(config)#interface ethernet 1/1
Console(config-if)#switchport mtu 1522
Console(config-if)#
```

## 7.18 Layer 2 over MPLS Commands

This section describes commands used to configure L2MPLS.

Table 97 L2MPLS Commands

| Command                      | Function                                            | Mode | Page |
|------------------------------|-----------------------------------------------------|------|------|
| <b>system mode</b>           | Configures the ECN330-switch to L2MPLS mode         | PE   | 552  |
| <b>show system mode</b>      | Displays the ECN330-switch system mode              | PE   | 553  |
| <b>mpls</b>                  | Sets the MPLS characteristics for an uplink port    | IC   | 891  |
| <b>mpls 12</b>               | Configures a VLAN to operate as an L2MPLS tunnel    | IC   | 893  |
| <b>mpls static binding</b>   | Associates input and output MPLS labels with a VLAN | GC   | 893  |
| <b>show mpls 12transport</b> | Displays the L2MPLS link information                | PE   | 894  |
| <b>switchport mtu</b>        | Sets the maximum transfer unit for an interface     | IC   | 887  |

### General Configuration Guidelines for L2MPLS

1. Configure the ECN330-switch to L2MPLS mode (**system mode 12mpls**, section 7.5.7 on page 552).
2. Create a normal VLAN (**vlan**, section 7.17.3 on page 850).
3. Enable L2MPLS mode on the VLAN interface (**mpls 12**, section 7.18.2 on page 893).
4. Associate L2MPLS VLAN to a Virtual Channel, specifying the MPLS input and output labels. (**mpls static binding**, section 7.18.3 on page 893).
5. Configure a Gigabit Ethernet port to L2MPLS uplink mode (**mpls 12**, section 7.18.1 on page 891).
6. Specify the tunnel label, virtual channel (VC), and next hop used by the L2MPLS uplink port (**mpls tunnel**, **mpls vc**, and **mpls next-hop**, section 7.18.1 on page 891).

7. Configure port MTU to be bigger than 1544 bytes (**switchport mtu**, section 7.17.30 on page 889).

### 7.18.1

## **mpls**

This command sets the MPLS characteristics for an uplink port. Use the **no** form to restore the default values.

### **Syntax**

```
mpls {12 | tunnel <tunnel-label> | vc <vc-label> |
 next-hop <ip-address>}
```

```
no mpls {12 | tunnel | vc | next-hop}
```

- **12** - Configures a port to enter L2MPLS uplink port mode. Ports 1 - 27 can be configured as L2MPLS ports.
- *tunnel-label* - Sets the MPLS tunnel label that will be used to construct the MPLS header on the L2MPLS uplink port. This label is used by switches within the MPLS core network to establish a path from the entry point to the exit point. (Range: 0-1048574)
- *vc-label* - Sets the MPLS port-based virtual channel (VC) label. All incoming packets forwarded to MPLS ports will use this VC to generate the MPLS label. The VC is used to map traffic to a specific customer port on the edge switches at the boundaries of the MPLS network. (Range: 0-1048574)
- *ip-address* - Configures the next hop MPLS switch/router IP address. This IP address will be used to identify the next hop across the MPLS network or, more commonly, the edge switch where traffic is passed on to the customer.

### **Default Setting**

- **no mpls 12** uplink port mode
- **no mpls tunnel** label
- **no mpls vc** label
- **no mpls next-hop**

## Command Mode

Interface Configuration (Ethernet, Port Channel)

## Command Usage

- Use the **system mode** command (section 7.5.7 on page 552) to enable L2MPLS on the ECN330-switch prior to using the L2MPLS commands described in this section.
- The **mpls tunnel** and **mpls next-hop** commands can be entered even if the **mpls 12** command has not yet been used to set an interface as an MPLS uplink port. However, the MPLS header will be constructed and inserted into each frame only after a port has been configured as an L2MPLS uplink port.

## Example

The following example configures port 25 as an L2MPLS uplink port, and then specifies the tunnel label, the VC, and the next hop.

```
Console(config)#system mode l2mpls
Console(config)#interface ethernet 1/25
Console(config-if)#mpls tunnel 9
Console(config-if)#mpls vc 9
Console(config-if)#mpls next-hop 192.168.1.19
Console(config-if)#
```

## Related Commands

**system mode** (section 7.5.7 on page 552)

## 7.18.2 mpls l2

This command configures a VLAN to operate as an L2MPLS tunnel. Use the **no** form to reset a VLAN to normal mode.

### Syntax

```
[no] mpls l2
```

### Default Setting

```
no mpls l2 VLAN tunnel
```

### Command Mode

Interface Configuration (VLAN)

### Example

```
Console(config)#system mode l2mpls
Console(config)#interface vlan 9
Console(config-if)#mpls l2
Console(config-if)#
```

## 7.18.3 mpls static binding

This command associates input and output MPLS labels with a VLAN. Use the **no** form to reset a VLAN and disassociate the labels.

### Syntax

```
mpls static binding vlan <vlan-id> input <input_label>
output <output_label>
```

```
no mpls static binding vlan <vid>
```

- *vlan-id* - VLAN ID (Range: 1-4094, no leading zeroes)
- *input\_label* - Input MPLS label. (Range: 0-1048574)
- *output\_label* - Output MPLS label. (Range: 0-1048574)

## Default Setting

**no mpls static binding**

## Command Mode

Global Configuration

## Command Usage

The associated VLAN must be an L2MPLS VLAN. This means that the **mpls 12** command (section 7.18.2 on page 893) must be used to set the VLAN to L2MPLS mode before using the **mpls static binding** command.

## Example

```
Console(config)#system mode l2mpls
Console(config)#interface vlan 9
Console(config-if)#mpls 12
Console(config-if)#exit
Console(config)#mpls static binding vlan 9 input 5 output 5
Console(config)#
```

## Related Commands

**mpls 12** (section 7.18.2 on page 893)

## 7.18.4 show mpls l2transport

This command displays the L2MPLS link information.

## Command Mode

Privileged Exec

## Command Usage

When no input and output labels are configured with the **mpls static binding** command (section 7.18.3 on page 893), the VC state is down.



The default DA-MAC of MPLS uplink port is 00-00-00-00-00-00, and the default tunnel label is disabled.

### Example

```

Console#show mpls l2transport
MPLS Vlan Infomation:
[Client Intf] [VC State] [Local VC Label] [Remote VC Label]
Vlan2 Up 100 200
Vlan3 Down N/A N/A

MPLS Up-link Port Information:
[Up-Link Intf] [Tunnel Label] [Vc Label] [NextHopIP] [Da-Mac]
port:25 9 9 192.168.1.19 00-E0-29-94-34-64
port:26 N/A N/A 0.0.0.0 00-00-22-22-33-33
port:27 100 100 192.168.1.35 00-00-00-00-00-00
Console#

```

**Table 98** *show mpls l2transport - Display Description*

| Field                        | Description                                                                                                                                                                                                                                                                                                                                                                                                |
|------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>MPLS VLAN Information</i> |                                                                                                                                                                                                                                                                                                                                                                                                            |
| Client Intf                  | A VLAN configured to operate as an L2MPLS tunnel. This VLAN is connected to the client interface on the edge switch of the service provider's network.                                                                                                                                                                                                                                                     |
| VC State                     | <p>The status of the Virtual Channel can be one of the following:</p> <ul style="list-style-type: none"> <li>• UP – The VC can carry traffic between the two endpoints.</li> <li>• DOWN – The VC is not ready to carry traffic between the two endpoints. When no input and output labels are configured, the VC state is down</li> <li>• ADMIN DOWN—The VC has been administratively disabled.</li> </ul> |
| Local VC Label               | This label determines the egress interface of a packet arriving from the MPLS backbone.                                                                                                                                                                                                                                                                                                                    |

| Field                               | Description                                                                                                                                        |
|-------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------|
| Remote VC Label                     | This label is used by a remote peer switch.                                                                                                        |
| <i>MPLS Uplink Port Information</i> |                                                                                                                                                    |
| Uplink Intf                         | The uplink port connected to the client interface.                                                                                                 |
| Tunnel Label                        | The MPLS tunnel label that is used by switches within the MPLS core network to establish a path from the entry point to the exit point.            |
| VC Label                            | The Virtual Channel identifier that is used to map traffic to a specific customer port on the edge switches at the boundaries of the MPLS network. |
| NextHopIP                           | The IP address of the next hop across the MPLS network.                                                                                            |
| DA MAC                              | The MAC address of the remote switch's interface at the other end of the VC. The default DA-MAC of MPLS uplink port is 00-00-00-00-00-00.          |

## 7.19 Class of Service Commands

The commands described in this section enable those data packets to be specified which have greater precedence when traffic is buffered in the ECN330-switch due to congestion. The ECN330-switch supports CoS with eight priority queues for each port. Data packets in a port's high-priority queue will be transmitted before those in the lower-priority queues. The default priority can be set for each interface, also the queue service mode and the mapping of frame priority tags to the ECN330-switch's priority queues.

*Table 99 Priority Commands*

| Command Groups           | Function                                                                                                               | Page |
|--------------------------|------------------------------------------------------------------------------------------------------------------------|------|
| Priority (Layer 2)       | Configures default priority for untagged frames, sets queue weights, and maps class of service tags to hardware queues | 897  |
| Priority (Layer 3 and 4) | Maps TCP ports, IP precedence tags, or IP DSCP tags to class of service values                                         | 909  |

### Priority Commands (Layer 2)

This section describes commands used to configure Layer 2 traffic priority on the ECN330-switch.

*Table 100 Priority Commands (Layer 2)*

| Command                            | Function                                                                                            | Mode | Page |
|------------------------------------|-----------------------------------------------------------------------------------------------------|------|------|
| <b>queue mode</b>                  | Sets the queue mode to strict priority, Weighted Fair Queueing (WFQ), or Weighted Round-Robin (WRR) | GC   | 898  |
| <b>switchport priority default</b> | Sets a port priority for incoming untagged frames                                                   | IC   | 900  |
| <b>queue bandwidth</b>             | Assigns round-robin weights to the priority queues                                                  | IC   | 902  |

| Command                           | Function                                                              | Mode | Page |
|-----------------------------------|-----------------------------------------------------------------------|------|------|
| <b>queue min-bandwidth</b>        | Assigns fair queueing minimum bandwidth to the priority queues        | IC   | 903  |
| <b>queue cos map</b>              | Assigns class of service values to the priority queues                | IC   | 904  |
| <b>show queue mode</b>            | Shows the current queue mode                                          | PE   | 906  |
| <b>show queue bandwidth</b>       | Shows round-robin weights assigned to the priority queues             | PE   | 906  |
| <b>show queue min-bandwidth</b>   | Shows fair queueing minimum bandwidth assigned to the priority queues | PE   | 907  |
| <b>show queue cos-map</b>         | Shows the class of service map                                        | PE   | 908  |
| <b>show interfaces switchport</b> | Displays the administrative and operational status of an interface    | PE   | 753  |

### 7.19.1 queue mode

This command sets the queue mode used the class of service (CoS) priority queues. The options include strict priority, Weighted Fair Queueing (WFQ), Weighted Round-Robin (WRR), or a combination of strict and weighted queueing. Use the **no** form to restore the default value.

#### Syntax

```
queue mode {strict | wfq | wrr | strict-wfq <sp-queue> |
 strict-wrr <sp-queue>}
```

```
no queue mode
```

- **strict** - Services the egress queues in sequential order, transmitting all traffic in the higher priority queues before servicing lower priority queues. This ensures that the highest priority packets are always serviced first, ahead of all other traffic.

- **wfq** - Weighted Fair Queueing shares bandwidth at the egress ports by specifying a minimum bandwidth for each queue. Guaranteed bandwidth is first supplied to each queue, any remaining bandwidth is distributed in a round-robin fashion.
- **wrr** - Weighted Round-Robin shares bandwidth at the egress ports by using scheduling weights.
- **strict-wfq** - Strict priority is used for the high-priority queues and Weighted Fair Queueing for the rest of the queues.
- **strict-wrr** - Strict priority is used for the high-priority queues and Weighted Round-Robin for the rest of the queues.
- **sp-queue** - Specifies the strict priority queues used for the **strict-wrr** and **strict-wfq** options. This assigns the specified queue up to the highest priority queue. (Range: 0-7)

### Default Setting

Strict priority

### Command Mode

Global Configuration

### Command Usage

- The ECN330-switch can be set to service the port queues based on strict priority, WFQ, WRR, or a combination of strict and weighted queueing.
- Strict priority requires all traffic in a higher priority queues to be processed before lower priority queues are serviced.
- WFQ shares bandwidth at the egress ports by specifying a minimum bandwidth for each queue. Guaranteed bandwidth is first supplied to each queue, any remaining bandwidth is distributed in a round-robin fashion. Use the **queue min-bandwidth** command (section 7.19.4 on page 903) to assign the minimum bandwidth to each of the eight priority queues.
- WRR queueing specifies a relative weight of each queue. WRR uses a predefined relative weight for each queue that determines the percentage of service time the ECN330-switch services each queue

before moving on to the next queue. This prevents the head-of-line blocking that can occur with strict priority queuing. Use the **queue bandwidth** command (section 7.19.3 on page 902) to assign weights for WRR queueing to the eight priority queues.

### Example

The following example sets the queue mode to Strict-WFQ, with queue 5-7 using strict priority and the other queues using WFQ:

```
Console(config)#queue mode strict-wfq sp-queue 5
Console(config)#
```

### Related Commands

**queue bandwidth** (section 7.19.3 on page 902)  
**queue min-bandwidth** (section 7.19.4 on page 903)  
**show queue mode** (section 7.19.6 on page 906)

## 7.19.2 switchport priority default

This command sets a priority for incoming untagged frames. Use the **no** form to restore the default value.

### Syntax

```
switchport priority default <default-priority-id>
no switchport priority default
```

*default-priority-id* - The priority number for untagged ingress traffic. The priority is a number from 0 to 7. Seven is the highest priority.

### Default Setting

The priority is not set, and the default value for untagged frames received on the interface is zero.

## Command Mode

Interface Configuration (Ethernet, Port Channel)

## Command Usage

- The precedence for priority mapping is IP Port, IP Precedence or IP DSCP, and default switchport priority.
- The default priority applies for an untagged frame received on a port set to accept all frame types (that is, receives both untagged and tagged frames). This priority does not apply to IEEE 802.1Q VLAN tagged frames. If the incoming frame is an IEEE 802.1Q VLAN tagged frame, the IEEE 802.1p User Priority bits will be used.
- The ECN330-switch provides eight priority queues for each port. It can be configured to use strict priority queuing or Weighted Round Robin using the **queue mode** command. Inbound frames that do not have VLAN tags are tagged with the input port's default ingress user priority, and then placed in the appropriate priority queue at the output port. The default priority for all ingress ports is zero. Therefore, any inbound frames that do not have priority tags will be placed in queue 0 of the output port. (Note that if the output port is an untagged member of the associated VLAN, these frames are stripped of all VLAN tags prior to transmission.)

## Example

The following example shows how to set a default priority on port 3 to 5:

```
Console(config)#interface ethernet 1/3
Console (config-if)#switchport priority default 5
```

## Related Commands

**show interfaces switchport** (section 7.9.13 on page 753)

### 7.19.3 **queue bandwidth**

This command assigns weighted round-robin (WRR) weights to the eight class of service (CoS) priority queues. Use the **no** form to restore the default weights.

#### **Syntax**

```
queue bandwidth <weight0...weight7>
```

```
no queue bandwidth
```

*weight0...weight7* - The ratio of weights for queues 0 - 7 determines the weights used by the WRR scheduler. (Range: 1 - 15)

#### **Default Setting**

Weights 1, 2, 4, 6, 8, 10, 12, 14 are assigned to queues 0 - 7 respectively.

#### **Command Mode**

Interface Configuration (Ethernet, Port Channel)

#### **Command Usage**

WRR controls bandwidth sharing at the egress port by defining scheduling weights.

#### **Example**

The following example shows how to assign WRR weights of 1, 3, 5 and 7 to the CoS priority queues 0, 1, 2 and 3:

```
Console#configure
Console(config)#int eth 1/5
Console(config-if)#queue bandwidth 1 3 5 7 9 11 13 15
Console(config-if)#
```

#### **Related Commands**

**show queue bandwidth** (section 7.19.7 on page 906)



## 7.19.4 queue min-bandwidth

This command assigns a minimum bandwidth to each of the priority queues that is used for Weighted Fair Queueing (WFQ). Use the **no** form to restore the default bandwidth for each queue.

### Syntax

**queue min-bandwidth** <*bandwidth0...bandwidth7*>

**no queue bandwidth**

*bandwidth0...bandwidth7* - The minimum bandwidth assigned to queues 0 - 7. (Range: 1-100000 kbps for Fast Ethernet ports, 1-100000000 kbps for Gigabit Ethernet ports; Granularity: 64 kbps)

### Default Setting

Queue bandwidth (kbps): 1754, 3508, 7017, 10526, 14035, 17534, 21052, 24561 are assigned to queues 0 - 7 respectively

### Command Mode

Interface Configuration (Ethernet, Port Channel)

### Command Usage

- WFQ shares bandwidth at the egress ports by specifying a minimum bandwidth for each queue. Guaranteed bandwidth is first supplied to each queue, any remaining bandwidth is distributed in a round-robin fashion.
- Use the **queue mode** command (section 7.19.1 on page 898) to set the queue mode to **wfq** or **strict-wfq** before setting the minimum queue bandwidths.

## Example

The following example shows how to assign a minimum bandwidth to each of the CoS priority queues:

```
Console#configure
Console(config)#queue mode wfq
Console(config)#int eth 1/5
Console(config-if)#queue min-bandwidth 64 128 256 512 1024 2048 4096
8190
Console(config-if)#
```

## Related Commands

**show queue min-bandwidth** (section 7.19.8 on page 907)

## 7.19.5

### queue cos-map

This command assigns class of service (CoS) values to the priority queues (that is, hardware output queues 0 - 7). Use the **no** form to set the CoS map to the default values.

## Syntax

**queue cos-map** <queue\_id> [*cos1* ... *cosn*]

**no queue cos-map**

- *queue\_id* - The ID of the priority queue.  
Range is 0 to 7, where 7 is the highest priority queue.
- *cos1* ... *cosn* - The CoS values that are mapped to the queue ID. It is a space-separated list of numbers. The CoS value is a number from 0 to 7, where 7 is the highest priority.

## Default Setting

The ECN330-switch supports Class of Service by using four priority queues, with strict priority queuing for each port. Eight separate traffic classes are defined in IEEE 802.1p. The default priority levels are assigned as shown in the following table.

*Table 101 Default CoS Priority Levels*

| Queue    | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|----------|---|---|---|---|---|---|---|---|
| Priority | 2 | 0 | 1 | 3 | 4 | 5 | 6 | 7 |

**Command Mode**

Interface Configuration (Ethernet, Port Channel)

**Command Usage**

- CoS assigned at the ingress port is used to select a CoS priority at the egress port.
- This command sets the CoS priority for all interfaces.

**Example**

The following example shows how to change the CoS assignments to a one-to-one mapping:

```

Console(config)#interface ethernet 1/1
Console(config-if)#queue cos-map 0 0
Console(config-if)#queue cos-map 1 1
Console(config-if)#queue cos-map 2 2
Console(config-if)#exit
Console#show queue cos-map ethernet 1/1
Information of Eth 1/1
 Traffic Class : 0 1 2 3 4 5 6 7
 Priority Queue: 0 1 2 3 4 5 6 7
Console#

```

**Related Commands**

**show queue cos-map** (section 7.19.9 on page 908)

## 7.19.6 **show queue mode**

This command shows the current queue servicing mode.

### **Default Setting**

None

### **Command Mode**

Privileged Exec

### **Example**

```
Console#sh queue mode

Queue mode: strict
Console#
```

## 7.19.7 **show queue bandwidth**

This command displays the weighted round-robin (WRR) bandwidth allocation for the priority queues.

### **Default Setting**

None

### **Command Mode**

Privileged Exec

## Example

```

Console#show queue bandwidth
Information of Eth 1/1
Queue ID Weight
----- -
 0 1
 1 2
 2 4
 3 6
 4 8
 5 10
 6 12
 7 14
.
.
.

```

### 7.19.8 show queue min-bandwidth

This command displays the minimum bandwidth assigned to each of the priority queues when using Weighted Fair Queueing (WFQ).

#### Syntax

```
show queue min-bandwidth [interface]
```

*interface*

- **ethernet** <*unit*>/<*port*>
  - *unit* - This is device 1.
  - *port* - Physical port number on the ECN330 (Range: 1-28).
- **port-channel** <*channel-id*> - The assigned number of an aggregated link (Range: 1-13)

#### Default Setting

None

**Command Mode**

Privileged Exec

**Example**

```

Console#sh queue min-bandwidth e 1/2
Information of Eth 1/2
Queue ID Min Bandwidth

0 1754
1 3508
2 7017
3 10526
4 14035
5 17543
6 21052
7 24561
Console#

```

**7.19.9 show queue cos-map**

This command shows the class of service priority map.

**Syntax**

```
show queue cos-map [interface]
```

*interface*

- **ethernet** <*unit*>/<*port*>
  - *unit* - This is device 1.
  - *port* - Physical port number on the ECN330 (Range: 1-28).
- **port-channel** <*channel-id*> - The assigned number of an aggregated link (Range: 1-13)

**Default Setting**

None

## Command Mode

Privileged Exec

## Example

```
Console#show queue cos-map ethernet 1/1
Information of Eth 1/1
 CoS Value : 0 1 2 3 4 5 6 7
 Priority Queue: 2 0 1 3 4 5 6 7
Console#
```

## Priority Commands (Layer 3 and 4)

This section describes commands used to configure Layer 3 and 4 priority mapping on the ECN330.

*Table 102 Priority Commands (Layer 3 and 4)*

| Command                       | Function                                       | Mode | Page |
|-------------------------------|------------------------------------------------|------|------|
| <b>map ip port</b>            | Enables TCP or UDP class of service mapping    | GC   | 910  |
| <b>map ip port</b>            | Maps TCP or UDP socket to a class of service   | IC   | 911  |
| <b>map ip precedence</b>      | Enables IP precedence class of service mapping | GC   | 912  |
| <b>map ip precedence</b>      | Maps IP precedence value to a class of service | IC   | 913  |
| <b>map ip dscp</b>            | Enables IP DSCP class of service mapping       | GC   | 914  |
| <b>map ip dscp</b>            | Maps IP DSCP value to a class of service       | IC   | 915  |
| <b>show map ip port</b>       | Shows the IP port map                          | PE   | 916  |
| <b>show map ip precedence</b> | Shows the IP precedence map                    | PE   | 917  |
| <b>show map ip dscp</b>       | Shows the IP DSCP map                          | PE   | 919  |

### 7.19.10 **map ip port** (Global Configuration)

This command enables IP port mapping (that is, class of service mapping for TCP or UDP sockets). Use the **no** form to disable IP port mapping.

#### **Syntax**

```
[no] map ip port
```

#### **Default Setting**

Disabled

#### **Command Mode**

Global Configuration

#### **Command Usage**

The precedence for priority mapping is IP Port, IP Precedence or IP DSCP, and default switchport priority.

#### **Example**

The following example shows how to enable TCP or UDP port mapping globally:

```
Console(config)#map ip port
Console(config)#
```



### 7.19.11 map ip port (Interface Configuration)

This command sets IP port priority (TCP or UDP port priority). Use the **no** form to remove a specific setting.

#### Syntax

```
map ip port <port-number> cos <cos-value>
```

```
no map ip port <port-number>
```

- *port-number* - 16-bit TCP or UDP port number. (Range: 0-65535)
- *cos-value* - Class-of-Service value (Range: 0-7)

#### Default Setting

None

#### Command Mode

Interface Configuration (Ethernet, Port Channel)

#### Command Usage

- The precedence for priority mapping is IP Port, IP Precedence or IP DSCP, and default switchport priority.
- This command sets the IP port priority for all interfaces.

#### Example

The following example shows how to map HTTP traffic to CoS value 0:

```
Console(config)#interface ethernet 1/5
Console(config-if)#map ip port 80 cos 0
Console(config-if)#
```

### 7.19.12 **map ip precedence** (Global Configuration)

This command enables IP precedence mapping (IP Type of Service). Use the **no** form to disable IP precedence mapping.

#### **Syntax**

```
[no] map ip precedence
```

#### **Default Setting**

Disabled

#### **Command Mode**

Global Configuration

#### **Command Usage**

- The precedence for priority mapping is IP Port, IP Precedence or IP DSCP, and default switchport priority.
- IP Precedence and IP DSCP cannot both be enabled. Enabling one of these priority types will automatically disable the other type.

#### **Example**

The following example shows how to enable IP precedence mapping globally:

```
Console(config)#map ip precedence
Console(config)#
```

### 7.19.13 **map ip precedence** (Interface Configuration)

This command sets IP precedence priority (IP Type of Service priority). Use the **no** form to restore the default table.

#### Syntax

```
map ip precedence <ip-precedence-value> cos <cos-value>
```

```
no map ip precedence
```

- *precedence-value* - 3-bit precedence value. (Range: 0-7)
- *cos-value* - Class-of-Service value (Range: 0-7)

#### Default Setting

The list in Table 103 shows the default priority mapping.

*Table 103 Mapping IP Precedence to CoS Values*

| IP Precedence Value | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---------------------|---|---|---|---|---|---|---|---|
| CoS Value           | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |

#### Command Mode

Interface Configuration (Ethernet, Port Channel)

#### Command Usage

- The precedence for priority mapping is IP Port, IP Precedence or IP DSCP, and default switchport priority.
- IP Precedence values are mapped to default Class of Service values on a one-to-one basis according to recommendations in the IEEE 802.1p standard, and then subsequently mapped to the eight hardware priority queues.
- This command sets the IP Precedence for all interfaces.

## Example

The following example shows how to map IP precedence value 1 to CoS value 0:

```
Console(config)#interface ethernet 1/5
Console(config-if)#map ip precedence 1 cos 0
Console(config-if)#
```

### 7.19.14 map ip dscp (Global Configuration)

This command enables IP DSCP mapping (Differentiated Services Code Point mapping). Use the **no** form to disable IP DSCP mapping.

#### Syntax

```
[no] map ip dscp
```

#### Default Setting

Disabled

#### Command Mode

Global Configuration

#### Command Usage

- The precedence for priority mapping is IP Port, IP Precedence or IP DSCP, and default switchport priority.
- IP Precedence and IP DSCP cannot both be enabled. Enabling one of these priority types will automatically disable the other type.

## Example

The following example shows how to enable IP DSCP mapping globally:

```
Console(config)#map ip dscp
Console(config)#
```

### 7.19.15 **map ip dscp** (Interface Configuration)

This command sets IP DSCP priority (Differentiated Services Code Point priority). Use the **no** form to restore the default table.

#### **Syntax**

```
map ip dscp <dscp-value> cos <cos-value>
```

```
no map ip dscp
```

- *dscp-value* - 8-bit DSCP value. (Range: 0-255)
- *cos-value* - Class-of-Service value (Range: 0-7)

#### **Default Setting**

The DSCP default values are defined in the following table. Note that all the DSCP values that are not specified are mapped to CoS value 0.

*Table 104 Mapping IP DSCP to CoS Values*

| <b>IP DSCP Value</b>   | <b>CoS Value</b> |
|------------------------|------------------|
| 0                      | 0                |
| 8                      | 1                |
| 10, 12, 14, 16         | 2                |
| 18, 20, 22, 24         | 3                |
| 26, 28, 30, 32, 34, 36 | 4                |
| 38, 40, 42             | 5                |
| 48                     | 6                |
| 46, 56                 | 7                |

#### **Command Mode**

Interface Configuration (Ethernet, Port Channel)

## Command Usage

- The precedence for priority mapping is IP Port, IP Precedence or IP DSCP, and default switchport priority.
- DSCP priority values are mapped to default Class of Service values according to recommendations in the IEEE 802.1p standard, and then subsequently mapped to the eight hardware priority queues.
- This command sets the IP DSCP priority for all interfaces.

## Example

The following example shows how to map IP DSCP value 1 to CoS value 0:

```
Console(config)#interface ethernet 1/5
Console(config-if)#map ip dscp 1 cos 0
Console(config-if)#
```

## 7.19.16

### show map ip port

This command shows the IP port priority map.

## Syntax

```
show map ip port [interface]
```

*interface*

- **ethernet** *<unit>/<port>*
  - *unit* - This is device 1.
  - *port* - Physical port number on the ECN330. (Range: 1-28)
- **port-channel** *<channel-id>* - The assigned number of an aggregated link (Range: 1-13)

## Default Setting

None

## Command Mode

Privileged Exec

## Example

The following shows that HTTP traffic has been mapped to CoS value 0:

```
Console#show map ip port
TCP port mapping status: disabled

 Port Port no. COS

 Eth 1/ 5 80 0
Console#
```

## Related Commands

- map ip port** (Global Configuration) (section 7.19.10 on page 910)
- map ip port** (Interface Configuration) (section 7.19.11 on page 911)

## 7.19.17 show map ip precedence

This command shows the IP precedence priority map.

### Syntax

```
show map ip precedence [interface]
```

*interface*

- **ethernet** *<unit>/<port>*
  - *unit* - This is device 1.
  - *port* - Physical port number on the ECN330 (Range: 1-28).
- **port-channel** *<channel-id>* - The assigned number of an aggregated link (Range: 1-13)

## Default Setting

None

## Command Mode

Privileged Exec

## Example

```
Console#show map ip precedence ethernet 1/5
Precedence mapping status: disabled

Port Precedence COS

Eth 1/ 5 0 0
Eth 1/ 5 1 1
Eth 1/ 5 2 2
Eth 1/ 5 3 3
Eth 1/ 5 4 4
Eth 1/ 5 5 5
Eth 1/ 5 6 6
Eth 1/ 5 7 7
Console#
```

## Related Commands

**map ip precedence** (Global Configuration) (section 7.19.12 on page 912)

**map ip precedence** (Interface Configuration) (section 7.19.13 on page 913)



## 7.19.18 **show map ip dscp**

This command shows the IP DSCP priority map.

### **Syntax**

```
show map ip dscp [interface]
```

*interface*

- **ethernet** <*unit*>/<*port*>
  - *unit* - This is device 1.
  - *port* - Physical port number on the ECN330 (Range: 1-28).
- **port-channel** <*channel-id*> - The assigned number of an aggregated link (Range: 1-13)

### **Default Setting**

None

### **Command Mode**

Privileged Exec

## Example

```
Console#show map ip dscp ethernet 1/1
DSCP mapping status: disabled

Port DSCP COS

Eth 1/ 1 0 0
Eth 1/ 1 1 0
Eth 1/ 1 2 0
Eth 1/ 1 3 0
.
.
.
Eth 1/ 1 61 0
Eth 1/ 1 62 0
Eth 1/ 1 63 0
Console#
```

## Related Commands

- map ip dscp** (Global Configuration) (section 7.19.14 on page 914)
- map ip dscp** (Interface Configuration) (section 7.19.15 on page 915)

## 7.20 Quality of Service Commands

The commands described in this section are used to configure Differentiated Services (DiffServ) classification criteria and service policies. Traffic can be classified according to access lists, IP Precedence or DSCP values, or VLANs. Using access lists, traffic can be selected based on Layer 2, Layer 3, or Layer 4 information contained in each packet.

*Table 105 Quality of Service Commands*

| Command                          | Function                                                                                                                                   | Mode | Page |
|----------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|------|------|
| <b>class-map</b>                 | Creates a class map for a type of traffic                                                                                                  | GC   | 923  |
| <b>match</b>                     | Defines the criteria used to classify traffic                                                                                              | CM   | 924  |
| <b>policy-map</b>                | Creates a policy map for multiple interfaces                                                                                               | GC   | 926  |
| <b>class</b>                     | Defines a traffic classification for the policy to act on                                                                                  | PM   | 927  |
| <b>set</b>                       | Classifies IP traffic by setting a CoS, DSCP, or IP-precedence value in a packet                                                           | PM-C | 929  |
| <b>police</b>                    | Defines an enforcer for classified traffic                                                                                                 | PM-C | 930  |
| <b>service-policy</b>            | Applies a policy map defined by the <b>policy-map</b> command to the input of a particular interface                                       | IC   | 931  |
| <b>show class-map</b>            | Displays the QoS class maps which define matching criteria used for classifying traffic                                                    | PE   | 932  |
| <b>show policy-map</b>           | Displays the QoS policy maps which define classification criteria for incoming traffic, and may include policers for bandwidth limitations | PE   | 933  |
| <b>show policy-map interface</b> | Displays the configuration of all classes configured for all service policies on the specified interface                                   | PE   | 934  |

To create a service policy for a specific category of ingress traffic, follow these steps:

1. Use the **class-map** command to designate a class name for a specific category of traffic, and enter the Class Map configuration mode.
2. Use the **match** command to select a specify type of traffic based on an access list, a DSCP or IP Precedence value, or a VLAN.
3. Set an ACL mask to enable filtering for the criteria specified in the **match** command.
4. Use the **policy-map** command to designate a policy name for a specific manner in which ingress traffic will be handled, and enter the Policy Map configuration mode.
5. Use the **class** command to identify the class map, and enter Policy Map Class configuration mode. A policy map can contain multiple class statements.
6. Use the **set** command to modify the QoS value for matching traffic class, and use the **policer** command to monitor the average flow and burst rate, and drop any traffic that exceeds the specified rate, or just reduce the DSCP service level for traffic exceeding the specified rate.
7. Use the **service-policy** command to assign a policy map to a specific interface.

**Note:** One rule per Class Map can be configured. However, multiple classes can be included in a Policy Map.

**Note:** Create a Class Map before creating a Policy Map.

## 7.20.1 class-map

This command creates a class map used for matching packets to the specified class, and enters Class Map configuration mode. Use the **no** form to delete a class map and return to Global configuration mode.

### Syntax

```
[no] class-map <class-map-name> [match-any]
```

- **match-any** - Match any condition within a class map.
- **class-map-name** - Name of the class map. (Range: 1-16 characters)

### Default Setting

None

### Command Mode

Global Configuration

### Command Usage

- First enter this command to designate a class map and enter the Class Map configuration mode. Then use the **match** command (page 924) to specify the criteria for ingress traffic that will be classified under this class map.
- Only one **match** command is permitted per class map, so the **match-any** field refers to the criteria specified by the lone **match** command for a class map.
- The class map uses the Access Control List filtering engine, so an ACL mask must also be set to enable filtering for the criteria specified in the **match** command. See “mask (IP ACL)” on page 699 or “mask (MAC ACL)” on page 713 for information on configuring an appropriate ACL mask.
- The class map is used with a policy map (section 7.20.3 on page 926) to create a service policy (section 7.20.7 on page 931) for a specific interface that defines packet classification, service tagging, and bandwidth policing.

## Example

This example creates a class map call “rd\_class,” and sets it to match packets marked for DSCP service value 3:

```
Console(config)#class-map rd_class match-any
Console(config-cmap)#match ip dscp 3
Console(config-cmap)#exit
Console(config)#access-list ip mask-precedence in
Console(config-ip-mask-acl)#mask any any dscp
Console(config-ip-mask-acl)#
```

## Related Commands

**show class-map** (section 7.20.8 on page 932)

## 7.20.2 match

This command defines the criteria used to classify traffic. Use the **no** form to delete the matching criteria.

### Syntax

```
[no] match {access-list <acl-name> | ip dscp <dscp> | ip
precedence <ip-precedence> | vlan <vlan>}
```

- **acl-name** - Name of the access control list. Any type of ACL can be specified, including standard or extended IP ACLs and MAC ACLs. (Range: 1-16 characters)
- **dscp** - A DSCP value. (Range: 0-63)
- **ip-precedence** - An IP Precedence value. (Range: 0-7)
- **vlan** - A VLAN. (Range:1-4094)

### Default Setting

None

## Command Mode

### Class Map Configuration

## Command Usage

- First enter the **class-map** command to designate a class map and enter the Class Map configuration mode. Then use the **match** command to specify the fields within ingress packets that must match to qualify for this class map.
- Only one **match** command can be entered per class map.
- The class map uses the Access Control List filtering engine, so an ACL mask must also be set to enable filtering for the criteria specified in the **match** command. See “mask (IP ACL)” on page 699 and “mask (MAC ACL)” on page 713 for information on configuring an appropriate ACL mask.

## Example

This example creates a class map called “rd\_class#1,” and sets it to match packets marked for DSCP service value 3:

```
Console(config)#class-map rd_class#1_ match-any
Console(config-cmap)#match ip dscp 3
Console(config-cmap)#exit
Console(config)#access-list ip mask-precedence in
Console(config-ip-mask-acl)#mask any any dscp
Console(config-ip-mask-acl)#
```

This example creates a class map call “rd\_class#2,” and sets it to match packets marked for IP Precedence service value 5:

```
Console(config)#class-map rd_class#2 match-any
Console(config-cmap)#match ip precedence 5
Console(config-cmap)#exit
Console(config)#access-list ip mask-precedence in
Console(config-ip-mask-acl)#mask any any precedence
Console(config-ip-mask-acl)#
```

This example creates a class map call “rd\_class#3,” and sets it to match packets marked for VLAN 1:

```
Console(config)#class-map rd_class#3 match-any
Console(config-cmap)#match vlan 1
Console(config-cmap)#exit
Console(config)#access-list mac mask-precedence in
Console(config-ip-mask-acl)#mask any any vid 1
Console(config-ip-mask-acl)#
```

### 7.20.3 policy-map

This command creates a policy map that can be attached to multiple interfaces, and enters Policy Map configuration mode. Use the **no** form to delete a policy map and return to Global configuration mode.

#### Syntax

**[no] policy-map** <*policy-map-name*>

*policy-map-name* - Name of the policy map. (Range: 1-16 characters)

#### Default Setting

None

#### Command Mode

Global Configuration

#### Command Usage

- Use the **policy-map** command to specify the name of the policy map, and then use the **class** command to configure policies for traffic that matches criteria defined in a class map.
- A policy map can contain multiple class statements that can be applied to the same interface with the **service-policy** command (section 7.20.7 on page 931).



- Create a Class Map (section 7.20.3 on page 926) before assigning it to a Policy Map.

### Example

This example creates a policy called “rd\_policy,” uses the **class** command to specify the previously defined “rd\_class,” uses the **set** command to classify the service that incoming packets will receive, and then uses the **police** command to limit the average bandwidth to 100,000 Kbps, the burst rate to 1522 bytes, and configure the response to drop any violating packets.

```
Console(config)#policy-map rd_policy
Console(config-pmap)#class rd_class
Console(config-pmap-c)#set ip dscp 3
Console(config-pmap-c)#police 100000 1522 exceed-action drop
Console(config-pmap-c)#
```

## 7.20.4

### class

This command defines a traffic classification upon which a policy can act, and enters Policy Map Class configuration mode. Use the **no** form to delete a class map and return to Policy Map configuration mode.

#### Syntax

**[no] class *class-map-name***

*class-map-name* - Name of the class map. (Range: 1-16 characters)

#### Default Setting

None

#### Command Mode

Policy Map Configuration

## Command Usage

- Use the **policy-map** command to specify a policy map and enter Policy Map configuration mode. Then use the **class** command to enter Policy Map Class configuration mode. And finally, use the **set** and **police** commands to specify the match criteria, where the:
  - **set** command classifies the service that an IP packet will receive.
  - **police** command defines the maximum throughput, burst rate, and the action that results from a policy violation.
- Currently only one rule may be configured per Class Map, one or more classes may be assigned to a policy map.

## Example

This example creates a policy called “rd\_policy,” uses the **class** command to specify the previously defined “rd\_class,” uses the **set** command to classify the service that incoming packets will receive, and then uses the **police** command to limit the average bandwidth to 100,000 Kbps, the burst rate to 1522 bytes, and configure the response to drop any violating packets.

```
Console(config)#policy-map rd_policy
Console(config-pmap)#class rd_class
Console(config-pmap-c)#set ip dscp 3
Console(config-pmap-c)#police 100000 1522 exceed-action drop
Console(config-pmap-c)#
```

## 7.20.5 **set**

This command services IP traffic by setting a CoS, DSCP, or IP Precedence value in a matching packet (as specified by the **match** command on page 924). Use the **no** form to remove the traffic classification.

### Syntax

```
[no] set {cos <new-cos> | ip dscp <new-dscp> | ip
precedence <new-precedence>}
```

- *new-cos* - New Class of Service (CoS) value. (Range: 0-7)
- *new-dscp* - New Differentiated Service Code Point (DSCP) value. (Range: 0-63)
- *new-precedence* - New IP Precedence value. (Range: 0-7)

### Default Setting

None

### Command Mode

Policy Map Class Configuration

### Example

This example creates a policy called “rd\_policy,” uses the **class** command to specify the previously defined “rd\_class,” uses the **set** command to classify the service that incoming packets will receive, and then uses the **police** command to limit the average bandwidth to 100,000 Kbps, the burst rate to 1522 bytes, and configure the response to drop any violating packets.

```
Console(config)#policy-map rd_policy
Console(config-pmap)#class rd_class
Console(config-pmap-c)#set ip dscp 3
Console(config-pmap-c)#police 100000 1522 exceed-action drop
Console(config-pmap-c)#
```

## 7.20.6 police

This command defines an policer for classified traffic. Use the **no** form to remove a policer.

### Syntax

```
[no] police <rate-kbps> <burst-byte> [exceed-action
{drop | set}]
```

- *rate-kbps* - Rate in kilobits per second. (Range: 1-100000 kbps or maximum port speed, whichever is lower)
- *burst-byte* - Burst in bytes. (Range: 64-1522 bytes)
- **drop** - Drop packet when specified rate or burst are exceeded.
- **set** - Set DSCP service to the specified value. (Range: 0-63)

### Default Setting

Drop out-of-profile packets.

### Command Mode

Policy Map Class Configuration

### Command Usage

- Up to 63 policers (that is, class maps) can be configured for Fast Ethernet and Gigabit Ethernet ingress ports.
- Policing is based on a token bucket, where bucket depth (that is, the maximum burst before the bucket overflows) is by specified the *burst-byte* field, and the average rate tokens are removed from the bucket is by specified by the *rate-bps* option.

## Example

This example creates a policy called “rd\_policy,” uses the **class** command to specify the previously defined “rd\_class,” uses the **set** command to classify the service that incoming packets will receive, and then uses the **police** command to limit the average bandwidth to 100,000 Kbps, the burst rate to 1522 bytes, and configure the response to drop any violating packets.

```
Console(config)#policy-map rd_policy
Console(config-pmap)#class rd_class
Console(config-pmap-c)#set ip dscp 3
Console(config-pmap-c)#police 100000 1522 exceed-action drop
Console(config-pmap-c)#
```

## 7.20.7

### service-policy

This command applies a policy map defined by the **policy-map** command to the ingress queue of a particular interface. Use the **no** form to remove the policy map from this interface.

#### Syntax

**[no] service-policy input <policy-map-name>**

- **input** - Apply to the input traffic.
- **policy-map-name** - Name of the policy map for this interface.  
(Range: 1-16 characters)

#### Default Setting

No policy map is attached to an interface.

#### Command Mode

Interface Configuration (Ethernet, Port Channel)

## Command Usage

- Only one policy map can be assigned to an interface.
- First define a class map, set an ACL mask to match the criteria defined in the class map, then define a policy map, and finally use the **service-policy** command to bind the policy map to the required interface.

## Example

This example applies a service policy to an ingress interface.

```
Console(config)#interface ethernet 1/1
Console(config-if)#service-policy input rd_policy
Console(config-if)#
```

## 7.20.8

### show class-map

This command displays the QoS class maps which define matching criteria used for classifying traffic.

### Syntax

```
show class-map [<class-map-name>]
```

*class-map-name* - Name of the class map. (Range: 1-16 characters)

### Default Setting

Displays all class maps.

### Command Mode

Privileged Exec

## Example

```

Console#show class-map
Class Map match-any rd_class#1
 Match ip dscp 3

Class Map match-any rd_class#2
 Match ip precedence 5

Class Map match-any rd_class#3
 Match vlan 1

Console#

```

### 7.20.9

## show policy-map

This command displays the QoS policy maps which define classification criteria for incoming traffic, and may include policers for bandwidth limitations.

### Syntax

```
show policy-map [<policy-map-name>] [class <class-map-name>]
```

- *policy-map-name* - Name of the policy map. (Range: 1-16 characters)
- *class-map-name* - Name of the class map. (Range: 1-16 characters)

### Default Setting

Displays all policy maps and all classes.

### Command Mode

Privileged Exec

## Example

```
Console#show policy-map
Policy Map rd_policy
 class rd_class
 set ip dscp 3
Console#show policy-map rd_policy class rd_class
Policy Map rd_policy
 class rd_class
 set ip dscp 3
Console#
```

### 7.20.10 show policy-map interface

This command displays the service policy assigned to the specified interface.

#### Syntax

```
show policy-map interface interface input
interface
```

- **ethernet** *<unit>/<port>*
  - *unit* - This is device 1.
  - *port* - Physical port number on the ECN330 (Range: 1-28).
- **port-channel** *<channel-id>* - The assigned number of an aggregated link (Range: 1-13)

#### Command Mode

Privileged Exec

#### Example

```
Console#show policy-map interface ethernet 1/5
Service-policy rd_policy input
Console#
```



## 7.21 Multicast Filtering Commands

The ECN330-switch uses IGMP (Internet Group Management Protocol) to query for any attached hosts that want to receive a specific multicast service. It identifies the ports containing hosts requesting a service and sends data out to those ports only. It then propagates the service request up to any neighboring multicast switch or router to ensure that it will continue to receive the multicast service.

Note that IGMP query can be enabled globally at Layer 2, or enabled for specific VLAN interfaces at Layer 3. (Layer 2 query is disabled if Layer 3 query is enabled.)

*Table 106 Multicast Filtering Commands*

| <b>Command Groups</b>    | <b>Function</b>                                                                                                                                                                                   | <b>Page</b> |
|--------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------|
| IGMP Snooping            | Configures multicast groups through IGMP snooping or static assignment, sets the IGMP version, displays current snooping and query settings, and displays the multicast service and group members | 936         |
| IGMP Query (Layer 2)     | Configures IGMP query parameters for multicast filtering at Layer 2                                                                                                                               | 942         |
| Static Multicast Routing | Configures static multicast router ports                                                                                                                                                          | 949         |
| IGMP (Layer 3)           | Configures the IGMP protocol used with multicast routing                                                                                                                                          | 952         |

## IGMP Snooping Commands

This section describes commands used to configure IGMP snooping on the ECN330-switch.

Table 107 IGMP Snooping Commands

| Command                                      | Function                                           | Mode | Page |
|----------------------------------------------|----------------------------------------------------|------|------|
| <b>ip igmp snooping</b>                      | Enables IGMP snooping globally                     | GC   | 936  |
| <b>ip igmp snooping</b>                      | Enables IGMP snooping per VLAN interface           | IC   | 937  |
| <b>ip igmp snooping<br/>vlan static</b>      | Adds an interface as a member of a multicast group | GC   | 938  |
| <b>ip igmp snooping<br/>version</b>          | Configures the IGMP version for snooping           | GC   | 939  |
| <b>show ip igmp<br/>snooping</b>             | Shows the IGMP snooping and query configuration    | PE   | 940  |
| <b>show mac-address-<br/>table multicast</b> | Shows the IGMP snooping MAC multicast list         | PE   | 941  |

### 7.21.1 ip igmp snooping (Global Configuration)

This command enables IGMP snooping globally on the ECN330-switch. Use the **no** form to disable it.

#### Syntax

```
[no] ip igmp snooping
```

#### Default Setting

Enabled

## Command Mode

Global Configuration

## Example

The following example enables IGMP snooping globally.

```
Console(config)#ip igmp snooping
Console(config)#
```

### 7.21.2

## ip igmp snooping (Interface Configuration)

This command enables IGMP snooping per VLAN interface. Use the **no** form to disable it.

## Syntax

```
[no] ip igmp snooping
```

## Default Setting

Enabled

## Command Mode

Interface Configuration (VLAN)

## Command Usage

- When IGMP snooping is enabled globally, the per VLAN interface settings for IGMP snooping take precedence.
- When IGMP snooping is disabled globally, snooping can still be configured per VLAN interface, but the interface settings will not take effect until snooping is re-enabled globally.

## Example

The following example enables IGMP snooping on VLAN 1.

```
Console(config)#interface vlan 1
Console(config-if)#ip igmp snooping
Console(config-if)#
```

### 7.21.3 ip igmp snooping vlan static

This command adds a port to a multicast group. Use the **no** form to remove the port.

#### Syntax

```
[no] ip igmp snooping vlan <vlan-id> static <ip-address>
<interface>
```

- **vlan-id** - VLAN ID (Range: 1-4094)
- **ip-address** - IP address for multicast group
- **interface**
  - **ethernet <unit>/<port>**
    - **unit** - This is device 1.
    - **port** - Physical port number on the ECN330 (Range: 1-28).
  - **port-channel <channel-id>** - The assigned number of an aggregated link (Range: 1-13)

#### Default Setting

None

#### Command Mode

Global Configuration

## Example

The following shows how to statically configure a multicast group on a port:

```
Console(config)#ip igmp snooping vlan 1 static 224.0.0.12 ethernet
1/5
Console(config)#
```

### 7.21.4 ip igmp snooping version

This command configures the IGMP snooping version. Use the **no** form to restore the default.

#### Syntax

```
ip igmp snooping version {1 | 2 | 3}
```

```
no ip igmp snooping version
```

- 1 - IGMP Version 1
- 2 - IGMP Version 2
- 3 - IGMP Version 3

#### Default Setting

IGMP Version 2

#### Command Mode

Global Configuration

#### Command Usage

- All systems on the subnet must support the same version. If there are legacy devices in the network that only support Version 1, the ECN330-switch must also be configured to use Version 1.
- Some commands are only enabled for IGMPv2 and v3 snooping, including **ip igmp snooping query-max-response-time**

(section 7.21.10 on page 946) and **ip igmp snooping query-interval** (section 7.21.9 on page 945).

- The **ip igmp snooping querier** command (section 7.21.7 on page 943) cannot be enabled when using IGMPv3 snooping.

### Example

The following configures the ECN330-switch to use IGMP Version 1:

```
Console(config)#ip igmp snooping version 1
Console(config)#
```

## 7.21.5 show ip igmp snooping

This command shows the IGMP snooping configuration.

### Default Setting

None

### Command Mode

Privileged Exec

### Command Usage

See “Configuring IGMP Snooping and Query Parameters” on page 355 for a description of the displayed items.

## Example

The following shows the current IGMP snooping configuration:

```
Console#show ip igmp snooping
Service status: Enabled
Querier status: Enabled
Query count: 2
Query interval: 125 sec
Query max response time: 10 sec
Query time-out: 300 sec
IGMP snooping version: Version 2
Console#
```

### 7.21.6 show mac-address-table multicast

This command shows known multicast addresses.

#### Syntax

```
show mac-address-table multicast [vlan <vlan-id>]
[user | igmp-snooping]
```

- **vlan-id** - VLAN ID (1 to 4094)
- **user** - Display only the user-configured multicast entries.
- **igmp-snooping** - Display only entries learned through IGMP snooping.

#### Default Setting

None

#### Command Mode

Privileged Exec

#### Command Usage

Member types displayed include IGMP or USER, depending on selected options.

## Example

The following shows the multicast entries learned through IGMP snooping for VLAN 1:

```
Console#show mac-address-table multicast vlan 1 igmp-snooping
VLAN M'cast IP addr. Member ports Type

 1 224.1.2.3 Eth1/11 IGMP
Console#
```

## IGMP Query Commands (Layer 2)

This section describes commands used to configure Layer 2 IGMP query on the ECN330-switch.

*Table 108 IGMP Query Commands (Layer 2)*

| Command                                          | Function                                                         | Mode | Page |
|--------------------------------------------------|------------------------------------------------------------------|------|------|
| <b>ip igmp snooping querier</b>                  | Allows the ECN330-switch to act as the querier for IGMP snooping | GC   | 943  |
| <b>ip igmp snooping query-count</b>              | Configures the query count                                       | GC   | 944  |
| <b>ip igmp snooping query-interval</b>           | Configures the query interval                                    | GC   | 945  |
| <b>ip igmp snooping query-max-response-time</b>  | Configures the report delay                                      | GC   | 946  |
| <b>ip igmp snooping report-suppression</b>       | Suppresses requirement for hosts to respond to queries           | GC   |      |
| <b>ip igmp snooping router-port-expire-timet</b> | Configures the query timeout                                     | GC   | 948  |



## 7.21.7 **ip igmp snooping querier**

This command enables the ECN330-switch as an IGMP querier. Use the **no** form to disable it.

### **Syntax**

```
[no] ip igmp snooping querier
```

### **Default Setting**

Enabled

### **Command Mode**

Global Configuration

### **Command Usage**

- IGMP snooping querier is not supported for IGMPv3 snooping (see **ip igmp snooping version**, section 7.21.4 on page 939).
- If enabled under IGMPv1 or v2 snooping, the ECN330-switch will serve as querier if elected. The querier is responsible for asking hosts if they want to receive multicast traffic.

### **Example**

```
Console(config)#ip igmp snooping querier
Console(config)#
```

## 7.21.8 ip igmp snooping query-count

This command configures the query count. Use the **no** form to restore the default.

### Syntax

```
ip igmp snooping query-count <count>
```

```
no ip igmp snooping query-count
```

*count* - The maximum number of queries issued for which there has been no response before the ECN330-switch takes action to drop a client from the multicast group. (Range: 1-10)

### Default Setting

2 times

### Command Mode

Global Configuration

### Command Usage

The query count defines how long the querier waits for a response from a multicast client before taking action. If a querier has sent a number of queries defined by this command, but a client has not responded, a countdown timer is started using the time defined by **ip igmp snooping query-max-response-time**. If the countdown finishes, and the client still has not responded, then that client is considered to have left the multicast group.

### Example

The following shows how to configure the query count to 10:

```
Console(config)#ip igmp snooping query-count 10
Console(config)#
```

## Related Commands

**ip igmp snooping query-max-response-time** (section 7.21.10 on page 946)

### 7.21.9 ip igmp snooping query-interval

This command configures the query interval. Use the **no** form to restore the default.

#### Syntax

**ip igmp snooping query-interval** <*seconds*>

**no ip igmp snooping query-interval**

*seconds* - The frequency at which the ECN330-switch sends IGMP host-query messages. (Range: 60-125)

#### Default Setting

125 seconds

#### Command Mode

Global Configuration

#### Example

The following shows how to configure the query interval to 100 seconds:

```
Console(config)#ip igmp snooping query-interval 100
Console(config)#
```

## 7.21.10 **ip igmp snooping query-max-response-time**

This command configures the snooping report delay. Use the **no** form of this command to restore the default.

### **Syntax**

```
ip igmp snooping query-max-response-time
 <tenths_of_second>
```

```
no ip igmp snooping query-max-response-time
```

*tenths\_of\_second* - The report delay advertised in IGMP queries.  
(Range: 1-255)

### **Default Setting**

10 seconds

### **Command Mode**

Global Configuration

### **Command Usage**

- The ECN330-switch must be using IGMPv2 or v3 snooping for this command to take effect.
- This command defines the time after a query, during which a response is expected from a multicast client. If a querier has sent a number of queries defined by the **ip igmp snooping query-count**, but a client has not responded, a countdown timer is started using an initial value set by this command. If the countdown finishes, and the client still has not responded, then that client is considered to have left the multicast group.

## Example

The following shows how to configure the maximum response time to 20 seconds:

```
Console(config)#ip igmp snooping query-max-response-time 200
Console(config)#
```

## Related Commands

**ip igmp snooping version** (section 7.21.4 on page 939)

**ip igmp snooping query-max-response-time** (section 7.21.10 on page 946)

### 7.21.11 ip igmp snooping report-suppression

This command restricts the number of IGMP report messages sent to multicast devices. Use the **no** form of this command to disable report suppression and forward all IGMP reports.

#### Syntax

```
[no] ip igmp snooping report-suppression
```

#### Default Setting

Enabled

#### Command Mode

Global Configuration

#### Command Usage

- IGMP report suppression is used to forward only one IGMP report per query to multicast devices. When IGMP router suppression is enabled, the ECN330-switch sends the first IGMP report from all hosts for a group to all the multicast routers.

- Report suppression is not supported when multicast query messages include IGMPv3 reports.

### Example

```
Console(config)#ip igmp snooping report suppression
Console(config)#
```

## 7.21.12 ip igmp snooping router-port-expire-time

This command configures the query timeout. Use the **no** form of this command to restore the default.

### Syntax

**ip igmp snooping router-port-expire-time <seconds>**

**no ip igmp snooping router-port-expire-time**

*seconds* - The time the ECN330-switch waits after the previous querier stops before it considers the router port (the interface which had been receiving query packets) to have expired. (Range: 300-500)

### Default Setting

300 seconds

### Command Mode

Global Configuration

### Command Usage

The ECN330-switch must use IGMPv2 or v3 snooping for this command to take effect.

## Example

The following shows how to configure the default timeout to 300 seconds:

```
Console(config)#ip igmp snooping query-time-out 300
Console(config)#
```

## Related Commands

**ip igmp snooping version** (section 7.21.4 on page 939)

## Static Multicast Routing Commands

This section describes commands used to configure static multicast routing on the ECN330-switch.

*Table 109 Static Multicast Routing Commands*

| Command                                  | Function                     | Mode | Page |
|------------------------------------------|------------------------------|------|------|
| <b>ip igmp snooping<br/>vlan mrouter</b> | Adds a multicast router port | GC   | 950  |
| <b>show ip igmp<br/>snooping mrouter</b> | Shows multicast router ports | PE   | 951  |

### 7.21.13 ip igmp snooping vlan mrouter

This command statically configures a multicast router port. Use the **no** form to remove the configuration.

#### Syntax

```
[no] ip igmp snooping vlan <vlan-id> mrouter <interface>
```

- *vlan-id* - VLAN ID (Range: 1-4094)
- *interface*
  - **ethernet** <unit>/<port>
    - *unit* - This is device 1.
    - *port* - Physical port number on the ECN330-switch. (Range: 1-27)
  - **port-channel** <channel-id> - The assigned number of an aggregated link (Range: 1-13)

#### Default Setting

No static multicast router ports are configured.

#### Command Mode

Global Configuration

#### Command Usage

Depending on network connections, IGMP snooping may not always be able to locate the IGMP querier. Therefore, if the IGMP querier is a known multicast router or switch connected over the network to an interface (port or trunk) on the ECN330-switch, that interface can be manually configured to join all the current multicast groups.



## Example

The following shows how to configure port 11 as a multicast router port within VLAN 1:

```
Console(config)#ip igmp snooping vlan 1 mrouter ethernet 1/11
Console(config)#
```

## 7.21.14 show ip igmp snooping mrouter

This command displays information on statically configured and dynamically learned multicast router ports.

### Syntax

```
show ip igmp snooping mrouter [vlan <vlan-id>]
```

*vlan-id* - VLAN ID (Range: 1-4094)

### Default Setting

Displays multicast router ports for all configured VLANs.

### Command Mode

Privileged Exec

### Command Usage

Multicast router port types displayed include Static or Dynamic.

## Example

The following shows the ports in VLAN 1 which are attached to multicast routers:

```

Console#show ip igmp snooping mrouter vlan 1
VLAN M'cast Router Ports Type

1 Eth 1/11 Static
2 Eth 1/12 Dynamic
Console#

```

## IGMP Commands (Layer 3)

This section describes commands used to configure Layer 3 IGMP on the ECN330-switch.

Table 110 IGMP Commands (Layer 3)

| Command                                 | Function                                                            | Mode   | Page |
|-----------------------------------------|---------------------------------------------------------------------|--------|------|
| <b>ip igmp</b>                          | Enables IGMP for the specified interface                            | IC     | 953  |
| <b>ip igmp robustval</b>                | Configures the expected packet loss                                 | IC     | 954  |
| <b>ip igmp query-interval</b>           | Configures frequency for sending host query messages                | IC     | 955  |
| <b>ip igmp max-resp-interval</b>        | Configures the maximum host response time                           | IC     | 956  |
| <b>ip igmp last-memb-query-interval</b> | Configures frequency for sending group-specific host query messages | IC     | 957  |
| <b>ip igmp version</b>                  | Configures IGMP version used on this interface                      | IC     | 958  |
| <b>show ip igmp interface</b>           | Displays the IGMP configuration for specified interfaces            | NE, PE | 959  |

| Command                    | Function                                      | Mode   | Page |
|----------------------------|-----------------------------------------------|--------|------|
| <b>clear ip igmp group</b> | Deletes entries from the IGMP cache           | PE     | 960  |
| <b>show ip igmp groups</b> | Displays detailed information for IGMP groups | NE, PE | 961  |

### 7.21.15 ip igmp

This command enables IGMP on a VLAN interface. Use the **no** form of this command to disable IGMP on the specified interface.

#### Syntax

**[no] ip igmp**

#### Default Setting

Disabled

#### Command Mode

Interface Configuration (VLAN)

#### Command Usage

IGMP query can be enabled globally at Layer 2 through the **ip igmp snooping** command, or enabled for specific VLAN interfaces at Layer 3 through the **ip igmp** command. (Layer 2 query is disabled if Layer 3 query is enabled.)

## Example

```
Console(config)#interface vlan 1
Console(config-if)#ip igmp
Console(config-if)#end
Console#show ip igmp interface
Vlan 1 is up
 IGMP is enable, version is 2
 Robustness variable is 2
 Query interval is 125 sec
 Query Max Response Time is 10 sec, Last Member Query Interval is 1
 sec
 Querier is 10.1.0.253

Console#
```

## Related Commands

**ip igmp snooping** (section 7.21.1 on page 936)  
**show ip igmp snooping** (section 7.21.5 on page 940)

### 7.21.16 ip igmp robustval

This command specifies the robustness (expected packet loss) for this interface. Use the **no** form of this command to restore the default value.

#### Syntax

```
ip igmp robustval <robust-value>
no ip igmp robustval

robust-value - The robustness of this interface. (Range: 1-255)
```

#### Default Setting

2

#### Command Mode

Interface Configuration (VLAN)

## Command Usage

The robustness value is used in calculating the appropriate range for other IGMP variables, such as the Group Membership Interval (**ip igmp last-memb-query-interval**, page 957), as well as the Other Querier Present Interval, and the Startup Query Count (RFC 2236).

## Example

```
Console(config-if)#ip igmp robustval 3
Console(config-if)#
```

### 7.21.17 ip igmp query-interval

This command configures the frequency at which host query messages are sent. Use the **no** form to restore the default.

## Syntax

**ip igmp query-interval** <*seconds*>

**no ip igmp query-interval**

*seconds* - The frequency at which the ECN330-switch sends IGMP host-query messages. (Range: 1-255)

## Default Setting

125 seconds

## Command Mode

Interface Configuration (VLAN)

## Command Usage

- Multicast routers send host query messages to determine the interfaces that are connected to downstream hosts requesting a specific multicast service. Only the designated multicast router for a subnet sends host

query messages, which are addressed to the multicast address 224.0.0.1.

- For IGMP Version 1, the designated router is elected according to the multicast routing protocol that runs on the LAN. But for IGMP Version 2, the designated querier is the lowest IP-addressed multicast router on the subnet.

### Example

The following shows how to configure the query interval to 100 seconds:

```
Console(config-if)#ip igmp query-interval 100
Console(config-if)#
```

## 7.21.18 ip igmp max-resp-interval

This command configures the maximum response time advertised in IGMP queries. Use the **no** form of this command to restore the default.

### Syntax

**ip igmp max-resp-interval** <*seconds*>

**no ip igmp max-resp-interval**

*seconds* - The report delay advertised in IGMP queries. (Range: 1-255)

### Default Setting

10 seconds

### Command Mode

Interface Configuration (VLAN)

### Command Usage

- The ECN330-switch must be using IGMPv2 for this command to take effect.

- This command defines how long any responder (that is, client or router) still in the group has to respond to a query message before the router deletes the group.
- By varying the Maximum Response Interval, the burstiness of IGMP messages passed on the subnet can be tuned; where larger values make the traffic less bursty, as host responses are spread out over a larger interval.
- The number of seconds represented by the maximum response interval must be less than the Query Interval (page 955).

### Example

The following shows how to configure the maximum response time to 20 seconds:

```
Console(config-if)#ip igmp max-resp-interval 20
Console(config-if)#
```

### Related Commands

**ip igmp version** (section 7.21.20 on page 958)  
**ip igmp query-interval** (section 7.21.17 on page 955)

## 7.21.19 ip igmp last-memb-query-interval

This command configures the last member query interval. Use the **no** form of this command to restore the default.

### Syntax

**ip igmp last-memb-query-interval** <*seconds*>

**no ip igmp last-memb-query-interval**

*seconds* - The report delay for the last member query. (Range: 1-255)

### Default Setting

1 second

## Command Mode

Interface Configuration (VLAN)

## Command Usage

- A multicast client sends an IGMP leave message when it leaves a group. The router then checks to see if this was the last host in the group by sending an IGMP query and starting a timer based on this command. If no reports are received before the timer expires, the group is deleted.
- This value may be tuned to modify the leave latency of the network. A reduced value results in reduced time to detect the loss of the last member of a group.

## Example

The following shows how to configure the maximum response time to 10 seconds:

```
Console(config-if)#ip igmp last-memb-query-interval 10
Console(config-if)#
```

## 7.21.20

### ip igmp version

This command configures the IGMP version used on an interface. Use the **no** form of this command to restore the default.

## Syntax

```
ip igmp version {1 | 2}
```

```
no ip igmp version
```

- **1** - IGMP Version 1
- **2** - IGMP Version 2

## Default Setting

IGMP Version 2



## Command Mode

Interface Configuration (VLAN)

## Command Usage

- All routers on the subnet must support the same version. However, the multicast hosts on the subnet may support either IGMP version 1 or 2.
- The ECN330-switch must be set to version 2 to enable the **ip igmp max-resp-interval** (page 956).

## Example

The following configures the ECN330-switch to use IGMP Version 1 on the selected interface:

```
Console(config-if)#ip igmp version 1
Console(config-if)#
```

### 7.21.21

## show ip igmp interface

This command shows the IGMP configuration for a specific VLAN interface or for all interfaces.

## Syntax

```
show ip igmp interface [vlan <vlan-id>]
```

*vlan-id* - VLAN ID (Range: 1-4094)

## Default Setting

None

## Command Mode

Normal Exec, Privileged Exec

## Example

The following example shows the IGMP configuration for VLAN 1, as well as the device currently serving as the IGMP querier for this multicast service.

```
Console#show ip igmp interface vlan 1
Vlan 1 is up
 IGMP is enable, version is 2
 Robustness variable is 2
 Query interval is 125 sec
 Query Max Response Time is 10 sec, Last Member Query Interval is 1
 sec
 Querier is 10.1.0.253
Console#
```

## 7.21.22

### clear ip igmp group

This command deletes entries from the IGMP cache.

#### Syntax

```
clear ip igmp group [<group-address> | interface vlan
 <vlan-id>]
```

- *group-address* - IP address of the multicast group.
- *vlan-id* - VLAN ID (Range: 1-4094)

#### Default Setting

Deletes all entries in the cache if no options are selected.

#### Command Mode

Privileged Exec

#### Command Usage

Enter the address for a multicast group to delete all entries for the specified group. Enter the interface option to delete all multicast groups for the specified interface. Enter no options to clear all multicast groups from the cache.

## Example

The following example clears all multicast group entries for VLAN 1:

```
Console#clear ip igmp group interface vlan 1
Console#
```

### 7.21.23 show ip igmp groups

This command displays information on multicast groups active on the ECN330-switch.

#### Syntax

```
show ip igmp groups [<group-address> | interface vlan
 <vlan-id>]
```

- *group-address* - IP address of the multicast group.
- *vlan-id* - VLAN ID (Range: 1-4094)

#### Default Setting

Displays information for all known groups.

#### Command Mode

Normal Exec, Privileged Exec

#### Command Usage

- This command displays information for multicast groups learned through IGMP, not static groups.
- If the ECN330-switch receives an IGMP Version 1 Membership Report, it sets a timer to note that there are Version 1 hosts present which are members of the group for which it heard the report.
- If there are Version 1 hosts present for a particular group, the ECN330-switch will ignore any Leave Group messages that it receives for that group.

## Example

The following shows the IGMP groups currently active on VLAN 1:

```

Console#show ip igmp groups vlan 1

```

| GroupAddress | InterfaceVlan | Lastreporter | Uptime | Expire | VlTimer |
|--------------|---------------|--------------|--------|--------|---------|
| 234.5.6.8    | 1             | 10.1.5.19    | 7068   | 220    | 0       |

```

Console#

```

**Table 111** *show ip igmp groups - Display Description*

| Field         | Description                                                                                                                                                                                           |
|---------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| GroupAddress  | IP multicast group address with subscribers directly attached or downstream from the ECN330-switch.                                                                                                   |
| InterfaceVlan | The interface on the ECN330-switch that has received traffic directed to the multicast group address.                                                                                                 |
| Lastreporter  | The IP address of the source of the last membership report received for this multicast group address on this interface. If no membership report has been received, this object has the value 0.0.0.0. |
| Uptime        | The time elapsed since this entry was created.                                                                                                                                                        |
| Expire        | The time remaining before this entry will be aged out. (The default is 260 seconds.)                                                                                                                  |
| VlTimer       | The time remaining until the ECN330-switch assumes that there are no longer any IGMP Version 1 members on the IP subnet attached to this interface. (The default is 260 seconds.)                     |

## 7.22 Domain Name Service Commands

These commands are used to configure Domain Naming System (DNS) services. Entries can be manually configured in the DNS domain name to IP address mapping table, default domain names configured, or one or more name servers specified to use for domain name to address translation.

Note that domain name services will not be enabled until at least one name server is specified with the **ip name-server** command and domain lookup is enabled with the **ip domain-lookup** command.

Table 112 DNS Commands

| Command                 | Function                                                                                      | Mode | Page |
|-------------------------|-----------------------------------------------------------------------------------------------|------|------|
| <b>ip host</b>          | Creates a static host name-to-address mapping                                                 | GC   | 964  |
| <b>clear host</b>       | Deletes entries from the host name-to-address table                                           | PE   | 965  |
| <b>ip domain-name</b>   | Defines a default domain name for incomplete host names                                       | GC   | 966  |
| <b>ip domain-list</b>   | Defines a list of default domain names for incomplete host names                              | GC   | 967  |
| <b>ip name-server</b>   | Specifies the address of one or more name servers to use for host name-to-address translation | GC   | 968  |
| <b>ip domain-lookup</b> | Enables DNS-based host name-to-address translation                                            | GC   | 969  |
| <b>show hosts</b>       | Displays the static host name-to-address mapping table                                        | PE   | 971  |
| <b>show dns</b>         | Displays the configuration for DNS services                                                   | PE   | 971  |
| <b>show dns cache</b>   | Displays entries in the DNS cache                                                             | PE   | 972  |
| <b>clear dns cache</b>  | Clears all entries from the DNS cache                                                         | PE   | 973  |

### 7.22.1 **ip host**

This command creates a static entry in the DNS table that maps a host name to an IP address. Use the **no** form to remove an entry.

#### **Syntax**

```
[no] ip host <name> <address1> [<address2> ... <address8>]
```

- *name* - Name of the host. (Range: 1-64 characters)
- *address1* - Corresponding IP address.
- *address2 ... address8* - Additional corresponding IP addresses.

#### **Default Setting**

No static entries

#### **Command Mode**

Global Configuration

#### **Command Usage**

Servers or other network devices may support one or more connections through multiple IP addresses. If more than one IP address is associated with a host name using this command, a DNS client can try each address in succession, until it establishes a connection with the target device.

## Example

This example maps two address to a host name.

```
Console(config)#ip host rd5 192.168.1.55 10.1.0.55
Console(config)#end
Console#show hosts

Hostname
 rd5
Inet address
 10.1.0.55 192.168.1.55
Alias
Console#
```

### 7.22.2

## clear host

This command deletes entries from the DNS table.

## Syntax

```
clear host {<name> | *}
```

- *name* - Name of the host. (Range: 1-64 characters)
- \* - Removes all entries.

## Default Setting

None

## Command Mode

Privileged Exec

## Example

This example clears all static entries from the DNS table.

```
Console(config)#clear host *
Console(config)#
```

### 7.22.3 **ip domain-name**

This command defines the default domain name appended to incomplete host names (that is, host names passed from a client that are not formatted with dotted notation). Use the **no** form to remove the current domain name.

#### **Syntax**

```
ip domain-name <name>
```

```
no ip domain-name
```

*name* - Name of the host. Do not include the initial dot that separates the host name from the domain name. (Range: 1-64 characters)

#### **Default Setting**

None

#### **Command Mode**

Global Configuration

#### **Example**

```
Console(config)#ip domain-name sample.com
Console(config)#end
Console#show dns
Domain Lookup Status:
 DNS disabled
Default Domain Name:
 .sample.com
Domain Name List:
Name Server List:
Console#
```

#### **Related Commands**

**ip domain-list** (section 7.22.4 on page 967)

**ip name-server** (section 7.22.5 on page 968)

**ip domain-lookup** (section 7.22.6 on page 969)



## 7.22.4 **ip domain-list**

This command defines a list of domain names that can be appended to incomplete host names (that is, host names passed from a client that are not formatted with dotted notation). Use the **no** form to remove a name from this list.

### **Syntax**

```
[no] ip domain-list <name>
```

*name* - Name of the host. Do not include the initial dot that separates the host name from the domain name. (Range: 1-64 characters)

### **Default Setting**

None

### **Command Mode**

Global Configuration

### **Command Usage**

- Domain names are added to the end of the list one at a time.
- When an incomplete host name is received by the DNS service on the ECN330-switch, it will work through the domain list, appending each domain name in the list to the host name, and checking with the specified name servers for a match.
- If there is no domain list, the domain name specified with the **ip domain-name** command is used. If there is a domain list, the default domain name is not used.

## Example

This example adds two domain names to the current list and then displays the list.

```
Console(config)#ip domain-list sample.com.jp
Console(config)#ip domain-list sample.com.uk
Console(config)#end
Console#show dns
Domain Lookup Status:
 DNS disabled
Default Domain Name:
 .sample.com
Domain Name List:
 .sample.com.jp
 .sample.com.uk
Name Server List:
Console#
```

## Related Commands

**ip domain-name** (section 7.22.3 on page 966)

### 7.22.5 ip name-server

This command specifies the address of one or more domain name servers to use for name-to-address resolution. Use the **no** form to remove a name server from this list.

#### Syntax

```
[no] ip name-server <server-address1> [<server-address2>
... <server-address6>]
```

- *server-address1* - IP address of domain-name server.
- *server-address2 ... server-address6* - IP address of additional domain-name servers.

#### Default Setting

None

## Command Mode

### Global Configuration

## Command Usage

The listed name servers are queried in the specified sequence until a response is received, or the end of the list is reached with no response.

## Example

This example adds two domain-name servers to the list and then displays the list.

```
Console(config)#ip domain-server 192.168.1.55 10.1.0.55
Console(config)#end
Console#show dns
Domain Lookup Status:
 DNS disabled
Default Domain Name:
 .sample.com
Domain Name List:
 .sample.com.jp
 .sample.com.uk
Name Server List:
 192.168.1.55
 10.1.0.55
Console#
```

## Related Commands

**ip domain-name** (section 7.22.3 on page 966)

**ip domain-lookup** (section 7.22.6 on page 969)

## 7.22.6

### ip domain-lookup

This command enables DNS host name-to-address translation. Use the **no** form to disable DNS.

## Syntax

```
[no] ip domain-lookup
```

## Default Setting

Disabled

## Command Mode

Global Configuration

## Command Usage

- At least one name server must be specified before DNS can be enabled.
- If all name servers are deleted, DNS will automatically be disabled.

## Example

This example enables DNS and then displays the configuration.

```
Console(config)#ip domain-lookup
Console(config)#end
Console#show dns
Domain Lookup Status:
 DNS enabled
Default Domain Name:
 .sample.com
Domain Name List:
 .sample.com.jp
 .sample.com.uk
Name Server List:
 192.168.1.55
 10.1.0.55
```

## Related Commands

**ip domain-name** (section 7.22.3 on page 966)

**ip name-server** (section 7.22.5 on page 968)

### 7.22.7 **show hosts**

This command displays the static host name-to-address mapping table.

#### **Command Mode**

Privileged Exec

#### **Example**

Note that a host name will be displayed as an alias if it is mapped to the same address(es) as a previously configured entry.

```
Console#show hosts

Hostname
 rd5
Inet address
 10.1.0.55 192.168.1.55
Alias
 1.rd6
Console#
```

### 7.22.8 **show dns**

This command displays the configuration of the DNS server.

#### **Command Mode**

Privileged Exec

## Example

```

Console#show dns
Domain Lookup Status:
 DNS enabled
Default Domain Name:
 sample.com
Domain Name List:
 sample.com.jp
 sample.com.uk
Name Server List:
 192.168.1.55
 10.1.0.55
Console#

```

### 7.22.9

## show dns cache

This command displays entries in the DNS cache.

### Command Mode

Privileged Exec

## Example

```

Console#show dns cache
NO FLAG TYPE IP TTL DOMAIN
0 4 CNAME 10.2.44.96 893
 pttch_pc.accton.com.tw
1 4 CNAME 10.2.44.3 898 ahten.com.tw
2 4 CNAME 66.218.71.84 298 www.yahoo.akadns.net
3 4 CNAME 66.218.71.83 298 www.yahoo.akadns.net
4 4 CNAME 66.218.71.81 298 www.yahoo.akadns.net
5 4 CNAME 66.218.71.80 298 www.yahoo.akadns.net
6 4 CNAME 66.218.71.89 298 www.yahoo.akadns.net
7 4 CNAME 66.218.71.86 298 www.yahoo.akadns.net
8 4 ALIAS POINTER TO:7 298 www.yahoo.com
Console#

```

*Table 113 show dns cache - Display Description*

| Field  | Description                                                                                                                                                                                          |
|--------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| NO     | The entry number for each resource record.                                                                                                                                                           |
| FLAG   | The flag is always “4” indicating a cache entry and therefore unreliable.                                                                                                                            |
| TYPE   | This field includes CNAME which specifies the canonical or primary name for the owner, and ALIAS which specifies multiple domain names which are mapped to the same IP address as an existing entry. |
| IP     | The IP address associated with this record.                                                                                                                                                          |
| TTL    | The time to live reported by the name server.                                                                                                                                                        |
| DOMAIN | The domain name associated with this record.                                                                                                                                                         |

### 7.22.10 clear dns cache

This command clears all entries in the DNS cache.

#### Command Mode

Privileged Exec

#### Example

```

Console#clear dns cache
Console#show dns cache
NO FLAG TYPE IP TTL DOMAIN
Console#

```

## 7.23 Dynamic Host Configuration Protocol Commands

These commands are used to configure Dynamic Host Configuration Protocol (DHCP) client, relay, and server functions. Any VLAN interface can be configured to be automatically assigned an IP address through DHCP. The ECN330-switch can be configured to relay DHCP client configuration requests to a DHCP server on another network, or it can be configured to provide DHCP service directly to any client.

*Table 114 DHCP Commands*

| Command Group | Function                                                        | Page |
|---------------|-----------------------------------------------------------------|------|
| DHCP Client   | Allows interfaces to dynamically acquire IP address information | 974  |
| DHCP Relay    | Relays DHCP requests from local hosts to a remote DHCP server   | 977  |
| DHCP Server   | Configures DHCP service using address pools or static bindings  | 980  |

### DHCP Client

Use the commands in this section to allow ECN330-switch VLAN interfaces to dynamically acquire IP address information.

*Table 115 DHCP Client Commands*

| Command                          | Function                                                   | Mode | Page |
|----------------------------------|------------------------------------------------------------|------|------|
| <b>ip dhcp client-identifier</b> | Specifies the DHCP client identifier for the ECN330-switch | IC   | 975  |
| <b>ip dhcp restart client</b>    | Submits a BOOTP or DHCP client request                     | PE   | 976  |



### 7.23.1 ip dhcp client-identifier

This command specifies the DHCP client identifier for the current interface. Use the **no** form to remove this identifier.

#### Syntax

```
ip dhcp client-identifier {text <text >| hex <hex>}
no ip dhcp client-identifier
```

- *text* - A text string. (Range: 1-15 characters)
- *hex* - The hexadecimal value.

#### Default Setting

None

#### Command Mode

Interface Configuration (VLAN)

#### Command Usage

This command is used to include a client identifier in all communications with the DHCP server. The identifier type depends on the requirements of the DHCP server.

#### Example

```
Console(config)#interface vlan 2
Console(config-if)#ip dhcp client-identifier hex 00-00-e8-66-65-72
Console(config-if)#
```

#### Related Commands

**ip dhcp restart client** (section 7.23.2 on page 976)

### 7.23.2 ip dhcp restart client

This command submits a BOOTP or DHCP client request.

#### Default Setting

None

#### Command Mode

Privileged Exec

#### Command Usage

- This command issues a BOOTP or DHCP client request for any IP interface that has been set to BOOTP or DHCP mode through the **ip address** command.
- DHCP requires the server to reassign the client's last address if available.
- If the BOOTP or DHCP server has been moved to a different domain, the network portion of the address provided to the client will be based on this new domain.

#### Example

In the following example, the device is reassigned the same address.

```
Console(config)#interface vlan 1
Console(config-if)#ip address dhcp
Console(config-if)#exit
Console#ip dhcp restart client
Console#show ip interface

Vlan 1 is up, addressing mode is DHCP
 Interface address is 192.168.1.54, mask is 255.255.255.0, Primary
 MTU is 1500 bytes
 Proxy ARP is disabled
 Split horizon is enabled
Console#
```

## Related Commands

**ip address** (section 7.25.1 on page 1016)

## DHCP Relay

Use the commands in this section to configure the ECN330-switch to relay DHCP requests from local hosts to a remote DHCP server.

*Table 116 DHCP Relay Commands*

| Command                      | Function                                  | Mode | Page |
|------------------------------|-------------------------------------------|------|------|
| <b>ip dhcp restart relay</b> | Enables DHCP relay agent                  | IC   | 977  |
| <b>ip dhcp relay server</b>  | Specifies DHCP server addresses for relay | IC   | 979  |

### 7.23.3 ip dhcp restart relay

This command enables DHCP relay for the specified VLAN. Use the **no** form to disable it.

#### Syntax

```
[no] ip dhcp relay
```

#### Default Setting

Disabled

#### Command Mode

Interface Configuration (VLAN)

## Command Usage

This command is used to configure DHCP relay functions for host devices attached to the ECN330-switch. If DHCP relay service is enabled, and the ECN330-switch sees a DHCP request broadcast, it inserts its own IP address into the request so the DHCP server will know the subnet where the client is located. Then, the ECN330-switch forwards the packet to the DHCP server on another network. When the server receives the DHCP request, it allocates a free IP address for the DHCP client from its defined scope for the DHCP client's subnet, and sends a DHCP response back to the DHCP relay agent (that is, the ECN330-switch). The ECN330-switch then broadcasts the DHCP response received from the server to the client.

## Example

In the following example, the device is reassigned the same address.

```
Console(config)#interface vlan 1
Console(config-if)#ip dhcp relay
Console(config-if)#end
Console#show ip interface

Vlan 1 is up, addressing mode is Dhcp
 Interface address is 10.1.0.254, mask is 255.255.255.0, Primary
 MTU is 1500 bytes
 Proxy ARP is disabled
 Split horizon is enabled
Console#
```

## Related Commands

**ip dhcp relay server** (section 7.23.4 on page 979)

## 7.23.4 ip dhcp relay server

This command specifies the addresses of DHCP servers to be used by the ECN330-switch's DHCP relay agent. Use the **no** form to clear all addresses.

### Syntax

```
ip dhcp relay server <address1> [address2 [address3
...]]
```

```
no ip dhcp relay server
```

*address* - IP address of DHCP server. (Range: 1-3 addresses)

### Default Setting

None

### Command Mode

Interface Configuration (VLAN)

### Command Usage

- The IP address for at least one DHCP server must be specified. Otherwise, the ECN330-switch's DHCP relay agent will not forward client requests to a DHCP server.
- To start DHCP relay service, enter the **ip dhcp restart relay** command.

### Example

```
Console(config)#interface vlan 1
Console(config-if)#ip dhcp relay server 10.1.0.99
Console(config-if)#
```

### Related Commands

**ip dhcp restart relay** (section 7.23.3 on page 977)

## DHCP Server

The commands in this section configure a DHCP service on the ECN330-switch using address pools or static bindings.

Table 117 DHCP Server Commands

| Command                         | Function                                                                                                   | Mode | Page |
|---------------------------------|------------------------------------------------------------------------------------------------------------|------|------|
| <b>service dhcp</b>             | Enables the DHCP server feature on the ECN330-switch                                                       | GC   | 981  |
| <b>ip dhcp excluded-address</b> | Specifies IP addresses that a DHCP server should not assign to DHCP clients                                | GC   | 982  |
| <b>ip dhcp pool</b>             | Configures a DHCP address pool on a DHCP Server                                                            | GC   | 983  |
| <b>network</b>                  | Configures the subnet number and mask for a DHCP address pool                                              | DC   | 984  |
| <b>default-router</b>           | Specifies the default router list for a DHCP client                                                        | DC   | 985  |
| <b>domain-name</b>              | Specifies the domain name for a DHCP client                                                                | DC   | 986  |
| <b>dns-server</b>               | Specifies the Domain Name Server (DNS) servers available to a DHCP client                                  | DC   | 986  |
| <b>next-server</b>              | Configures the next server in the boot process of a DHCP client                                            | DC   | 987  |
| <b>bootfile</b>                 | Specifies a default boot image for a DHCP client                                                           | DC   | 988  |
| <b>netbios-name-server</b>      | Configures NetBIOS Windows Internet Naming Service (WINS) name servers available to Microsoft DHCP clients | DC   | 989  |
| <b>netbios-node-type</b>        | Configures NetBIOS node type for Microsoft DHCP clients                                                    | DC   | 990  |
| <b>lease</b>                    | Sets the duration an IP address is assigned to a DHCP client                                               | DC   | 991  |

| Command                      | Function                                                                    | Mode   | Page |
|------------------------------|-----------------------------------------------------------------------------|--------|------|
| <b>host*</b>                 | Specifies the IP address and network mask to manually bind to a DHCP client | DC     | 992  |
| <b>client-identifier*</b>    | Specifies a client identifier for a DHCP client                             | DC     | 993  |
| <b>hardware-address*</b>     | Specifies the hardware address of a DHCP client                             | DC     | 994  |
| <b>clear ip dhcp binding</b> | Deletes an automatic address binding from the DHCP server database          | PE     | 995  |
| <b>show ip dhcp binding</b>  | Displays address bindings on the DHCP server                                | PE, NE | 996  |

\* These commands are used for manually binding an address to a client.

### 7.23.5 service dhcp

This command enables the DHCP server on the ECN330-switch. Use the **no** form to disable the DHCP server.

#### Syntax

**[no] service dhcp**

#### Default Setting

Enabled

#### Command Mode

Global Configuration

#### Command Usage

If the DHCP server is running, it must be restarted to implement any configuration changes.

## Example

```
Console(config)#service dhcp
Console(config)#
```

### 7.23.6 ip dhcp excluded-address

This command specifies IP addresses that the DHCP server should not assign to DHCP clients. Use the **no** form to remove the excluded IP addresses.

#### Syntax

```
[no] ip dhcp excluded-address <low-address> [high-address]
```

- *low-address* - An excluded IP address, or the first IP address in an excluded address range.
- *high-address* - The last IP address in an excluded address range.

#### Default Setting

All IP pool addresses may be assigned.

#### Command Mode

Global Configuration

## Example

```
Console(config)#ip dhcp excluded-address 10.1.0.19
Console(config)#
```



### 7.23.7 ip dhcp pool

This command configures a DHCP address pool and enter DHCP Pool Configuration mode. Use the **no** form to remove the address pool.

#### Syntax

```
[no] ip dhcp pool <name>
```

*name* - A string or integer. (Range: 1-8 characters)

#### Default Setting

DHCP address pools are not configured.

#### Command Mode

Global Configuration

#### Command Usage

- After executing this command, the ECN330-switch changes to DHCP Pool Configuration mode, identified by the `(config-dhcp) #` prompt.
- From this mode, first configure address pools for the network interfaces (using the **network** command). An address can also be manually bound to a specific client (with the **host** command) if required. Up to 8 network address pools can be configured, and up to 32 manually bound host address pools (that is, listing one host address per pool). However, note that any address specified in a **host** command must fall within the range of a configured network address pool.

#### Example

```
Console(config)#ip dhcp pool R&D
Console(config-dhcp)#
```

#### Related Commands

**network** (section 7.23.8 on page 984)

**host** (section 7.23.17 on page 992)

### 7.23.8 network

This command configures the subnet number and mask for a DHCP address pool. Use the **no** form to remove the subnet number and mask.

#### Syntax

```
network <network-number> [mask]
```

```
no network
```

- *network-number* - The IP address of the DHCP address pool.
- *mask* - The bit combination that identifies the network (or subnet) and the host portion of the DHCP address pool.

#### Command Mode

DHCP Pool Configuration

#### Command Usage

- When a client request is received, the ECN330-switch first checks for a network address pool matching the gateway where the request originated (that is, if the request was forwarded by a relay server). If there is no gateway in the client request (that is, the request was not forwarded by a relay server), the ECN330-switch searches for a network pool matching the interface through which the client request was received. It then searches for a manually configured host address that falls within the matching network pool. If no manually configured host address is found, it assigns an address from the matching network address pool. However, if no matching address pool is found the request is ignored.
- This command is valid for DHCP network address pools only. If the mask is not specified, the class A, B, or C natural mask is used (see page 428). The DHCP server assumes that all host addresses are available. Subsets of the address space can be excluded by using the **ip dhcp excluded-address** command.

## Example

```
Console(config-dhcp)#network 10.1.0.0 255.255.255.0
Console(config-dhcp)#
```

### 7.23.9

## default-router

This command specifies default routers for a DHCP pool. Use the **no** form to remove the default routers.

### Syntax

**default-router** <*address1*> [*address2*]

**no default-router**

- *address1* - Specifies the IP address of the primary router.
- *address2* - Specifies the IP address of an alternate router.

### Default Setting

None

### Command Mode

DHCP Pool Configuration

### Command Usage

The IP address of the router should be on the same subnet as the client. Up to two routers can be specified. Routers are listed in order of preference (starting with *address1* as the most preferred router).

## Example

```
Console(config-dhcp)#default-router 10.1.0.54 10.1.0.64
Console(config-dhcp)#
```

### 7.23.10 domain-name

This command specifies the domain name for a DHCP client. Use the **no** form to remove the domain name.

#### Syntax

```
domain-name <domain>
```

```
no domain-name
```

*domain* - Specifies the domain name of the client.  
(Range: 1-32 characters)

#### Default Setting

None

#### Command Mode

DHCP Pool Configuration

#### Example

```
Console(config-dhcp)#domain-name sample.com
Console(config-dhcp)#
```

### 7.23.11 dns-server

This command specifies the Domain Name System (DNS) IP servers available to a DHCP client. Use the **no** form to remove the DNS server list.

#### Syntax

```
dns-server <address1> [address2]
```

```
no dns-server
```

- *address1* - Specifies the IP address of the primary DNS server.
- *address2* - Specifies the IP address of the alternate DNS server.

**Default Setting**

None

**Command Mode**

DHCP Pool Configuration

**Command Usage**

- If DNS IP servers are not configured for a DHCP client, the client cannot correlate host names to IP addresses.
- Servers are listed in order of preference (starting with *address1* as the most preferred server).

**Example**

```
Console(config-dhcp)#dns-server 10.1.1.253 192.168.3.19
Console(config-dhcp)#
```

**7.23.12****next-server**

This command configures the next server in the boot process of a DHCP client. Use the **no** form to remove the boot server list.

**Syntax**

**[no] next-server <address>**

*address* - Specifies the IP address of the next server in the boot process, which is typically a Trivial File Transfer Protocol (TFTP) server.

**Default Setting**

None

**Command Mode**

DHCP Pool Configuration

## Example

```
Console(config-dhcp)#next-server 10.1.0.21
Console(config-dhcp)#
```

## Related Commands

**bootfile** (section 7.23.13 on page 988)

### 7.23.13

## bootfile

This command specifies the name of the default boot image for a DHCP client. This file should be placed on the Trivial File Transfer Protocol (TFTP) server specified with the **next-server** command. Use the **no** form to delete the boot image name.

## Syntax

**bootfile** <*filename*>

**no bootfile**

*filename* - Name of the file that is used as a default boot image.

## Default Setting

None

## Command Mode

DHCP Pool Configuration

## Example

```
Console(config-dhcp)#bootfile wme.bat
Console(config-dhcp)#
```

## Related Commands

**next-server** (section 7.23.12 on page 987)

### 7.23.14 netbios-name-server

This command configures NetBIOS Windows Internet Naming Service (WINS) name servers that are available to Microsoft DHCP clients. Use the **no** form to remove the NetBIOS name server list.

#### Syntax

**netbios-name-server** <*address1*> [*address2*]

**no netbios-name-server**

- *address1* - Specifies IP address of primary NetBIOS WINS name server.
- *address2* - Specifies IP address of alternate NetBIOS WINS name server.

#### Default Setting

None

#### Command Mode

DHCP Pool Configuration

#### Command Usage

Servers are listed in order of preference (starting with *address1* as the most preferred server).

#### Example

```
Console(config-dhcp)#netbios-name-server 10.1.0.33 10.1.0.34
Console(config-dhcp)#
```

## Related Commands

**netbios-node-type** (section 7.23.15 on page 990)

### 7.23.15 netbios-node-type

This command configures the NetBIOS node type for Microsoft DHCP clients. Use the **no** form to remove the NetBIOS node type.

#### Syntax

**netbios-node-type** <type>

**no netbios-node-type**

*type* - Specifies the NetBIOS node type:

- **broadcast**
- **hybrid** (recommended)
- **mixed**
- **peer-to-peer**

#### Default Setting

None

#### Command Mode

DHCP Pool Configuration

#### Example

```
Console(config-dhcp)#netbios-node-type hybrid
Console(config-dhcp)#
```

## Related Commands

**netbios-name-server** (section 7.23.14 on page 989)



## 7.23.16 **lease**

This command configures the duration that an IP address is assigned to a DHCP client. Use the **no** form to restore the default value.

### **Syntax**

```
lease {days [hours] [minutes] | infinite}
```

```
no lease
```

- *days* - Specifies the duration of the lease in numbers of days. (Range: 0-364)
- *hours* - Specifies the number of hours in the lease. A *days* value must be supplied before *hours* can be configured. (Range: 0-23)
- *minutes* - Specifies the number of minutes in the lease. A *days* and *hours* value must be supplied before *minutes* can be configured. (Range: 0-59)
- **infinite** - Specifies that the lease time is unlimited. This option is normally used for addresses manually bound to a BOOTP client through the **host** command.

### **Default Setting**

One day

### **Command Modes**

DHCP Pool Configuration

### **Example**

The following example leases an address to clients using this pool for 7 days.

```
Console(config-dhcp)#lease 7
Console(config-dhcp)#
```

## 7.23.17 **host**

Use this command to specify the IP address and network mask to manually bind to a DHCP client. Use the **no** form to remove the IP address for the client.

### Syntax

```
host <address> [mask]
```

```
no host
```

- *address* - Specifies the IP address of a client.
- *mask* - Specifies the network mask of the client.

### Default Setting

None

### Command Mode

DHCP Pool Configuration

### Command Usage

- Host addresses must fall within the range specified for an existing network pool.
- When a client request is received, the ECN330-switch first checks for a network address pool matching the gateway where the request originated (that is, if the request was forwarded by a relay server). If there is no gateway in the client request (that is, the request was not forwarded by a relay server), the ECN330-switch searches for a network pool matching the interface through which the client request was received. It then searches for a manually configured host address that falls within the matching network pool.
- When searching for a manual binding, the ECN330-switch compares the client identifier for DHCP clients, and then compares the hardware address for DHCP or BOOTP clients.
- If no manual binding has been specified for a host entry with the **client-identifier** or **hardware-address** commands, then the ECN330-switch will assign an address from the matching network pool.

- If the mask is unspecified, DHCP examines its address pools. If no mask is found in the pool database, the Class A, B, or C natural mask is used (see page 428). This command is valid for manual bindings only.
- The **no host** command only clears the address from the DHCP server database. It does not cancel the IP address currently in use by the host.

### Example

```
Console(config-dhcp)#host 10.1.0.21 255.255.255.0
Console(config-dhcp)#
```

### Related Commands

**client-identifier** (section 7.23.18 on page 993)  
**hardware-address** (section 7.23.19 on page 994)

## 7.23.18

### client-identifier

This command specifies the client identifier of a DHCP client. Use the **no** form to remove the client identifier.

#### Syntax

```
client-identifier {text <text> | hex <hex>}

no client-identifier
```

- *text* - A text string. (Range: 1-15 characters)
- *hex* - The hexadecimal value.

#### Default Setting

None

#### Command Mode

DHCP Pool Configuration

## Command Usage

- This command identifies a DHCP client to bind to an address specified in the **host** command. If both a client identifier and hardware address are configured for a host address, the client identifier takes precedence over the hardware address in the search procedure.
- BOOTP clients cannot transmit a client identifier. To bind an address to a BOOTP client, a hardware address must be associated with the host entry.

## Example

```
Console(config-dhcp)#client-identifier text steve
Console(config-dhcp)#
```

## Related Commands

**host** (section 7.23.17 on page 992)

## 7.23.19

### hardware-address

This command specifies the hardware address of a DHCP client. This command is valid for manual bindings only. Use the **no** form to remove the hardware address.

## Syntax

**hardware-address** *<hardware-address>* *<type>*

**no hardware-address**

- *hardware-address* - Specifies the MAC address of the client device.
- *type* - Indicates the following protocol used on the client device:
  - **ethernet**
  - **ieee802**
  - **fddi**

### Default Setting

If no type is specified, the default protocol is Ethernet.

### Command Mode

DHCP Pool Configuration

### Command Usage

This command identifies a DHCP or BOOTP client to bind to an address specified in the **host** command. BOOTP clients cannot transmit a client identifier. To bind an address to a BOOTP client, a hardware address must be associated with the host entry.

### Example

```

Console(config-dhcp)#hardware-address 00-e0-29-94-34-28 ethernet
Console(config-dhcp)#

```

### Related Commands

**host** (section 7.23.17 on page 992)

## 7.23.20 clear ip dhcp binding

This command deletes an automatic address binding from the DHCP server database.

### Syntax

**clear ip dhcp binding {*address* | \* }**

- *address* - The address of the binding to clear.
- \* - Clears all automatic bindings.

### Default Setting

None

## Command Mode

Privileged Exec

## Command Usage

- An *address* specifies the client's IP address. If an asterisk (\*) is used as the address parameter, the DHCP server clears all automatic bindings.
- Use the **no host** command to delete a manual binding.
- This command is normally used after modifying the address pool, or after moving DHCP service to another device.

## Example

```
Console#clear ip dhcp binding *
Console#
```

## Related Commands

**show ip dhcp binding** (section 7.23.21 on page 996)

### 7.23.21 show ip dhcp binding

This command displays address bindings on the DHCP server.

## Syntax

**show ip dhcp binding [address]**

*address* - Specifies the IP address of the DHCP client for which bindings will be displayed.

## Default Setting

None

**Command Mode**

Normal Exec, Privileged Exec

**Example**

```
Console#show ip dhcp binding
```

| IP         | MAC               | Lease Time<br>(dd/hh/mm/ss) | Start                |
|------------|-------------------|-----------------------------|----------------------|
| -----      |                   |                             |                      |
| 192.1.3.21 | 00-00-e8-98-73-21 | 86400                       | Dec 25 08:01:57 2002 |

```
Console#
```

## 7.24 Router Redundancy Commands

Router redundancy protocols use a virtual IP address to support a primary router and multiple backup routers. The backup routers can be configured to take over the workload if the master router fails, or can also be configured to share the traffic load. The primary goal of router redundancy is to allow a host device which has been configured with a fixed gateway to maintain network connectivity in case the primary gateway goes down.

*Table 118 Router Redundancy Commands*

| Command Groups                     | Function                               | Page |
|------------------------------------|----------------------------------------|------|
| Virtual Router Redundancy Protocol | Configures interface settings for VRRP | 999  |



## Virtual Router Redundancy Protocol Commands

To configure VRRP, select an interface on one router in the group to serve as the master virtual router. This physical interface is used as the virtual address for the router group. Now set the same virtual address and a priority on the backup routers, and configure an authentication string. The preempt feature can also be enabled, which allows a router to take over as the master router when it comes on line.

*Table 119 VRRP Commands*

| Command                          | Function                                                                                                                                        | Mode | Page |
|----------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------|------|------|
| <b>vrrp</b>                      | Creates a VRRP group on a VLAN interface                                                                                                        | IC   | 1000 |
| <b>vrrp ip</b>                   | Enables VRRP and sets the IP address of the virtual router                                                                                      | IC   | 1001 |
| <b>vrrp authentication</b>       | Configures a key used to authenticate VRRP packets received from other routers                                                                  | IC   | 1002 |
| <b>vrrp priority</b>             | Sets the priority of this router in the VRRP group                                                                                              | IC   | 1003 |
| <b>vrrp timers advertise</b>     | Sets the interval between successive advertisements by the master virtual router                                                                | IC   | 1004 |
| <b>vrrp preempt</b>              | Configures the router to take over as master virtual router for a VRRP group if it has a higher priority than the current master virtual router | IC   | 1005 |
| <b>show vrrp</b>                 | Displays VRRP status information                                                                                                                | PE   | 1007 |
| <b>show vrrp all</b>             | Displays a full listing of status information for all VRRP groups                                                                               | PE   | 1010 |
| <b>show vrrp interface</b>       | Displays VRRP status information for the specified interface                                                                                    | PE   | 1011 |
| <b>show vrrp router counters</b> | Displays VRRP statistics                                                                                                                        | PE   | 1012 |

| Command                              | Function                                             | Mode | Page |
|--------------------------------------|------------------------------------------------------|------|------|
| <b>show vrrp interface counters</b>  | Displays VRRP statistics for the specified interface | PE   | 1013 |
| <b>clear vrrp router counters</b>    | Clears VRRP router statistics                        | PE   | 1014 |
| <b>clear vrrp interface counters</b> | Clears VRRP interface statistics                     | PE   | 1014 |

### 7.24.1 vrrp

This command creates a Virtual Router Redundancy Protocol (VRRP) group on an interface. Use the **no** form to delete a VRRP group on an interface.

#### Syntax

**[no] vrrp <group>**

*group* - Identifies the virtual router group. (Range: 1-255)

#### Default Setting

No virtual router groups are configured.

#### Command Mode

Interface (VLAN)

#### Example

This example creates VRRP group 1 on VLAN 1.

```
Console(config)#interface vlan 1
Console(config-if)#vrrp 1
Console(config-if)#
```

## 7.24.2 vrrp ip

This command enables the Virtual Router Redundancy Protocol (VRRP) on an interface and specify the IP address of the virtual router. Use the **no** form to disable VRRP on an interface and remove the IP address from the virtual router.

### Syntax

```
[no] vrrp <group> ip <ip-address>
```

- *group* - Identifies the virtual router group. (Range: 1-255)
- *ip-address* - The IP address of the virtual router.

### Default Setting

No virtual router groups are configured.

### Command Mode

Interface (VLAN)

### Command Usage

- The interfaces of all routers participating in a virtual router group must be within the same IP subnet.
- The IP address assigned to the virtual router must already be configured on the router that will be the Owner. In other words, the IP address specified in this command must already exist on one, and only one, router in the virtual router group, and the network mask for the virtual router address is derived from the Owner. The Owner will also assume the role of the Master virtual router in the group.
- VRRP is enabled as soon as this command is entered. To customize any of the other parameters for VRRP, such as authentication, priority, or advertisement interval, then first configure these parameters before enabling VRRP.

## Example

This example creates VRRP group 1 using the primary interface for VLAN 1 as the VRRP group Owner.

```
Console(config)#interface vlan 1
Console(config-if)#vrrp 1 ip 192.168.1.6
Console(config-if)#
```

### 7.24.3 vrrp authentication

This command specifies the key used to authenticate VRRP packets received from other routers. Use the **no** form to prevent authentication.

#### Syntax

**vrrp <group> authentication <key>**

**no vrrp <group> authentication**

- *group* - Identifies the virtual router group. (Range: 1-255)
- *key* - Authentication string. (Range: 1-8 alphanumeric characters)

#### Default Setting

No key is defined.

#### Command Mode

Interface (VLAN)

#### Command Usage

- All routers in the same VRRP group must be configured with the same authentication key.
- When a VRRP packet is received from another router in the group, its authentication key is compared to the string configured on this router. If the keys match, the message is accepted. Otherwise, the packet is discarded.

- Plain text authentication does not provide any real security. It is supported only to prevent a misconfigured router from participating in VRRP.

### Example

```
Console(config-if)#vrrp 1 authentication bluebird
Console(config-if)#
```

## 7.24.4

### vrrp priority

This command sets the priority of this router in a VRRP group. Use the **no** form to restore the default setting.

#### Syntax

**vrrp <group> priority <level>**

**no vrrp <group> priority**

- *group* - Identifies the VRRP group. (Range: 1-255)
- *level* - Priority of this router in the VRRP group. (Range: 1-254)

#### Default Setting

100

#### Command Mode

Interface (VLAN)

#### Command Usage

- A router that has a physical interface with the same IP address as that used for the virtual router will become the master virtual router. The backup router with the highest priority will become the master router if the current master fails. When the original master router recovers, it will take over as the active master router again.

- If two or more routers are configured with the same VRRP priority, the router with the higher IP address is elected as the new master router if the current master fails.
- If the backup preempt function is enabled with the **vrrp preempt** command, and a backup router with a priority higher than the current acting master comes on line, this backup router will take over as the new acting master. However, note that if the original master (that is, the owner of the VRRP IP address) comes back on line, it will always resume control as the master.

### Example

```
Console(config-if)#vrrp 1 priority 1
Console(config-if)#
```

### Related Commands

**vrrp preempt** (section 7.24.6 on page 1005)

## 7.24.5 vrrp timers advertise

This command sets the interval at which the master virtual router sends advertisements communicating its state as the master. Use the **no** form to restore the default interval.

### Syntax

**vrrp <group> timers advertise <interval>**

**no vrrp <group> timers advertise**

- *group* - Identifies the VRRP group. (Range: 1-255)
- *interval* - Advertisement interval for the master virtual router. (Range: 1-255 seconds)

### Default Setting

1 second

## Command Mode

Interface (VLAN)

## Command Usage

- VRRP advertisements from the current master virtual router include information about its priority and current state as the master.
- VRRP advertisements are sent to the multicast address 224.0.0.8. Using a multicast address reduces the amount of traffic that has to be processed by network devices that are not part of the designated VRRP group.
- If the master router stops sending advertisements, backup routers will bid to become the master router based on priority. The dead interval before attempting to take over as the master is three times the hello interval plus half a second

## Example

```
Console(config-if)#vrrp 1 timers advertise 5
Console(config-if)#
```

### 7.24.6

## vrrp preempt

This command configures the router to take over as the master virtual router for a VRRP group if it has a higher priority than the current acting master router. Use the **no** form to disable preemption.

## Syntax

```
vrrp <group> preempt [delay <seconds>]
```

```
no vrrp <group> preempt
```

- *group* - Identifies the VRRP group. (Range: 1-255)
- *seconds* - The time to wait before issuing a claim to become the master. (Range: 0-120 seconds)

## Default Setting

Preempt: Enabled  
Delay: 0 seconds

## Command Mode

Interface (VLAN)

## Command Usage

- If preempt is enabled, and this backup router has a priority higher than the current acting master, it will take over as the new master. However, note that if the original master (that is, the owner of the VRRP IP address) comes back on line, it will always resume control as the master.
- The delay can give additional time to receive an advertisement message from the current master before taking control. If the router attempting to become the master has just come on line, this delay also gives it time to gather information for its routing table before actually preempting the currently active router.

## Example

```
Console(config-if)#vrrp 1 preempt delay 10
Console(config-if)#
```

## Related Commands

**vrrp priority** (section 7.24.4 on page 1003)



## 7.24.7 **show vrrp**

This command displays status information for VRRP.

### **Syntax**

```
show vrrp [brief | <group>]
```

- **brief** - Displays summary information for all VRRP groups on this router.
- *group* - Identifies a VRRP group. (Range: 1-255)

### **Defaults**

None

### **Command Mode**

Privileged Exec

### **Command Usage**

- Use this command without any keywords to display the full listing of status information for all VRRP groups configured on this router.
- Use this command with the **brief** keyword to display a summary of status information for all VRRP groups configured on this router.
- Specify a group number to display status information for a specific group

## Example

This example displays the full listing of status information for all groups.

```

Console#show vrrp
Vlan 1 - Group 1,
state Master
Virtual IP address 192.168.1.6
Virtual MAC address 00-00-5E-00-01-01
Advertisement interval 5 sec
Preemption enabled
Min delay 10 sec
Priority 1
Authentication SimpleText
Authentication key bluebird
Master Router 192.168.1.6
Master priority 255
Master Advertisement interval 5 sec
Master down interval 15
Console#

```

**Table 120** *show vrrp - Display Description*

| Field                  | Description                                                                         |
|------------------------|-------------------------------------------------------------------------------------|
| State                  | VRRP role of this interface (master or backup)                                      |
| Virtual IP address     | Virtual address that identifies this VRRP group                                     |
| Virtual MAC address    | Virtual MAC address derived from the owner of the virtual IP address                |
| Advertisement interval | Interval at which the master virtual router advertises its role as the master       |
| Preemption             | Shows whether or not a higher priority router can preempt the current acting master |
| Min delay              | Delay before a router with a higher priority can preempt the current acting master  |
| Priority               | Priority of this router                                                             |

| Field                         | Description                                                                                                                                |
|-------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------|
| Authentication                | Authentication mode used to verify VRRP packets                                                                                            |
| Authentication key            | Key used to authenticate VRRP packets received from other routers                                                                          |
| Master Router                 | IP address of the router currently acting as the VRRP group master                                                                         |
| Master priority               | The priority of the router currently acting as the VRRP group master                                                                       |
| Master Advertisement interval | The advertisement interval configured on the VRRP master.                                                                                  |
| Master down interval          | The down interval configured on the VRRP master (This interval is used by all the routers in the group regardless of their local settings) |

This example displays the brief listing of status information for all groups.

|                         |     |        |              |     |     |      |
|-------------------------|-----|--------|--------------|-----|-----|------|
| Console#show vrrp brief |     |        |              |     |     |      |
| Interface               | Grp | State  | Virtual addr | Int | Pre | Prio |
| -----                   |     |        |              |     |     |      |
| vlan 1                  | 1   | Master | 192.168.1.6  | 5   | E   | 1    |
| Console#                |     |        |              |     |     |      |

**Table 121** *show vrrp brief - Display Description*

| Field        | Description                                     |
|--------------|-------------------------------------------------|
| Interface    | VLAN interface                                  |
| Grp          | VRRP group                                      |
| State        | VRRP role of this interface (master or backup)  |
| Virtual addr | Virtual address that identifies this VRRP group |

| Field | Description                                                                         |
|-------|-------------------------------------------------------------------------------------|
| Int   | Interval at which the master virtual router advertises its role as the master       |
| Pre   | Shows whether or not a higher priority router can preempt the current acting master |
| Prio  | Priority of this router                                                             |

### 7.24.8 **show vrrp all**

This command displays a full listing of status information for all VRRP groups.

#### **Syntax**

```
show vrrp all [interface vlan <vlan-id>]
```

- **interface vlan** - Displays all VRRP status information for the specified VLAN interface.
- **vlan-id** - Identifier of configured VLAN interface. (Range: 1-4094)

#### **Defaults**

None

#### **Command Mode**

Privileged Exec

## Example

This example displays the full listing of status information for all groups.

```

Console#show vrrp all
Vlan 1 - Group 1,
state Master
Virtual IP address 192.168.1.6
Virtual MAC address 00-00-5E-00-01-01
Advertisement interval 5 sec
Preemption enabled
Min delay 10 sec
Priority 1
Authentication SimpleText
Authentication key bluebird
Master Router 192.168.1.6
Master priority 255
Master Advertisement interval 5 sec
Master down interval 15
Console#

```

### 7.24.9

## show vrrp interface

This command displays status information for the specified VRRP interface.

### Syntax

**show vrrp interface vlan <vlan-id> [brief]**

- **vlan-id** - Identifier of configured VLAN interface. (Range: 1-4094)
- **brief** - Displays summary information for all VRRP groups on this router.

### Defaults

None

### Command Mode

Privileged Exec

## Example

This example displays the full listing of status information for VLAN 1.

```

Console#show vrrp interface vlan 1
Vlan 1 - Group 1,
state Master
Virtual IP address 192.168.1.6
Virtual MAC address 00-00-5E-00-01-01
Advertisement interval 5 sec
Preemption enabled
Min delay 10 sec
Priority 1
Authentication SimpleText
Authentication key bluebird
Master Router 192.168.1.6
Master priority 1
Master Advertisement interval 5 sec
Master down interval 15
Console#

```

Refer to “show vrrp” on page 1007 for a description of the display items.

### 7.24.10 show vrrp router counters

This command displays counters for errors found in VRRP protocol packets.

#### Command Mode

Privileged Exec

#### Example

Note that unknown errors indicate VRRP packets received with an unknown or unsupported version number.

```

Console#show vrrp router counters
Total Number of VRRP Packets with Invalid Checksum : 0
Total Number of VRRP Packets with Unknown Error : 0
Total Number of VRRP Packets with Invalid VRID : 0
Console#

```

## 7.24.11 show vrrp interface counters

This command displays counters for VRRP protocol events and errors that have occurred for the specified group and interface.

### Syntax

**show vrrp <group> interface vlan <interface> counters**

- *group* - Identifies a VRRP group. (Range: 1-255)
- *interface* - Identifier of configured VLAN interface. (Range: 1-4094)

### Defaults

None

### Command Mode

Privileged Exec

### Example

```
Console#show vrrp 1 interface vlan 1 counters
Total Number of Times Transitioned to MASTER : 6
Total Number of Received Advertisements Packets : 0
Total Number of Received Error Advertisement Interval Packets : 0
Total Number of Received Authentication Failures Packets : 0
Total Number of Received Error IP TTL VRRP Packets : 0
Total Number of Received Priority 0 VRRP Packets : 0
Total Number of Sent Priority 0 VRRP Packets : 5
Total Number of Received Invalid Type VRRP Packets : 0
Total Number of Received Error Address List VRRP Packets : 0
Total Number of Received Invalid Authentication Type VRRP Packets : 0
Total Number of Received Mismatch Authentication Type VRRP Packets : 0
Total Number of Received Error Packet Length VRRP Packets : 0
Console#
```

Refer to “Displaying VRRP Group Statistics” on page 395 for a description of the display items.

## 7.24.12 clear vrrp router counters

This command clears VRRP system statistics.

### Command Mode

Privileged Exec

### Example

```
Console#clear vrrp router counters
Console#
```

## 7.24.13 clear vrrp interface counters

This command clears VRRP system statistics for the specified group and interface.

### Syntax

```
clear vrrp <group> interface <interface> counters
```

- *group* - Identifies a VRRP group. (Range: 1-255)
- *interface* - Identifier of configured VLAN interface. (Range: 1-4094)

### Defaults

None

### Command Mode

Privileged Exec

### Example

```
Console#clear vrrp 1 interface 1 counters
Console#
```



## 7.25 IP Interface Commands

An IP address may be used for management access to the ECN330-switch over the network or to connect the ECN330-switch to existing IP subnets. By default, there are no IP addresses assigned to the , it uses DHCP to obtain IP settings for VLAN 247. A default gateway may also need to be established between the ECN330-switch and management stations that exist on other network segments (if routing is not enabled).

This section includes commands for configuring IP interfaces, the Address Resolution Protocol (ARP) and Proxy ARP. These commands are used to connect subnetworks to the enterprise network.

*Table 122 IP Interface Commands*

| Command Group                     | Function                                                        | Page |
|-----------------------------------|-----------------------------------------------------------------|------|
| Basic IP Configuration            | Configures the IP address for interfaces and the gateway router | 1015 |
| Address Resolution Protocol (ARP) | Configures static, dynamic and proxy ARP service                | 1023 |

### Basic IP Configuration

This section describes commands used to configure IP addresses for VLAN interfaces on the ECN330-switch.

*Table 123 Basic IP Configuration Commands*

| Command                   | Function                                                                                | Mode | Page |
|---------------------------|-----------------------------------------------------------------------------------------|------|------|
| <b>ip address</b>         | Sets the IP address for the current interface                                           | IC   | 1016 |
| <b>ip default-gateway</b> | Defines the default gateway through which the ECN330-switch can reach other subnetworks | GC   | 1018 |
| <b>show ip interface</b>  | Displays the IP settings for the ECN330-switch                                          | PE   | 1019 |

| Command                  | Function                                                       | Mode   | Page |
|--------------------------|----------------------------------------------------------------|--------|------|
| <b>show ip redirects</b> | Displays the default gateway configured for the ECN330-switch  | PE     | 1020 |
| <b>ping</b>              | Sends ICMP echo request packets to another node on the network | NE, PE | 1021 |

### 7.25.1 ip address

This command sets the IP address for the currently selected VLAN interface. Use the **no** form to restore the default IP address.

#### Syntax

```
ip address {<ip-address> <netmask> | bootp | dhcp}
[secondary]
```

```
no ip address
```

- *ip-address* - IP address
- *netmask* - Network mask for the associated IP subnet. This mask identifies the host address bits used for routing to specific subnets.
- **bootp** - Obtains IP address from BOOTP.
- **dhcp** - Obtains IP address from DHCP.
- *secondary* - Specifies a secondary IP address.

#### Default Setting

DHCP

#### Command Mode

Interface Configuration (VLAN)

## Command Usage

- If the ECN330-switch is directly connected to end node devices (or connected to end nodes through shared media) that will be assigned to a specific subnet, then create a router interface for each VLAN that will support routing. The router interface consists of an IP address and subnet mask. This interface address defines both the network number to which the router interface is attached and the router's host number on that network. In other words, a router interface address defines the network and subnetwork numbers of the segment that is connected to that interface, and allows IP packets to be sent to or from the ECN330-switch.
- Before any network interfaces are configured on the , first create a VLAN for each unique user group, or for each network application and its associated users. Then assign the ports associated with each of these VLANs.
- An IP address must be assigned to gain management access over the network or to connect the ECN330-switch to existing IP subnets. A specific IP address can be manually configured, or the ECN330-switch can be directed to obtain an address from a BOOTP or DHCP server. Valid IP addresses consist of four numbers, 0 to 255, separated by periods. Anything other than this format is not be accepted by the configuration program.
- An interface can have only one primary IP address, but can have many secondary IP addresses. In other words, secondary addresses need to be specified if more than one IP subnet can be accessed through this interface.
- If the **bootp** or **dhcp** option is selected, IP is enabled but does not function until a BOOTP or DHCP reply has been received. Requests are broadcast periodically by the ECN330-switch in an effort to learn its IP address. (BOOTP and DHCP values can include the IP address, default gateway, and subnet mask).
- BOOTP or DHCP requests can be broadcast by entering the **ip dhcp restart client** command, or by rebooting the ECN330.

**Note:** Before the primary IP address can be changed on an interface, the current address must first be cleared with the **no** form of this command.

## Example

In the following example, the device is assigned an address in VLAN 246.

```
Console(config)#interface vlan 246
Console(config-if)#ip address 192.168.1.5 255.255.255.0
Console(config-if)#
```

## Related Commands

**ip dhcp restart client** (section 7.23.2 on page 976)

### 7.25.2

## ip default-gateway

This command specifies the default gateway for destinations not found in the local routing tables. Use the **no** form to remove a default gateway.

## Syntax

**ip default-gateway** <gateway>

**no ip default-gateway**

*gateway* - IP address of the default gateway

## Default Setting

No default gateway is established.

## Command Mode

Global Configuration

## Command Usage

- The gateway specified in this command is only valid if routing is disabled with the **no ip routing** command. If IP routing is disabled, a gateway must be defined if the target device is located in a different subnet.
- If routing is enabled, the gateway must be defined with the **ip route** command.

## Example

The following example defines a default gateway for the ECN330-switch:

```
Console(config)#ip default-gateway 10.1.0.254
Console(config)#
```

## Related Commands

**show ip redirects** (section 7.25.4 on page 1020)  
**ip routing** (section 7.26.1 on page 1029)  
**ip route** (section 7.26.2 on page 1030)

### 7.25.3

## show ip interface

This command displays the settings of an IP interface.

## Default Setting

All interfaces

## Command Mode

Privileged Exec

## Example

```
Console#show ip interface

Vlan 1 is up, addressing mode is User
 Management VLAN is enabled.
 Interface address is 192.168.1.2, mask is 255.255.255.0, Primary
 MTU is 1500 bytes
 Proxy ARP is disabled
 Split horizon is enabled

Vlan 246 is up, addressing mode is DHCP
 MTU is 1500 bytes
 Proxy ARP is disabled
 Split horizon is disabled
Console#
```

## Related Commands

**show ip redirects** (section 7.25.4 on page 1020)

### 7.25.4 show ip redirects

This command shows the default gateway configured for the ECN330-switch.

#### Default Setting

None

#### Command Mode

Privileged Exec

#### Example

```
Console#show ip redirects
ip default gateway 10.1.0.254
Console#
```

## Related Commands

**ip default-gateway** (section 7.25.2 on page 1018)

## 7.25.5 ping

This command sends ICMP echo request packets to another node on the network.

### Syntax

```
ping <host> [count <count>][size <size>]
```

- *host* - IP address or IP alias of the host.
- *count* - Number of packets to send. (Range: 1-16, default: 5)
- *size* - Number of bytes in a packet. (Range: 32-512, default: 32)  
The actual packet size will be eight bytes larger than the size specified because the ECN330-switch adds header information.

### Default Setting

This command has no default for the host.

### Command Mode

Normal Exec, Privileged Exec

### Command Usage

- Use the **ping** command to verify connectivity between the ECN330-switch and another node.
- Following are some results of the **ping** command:
  - `Normal response` - The normal response occurs in one to ten seconds, depending on network traffic.
  - `Destination does not respond` - If the host does not respond, a “timeout” appears in ten seconds.
  - `Destination unreachable` - The gateway for this destination indicates that the destination is unreachable.
  - `Network or host unreachable` - The gateway found no corresponding entry in the route table.
- Press <Esc> to stop pinging.

## Example

```
Console#ping 10.1.0.9
Type ESC to abort.
PING to 10.1.0.9, by 5 32-byte payload ICMP packets, timeout is 5
seconds
response time: 10 ms
response time: 10 ms
response time: 10 ms
response time: 10 ms
response time: 0 ms
Ping statistics for 10.1.0.9:
 5 packets transmitted, 5 packets received (100%), 0 packets lost
 (0%)
Approximate round trip times:
 Minimum = 0 ms, Maximum = 10 ms, Average = 8 ms
Console#
```

## Related Commands

**interface** (section 7.9.1 on page 737)



## Address Resolution Protocol (ARP)

This section describes commands used to configure ARP on the ECN330-switch.

*Table 124 Address Resolution Protocol Commands*

| Command                | Function                                               | Mode   | Page |
|------------------------|--------------------------------------------------------|--------|------|
| <b>arp</b>             | Adds a static entry in the ARP cache                   | GC     | 1023 |
| <b>arp-timeout</b>     | Sets the time a dynamic entry remains in the ARP cache | GC     | 1024 |
| <b>clear arp-cache</b> | Deletes all dynamic entries from the ARP cache         | PE     | 1025 |
| <b>show arp</b>        | Displays entries in the ARP cache                      | NE, PE | 1026 |
| <b>ip proxy-arp</b>    | Enables proxy ARP service                              | VC     | 1027 |

### 7.25.6 arp

This command adds a static entry in the Address Resolution Protocol (ARP) cache. Use the **no** form to remove an entry from the cache.

#### Syntax

**arp** *<ip-address>* *<hardware-address>*

**no arp** *<ip-address>*

- *ip-address* - IP address to map to a specified hardware address.
- *hardware-address* - Hardware address to map to a specified IP address. (The format for this address is xx-xx-xx-xx-xx-xx.)

#### Default Setting

No default entries

## Command Mode

Global Configuration

## Command Usage

- The ARP cache is used to map 32-bit IP addresses into 48-bit hardware (that is, Media Access Control) addresses. This cache includes entries for hosts and other routers on local network interfaces defined on this router.
- The maximum number of static entries allowed in the ARP cache is 128.
- A static entry may need to be entered in the cache if there is no response to an ARP broadcast message. For example, some applications may not respond to ARP requests or the response arrives too late, causing network operations to time out.

## Example

```
Console(config)#arp 10.1.0.19 01-02-03-04-05-06
Console(config)#
```

## Related Commands

**clear arp-cache** (section 7.25.8 on page 1025)  
**show arp** (section 7.25.9 on page 1026)

### 7.25.7

## arp-timeout

This command sets the aging time for dynamic entries in the Address Resolution Protocol (ARP) cache. Use the **no** form to restore the default.

## Syntax

```
arp-timeout <seconds>
no arp-timeout
```

*seconds* - The time a dynamic entry remains in the ARP cache.  
(Range: 300-86400; 86400 is one day)

**Default Setting**

1200 seconds (20 minutes)

**Command Mode**

Global Configuration

**Command Usage**

Use the **show arp** command to display the current cache timeout value.

**Example**

This example sets the ARP cache timeout for 15 minutes (that is, 900 seconds).

```
Console(config)#arp-timeout 900
Console(config)#
```

**7.25.8****clear arp-cache**

This command deletes all dynamic entries from the Address Resolution Protocol (ARP) cache.

**Command Mode**

Privileged Exec

**Example**

This example clears all dynamic entries in the ARP cache.

```
Console#clear arp-cache
This operation will delete all the dynamic entries in ARP Cache.
Are you sure to continue this operation (y/n)?y
Console#
```

## 7.25.9 show arp

This command displays entries in the Address Resolution Protocol (ARP) cache.

### Command Mode

Normal Exec, Privileged Exec

### Command Usage

This command displays information about the ARP cache. The first line shows the cache timeout. It also shows each cache entry, including the corresponding IP address, MAC address, type (static, dynamic, other), and VLAN interface. Note that entry type “other” indicates local addresses for this router.

### Example

This example displays all entries in the ARP cache.

```
Console#show arp
Arp cache timeout: 1200 (seconds)

 IP Address MAC Address Type Interface

 10.1.0.0 ff-ff-ff-ff-ff-ff other 1
 10.1.0.254 00-00-ab-cd-00-00 other 1
 10.1.0.255 ff-ff-ff-ff-ff-ff other 1
 123.20.10.123 02-10-20-30-40-50 static 2
 345.30.20.23 09-50-40-30-20-10 dynamic 3

Total entry : 5
Console#
```

## 7.25.10 **ip proxy-arp**

This command enables proxy Address Resolution Protocol (ARP). Use the **no** form to disable proxy ARP.

### **Syntax**

```
[no] ip proxy-arp
```

### **Default Setting**

Disabled

### **Command Mode**

Interface Configuration (VLAN)

### **Command Usage**

Proxy ARP allows a non-routing device to determine the MAC address of a host on another subnet or network.

### **Example**

```
Console(config)#interface vlan 3
Console(config-if)#ip proxy-arp
Console(config-if)#
```

## 7.26 IP Routing Commands

After network interfaces are configured for the , the paths used to send traffic between different interfaces must be set. If routing is enabled on the ECN330-switch, traffic will automatically be forwarded between all of the local subnetworks. However, to forward traffic to devices on other subnetworks, either configure fixed paths with static routing commands, or enable a dynamic routing protocol that exchanges information with other routers on the network to automatically determine the best path to any subnetwork.

This section includes commands for both static and dynamic routing. These commands are used to connect between different local subnetworks or to connect the ECN330-switch to the enterprise network.

*Table 125 IP Routing Commands*

| Command Group                      | Function                                                                                                                                                   | Page |
|------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------|------|
| Global Routing Configuration       | Configures global parameters for static and dynamic routing, displays the routing table, and statistics for protocols used to exchange routing information | 1029 |
| Routing Information Protocol (RIP) | Configures global and interface specific parameters for RIP                                                                                                | 1035 |
| Open Shortest Path First (OSPF)    | Configures global and interface specific parameters for OSPF                                                                                               | 1053 |

## Global Routing Configuration

This section describes commands used to configure global parameters for static and dynamic routing on the ECN330-switch.

*Table 126 Global Routing Configuration Commands*

| Command                   | Function                                                     | Mode | Page |
|---------------------------|--------------------------------------------------------------|------|------|
| <b>ip routing</b>         | Enables static and dynamic IP routing                        | GC   | 1029 |
| <b>ip route</b>           | Configures static routes                                     | GC   | 1030 |
| <b>clear ip route</b>     | Deletes specified entries from the routing table             | PE   | 1031 |
| <b>show ip route</b>      | Displays specified entries in the routing table              | PE   | 1032 |
| <b>show ip host-route</b> | Displays displays the interface associated with known routes | PE   | 1033 |
| <b>show ip traffic</b>    | Displays statistics for IP, ICMP, UDP, TCP and ARP protocols | PE   | 1034 |

### 7.26.1 ip routing

This command enables IP routing. Use the **no** form to disable IP routing.

#### Syntax

**[no] ip routing**

#### Default Setting

Enabled

#### Command Mode

Global Configuration

## Command Usage

- The command affects both static and dynamic unicast routing.
- If IP routing is enabled, all IP packets are routed using either static routing or dynamic routing through RIP or OSPF, and other packets for all non-IP protocols (for example, NetBuei, NetWare or AppleTalk) are switched based on MAC addresses. If IP routing is disabled, all packets are switched, with filtering and forwarding decisions based strictly on MAC addresses.

## Example

```
Console(config)#ip routing
Console(config)#
```

## 7.26.2

### ip route

This command configures static routes. Use the **no** form to remove static routes.

#### Syntax

```
ip route {<destination-ip> <netmask> | default}
 {<gateway> [metric <metric>]}

no ip route {<destination-ip> <netmask> | default | *}
```

- *destination-ip* – IP address of the destination network, subnetwork, or host.
- *netmask* - Network mask for the associated IP subnet. This mask identifies the host address bits used for routing to specific subnets.
- **default** – Sets this entry as the default route.
- *gateway* – IP address of the gateway used for this route.
- *metric* – Selected RIP cost for this interface. (Range: 1-5, default: 1)
- **\*** – Removes all static routing table entries.



## Default Setting

No static routes are configured.

## Command Mode

Global Configuration

## Command Usage

- Up to 1K static routes can be configured.
- Static routes take precedence over dynamically learned routes.
- Static routes are included in RIP and OSPF updates periodically sent by the router.

## Example

This example forwards all traffic for subnet 192.168.1.0 to the router 192.168.5.254, using the default metric of 1.

```
Console(config)#ip route 192.168.1.0 255.255.255.0 192.168.5.254
Console(config)#
```

### 7.26.3

## clear ip route

This command removes dynamically learned entries from the IP routing table.

## Syntax

```
clear ip route {<network> [netmask] | *}
```

- *network* – Network or subnet address.
- *netmask* - Network mask for the associated IP subnet. This mask identifies the host address bits used for routing to specific subnets.
- \* – Removes all dynamic routing table entries.

## Command Mode

Privileged Exec

## Command Usage

- This command only clears dynamically learned routes.
- Use the **no ip address** command to remove a local interface.
- Use the **no ip route** command to remove a static route.

## Example

```
Console#clear ip route 10.1.5.0
Console#
```

### 7.26.4

## show ip route

This command displays information in the IP routing table.

## Syntax

```
show ip route [config | <address> [netmask]]
```

- **config** – Displays all static routing entries.
- **address** – IP address of the destination network, subnetwork or host for which routing information is to be displayed.
- **netmask** - Network mask for the associated IP subnet. This mask identifies the host address bits used for routing to specific subnets.

## Command Mode

Privileged Exec

## Command Usage

If the *address* is specified without the *netmask* parameter, the router displays all routes for the corresponding natural class address (page 1039).

## Example

```

Console#show ip route

```

| Ip Address  | Netmask       | Next Hop    | Protocol    | Metric | Interface |
|-------------|---------------|-------------|-------------|--------|-----------|
| 192.168.1.0 | 255.255.255.0 | 192.168.1.2 | local, MGMT | 1      | 1         |
| 0.0.0.0     | 0.0.0.0       | 10.2.48.102 | static      | 0      | 1         |
| 10.2.48.2   | 255.255.252.0 | 10.2.48.16  | local       | 0      | 1         |
| 10.2.5.6    | 255.255.255.0 | 10.2.8.12   | RIP         | 1      | 2         |
| 10.3.9.1    | 255.255.255.0 | 10.2.9.254  | OSPF-intra  | 2      | 3         |

```

Total entry: 5
Console#

```

*Table 127 show ip route - display description*

| Field      | Description                                                                                                                              |
|------------|------------------------------------------------------------------------------------------------------------------------------------------|
| Ip Address | IP address of the destination network, subnetwork, or host. Note that the address 0.0.0.0 indicates the default gateway for this router. |
| Netmask    | Network mask for the associated IP subnet.                                                                                               |
| Next Hop   | IP address of the next hop (or gateway) used for this route.                                                                             |
| Protocol   | The protocol which generated this route information. (Values: static, local, MGMT, RIP, OSPF)                                            |
| Metric     | Cost for this interface.                                                                                                                 |
| Interface  | VLAN interface through which this address can be reached.                                                                                |

## 7.26.5 show ip host-route

This command displays the interface associated with known routes.

### Command Mode

Privileged Exec

## Example

```

Console#show ip host-route
Total count: 0
 IP address Mac address VLAN Port

192.168. 1.250 00-00-30-01-01-01 3 1/ 1
 10. 2. 48. 2 00-00-30-01-01-02 1 1/ 1
 10. 2. 5. 6 00-00-30-01-01-03 1 1/ 2
 10. 3. 9. 1 00-00-30-01-01-04 2 1/ 3

Console#

```

*Table 128 show ip host-route - Display Description*

| Field       | Description                                                 |
|-------------|-------------------------------------------------------------|
| Ip address  | IP address of the destination network, subnetwork, or host. |
| Mac address | The physical layer address associated with the IP address.  |
| VLAN        | The VLAN that connects to this IP address.                  |
| Port        | The port that connects to this IP address.                  |

## 7.26.6 show ip traffic

This command displays statistics for IP, ICMP, UDP, TCP and ARP protocols.

### Command Mode

Privileged Exec

### Command Usage

For a description of the information shown by this command, see “Displaying Statistics for IP Protocols” on page 413.

## Example

```

Console#show ip traffic
IP statistics:
 Rcvd: 5 total, 5 local destination
 0 checksum errors
 0 unknown protocol, 0 not a gateway
 Frags: 0 reassembled, 0 timeouts
 0 fragmented, 0 couldn't fragment
 Sent: 9 generated
 0 no route
ICMP statistics:
 Rcvd: 0 checksum errors, 0 redirects, 0 unreachable, 0 echo
 5 echo reply, 0 mask requests, 0 mask replies, 0 quench
 0 parameter, 0 timestamp
 Sent: 0 redirects, 0 unreachable, 0 echo, 0 echo reply
 0 mask requests, 0 mask replies, 0 quench, 0 timestamp
 0 time exceeded, 0 parameter problem
UDP statistics:
 Rcvd: 0 total, 0 checksum errors, 0 no port
 Sent: 0 total
TCP statistics:
 Rcvd: 0 total, 0 checksum errors
 Sent: 0 total
ARP statistics:
 Rcvd: 0 requests, 1 replies
 Sent: 1 requests, 0 replies
Console#

```

## Routing Information Protocol (RIP)

This section describes commands used to configure RIP global and interface parameters for dynamic routing on the ECN330-switch.

*Table 129 Routing Information Protocol Commands*

| Command             | Function                                                         | Mode | Page |
|---------------------|------------------------------------------------------------------|------|------|
| <b>router rip</b>   | Enables the RIP routing protocol                                 | GC   | 1037 |
| <b>timers basic</b> | Sets basic timers, including update, timeout, garbage collection | RC   | 1038 |

| <b>Command</b>                    | <b>Function</b>                                                                                                                      | <b>Mode</b> | <b>Page</b> |
|-----------------------------------|--------------------------------------------------------------------------------------------------------------------------------------|-------------|-------------|
| <b>network</b>                    | Specifies the network interfaces that are to use RIP routing                                                                         | RC          | 1039        |
| <b>neighbor</b>                   | Defines a neighboring router with which to exchange information                                                                      | RC          | 1040        |
| <b>version</b>                    | Specifies the RIP version to use on all network interfaces (if not already specified with a receive version or send version command) | RC          | 1041        |
| <b>ip rip receive version</b>     | Sets the RIP receive version to use on a network interface                                                                           | IC          | 1043        |
| <b>ip rip send version</b>        | Sets the RIP send version to use on a network interface                                                                              | IC          | 1044        |
| <b>ip split-horizon</b>           | Enables split-horizon or poison-reverse loop prevention                                                                              | IC          | 1046        |
| <b>ip rip authentication key</b>  | Enables authentication for RIP2 packets and specifies keys                                                                           | IC          | 1047        |
| <b>ip rip authentication mode</b> | Specifies the type of authentication used for RIP2 packets                                                                           | IC          | 1048        |
| <b>show rip globals</b>           | Displays global configuration settings and statistics for RIP                                                                        | PE          | 1049        |
| <b>show ip rip</b>                | Displays RIP configuration information for each network interface                                                                    | PE          | 1050        |

## 7.26.7 **router rip**

This command enables Routing Information Protocol (RIP) routing for all IP interfaces on the router except the defined management IP interface. Use the **no** form to disable it.

### **Syntax**

```
[no] router rip
```

### **Command Mode**

Global Configuration

### **Default Setting**

Disabled

### **Command Usage**

- RIP is used to specify how routers exchange routing table information.
- This command is also used to enter router configuration mode.

### **Example**

```
Console(config)#router rip
Console(config-router)#
```

### **Related Commands**

**network** (section 7.26.9 on page 1039)

## 7.26.8 timers basic

This command configures the RIP update timer, timeout timer, and garbage-collection timer. Use the **no** form to restore the defaults.

### Syntax

```
timers basic <update-seconds>
```

```
no timers basic
```

*update-seconds* – Sets the update timer to the specified value, sets the timeout time value to 6 times the update time, and sets the garbage-collection timer to 4 times the update time. (Range for update timer: 15-60 seconds)

### Command Mode

Router Configuration

### Default Setting

Update: 30 seconds  
Timeout: 180 seconds  
Garbage collection: 120 seconds

### Command Usage

- The *update* timer sets the rate at which updates are sent. This is the fundamental timer used to control all basic RIP processes.
- The *timeout* timer is the time after which there have been no update messages that a route is declared dead. The route is marked inaccessible (that is, the metric set to infinite) and advertised as unreachable. However, packets are still forwarded on this route.
- After the *timeout* interval expires, the router waits for an interval specified by the *garbage-collection* timer before removing this entry from the routing table. This timer allows neighbors to become aware of an invalid route prior to purging it.
- Setting the update timer to a short interval can cause the router to spend an excessive amount of time processing updates.



- These timers must be set to the same values for all routers in the network.

### Example

This example sets the update timer to 40 seconds. The timeout timer is subsequently set to 240 seconds, and the garbage-collection timer to 160 seconds.

```
Console(config-router)#timers basic 15
Console(config-router)#
```

## 7.26.9

### network

This command specifies the network interfaces that will be included in the RIP routing process. Use the **no** form to remove an entry.

#### Syntax

**[no] network <subnet-address>**

*subnet-address* – IP address of a network directly connected to this router.

#### Command Mode

Router Configuration

#### Default Setting

No networks are specified.

#### Command Usage

- RIP only sends updates to interfaces specified by this command.

- Subnet addresses are interpreted as class A, B or C, based on the first field in the specified address. In other words, if a subnet address `nnn.xxx.xxx.xxx` is entered, the first field (`nnn`) determines the class:
  - 0 - 127 is class A, and only the first field in the network address is used.
  - 128 - 191 is class B, and the first two fields in the network address are used.
  - 192 - 223 is class C, and the first three fields in the network address are used.

### Example

This example includes network interface 10.1.0.0 in the RIP routing process.

```
Console(config-router)#network 10.1.0.0
Console(config-router)#
```

### Related Commands

**router rip** (section 7.26.7 on page 1037)

## 7.26.10

### neighbor

This command defines a neighboring router with which this router will exchange routing information. Use the **no** form to remove an entry.

### Syntax

**[no] neighbor <ip-address>**

*ip-address* - IP address to map to a specified hardware address.

### Command Mode

Router Configuration

### Default Setting

No neighbors are defined.

### Command Usage

This command can be used to configure a static neighbor with which this router will exchange information, rather than relying on broadcast messages generated by the RIP protocol.

### Example

```
Console(config-router)#neighbor 10.2.0.254
Console(config-router)#
```

## 7.26.11

### version

This command specifies a RIP version used globally by the router. Use the **no** form to restore the default value.

### Syntax

```
version {1 | 2}
```

```
no version
```

- **1** - RIP Version 1
- **2** - RIP Version 2

### Command Mode

Router Configuration

### Default Setting

RIP Version 1

## Command Usage

- When this command is used to specify a global RIP version, any VLAN interface not previously set by the **ip rip receive version** or **ip rip send version** command will be set to the following values:
  - RIP Version 1 configures the unset interfaces to send RIPv1 compatible protocol messages and receive either RIPv1 or RIPv2 protocol messages.
  - RIP Version 2 configures the unset interfaces to use RIPv2 for both sending and receiving protocol messages.
- When the **no** form of this command is used to restore the default value, any VLAN interface not previously set by the **ip rip receive version** or **ip rip send version** command will be set to the default send or receive version.

## Example

This example sets the global version for RIP to send and receive version 2 packets.

```
Console(config-router)#version 2
Console(config-router)#
```

## Related Commands

**ip rip receive version** (section 7.26.12 on page 1043)  
**ip rip send version** (section 7.26.13 on page 1044)

## 7.26.12 **ip rip receive version**

This command specifies a RIP version to receive on an interface. Use the **no** form to restore the default value.

### Syntax

```
ip rip receive version {none | 1 | 2 | 1 2}
```

```
no ip rip receive version
```

- **none** - Does not accept incoming RIP packets.
- **1** - Accepts only RIPv1 packets.
- **2** - Accepts only RIPv2 packets.
- **1 2** - Accepts RIPv1 or RIPv2 packets

### Command Mode

Interface Configuration (VLAN)

### Default Setting

The default depends on the setting specified with the **version** command:

Global RIPv1 - RIPv1 or RIPv2 packets

Global RIPv2 - RIPv2 packets

### Command Usage

- Use this command to override the global setting specified by the RIP **version** command.
- The receive version can be specified based on these options:
  - Use **none** to not add any dynamic entries to the routing table for an interface. (For example, to allow only static routes for a specific interface.)
  - Use **1** or **2** if all routers in the local network are based on RIPv1 or RIPv2, respectively.

- Use **1 2** if some routers in the local network are using RIPv2, but there are still some older routers using RIPv1.

### Example

This example sets the interface version for VLAN 1 to receive RIPv1 packets.

```
Console(config)#interface vlan 1
Console(config-if)#ip rip receive version 1
Console(config-if)#
```

### Related Commands

**version** (section 7.26.11 on page 1041)

## 7.26.13

### ip rip send version

This command specifies a RIP version to send on an interface. Use the **no** form to restore the default value.

#### Syntax

```
ip rip send version {none | 1 | 2 | v2-broadcast}
```

```
no ip rip send version
```

- **none** - Does not transmit RIP updates.
- **1** - Sends only RIPv1 packets.
- **2** - Sends only RIPv2 packets.
- **v2-broadcast** - Route information is broadcast to other routers with RIPv2.

#### Command Mode

Interface Configuration (VLAN)

## Default Setting

The default depends on the setting specified with the **version** command:

Global RIPv1 - Route information is broadcast to other routers with RIPv2

Global RIPv2 - RIPv2 packets

## Command Usage

- Use this command to override the global setting specified by the RIP **version** command.
- The receive version can be specified based on these options:
  - Use **none** to passively monitor route information advertised by other routers attached to the network.
  - Use **1** or **2** if all routers in the local network are based on RIPv1 or RIPv2, respectively.
  - Use **v2-broadcast** to propagate route information by broadcasting to other routers on the network using RIPv2, instead of multicasting as normally required by RIPv2. (Using this mode allows RIPv1 routers to receive these protocol messages, but still allows RIPv2 routers to receive the additional information provided by RIPv2, including subnet mask, next hop and authentication information.)

## Example

This example sets the interface version for VLAN 1 to send RIPv1 packets.

```
Console(config)#interface vlan 1
Console(config-if)#ip rip send version 1
Console(config-if)#
```

## Related Commands

**version** (section 7.26.11 on page 1041)

## 7.26.14 ip split-horizon

This command enables split-horizon or poison-reverse (a variation) on an interface. Use the **no** form to disable split-horizon.

### Syntax

```
ip split-horizon [poison-reverse]
```

```
no ip split-horizon
```

**poison-reverse** - Enables poison-reverse on the current interface.

### Command Mode

Interface Configuration (VLAN)

### Default Setting

split-horizon

### Command Usage

- Split horizon never propagates routes back to an interface from which they have been acquired.
- Poison reverse propagates routes back to an interface port from which they have been acquired, but sets the distance-vector metrics to infinity. (This provides faster convergence.)

### Example

This example propagates routes back to the source using poison-reverse.

```
Console(config)#interface vlan 1
Console(config-if)#ip split-horizon poison-reverse
Console(config-if)#
```



## 7.26.15 ip rip authentication key

This command enables authentication for RIPv2 packets and to specify the key that must be used on an interface. Use the **no** form to prevent authentication.

### Syntax

```
ip rip authentication key <key-string>
```

```
no ip rip authentication
```

*key-string* - A password used for authentication.  
(Range: 1-16 characters, case sensitive)

### Command Mode

Interface Configuration (VLAN)

### Default Setting

No authentication

### Command Usage

- This command can be used to restrict the interfaces that can exchange RIPv2 routing information. (Note that this command does not apply to RIPv1.)
- For authentication to function properly, both the sending and receiving interface must be configured with the same password.

### Example

This example sets an authentication password of “small” to verify incoming routing messages and to tag outgoing routing messages.

```
Console(config)#interface vlan 1
Console(config-if)#ip rip authentication key small
Console(config-if)#
```

## Related Commands

**ip rip authentication mode** (section 7.26.16 on page 1048)

### 7.26.16 ip rip authentication mode

This command specifies the type of authentication that can be used on an interface. Note that the current firmware version only supports a simple password. Use the **no** form to restore the default value.

#### Syntax

**ip rip authentication mode {text}**

**no ip rip authentication mode**

**text** - Indicates that a simple password will be used.

#### Command Mode

Interface Configuration (VLAN)

#### Default Setting

No authentication

#### Command Usage

- The password to be used for authentication is specified in the **ip rip authentication key** command (section 7.26.15 on page 1047).
- This command requires the interface to exchange routing information with other routers based on an authorized password. (Note that this command only applies to RIPv2.)
- For authentication to function properly, both the sending and receiving interface must be configured with the same password or authentication key.

## Example

This example sets the authentication mode to plain text.

```
Console(config)#interface vlan 1
Console(config-if)#ip rip authentication mode text
Console(config-if)#
```

## Related Commands

**ip rip authentication key** (section 7.26.15 on page 1047)

## 7.26.17 show rip globals

This command displays global configuration settings for RIP.

## Command Mode

Privileged Exec

## Example

```
Console#show rip globals

RIP Process: Enabled
Update Time in Seconds: 30
Number of Route Change: 0
Number of Queries: 1
Console#
```

**Table 130**    *show rip globals - Display Description*

| Field                  | Description                                                                         |
|------------------------|-------------------------------------------------------------------------------------|
| RIP Process            | Indicates if RIP has been enabled or disabled.                                      |
| Update Time in Seconds | The interval at which RIP advertises known route information. (Default: 30 seconds) |

| Field                   | Description                                                |
|-------------------------|------------------------------------------------------------|
| Number of Route Changes | Number of times routing information has changed.           |
| Number of Queries       | Number of router database queries received by this router. |

### 7.26.18 **show ip rip**

This command displays information about interfaces configured for RIP.

#### **Syntax**

```
show ip rip {configuration | status | peer}
```

- **configuration** - Shows RIP configuration settings for each interface.
- **status** - Shows the status of routing messages on each interface.
- **peer** - Shows information on neighboring routers, along with information about the last time a route update was received, the RIP version used by the neighbor, and the status of routing messages received from this neighbor.

#### **Command Mode**

Privileged Exec

**Example**

```

Console#show ip rip configuration

```

| Interface  | SendMode       | ReceiveMode | Poison       | Authentication   |
|------------|----------------|-------------|--------------|------------------|
| 10.1.0.253 | rip1Compatible | RIPv1Orv2   | SplitHorizon | noAuthentication |
| 10.1.1.253 | rip1Compatible | RIPv1Orv2   | SplitHorizon | noAuthentication |

```

Console#show ip rip status

```

| Interface  | RcvBadPackets | RcvBadRoutes | SendUpdates |
|------------|---------------|--------------|-------------|
| 10.1.0.253 | 0             | 0            | 13          |
| 10.1.1.253 | 0             | 0            | 13          |

```

Console#show ip rip peer

```

| Peer       | UpdateTime | Version | RcvBadPackets | RcvBadRoutes |
|------------|------------|---------|---------------|--------------|
| 10.1.0.254 | 1625       | 2       | 0             | 0            |
| 10.1.1.254 | 1625       | 2       | 0             | 0            |

```

Console#

```

**Table 131** *show ip rip - Display Description*

| Field                            | Description                                                                                          |
|----------------------------------|------------------------------------------------------------------------------------------------------|
| <b>show ip rip configuration</b> |                                                                                                      |
| Interface                        | IP address of the interface.                                                                         |
| SendMode                         | RIP version sent on this interface (none, RIPv1, RIPv2, or RIPv2-broadcast)                          |
| ReceiveMode                      | RIP version received on this interface (none, RIPv1, RIPv2, RIPv1 or RIPv2)                          |
| Poison                           | Shows if split-horizon, poison-reverse, or no protocol message loopback prevention method is in use. |
| Authentication                   | Shows if authentication is set to simple password or none.                                           |
| <b>show ip rip status</b>        |                                                                                                      |
| Interface                        | IP address of the interface.                                                                         |

| Field                   | Description                                                  |
|-------------------------|--------------------------------------------------------------|
| RcvBadPackets           | Number of bad RIP packets received.                          |
| RcvBadRoutes            | Number of bad routes received.                               |
| SendUpdates             | Number of route changes.                                     |
| <b>show ip rip peer</b> |                                                              |
| Peer                    | IP address of a neighboring RIP router.                      |
| UpdateTime              | Last time a route update was received from this peer.        |
| Version                 | Whether RIPv1 or RIPv2 packets were received from this peer. |
| RcvBadPackets           | Number of bad RIP packets received from this peer.           |
| RcvBadRoutes            | Number of bad routes received from this peer.                |

## Open Shortest Path First (OSPF)

This section describes commands used to configure OSPF global and interface parameters for dynamic routing on the ECN330-switch.

*Table 132 Open Shortest Path First Commands*

| Command                              | Function                                                           | Mode | Page |
|--------------------------------------|--------------------------------------------------------------------|------|------|
| <i>General Configuration</i>         |                                                                    |      |      |
| <b>router ospf</b>                   | Enables or disables OSPF                                           | GC   | 1055 |
| <b>router-id</b>                     | Sets the router ID for this device                                 | RC   | 1056 |
| <b>compatible rfc1583</b>            | Calculates summary route costs using RFC 1583 (OSPFv1)             | RC   | 1057 |
| <b>default-information originate</b> | Generates a default external route into an autonomous system       | RC   | 1058 |
| <b>timers spf</b>                    | Configures the hold time between consecutive SPF calculations      | RC   | 1060 |
| <i>Route Metrics and Summaries</i>   |                                                                    |      |      |
| <b>area range</b>                    | Summarizes routes advertised by an ABR                             | RC   | 1061 |
| <b>area default-cost</b>             | Sets the cost for a default summary route sent into a stub or NSSA | RC   | 1062 |
| <b>summary-address</b>               | Summarizes routes advertised by an ASBR                            | RC   | 1063 |
| <b>redistribute</b>                  | Redistribute routes from one routing domain to another             | RC   | 1064 |
| <i>Area Configuration</i>            |                                                                    |      |      |
| <b>network area</b>                  | Assigns specified interface to an area                             | RC   | 1066 |

| Command                            | Function                                                                                       | Mode | Page |
|------------------------------------|------------------------------------------------------------------------------------------------|------|------|
| <b>area stub</b>                   | Defines a stubby area that cannot send or receive LSAs                                         | RC   | 1067 |
| <b>area nssa</b>                   | Defines a not-so-stubby that can import external routes                                        | RC   | 1068 |
| <b>area virtual-link</b>           | Defines a virtual link from an area border routers to the backbone                             | RC   | 1070 |
| <i>Interface Configuration</i>     |                                                                                                |      |      |
| <b>ip ospf authentication</b>      | Specifies the authentication type for an interface                                             | IC   | 1073 |
| <b>ip ospf authentication -key</b> | Assigns a simple password to be used by neighboring routers                                    | IC   | 1075 |
| <b>ip ospf message-digest-key</b>  | Enables MD5 authentication and sets the key for an interface                                   | IC   | 1076 |
| <b>ip ospf cost</b>                | Specifies the cost of sending a packet on an interface                                         | IC   | 1077 |
| <b>ip ospf dead-interval</b>       | Sets the interval at which hello packets are not seen before neighbors declare the router down | IC   | 1078 |
| <b>ip ospf hello-interval</b>      | Specifies the interval between sending hello packets                                           | IC   | 1079 |
| <b>ip ospf priority</b>            | Sets the router priority used to determine the designated router                               | IC   | 1080 |
| <b>ip ospf retransmit-interval</b> | Specifies the time between resending a link-state advertisement                                | IC   | 1081 |
| <b>ip ospf transmit-delay</b>      | Estimates time to send a link-state update packet over an interface                            | IC   | 1082 |



| Command                             | Function                                                                                                   | Mode | Page |
|-------------------------------------|------------------------------------------------------------------------------------------------------------|------|------|
| <i>Display Information</i>          |                                                                                                            |      |      |
| <b>show ip ospf</b>                 | Displays general information about the routing processes                                                   | PE   | 1083 |
| <b>show ip ospf border-routers</b>  | Displays routing table entries for Area Border Routers (ABR) and Autonomous System Boundary Routers (ASBR) | PE   | 1084 |
| <b>show ip ospf database</b>        | Shows information about different LSAs in the database                                                     | PE   | 1085 |
| <b>show ip ospf interface</b>       | Displays interface information                                                                             | PE   | 1097 |
| <b>show ip ospf neighbor</b>        | Displays neighbor information                                                                              | PE   | 1099 |
| <b>show ip ospf summary-address</b> | Displays all summary address redistribution information                                                    | PE   | 1101 |
| <b>show ip ospf virtual-links</b>   | Displays parameters and the adjacency state of virtual links                                               | PE   | 1101 |

### 7.26.19 router ospf

This command enables Open Shortest Path First (OSPF) routing for all IP interfaces on the router. Use the **no** form to disable it.

#### Syntax

**[no] router ospf**

#### Command Mode

Global Configuration

## Default Setting

Disabled

## Command Usage

- OSPF is used to specify how routers exchange routing table information.
- This command is also used to enter router configuration mode.

## Example

```
Console(config)#router ospf
Console(config-router)#
```

## Related Commands

**network area** (section 7.26.28 on page 1066)

## 7.26.20

### router-id

This command assigns a unique router ID for this device within the autonomous system. Use the **no** form to use the default router identification method (that is, the lowest interface address).

## Syntax

**router-id** <*ip-address*>

**no router-id**

*ip-address* - Router ID formatted as an IP address.

## Command Mode

Router Configuration

## Default Setting

Lowest interface address

## Command Usage

- The router ID must be unique for every router in the autonomous system. Using the default setting based on the lowest interface address ensures that each router ID is unique. Also, note that the router ID cannot be set to 0.0.0.0 or 255.255.255.255.
- If this router already has registered neighbors, the new router ID will be used when the router is rebooted, or manually restarted by entering the **no router ospf** followed by the **router ospf** command.
- If the priority values of the routers bidding to be the designated router or backup designated router for an area are equal, the router with the highest ID is elected.

## Example

```
Console(config-router)#router-id 10.1.1.1
Console(config-router)#
```

## Related Commands

**router ospf** (section 7.26.19 on page 1055)

### 7.26.21

## compatible rfc1583

This command calculates summary route costs using RFC 1583 (OSPFv1). Use the **no** form to calculate costs using RFC 2328 (OSPFv2).

## Syntax

**[no] compatible rfc1583**

## Command Mode

Router Configuration

## Default Setting

RFC 1583 compatible

## Command Usage

All routers in an OSPF routing domain should use the same RFC for calculating summary routes.

## Example

```
Console(config-router)#compatible rfc1583
Console(config-router)#
```

## 7.26.22 default-information originate

This command generates a default external route into an autonomous system. Use the **no** form to disable this feature.

### Syntax

```
default-information originate [always] [metric
 <interface-metric>] [metric-type <metric-type>]
```

```
no default-information originate
```

- **always** - Always advertise a default route to the local AS regardless of whether the router has a default route. (See 7.26.2 "ip route" 1030.)
- *interface-metric* - Metric assigned to the default route. (Range: 1-65535; Default: 10)
- *metric-type* - External link type used to advertise the default route. (Options: Type 1, Type 2; Default: Type 2)

### Command Mode

Router Configuration

## Default Setting

Disabled

## Command Usage

- The metric for the default external route is used to calculate the path cost for traffic passed from other routers within the AS out through the ASBR.
- When this command is used to redistribute routes into a routing domain (that is, an Autonomous System, this router automatically becomes an Autonomous System Boundary Router (ASBR). However, an ASBR does not, by default, generate a default route into the routing domain.
  - If the **always** keyword is used, the router will advertise itself as a default external route into the AS, even if a default external route does not actually exist. (To define a default route, use the **ip route** command.)
  - If the **always** keyword is *not* used, the router can only advertise a default external route into the AS if the **redistribute** command is used to import external routes through RIP or static routing, and such a route is known.
- Type 1 route advertisements add the internal cost to the external route metric. Type 2 routes do not add the internal cost metric. When comparing Type 2 routes, the internal cost is only used as a tie-breaker if several Type 2 routes have the same cost.

## Example

This example assigns a metric of 20 to the default external route advertised into an autonomous system, sending it as a Type 2 external metric.

```
Console(config-router)#default-information originate metric 20
metric-type 2
Console(config-router)#
```

## Related Commands

**ip route** (section 7.26.2 on page 1030)

**redistribute** (section 7.26.27 on page 1064)

## 7.26.23 timers spf

This command configures the hold time between making two consecutive shortest path first (SPF) calculations. Use the **no** form to restore the default value.

### Syntax

```
timers spf <spf-holdtime>
```

```
no timers spf
```

*spf-holdtime* - Minimum time between two consecutive SPF calculations. (Range: 0-65535 seconds)

### Command Mode

Router Configuration

### Default Setting

10 seconds

### Command Usage

- Setting the SPF holdtime to 0 means that there is no delay between consecutive calculations.
- Using a low value allows the router to switch to a new path faster, but uses more CPU processing time.

### Example

```
Console(config-router)#timers spf 20
Console(config-router)#
```

## 7.26.24 **area range**

This command summarizes the routes advertised by an Area Border Router (ABR). Use the **no** form to disable this function.

### **Syntax**

```
[no] area <area-id> range <ip-address> <netmask>
[advertise | not-advertise]
```

- *area-id* - Identifies an area for which the routes are summarized. (The area ID must be in the form of an IP address.)
- *ip-address* - Base address for the routes to summarize.
- *netmask* - Network mask for the summary route.
- **advertise** - Advertises the specified address range.
- **not-advertise** - The summary is not sent, and the routes remain hidden from the rest of the network.

### **Command Mode**

Router Configuration

### **Default Setting**

Disabled

### **Command Usage**

- This command can be used to advertise routes between areas.
- If routes are set to be advertised, the router will issue a Type 3 summary LSA for each address range specified with this command.
- This router supports up to 64 summary routes for area ranges.

## Example

This example creates a summary address for all area routes in the range of 10.2.x.x.

```
Console(config-router)#area 10.2.0.0 range 10.2.0.0 255.255.0.0
 advertise
Console(config-router)#
```

## 7.26.25 area default-cost

This command specifies a cost for the default summary route sent into a stub or not-so-stubby area (NSSA) from an Area Border Router (ABR). Use the **no** form to remove the assigned default cost.

### Syntax

**area <area-id> default-cost <cost>**

**no area <area-id> default-cost**

- **area-id** - Identifier for a stub or NSSA, in the form of an IP address.
- **cost** - Cost for the default summary route sent to a stub or NSSA. (Range: 0-65535)

### Command Mode

Router Configuration

### Default Setting

1

### Command Usage

- If this command is entered for a normal area, it will be changed to a stub.
- If the default cost is set to "0," the router will not advertise a default route into the attached stub or NSSA.



## Example

```
Console(config-router)#area 10.3.9.0 default-cost 10
Console(config-router)#
```

## Related Commands

**area stub** (section 7.26.29 on page 1067)

## 7.26.26 summary-address

This command aggregates routes learned from other protocols. Use the **no** form to remove a summary address.

### Syntax

**[no] summary-address** <*summary-address*> <*netmask*>

- *summary-address* - Summary address covering a range of addresses.
- *netmask* - Network mask for the summary route.

### Command Mode

Router Configuration

### Default Setting

Disabled

### Command Usage

- An Autonomous System Boundary Router (ASBR) can redistribute routes learned from other protocols by advertising an aggregate route into all attached autonomous systems.
- This router supports up to 16 Type-5 summary routes.

## Example

This example creates a summary address for all routes contained in 192.168.x.x.

```
Console(config-router)#summary-address 192.168.0.0 255.255.0.0
Console(config-router)#
```

## Related Commands

**area range** (section 7.26.24 on page 1061)

## 7.26.27

## redistribute

This command imports external routing information from other routing domains (that is, protocols) into the autonomous system. Use the **no** form to disable this feature.

## Syntax

```
[no] redistribute [rip | static] [metric <metric-value>]
[metric-type <type-value>]
```

- **rip** - External routes will be imported from the Routing Information Protocol into this Autonomous System.
- **static** - Static routes will be imported into this Autonomous System.
- **metric-value** - Metric assigned to all external routes for the specified protocol. (Range: 1-65535; Default: 10)
- **type-value**
  - **1** - Type 1 external route
  - **2** - Type 2 external route (default) - Routers do not add internal route metric to external route metric.

## Command Mode

Router Configuration

## Default Setting

redistribution - none  
protocol - RIP and static  
metric-value - 0  
type-metric - 2

## Command Usage

- This router supports redistribution for both RIP and static routes.
- When external routes are redistributed into an OSPF autonomous system (AS), the router automatically becomes an autonomous system boundary router (ASBR). If the **redistribute** command is used in conjunction with the **default-information originate** command to generate a “default” external route into the AS, the metric value specified in this command supersedes the metric specified in the **default-information originate** command.
- Metric type specifies the way to advertise routes to destinations outside the AS through External LSAs. Specify Type 1 to add the internal cost metric to the external route metric. In other words, the cost of the route from any router within the AS is equal to the cost associated with reaching the advertising ASBR, plus the cost of the external route. Specify Type 2 to only advertise the external route metric.

## Example

This example redistributes routes learned from RIP as Type 1 external routes.

```
Console(config-router)#redistribute rip metric-type 1
Console(config-router)#
```

## Related Commands

**default-information originate** (section 7.26.22 on page 1058)

## 7.26.28 network area

This command defines an OSPF area and the interfaces that operate within this area. Use the **no** form to disable OSPF for a specified interface.

### Syntax

```
[no] network <ip-address> <netmask> area <area-id>
```

- *ip-address* - Address of the interfaces to add to the area.
- *netmask* - Network mask of the address range to add to the area.
- *area-id* - Area to which the specified address or range is assigned. An OSPF area identifies a group of routers that share common routing information. (The area ID must be in the form of an IP address.)

### Command Mode

Router Configuration

### Default Setting

Disabled

### Command Usage

- An area ID uniquely defines an OSPF broadcast area. The area ID 0.0.0.0 indicates the OSPF backbone for an autonomous system. Each router must be connected to the backbone through a direct connection or a virtual link.
- Set the area ID to the same value for all routers on a network segment using the network mask to add one or more interfaces to an area.
- Be sure to include the primary address for an interface in the network area, otherwise, OSPF will not operate for any secondary addresses covered by the command.
- An interface can only be assigned to a single area. If an address range is overlapped in subsequent network area commands, the router will implement the address range for the area specified in first command, and ignore the overlapping ranges in subsequent commands. However,

note that if a more specific address range is removed from an area, the interface belonging to that range may still remain active if a less specific address range covering that area has been specified.

- This router supports up to 64 OSPF router interfaces, and up to 16 total areas (either normal transit areas, stubs, or NSSAs).

### Example

This example creates the backbone 0.0.0.0 covering class B addresses 10.1.x.x, and a normal transit area 10.2.9.0 covering the class C addresses 10.2.9.x.

```
Console(config-router)#network 10.1.0.0 255.255.0.0 area 0.0.0.0
Console(config-router)#network 10.2.9.0 255.255.255.0 area 10.1.0.0
Console(config-router)#
```

## 7.26.29

### area stub

This command defines a stub area. To remove a stub, use the **no** form without the optional keyword. To remove the summary attribute, use the **no** form with the summary keyword.

### Syntax

**[no] area <area-id> stub [summary]**

- **area-id** - Identifies the stub area.  
(The area ID must be in the form of an IP address.)
- **summary** - Makes an Area Border Router (ABR) send a summary link advertisement into the stub area. (Default: no summary)

### Command Mode

Router Configuration

### Default Setting

No stub is configured.

## Command Usage

- All routers in a stub must be configured with the same area ID.
- Routing table space is saved in a stub by blocking Type-4 AS summary LSAs and Type 5 external LSAs. The default setting for this command completely isolates the stub by blocking Type-3 summary LSAs that advertise the default route for destinations external to the local area or the autonomous system.
- Use the **area default-cost** command to specify the cost of a default summary route sent into a stub by an ABR.
- This router supports up to 16 total areas (either normal transit areas, stubs, or NSSAs).

## Example

This example creates a stub area 10.2.0.0, and assigns all interfaces with class B addresses 10.2.x.x to the stub.

```
Console(config-router)#area 10.2.0.0 stub
Console(config-router)#network 10.2.0.0 0.255.255.255 area 10.2.0.0
Console(config-router)#
```

## Related Commands

**area default-cost** (section 7.26.25 on page 1062)

### 7.26.30

## area nssa

This command defines a not-so-stubby area (NSSA). To remove an NSSA, use the **no** form without any optional keywords. To remove an optional attribute, use the **no** form without the relevant keyword.

## Syntax

```
[no] area <area-id> nssa [no- redistribution] [default-
information-originate]
```

- *area-id* - Identifies the NSSA.  
(The area ID must be in the form of an IP address.)

- **no-redistribution** - Use this keyword when the router is an NSSA Area Border Router (ABR) and the **redistribute** command is required to import routes only into normal areas, and not into the NSSA. In other words, this keyword prevents the NSSA ABR from advertising external routing information (learned through routers in other areas) into the NSSA.
- **default-information-originate** - When the router is an NSSA Area Border Router (ABR) or an NSSA Autonomous System Boundary Router (ASBR), this parameter causes it to generate Type-7 default LSA into the NSSA. This default provides a route to other areas within the AS for an NSSA ABR, or to areas outside the AS for an NSSA ASBR.

## Command Mode

Router Configuration

## Default Setting

No NSSA is configured.

## Command Usage

- All routers in a NSSA must be configured with the same area ID.
- An NSSA is similar to a stub, because when the router is an ABR, it can send a default route for other areas in the AS into the NSSA using the **default-information-originate** keyword. However, an NSSA is different from a stub, because when the router is an ASBR, it can import a default external AS route (for routing protocol domains adjacent to the NSSA but not within the OSPF AS) into the NSSA using the **default-information-originate** keyword.
- External routes advertised into an NSSA can include network destinations outside the AS learned through OSPF, the default route, static routes, routes imported from other routing protocols such as RIP, and networks directly connected to the router that are not running OSPF.
- NSSA external LSAs (Type 7) are converted by any ABR adjacent to the NSSA into external LSAs (Type-5), and propagated into other areas within the AS.

- Also, note that unlike stub areas, all Type-3 summary LSAs are always imported into NSSAs to ensure that internal routes are always chosen over Type-7 NSSA external routes.
- This router supports up to 16 total areas (either normal transit areas, stubs, or NSSAs).

### Example

This example creates a stub area 10.3.0.0, and assigns all interfaces with class B addresses 10.3.x.x to the NSSA. It also instructs the router to generate external LSAs into the NSSA when it is an NSSA ABR or NSSA ASBR.

```
Console(config-router)#area 10.3.0.0 nssa default-information-
 originate
Console(config-router)#network 10.3.0.0 255.255.0.0 area 10.2.0.0
Console(config-router)#
```

## 7.26.31

### area virtual-link

This command defines a virtual link. To remove a virtual link, use the **no** form with no optional keywords. To restore the default value for an attribute, use the **no** form with the required keyword.

#### Syntax

```
[no] area <area-id> virtual-link <router-id>
 [authentication [message-digest | null]] [hello-
interval <seconds>] [retransmit-interval <seconds>]
 [transmit-delay <seconds>] [dead-interval
 <seconds>] [[authentication-key <key>] | [message-
digest-key <key-id> md5 <key>]]
```

```
no area <area-id>
```

- *area-id* - Identifies the transit area for the virtual link. (The area ID must be in the form of an IP address.)
- *router-id* - Router ID of the virtual link neighbor. This must be an Area Border Router (ABR) that is adjacent to both the backbone and the transit area at the other end of the virtual link.



- **authentication** - Specifies the authentication mode. If no optional parameters follow this keyword, then plain text authentication is used along with the password specified by the **authentication-key**. If **message-digest** authentication is specified, then the **message-digest-key** and **md5** parameters must also be specified. If the **null** option is specified, then no authentication is performed on any OSPF routing protocol messages.
- **message-digest** - Specifies message-digest (MD5) authentication.
- **null** - Indicates that no authentication is used.
- **hello-interval** <*seconds*> - Specifies the transmit delay between sending hello packets. Setting the hello interval to a smaller value can reduce the delay in detecting topological changes, but will increase the routing traffic. This value must be the same for all routers attached to an autonomous system. (Range: 1-65535 seconds; Default: 10 seconds)
- **retransmit-interval** <*seconds*> - Specifies the interval at which the ABR retransmits link-state advertisements (LSA) over the virtual link. The retransmit interval should be set to a conservative value that provides an adequate flow of routing information, but does not produce unnecessary protocol traffic. However, note that this value should be larger for virtual links. (Range: 1-3600 seconds; Default: 5 seconds)
- **transmit-delay** <*seconds*> - Estimates the time required to send a link-state update packet over the virtual link, considering the transmission and propagation delays. LSAs have their age incremented by this amount before transmission. This value must be the same for all routers attached to an autonomous system. (Range: 1-3600 seconds; Default: 1 seconds)
- **dead-interval** <*seconds*> - Specifies the time that neighbor routers will wait for a hello packet before they declare the router down. This value must be the same for all routers attached to an autonomous system. (Range: 1-65535 seconds; Default: 4 x hello interval, or 40 seconds)
- **authentication-key** <*key*> - Sets a plain text password (up to 8 characters) that is used by neighboring routers on a virtual link to generate or verify the authentication field in

protocol message headers. A separate password can be assigned to each network interface. However, this key must be the same for all neighboring routers on the same network (that is, autonomous system). This key is only used when authentication is enabled for the backbone.

- **message-digest-key <key-id> md5 <key>** - Sets the key identifier and password to be used to authenticate protocol messages passed between neighboring routers and this router when using message digest (MD5) authentication. The *key-id* is an integer from 1-255, and the *key* is an alphanumeric string up to 16 characters long. If MD5 authentication is used on a virtual link, then it must be enabled on all routers within an autonomous system; and the key identifier and key must also be the same for all routers.

## Command Mode

Router Configuration

## Default Setting

```
area-id: None
router-id: None
hello-interval: 10 seconds
retransmit-interval: 5 seconds
transmit-delay: 1 second
dead-interval: 40 seconds
authentication-key: None
message-digest-key: None
```

## Command Usage

- All areas must be connected to a backbone area (0.0.0.0) to maintain routing connectivity throughout the autonomous system. If it is not possible to physically connect an area to the backbone, a virtual link can be used. A virtual link can provide a logical path to the backbone for an isolated area. Up to 32 virtual links can be specified on this router.
- Any area disconnected from the backbone must include the transit area ID and the router ID for a virtual link neighbor that is adjacent to the backbone.

- This router supports up to 64 virtual links.

### Example

This example creates a virtual link using the defaults for all optional parameters.

```
Console(config-router)#network 10.4.0.0 0.255.255.0.0 area 10.4.0.0
Console(config-router)#area 10.4.0.0 virtual-link 10.4.3.254
Console(config-router)#
```

This example creates a virtual link using MD5 authentication.

```
Console(config-router)#network 10.4.0.0 0.255.255.0.0 area 10.4.0.0
Console(config-router)#area 10.4.0.0 virtual-link 10.4.3.254
 message-digest-key 5 md5 ld83jdpq
Console(config-router)#
```

### Related Commands

**show ip ospf virtual-links** (section 7.26.47 on page 1101)

## 7.26.32 ip ospf authentication

This command specifies the authentication type used for an interface. Enter this command without any optional parameters to specify plain text (or simple password) authentication. Use the **no** form to restore the default of no authentication.

### Syntax

**ip ospf authentication [message-digest | null]**

**no ip ospf authentication**

- **message-digest** - Specifies message-digest (MD5) authentication.
- **null** - Indicates that no authentication is used.

## Command Mode

Interface Configuration (VLAN)

## Default Setting

No authentication

## Command Usage

- Before specifying plain-text password authentication for an interface, configure a password with the **ip ospf authentication-key** command. Before specifying MD5 authentication for an interface, configure the message-digest key-id and key with the **ip ospf message-digest-key** command.
- The plain-text authentication-key, or the MD5 *key-id* and *key*, must be used consistently throughout the autonomous system.

## Example

This example enables message-digest authentication for the specified interface.

```
Console(config)#interface vlan 1
Console(config-if)#ip ospf authentication message-digest
Console(config-if)#
```

## Related Commands

**ip ospf authentication-key** (section 7.26.33 on page 1075)  
**ip ospf message-digest-key** (section 7.26.34 on page 1076)

### 7.26.33 **ip ospf authentication-key**

This command assigns a simple password to be used by neighboring routers. Use the **no** form to remove the password.

#### **Syntax**

```
ip ospf authentication-key <key>
```

```
no ip ospf authentication-key
```

*key* - Sets a plain text password. (Range: 1-8 characters)

#### **Command Mode**

Interface Configuration (VLAN)

#### **Default Setting**

No password

#### **Command Usage**

- Before specifying plain-text password authentication for an interface, configure a password with the **ip ospf authentication-key** command. Before specifying MD5 authentication for an interface, configure the message-digest key-id and key with the **ip ospf message-digest-key** command.
- A different password can be assigned to each network interface basis, but the password must be used consistently on all neighboring routers throughout a network (that is, autonomous system).

#### **Example**

This example sets a password for the specified interface.

```
Console(config)#interface vlan 1
Console(config-if)#ip ospf authentication-key badboy
Console(config-if)#
```

## Related Commands

**ip ospf authentication** (section 7.26.32 on page 1073)

### 7.26.34 ip ospf message-digest-key

This command enables message-digest (MD5) authentication on the specified interface and to assign a key-id and key to be used by neighboring routers. Use the **no** form to remove an existing key.

#### Syntax

```
ip ospf message-digest-key <key-id> md5 <key>
```

```
no ip ospf message-digest-key <key-id>
```

- *key-id* - Index number of an MD5 key. (Range: 1-255)
- *key* - Alphanumeric password used to generate a 128 bit message digest or "fingerprint." (Range: 1-16 characters)

#### Command Mode

Interface Configuration (VLAN)

#### Default Setting

MD5 authentication is disabled.

#### Command Usage

- Normally, only one key is used per interface to generate authentication information for outbound packets and to authenticate incoming packets. Neighbor routers must use the same key identifier and key value.
- When changing to a new key, the router will send multiple copies of all protocol messages, one with the old key and another with the new key. Once all the neighboring routers start sending protocol messages back to this router with the new key, the router will stop using the old key. This rollover process gives the network administrator time to update all the routers on the network without affecting the network connectivity. Once

all the network routers have been updated with the new key, the old key should be removed for security reasons.

### Example

This example sets a message-digest key identifier and password.

```
Console(config)#interface vlan 1
Console(config-if)#ip ospf message-digest-key 1 md5 aiebel
Console(config-if)#
```

### Related Commands

**ip ospf authentication** (section 7.26.32 on page 1073)

## 7.26.35 ip ospf cost

This command explicitly sets the cost of sending a packet on an interface. Use the **no** form to restore the default value.

### Syntax

**ip ospf cost <cost>**

**no ip ospf cost**

*cost* - Link metric for this interface. Use higher values to indicate slower ports. (Range: 1-65535)

### Command Mode

Interface Configuration (VLAN)

### Default Setting

1

## Command Usage

Interface cost reflects the port speed. This router uses a default cost of 1 for all ports. Therefore, if any ports are used at 100 Mbps or greater, the cost may have to be reset to a value greater than 1.

## Example

```
Console(config)#interface vlan 1
Console(config-if)#ip ospf cost 10
Console(config-if)#
```

## 7.26.36 ip ospf dead-interval

This command sets the interval at which hello packets are not seen before neighbors declare the router down. Use the **no** form to restore the default value.

### Syntax

```
ip ospf dead-interval <seconds>
```

```
no ip ospf dead-interval
```

*seconds* - The maximum time that neighbor routers can wait for a hello packet before declaring the transmitting router down. This interval must be set to the same value for all routers on the network. (Range: 1-65535)

### Command Mode

Interface Configuration (VLAN)

### Default Setting

40, or four times the interval specified by the **ip ospf hello-interval** command.



## Example

```
Console(config)#interface vlan 1
Console(config-if)#ip ospf dead-interval 50
Console(config-if)#
```

## Related Commands

**ip ospf hello-interval** (section 7.26.37 on page 1079)

### 7.26.37 ip ospf hello-interval

This command specifies the interval between sending hello packets on an interface. Use the **no** form to restore the default value.

#### Syntax

**ip ospf hello-interval** <*seconds*>

**no ip ospf hello-interval**

*seconds* - Interval at which hello packets are sent from an interface.  
This interval must be set to the same value for all routers on the network.  
(Range: 1-65535)

#### Command Mode

Interface Configuration (VLAN)

#### Default Setting

10 seconds

#### Command Usage

Hello packets are used to inform other routers that the sending router is still active. Setting the hello interval to a smaller value can reduce the delay in detecting topological changes, but will increase routing traffic.

## Example

```
Console(config)#interface vlan 1
Console(config-if)#ip ospf hello-interval 5
Console(config-if)#
```

## 7.26.38

### ip ospf priority

This command sets the router priority used when determining the designated router (DR) and backup designated router (BDR) for an area. Use the **no** form to restore the default value.

#### Syntax

```
ip ospf priority <priority>
```

```
no ip ospf priority
```

*priority* - Sets the interface priority for this router. (Range: 0-255)

#### Command Mode

Interface Configuration (VLAN)

#### Default Setting

1

#### Command Usage

- Set the priority to zero to prevent a router from being elected as a DR or BDR. If set to any value other than zero, the router with the highest priority will become the DR and the router with the next highest priority becomes the BDR. If two or more routers are tied with the same highest priority, the router with the higher ID will be elected.
- If a DR already exists for an area when this interface comes up, the new router will accept the current DR regardless of its own priority. The DR will not change until the next time the election process is initiated.

## Example

```
Console(config)#interface vlan 1
Console(config-if)#ip ospf priority 5
Console(config-if)#
```

### 7.26.39 ip ospf retransmit-interval

This command specifies the time between resending link-state advertisements (LSAs). Use the **no** form to restore the default value.

#### Syntax

**ip ospf retransmit-interval** <*seconds*>

**no ip ospf retransmit-interval**

*seconds* - Sets the interval at which LSAs are retransmitted from this interface. (Range: 1-65535)

#### Command Mode

Interface Configuration (VLAN)

#### Default Setting

5 seconds

#### Command Usage

A router will resend an LSA to a neighbor if it receives no acknowledgment. The retransmit interval should be set to a conservative value that provides an adequate flow of routing information, but does not produce unnecessary protocol traffic. Note that this value should be larger for virtual links.

## Example

```
Console(config)#interface vlan 1
Console(config-if)#ip ospf retransmit-interval 7
Console(config-if)#
```

## 7.26.40 **ip ospf transmit-delay**

This command sets the estimated time to send a link-state update packet over an interface. Use the **no** form to restore the default value.

### **Syntax**

```
ip ospf transmit-delay <seconds>
```

```
no ip ospf transmit-delay
```

*seconds* - Sets the estimated time required to send a link-state update.  
(Range: 1-65535)

### **Command Mode**

Interface Configuration (VLAN)

### **Default Setting**

1 second

### **Command Usage**

LSAs have their age incremented by this delay before transmission. When estimating the transmit delay, consider both the transmission and propagation delays for an interface. Set the transmit delay according to link speed, using larger values for lower-speed links. The transmit delay must be the same for all routers attached to an autonomous system.

### **Example**

```
Console(config)#interface vlan 1
Console(config-if)#ip ospf transmit-delay 6
Console(config-if)#
```

**7.26.41 show ip ospf**

This command shows basic information about the routing configuration.

**Command Mode**

Privileged Exec

**Example**

```

Console#show ip ospf
Routing Process with ID 10.1.1.253
Supports only single TOS(TOS0) route
It is an area border and autonomous system boundary router
Redistributing External Routes from,
 rip with metric mapped to 10
Number of area in this router is 2
Area 0.0.0.0 (BACKBONE)
 Number of interfaces in this area is 1
 SPF algorithm executed 19 times
Area 10.1.0.0
 Number of interfaces in this area is 4
 SPF algorithm executed 19 times
Console#

```

**Table 133**    *show ip ospf - Display Description*

| Field                                 | Description                                                                              |
|---------------------------------------|------------------------------------------------------------------------------------------|
| Routing Process with ID               | Router ID                                                                                |
| Supports only single TOS (TOS0) route | Type of service is not supported, so only one cost per interface can be assigned         |
| It is an <i>router type</i>           | The types displayed include internal, area border, or autonomous system boundary routers |

| Field                          | Description                                                                           |
|--------------------------------|---------------------------------------------------------------------------------------|
| Number of areas in this router | The number of configured areas                                                        |
| Area <i>identifier</i>         | The area address, and area type if backbone, NSSA or stub                             |
| Number of interfaces           | The number of interfaces attached to this area                                        |
| SPF algorithm executed         | The number of times the shortest path first algorithm has been executed for this area |

## 7.26.42 show ip ospf border-routers

This command shows entries in the routing table that lead to an Area Border Router (ABR) or Autonomous System Boundary Router (ASBR).

### Command Mode

Privileged Exec

### Example

```
Console#show ip ospf border-routers
```

| Destination | Next Hop   | Cost | Type | RteType | Area     | SPF No |
|-------------|------------|------|------|---------|----------|--------|
| 10.1.1.252  | 10.1.1.253 | 0    | ABR  | INTRA   | 10.1.0.0 | 3      |
| 10.2.6.252  | 10.2.9.253 | 0    | ASBR | INTER   | 10.2.0.0 | 7      |

```
Console#
```

Table 134 *show ip ospf border-routers - Display Description*

| Field       | Description                                                                            |
|-------------|----------------------------------------------------------------------------------------|
| Destination | Identifier for the destination router                                                  |
| Next Hop    | IP address of the next hop toward the destination                                      |
| Cost        | Link metric for this route                                                             |
| Type        | Router type of the destination; either ABR, ASBR or both                               |
| RteType     | Route type; either intra-area or interarea route (INTRA or INTER)                      |
| Area        | The area from which this route was learned                                             |
| SPF No      | The number of times the shortest path first algorithm has been executed for this route |

### 7.26.43 **show ip ospf database**

This command shows information about different OSPF Link State Advertisements (LSAs) stored in this router's database.

#### **Syntax**

```

show ip ospf [area-id] database [adv-router [ip-
address]]

show ip ospf [area-id] database [asbr-summary] [link-
state-id]

show ip ospf [area-id] database [asbr-summary] [link-
state-id] [adv-router [ip-address]]

show ip ospf [area-id] database [asbr-summary] [link-
state-id] [self-originate] [link-state-id]

show ip ospf [area-id] database [database-summary]

show ip ospf [area-id] database [external] [link-state-
id]
```

```

show ip ospf [area-id] database [external] [link-state-id] [adv-router [ip-address]]

show ip ospf [area-id] database [external] [link-state-id] [self-originate] [ip-address]

show ip ospf [area-id] database [network] [link-state-id]

show ip ospf [area-id] database [network] [link-state-id] [adv-router [ip-address]]

show ip ospf [area-id] database [network] [link-state-id] [self-originate] [link-state-id]

show ip ospf [area-id] database [nssa-external] [link-state-id]

show ip ospf [area-id] database [nssa-external] [link-state-id] [adv-router [ip-address]]

show ip ospf [area-id] database [nssa-external] [link-state-id] [self-originate] [link-state-id]

show ip ospf [area-id] database [router] [link-state-id]

show ip ospf [area-id] database [[router] [adv-router [ip-address]]

show ip ospf [area-id] database [router] [self-originate] [link-state-id]

show ip ospf [area-id] database [self-originate] [link-state-id]

show ip ospf [area-id] database [summary] [link-state-id]

show ip ospf [area-id] database [summary] [link-state-id] [adv-router [ip-address]]

show ip ospf [area-id] database [summary] [link-state-id] [self-originate] [link-state-id]

```

- *area-id* - Area defined for which LSA information is to be viewed. (This item must be entered in the form of an IP address.)



- **adv-router** - IP address of the advertising router. If not entered, information about all advertising routers is displayed.
- **ip-address** - IP address of the specified router. If no address is entered, information about the local router is displayed.
- **asbr-summary** - Shows information about Autonomous System Boundary Router summary LSAs.
- **link-state-id** - The network portion described by an LSA. The *link-state-id* entered should be:
  - An IP network number for Type 3 Summary and External LSAs
  - A Router ID for Router, Network, and Type 4 AS Summary LSAs. Also, note that when an Type 5 ASBR External LSA is describing a default route, its *link-state-id* is set to the default destination (0.0.0.0).
- **self-originate** - Shows LSAs originated by this router.
- **database-summary** - Shows a count for each LSA type for each area stored in the database, and the total number of LSAs in the database.
- **external** - Shows information about external LSAs.
- **network** - Shows information about network LSAs.
- **nssa-external** - Shows information about NSSA external LSAs.
- **router** - Shows information about router LSAs.
- **summary** - Shows information about summary LSAs.

## Command Mode

Privileged Exec

## Examples

The following shows output for the **show ip ospf database** command.

```

Console#show ip ospf database

 Displaying Router Link States(Area 10.1.0.0)
 Link ID ADV Router Age Seq# Checksum

 10.1.1.252 10.1.1.252 26 0X80000005 0X89A1
 10.1.1.253 10.1.1.253 23 0X80000002 0X8D9D

 Displaying Net Link States(Area 10.1.0.0)
 Link ID ADV Router Age Seq# Checksum

 10.1.1.252 10.1.1.252 28 0X80000001 0X53E1
Console#

```

**Table 135**    *show ip ospf database - Display Description*

| Field      | Description                                                  |
|------------|--------------------------------------------------------------|
| Link ID    | Router ID                                                    |
| ADV Router | Advertising router ID                                        |
| Age        | Age of LSA (in seconds)                                      |
| Seq#       | Sequence number of LSA (used to detect older duplicate LSAs) |
| Checksum   | Checksum of the complete contents of the LSA                 |

The following shows output when using the **asbr-summary** keyword.

```

Console#show ip ospf database asbr-summary

OSPF Router with id(10.1.1.253)

 Displaying Summary ASB Link States(Area 0.0.0.0)

LS age: 433
Options: (No TOS-capability)
LS Type: Summary Links (AS Boundary Router)
Link State ID: 192.168.5.1 (AS Boundary Router's Router ID)
Advertising Router: 192.168.1.5
LS Sequence Number: 80000002
LS Checksum: 0x51E2
Length: 32
Network Mask: 255.255.255.0
Metric: 1

Console#

```

**Table 136** *show ip ospf asbr-summary - Display Description*

| Field              | Description                                                  |
|--------------------|--------------------------------------------------------------|
| OSPF Router id     | Router ID                                                    |
| LS age             | Age of LSA (in seconds)                                      |
| Options            | Optional capabilities associated with the LSA                |
| LS Type            | Summary Links - LSA describes routes to AS boundary routers  |
| Link State ID      | Interface address of the autonomous system boundary router   |
| Advertising Router | Advertising router ID                                        |
| LS Sequence Number | Sequence number of LSA (used to detect older duplicate LSAs) |
| LS Checksum        | Checksum of the complete contents of the LSA                 |

| Field        | Description                    |
|--------------|--------------------------------|
| Length       | The length of the LSA in bytes |
| Network Mask | Address mask for the network   |
| Metrics      | Cost of the link               |

The following shows output when using the **database-summary** keyword.

```
Console#show ip ospf database database-summary
```

```
Area ID (10.1.0.0)
```

```
Router Network Sum-Net Sum-ASBR External-AS External-Nssa
 2 1 1 0 0 0
```

```
Total LSA Counts : 4
```

```
Console#
```

**Table 137** *show ip ospf database-summary - Display Description*

| Field            | Description                               |
|------------------|-------------------------------------------|
| Area ID          | Area identifier                           |
| Router           | Number of router LSAs                     |
| Network          | Number of network LSAs                    |
| Sum-Net          | Number of summary LSAs                    |
| Sum-ASBR         | Number of summary ASBR LSAs               |
| External-AS      | Number of autonomous system external LSAs |
| External-Nssa    | Number of NSSA external network LSAs      |
| Total LSA Counts | Total number of LSAs                      |

The following shows output when using the **external** keyword.

```

Console#show ip ospf database external

OSPF Router with id(192.168.5.1) (Autonomous system 5)

 Displaying AS External Link States

LS age: 433
Options: (No TOS-capability)
LS Type: AS External Link
Link State ID: 10.1.1.253 (External Network Number)
Advertising Router: 10.1.2.254
LS Sequence Number: 80000002
LS Checksum: 0x51E2
Length: 32
Network Mask: 255.255.0.0
Metric Type: 2 (Larger than any link state path)
Metric: 1
Forward Address: 0.0.0.0
External Route Tag: 0

Console#

```

**Table 138** *show ip ospf external - Display Description*

| Field              | Description                                                                                                            |
|--------------------|------------------------------------------------------------------------------------------------------------------------|
| OSPF Router id     | Router ID                                                                                                              |
| LS age             | Age of LSA (in seconds)                                                                                                |
| Options            | Optional capabilities associated with the LSA                                                                          |
| LS Type            | AS External Links - LSA describes routes to destinations outside the AS (including default external routes for the AS) |
| Link State ID      | IP network number (External Network Number)                                                                            |
| Advertising Router | Advertising router ID                                                                                                  |

| Field              | Description                                                                                                                                                                       |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| LS Sequence Number | Sequence number of LSA (used to detect older duplicate LSAs)                                                                                                                      |
| LS Checksum        | Checksum of the complete contents of the LSA                                                                                                                                      |
| Length             | The length of the LSA in bytes                                                                                                                                                    |
| Network Mask       | Address mask for the network                                                                                                                                                      |
| Metric Type        | Type 1 or Type 2 external metric (see “redistribute” on page 1064)                                                                                                                |
| Metrics            | Cost of the link                                                                                                                                                                  |
| Forward Address    | Forwarding address for data to be passed to the advertised destination<br><br>(If set to 0.0.0.0, data is forwarded to the originator of the advertisement)                       |
| External Route Tag | 32-bit field attached to each external route<br><br>(Not used by OSPF; may be used to communicate other information between boundary routers as defined by specific applications) |

The following shows output when using the **network** keyword.

```

Console#show ip ospf database network

OSPF Router with id(10.1.1.253)

 Displaying Net Link States(Area 10.1.0.0)

Link State Data Network (Type 2)

LS age: 433
Options: Support External routing capability
LS Type: Network Links
Link State ID: 10.1.1.252 (IP interface address of the Designated
 Router)
Advertising Router: 10.1.1.252
LS Sequence Number: 80000002
LS Checksum: 0x51E2
Length: 32
Network Mask: 255.255.255.0

 Attached Router: 10.1.1.252
 Attached Router: 10.1.1.253
Console#

```

**Table 139**    *show ip ospf network - Display Description*

| Field              | Description                                                      |
|--------------------|------------------------------------------------------------------|
| OSPF Router id     | Router ID                                                        |
| LS age             | Age of LSA (in seconds)                                          |
| Options            | Optional capabilities associated with the LSA                    |
| LS Type            | Network Link - LSA describes the routers attached to the network |
| Link State ID      | Interface address of the designated router                       |
| Advertising Router | Advertising router ID                                            |

| Field              | Description                                                                                                                       |
|--------------------|-----------------------------------------------------------------------------------------------------------------------------------|
| LS Sequence Number | Sequence number of LSA (used to detect older duplicate LSAs)                                                                      |
| LS Checksum        | Checksum of the complete contents of the LSA                                                                                      |
| Length             | The length of the LSA in bytes                                                                                                    |
| Network Mask       | Address mask for the network                                                                                                      |
| Attached Router    | List of routers attached to the network; that is, fully adjacent to the designated router, including the designated router itself |

The following shows output when using the **router** keyword.

```

Console#show ip ospf database router

OSPF Router with id(10.1.1.253)

 Displaying Router Link States(Area 10.1.0.0)

Link State Data Router (Type 1)

LS age: 233
Options: Support External routing capability
LS Type: Router Links
Link State ID: 10.1.1.252 (Originating Router's Router ID)
Advertising Router: 10.1.1.252
LS Sequence Number: 80000011
LS Checksum: 0x7287
Length: 48
Router Role: Area Border Router
Number of Links: 1

Link ID: 10.1.7.0 (IP Network/Subnet Number)
 Link Data: 255.255.255.0 (Network's IP address mask)
 Link Type: Connection to a stub network
 Number of TOS metrics: 0
 Metrics: 1

Console#

```



Table 140 *show ip ospf router - Display Description*

| Field              | Description                                                                                                        |
|--------------------|--------------------------------------------------------------------------------------------------------------------|
| OSPF Router id     | Router ID                                                                                                          |
| LS age             | Age of LSA (in seconds)                                                                                            |
| Options            | Optional capabilities associated with the LSA                                                                      |
| LS Type            | Router Link - LSA describes the router's interfaces.                                                               |
| Link State ID      | Router ID of the router that originated the LSA                                                                    |
| Advertising Router | Advertising router ID                                                                                              |
| LS Sequence Number | Sequence number of LSA (used to detect older duplicate LSAs)                                                       |
| LS Checksum        | Checksum of the complete contents of the LSA                                                                       |
| Length             | The length of the LSA in bytes                                                                                     |
| Router Role        | Description of router type, including:<br>None, AS Boundary Router, Area Border Router, or Virtual Link            |
| Number of Links    | Number of links described by the LSA                                                                               |
| Link ID            | Link type and corresponding Router ID or network address                                                           |
| Link Data          | Router ID for transit network<br>Network's IP address mask for stub network<br>Neighbor Router ID for virtual link |
| Link Type          | Link-state type, including transit network, stub network, or virtual link                                          |

| Field                 | Description                                                                  |
|-----------------------|------------------------------------------------------------------------------|
| Number of TOS metrics | Type of Service metric – This router only supports TOS 0 (or normal service) |
| Metrics               | Cost of the link                                                             |

The following shows output when using the **summary** keyword.

```

Console#show ip ospf database summary

OSPF Router with id(10.1.1.253)

 Displaying Summary Net Link States(Area 10.1.0.0)

Link State Data Summary (Type 3)

LS age: 686
Options: Support External routing capability
LS Type: Summary Links(Network)
Link State ID: 10.2.6.0 (The destination Summary Network Number)
Advertising Router: 10.1.1.252
LS Sequence Number: 80000003
LS Checksum: 0x3D02
Length: 28
Network Mask: 255.255.255.0
Metric: 1

Console#

```

**Table 141** *show ip ospf summary - Display Description*

| Field          | Description                                      |
|----------------|--------------------------------------------------|
| OSPF Router id | Router ID                                        |
| LS age         | Age of LSA (in seconds)                          |
| Options        | Optional capabilities associated with the LSA    |
| LS Type        | Summary Links - LSA describes routes to networks |

| Field              | Description                                                  |
|--------------------|--------------------------------------------------------------|
| Link State ID      | Router ID of the router that originated the LSA              |
| Advertising Router | Advertising router ID                                        |
| LS Sequence Number | Sequence number of LSA (used to detect older duplicate LSAs) |
| LS Checksum        | Checksum of the complete contents of the LSA                 |
| Length             | The length of the LSA in bytes                               |
| Network Mask       | Destination network's IP address mask                        |
| Metrics            | Cost of the link                                             |

#### 7.26.44 **show ip ospf interface**

This command displays summary information for OSPF interfaces.

##### **Syntax**

```
show ip ospf interface [vlan <vlan-id>]
```

*vlan-id* - VLAN ID (Range: 1-4094)

##### **Command Mode**

Privileged Exec

## Example

```

Console#show ip ospf interface vlan 1

Vlan 1 is up
 Interface Address 10.1.1.253, Mask 255.255.255.0, Area 10.1.0.0
 Router ID 10.1.1.253, Network Type BROADCAST, Cost: 1
 Transmit Delay is 1 sec, State BDR, Priority 1
 Designated Router id 10.1.1.252, Interface address 10.1.1.252
 Backup Designated router id 10.1.1.253, Interface addr 10.1.1.253
 Timer intervals configured, Hello 10, Dead 40, Retransmit 5

Console#

```

**Table 142** *show ip ospf interface - Display Description*

| Field             | Description                                                   |
|-------------------|---------------------------------------------------------------|
| Vlan              | VLAN ID and Status of physical link                           |
| Interface Address | IP address of OSPF interface                                  |
| Mask              | Network mask for interface address                            |
| Area              | OSPF area to which this interface belongs                     |
| Router ID         | Router ID                                                     |
| Network Type      | Includes broadcast, non-broadcast, or point-to-point networks |
| Cost              | Interface transmit cost                                       |
| Transmit Delay    | Interface transmit delay (in seconds)                         |

| Field                    | Description                                                                                                                                                                                                                                                                                                                                                                              |
|--------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| State                    | <p>Disabled – OSPF not enabled on this interface</p> <p>Down – OSPF is enabled on this interface, but interface is down</p> <p>Loopback – This is a loopback interface</p> <p>Waiting – Router is trying to find the DR and BDR</p> <p>DR – Designated Router</p> <p>BDR – Backup Designated Router</p> <p>DRother – Interface is on a multiaccess network, but is not the DR or BDR</p> |
| Priority                 | Router priority                                                                                                                                                                                                                                                                                                                                                                          |
| Designated Router        | Designated router ID and respective interface address                                                                                                                                                                                                                                                                                                                                    |
| Backup Designated Router | Backup designated router ID and respective interface address                                                                                                                                                                                                                                                                                                                             |
| Timer intervals          | Configuration settings for timer intervals, including Hello, Dead and Retransmit                                                                                                                                                                                                                                                                                                         |

### 7.26.45 **show ip ospf neighbor**

This command displays information about neighboring routers on each interface within an OSPF area.

#### **Syntax**

```
show ip ospf neighbor
```

#### **Command Mode**

Privileged Exec

**Example**

```

Console#show ip ospf neighbor

 ID Pri State Address

 10.1.1.252 1 FULL/DR 10.1.1.252

Console#

```

**Table 143** *show ip ospf neighbor - Display Description*

| Field | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ID    | Neighbor's router ID                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Pri   | Neighbor's router priority                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| State | <p>OSPF state and identification flag</p> <p>States include:</p> <p>Down – Connection down</p> <p>Attempt – Connection down, but attempting contact (for non-broadcast networks)</p> <p>Init – Have received Hello packet, but communications not yet established</p> <p>Two-way – Bidirectional communications established</p> <p>ExStart – Initializing adjacency between neighbors</p> <p>Exchange – Database descriptions being exchanged</p> <p>Loading – LSA databases being exchanged</p> <p>Full – Neighboring routers now fully adjacent</p> <p>Identification flags include:</p> <p>D – Dynamic neighbor</p> <p>S – Static neighbor</p> <p>DR – Designated router</p> <p>BDR – Backup designated router</p> |

| Field   | Description                  |
|---------|------------------------------|
| Address | IP address of this interface |

### 7.26.46 **show ip ospf summary-address**

This command displays all summary address information.

#### **Syntax**

```
show ip ospf summary-address
```

#### **Command Mode**

Privileged Exec

#### **Example**

This example shows a summary address and associated network mask.

```
Console#show ip ospf summary-address
10.1.0.0/255.255.0.0
Console#
```

#### **Related Commands**

**summary-address** (section 7.26.26 on page 1063)

### 7.26.47 **show ip ospf virtual-links**

This command displays detailed information about virtual links.

#### **Syntax**

```
show ip ospf virtual-links
```

## Command Mode

Privileged Exec

## Example

```
Console#show ip ospf virtual-links
Virtual Link to router 10.1.1.253 is up
Transit area 10.1.1.0
Transmit Delay is 1 sec
Timer intervals configured, Hello 10, Dead 40, Retransmit 5
Console#
```

*Table 144 show ip ospf virtual-links - Display Description*

| Field                  | Description                                                                      |
|------------------------|----------------------------------------------------------------------------------|
| Virtual Link to router | OSPF neighbor and link state (up or down)                                        |
| Transit area           | Common area the virtual link crosses to reach the target router                  |
| Transmit Delay         | Estimated transmit delay (in seconds) on the virtual link                        |
| Timer intervals        | Configuration settings for timer intervals, including Hello, Dead and Retransmit |

## Related Commands

**area virtual-link** (section 7.26.31 on page 1070)



## 7.27 Multicast Routing Commands

This router uses IGMP snooping and query to determine the ports connected to downstream multicast hosts, and to propagate this information back up through the multicast tree to ensure that requested services are forwarded through each intermediate node between the multicast server and its hosts, and also to filter traffic from all of the other interfaces that do not require these services.

Multicast routers use snooping and query messages, along with a multicast routing protocol to deliver IP multicast packets across different subnetworks. This router supports both the Distance-Vector Multicast Routing Protocol (DVMRP) and Protocol Independent Multicasting (PIM). (Note that IGMP should be enabled for any interface that is using multicast routing.)

*Table 145 Multicast Routing Commands*

| Command Groups            | Function                                                                                                                                | Page |
|---------------------------|-----------------------------------------------------------------------------------------------------------------------------------------|------|
| Static Multicast Routing  | Configures static multicast router ports                                                                                                | 949  |
| General Multicast Routing | Enables IP multicast routing globally; also displays the IP multicast routing table created from static and dynamic routing information | 1104 |
| DVMRP Multicast Routing   | Configures global and interface settings for DVMRP                                                                                      | 1107 |
| PIM-DM Multicast Routing  | Configures global and interface settings for PIM-DM                                                                                     | 1122 |
| PIM-SM Multicast Routing  | Configures global and interface settings for PIM-SM                                                                                     | 1134 |

## General Multicast Routing Commands

This section describes commands used to configure multicast routing globally on the ECN330-switch.

Table 146 General Multicast Routing Commands

| Command                     | Function                             | Mode | Page |
|-----------------------------|--------------------------------------|------|------|
| <b>ip multicast-routing</b> | Enables IP multicast routing         | GC   | 1104 |
| <b>show ip mroute</b>       | Shows the IP multicast routing table | PE   | 1105 |

### 7.27.1 ip multicast-routing

This command enables IP multicast routing. Use the **no** form to disable IP multicast routing.

#### Syntax

```
[no] ip multicast-routing
```

#### Default Setting

Disabled

#### Command Mode

Global Configuration

#### Command Usage

This command is used to enable multicast routing globally for the router. A specific multicast routing protocol also needs to be globally enabled using the **router dvmrp** (section 7.27.3 on page 1108), **router pim dense-mode** (section 7.27.17 on page 1123) or **router pim sparse-mode** (section 7.27.28 on page 1136) command, and then the interfaces that will support multicast routing specified using the **ip dvmrp** (section 7.27.10 on

page 1115), **ip pim dense-mode** (section 7.27.18 on page 1124) or **ip pim sparse-mode** (section 7.27.39 on page 1154) commands.

### Example

```
Console(config)#ip multicast-routing
Console(config)#
```

## 7.27.2 show ip mroute

This command displays the IP multicast routing table.

### Syntax

**show ip mroute** [*<group-address>* *<source>*] [**summary**]

- *group-address* - An IP multicast group address with subscribers directly attached or downstream from this router.
- *source* - The IP subnetwork at the root of the multicast delivery tree. This subnetwork contains a known multicast source.
- **summary** - Displays summary information for each entry in the IP multicast routing table.

### Command Mode

Privileged Exec

### Command Usage

This command displays information for multicast routing. If no optional parameters are selected, detailed information for each entry in the multicast address table is displayed. If a multicast group and source pair are selected, detailed information is displayed only for the specified entry. If the **summary** option is selected, an abbreviated list of information for each entry is displayed on a single line.

## Example

This example shows detailed multicast information for a specified group/source pair.

```

Console#show ip mroute 224.0.255.3 192.111.46.8
IP Multicast Forwarding is enabled.

IP Multicast Routing Table

Flags: D - Dense, S - Sparse, C - Connected, P - Pruned,
 F - Register flag, R - RPT-bit set, T - SPT-bit set,
 J - Join SPT
Interface state: F - Forwarding, P - Pruned, L - Local
(192.111.46.0, 255.255.255.0, 224.0.255.3)
Owner: DVMRP
Upstream Interface: vlan1
Upstream Router: 148.122.34.9
Downstream: vlan2(P), vlan3(F)
Console#

```

**Table 147** *show ip mroute - Display Description*

| Field                          | Description                                                                                                                                                                                                                                  |
|--------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Source and netmask             | Subnetwork containing the IP multicast source.                                                                                                                                                                                               |
| Group address                  | IP multicast group address for a requested service.                                                                                                                                                                                          |
| Owner                          | The associated multicast protocol (DVMRP or PIM-DM).                                                                                                                                                                                         |
| Upstream Interface             | Interface leading to the upstream neighbor.                                                                                                                                                                                                  |
| Upstream Router                | IP address of the multicast router immediately upstream for this group.                                                                                                                                                                      |
| Downstream interface and flags | The interface(s) on which multicast subscribers have been recorded. The flags associated with each interface indicate prune (P) if the downstream interface has been recently terminated or forwarding (F) if the interface is still active. |

This example lists all entries in the multicast table in summary form:

```

Console#show ip mroute summary
IP Multicast Forwarding is enabled.

IP Multicast Routing Table (Summary)

Flags: P - Prune UP

 Group Source Source Mask Interface Owner Flags

 224.1.1.1 10.1.0.0 255.255.0.0 vlan1 DVMRP P
 224.2.2.2 10.1.0.0 255.255.0.0 vlan1 DVMRP --
Console#

```

## DVMRP Multicast Routing Commands

This section describes commands used to configure DVMRP dynamic multicast routing on the ECN330-switch.

*Table 148 DVMRP Multicast Routing Commands*

| Command                      | Function                                                                                       | Mode | Page |
|------------------------------|------------------------------------------------------------------------------------------------|------|------|
| <b>router dvmrp</b>          | Enables DVMRP and enters router configuration mode                                             | GC   | 1108 |
| <b>probe-interval</b>        | Sets the interval for sending neighbor probe messages                                          | RC   | 1110 |
| <b>nbr-timeout</b>           | Sets the delay before declaring an attached neighbor router down                               | RC   | 1111 |
| <b>report-interval</b>       | Sets the interval for propagating the complete set of routing tables to other neighbor routers | RC   | 1112 |
| <b>flash-update-interval</b> | Sets the interval for sending updates about changes to network topology                        | RC   | 1112 |
| <b>prune-lifetime</b>        | Defines how long a prune state remains in effect for a source-routed multicast tree            | RC   | 1113 |

| Command                        | Function                                                                                              | Mode      | Page |
|--------------------------------|-------------------------------------------------------------------------------------------------------|-----------|------|
| <b>default-gateway</b>         | Configures the default gateway for IP multicast routing                                               | RC        | 1114 |
| <b>ip dvmrp</b>                | Enables DVMRP on the specified interface                                                              | IC        | 1115 |
| <b>ip dvmrp metric</b>         | Sets the metric used when establishing reverse paths to some networks on directly attached interfaces | IC        | 1116 |
| <b>clear ip dvmrp route</b>    | Clears all dynamic routes in the multicast routing table                                              | PE        | 1117 |
| <b>show router dvmrp</b>       | Displays global DVMRP configuration settings                                                          | NE,<br>PE | 1117 |
| <b>show ip dvmrp route</b>     | Displays DVMRP routing information                                                                    | NE,<br>PE | 1118 |
| <b>show ip dvmrp neighbor</b>  | Displays DVMRP neighbor information                                                                   | NE,<br>PE | 1120 |
| <b>show ip dvmrp interface</b> | Displays DVMRP configuration settings for the interfaces                                              | NE,<br>PE | 1121 |

### 7.27.3 router dvmrp

This command enables Distance-Vector Multicast Routing (DVMRP) globally for the router and to enter router configuration mode. Use the **no** form to disable DVMRP multicast routing.

#### Syntax

```
[no] router dvmrp
```

#### Default Setting

Disabled

## Command Mode

Global Configuration

## Command Usage

This command enables DVMRP globally for the router and enters router configuration mode. Make any changes necessary to the global DVMRP parameters. Then specify the interfaces that will support DVMRP multicast routing using the **ip dvmrp** command, and set the metric for each interface.

## Example

```
Console(config)#router dvmrp
Console(config-router)#end
Console#show router dvmrp
Admin Status : enable
Probe Interval : 10
Nbr expire : 35
Minimum Flash Update Interval : 5
prune lifetime : 7200
route report : 60
Default Gateway : 0.0.0.0
Metric of Default Gateway : 0
Console#
```

## Related Commands

**ip dvmrp** (section 7.27.10 on page 1115)

**show router dvmrp** (section 7.27.13 on page 1117)

## 7.27.4 probe-interval

This command sets the interval for sending neighbor probe messages to the multicast group address for all DVMRP routers. Use the **no** form to restore the default value.

### Syntax

```
probe-interval <seconds>
```

```
no probe-interval
```

*seconds* - Interval between sending neighbor probe messages.  
(Range: 1-65535)

### Default Setting

10 seconds

### Command Mode

Router Configuration

### Command Usage

Probe messages are sent to neighboring DVMRP routers from which this device has received probes, and is used to verify whether or not these neighbors are still active members of the multicast tree.

### Example

```
Console(config-router)#probe-interval 30
Console(config-router)#
```



## 7.27.5 nbr-timeout

This command sets the interval to wait for messages from a DVMRP neighbor before declaring it dead. Use the **no** form to restore the default value.

### Syntax

```
nbr-timeout <seconds>
```

```
no nbr-timeout
```

*seconds* - Interval before declaring a neighbor dead. (Range: 1-65535)

### Default Setting

35 seconds

### Command Mode

Router Configuration

### Command Usage

This command is used for timing out routes, and for setting the children and leaf flags.

### Example

```
Console(config-router)#nbr-timeout 40
Console(config-router)#
```

### 7.27.6 report-interval

This command specifies how often to propagate the complete set of routing tables to other neighbor DVMRP routers. Use the **no** form to restore the default value.

#### Syntax

```
report-interval <seconds>
```

```
no report-interval
```

*seconds* - Interval between sending the complete set of routing tables.  
(Range: 1-65535)

#### Default Setting

60 seconds

#### Command Mode

Router Configuration

#### Example

```
Console(config-router)#report-interval 90
Console(config-router)#
```

### 7.27.7 flash-update-interval

This command specifies how often to send trigger updates, which reflect changes in the network topology. Use the **no** form to restore the default value.

#### Syntax

```
flash-update-interval <seconds>
```

```
no flash-update-interval
```

*seconds* - Interval between sending flash updates when network topology changes have occurred. (Range: 1-65535)

**Default Setting**

5 seconds

**Command Mode**

Router Configuration

**Example**

```
Console(config-router)#flash-update-interval 10
Console(config-router)#
```

**7.27.8****prune-lifetime**

This command specifies how long a prune state will remain in effect for a multicast tree. Use the **no** form to restore the default value.

**Syntax**

**prune-lifetime** <*seconds*>

**no prune-lifetime**

*seconds* - Prune state lifetime. (Range: 1-65535)

**Default Setting**

7200 seconds

**Command Mode**

Router Configuration

**Command Usage**

This command sets the prune state lifetime. After the prune state expires, the router will resume flooding multicast traffic from the multicast source device.

## Example

```
Console(config-router)#prune-lifetime 5000
Console(config-router)#
```

### 7.27.9

## default-gateway

This command specifies the default DVMRP gateway for IP multicast traffic. Use the **no** form to remove the default gateway.

### Syntax

**default-gateway** <*ip-address*>

**no default-gateway**

*ip-address* - IP address of the default DVMRP gateway.

### Default Setting

None

### Command Mode

Router Configuration

### Command Usage

- The specified interface advertises itself as a default route to neighboring DVMRP routers. It advertises the default route out through its other interfaces. Neighboring routers on the other interfaces return Poison Reverse messages for the default route back to the router. When the router receives these messages, it records all the downstream routers for the default route.
- When multicast traffic with an unknown source address (not found in the route table) is received on the default upstream route interface, the router forwards this traffic out through the other interfaces (with known downstream routers). However, when multicast traffic with an unknown source address is received on another interface, the router drops it

because only the default upstream interface can forward multicast traffic from an unknown source.

### Example

```
Console(config-router)#default-gateway 10.1.0.253
Console(config-router)#
```

## 7.27.10 ip dvmrp

This command enables DVMRP on the specified interface. Use the **no** form to disable DVMRP on this interface.

### Syntax

```
[no] ip dvmrp
```

### Default Setting

Disabled

### Command Mode

Interface Configuration (VLAN)

### Command Usage

To fully enable DVMRP, multicast routing needs to be enabled globally for the router with the **ip multicast-routing** command (page 1104), DVMRP enabled globally for the router with the **router dvmrp** command (page 1108), and also DVMRP enabled for each interface that will participate in multicast routing with the **ip dvmrp** command.

## Example

```
Console(config)#interface vlan 1
Console(config-if)#ip dvmrp
Console(config-if)#end
Console#show ip dvmrp interface
Vlan 1 is up
 DVMRP is enabled
 Metric is 1

Console#
```

### 7.27.11 ip dvmrp metric

This command configures the metric used in selecting the reverse path to networks connected directly to an interface on this router. Use the **no** form to restore the default value.

#### Syntax

```
ip dvmrp metric <interface-metric>
```

```
no ip dvmrp metric
```

*interface-metric* - Metric used to select the best reverse path.  
(Range: 1-31)

#### Default Setting

1

#### Command Mode

Interface Configuration (VLAN)

#### Command Usage

The DVMRP interface metric is used to choose the best reverse path when there are multiple paths to the same upstream destination. The lower cost path is the preferred path.

**Example**

```

Console(config)#interface vlan 1
Console(config-if)#ip dvmrp metric 2
Console(config-if)#

```

**7.27.12 clear ip dvmrp route**

This command clears all dynamic routes learned by DVMRP.

**Command Mode**

Privileged Exec

**Example**

As shown below, this command clears everything from the route table except for the default route.

```

Console#clear ip dvmrp route
clear all ip dvmrp route
Console#show ip dvmrp route

```

| Source   | Mask          | Upstream_nbr | Interface | Metric | UpTime | Expire |
|----------|---------------|--------------|-----------|--------|--------|--------|
| -----    | -----         | -----        | -----     | -----  | -----  | -----  |
| 10.1.0.0 | 255.255.255.0 | 10.1.0.253   | vlan1     | 1      | 1840   | 0      |

```

Console#

```

**7.27.13 show router dvmrp**

This command displays the global DVMRP configuration settings.

**Command Mode**

Normal Exec, Privileged Exec

## Command Usage

This command displays the global DVMRP settings described in the preceding pages:

- Admin Status, **router dvmrp**, (section 7.27.3 on page 1108)
- **probe-interval** (section 7.27.4 on page 1110)
- **nbr-timeout** (section 7.27.5 on page 1111)
- **flash-update-interval** (section 7.27.7 on page 1112)
- **prune-lifetime** (section 7.27.8 on page 1113)
- **report-interval** (section 7.27.6 on page 1112)
- **default-gateway** (section 7.27.9 on page 1114)
- **ip dvmrp metric** (section 7.27.11 on page 1116)

## Example

The default settings are shown in the following example:

```

Console#show route dvmrp
Admin Status : enable
Probe Interval : 10
Nbr expire : 35
Minimum Flash Update Interval : 5
prune lifetime : 7200
route report : 60
Default Gateway : 0.0.0.0
Metric of Default Gateway : 1
Console#

```

### 7.27.14 show ip dvmrp route

This command displays all entries in the DVMRP routing table.

#### Command Mode

Normal Exec, Privileged Exec



## Example

DMVRP routes are shown in the following example:

| Console#show ip dvmrp route |               |              |           |        |        |        |
|-----------------------------|---------------|--------------|-----------|--------|--------|--------|
| Source                      | Mask          | Upstream_nbr | Interface | Metric | UpTime | Expire |
| 10.1.0.0                    | 255.255.255.0 | 10.1.0.253   | vlan1     | 1      | 84438  | 0      |
| 10.1.1.0                    | 255.255.255.0 | 10.1.1.253   | vlan2     | 1      | 84987  | 0      |
| 10.1.8.0                    | 255.255.255.0 | 10.1.0.254   | vlan1     | 2      | 19729  | 97     |
| Console#                    |               |              |           |        |        |        |

**Table 149** *show ip dvmrp route - Display Description*

| Field        | Description                                                                                                                       |
|--------------|-----------------------------------------------------------------------------------------------------------------------------------|
| Source       | IP subnetwork that contains a multicast source, an upstream router, or an outgoing interface connected to multicast hosts.        |
| Mask         | Subnet mask that is used for the source address. This mask identifies the host address bits used for routing to specific subnets. |
| Upstream_nbr | The IP address of the network device immediately upstream for one or more multicast groups.                                       |
| Interface    | The IP interface on this router that connects to the upstream neighbor.                                                           |
| Metric       | The metric for this interface used to calculate distance vectors.                                                                 |
| UpTime       | The time elapsed since this entry was created.                                                                                    |
| Expire       | The time remaining before this entry will be aged out.                                                                            |

## 7.27.15 **show ip dvmrp neighbor**

This command displays all of the DVMRP neighbor routers.

### Command Mode

Normal Exec, Privileged Exec

### Example

| Console#show ip dvmrp neighbor |           |        |        |              |
|--------------------------------|-----------|--------|--------|--------------|
| Address                        | Interface | Uptime | Expire | Capabilities |
| -----                          | -----     | -----  | -----  | -----        |
| 10.1.0.254                     | vlan1     | 79315  | 32     | 6            |
| Console#                       |           |        |        |              |

*Table 150 show ip dvmrp neighbor - Display Description*

| Field     | Description                                                                                 |
|-----------|---------------------------------------------------------------------------------------------|
| Address   | The IP address of the network device immediately upstream for this multicast delivery tree. |
| Interface | The IP interface on this router that connects to the upstream neighbor.                     |
| Uptime    | The time since this device last became a DVMRP neighbor.                                    |
| Expire    | The time remaining before this entry will be aged out.                                      |

| Field        | Description                                                                                                                                                                                                                                                                                                                                                                                       |
|--------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Capabilities | <p>This is a hexadecimal value representing the set bits. The neighboring router's capabilities may include:</p> <p>Leaf (bit 0) - Neighbor has only one interface with neighbors.</p> <p>Prune (bit 1) - Neighbor supports pruning.</p> <p>Generation ID (bit 2) - Neighbor sends its Generation ID in probe messages.</p> <p>Mtrace (bit 3) - Neighbor can handle multicast trace requests.</p> |

## 7.27.16 show ip dvmrp interface

This command displays the DVMRP configuration for interfaces which have enabled DVMRP.

### Command Mode

Normal Exec, Privileged Exec

### Example

```

Console#show ip dvmrp interface
Vlan 1 is up
 DVMRP is enabled
 Metric is 1

Console#

```

## PIM-DM Multicast Routing Commands

This section describes commands used to configure PIM-DM dynamic multicast routing on the ECN330-switch.

*Table 151 PIM-DM Multicast Routing Commands*

| Command                              | Function                                                                                           | Mode      | Page |
|--------------------------------------|----------------------------------------------------------------------------------------------------|-----------|------|
| <b>router pim dense-mode</b>         | Enables PIM-DM globally for the router                                                             | GC        | 1123 |
| <b>ip pim dense-mode</b>             | Enables PIM-DM on the specified interface                                                          | IC        | 1124 |
| <b>ip pim hello-interval</b>         | Sets the interval between sending PIM-DM hello messages                                            | IC        | 1125 |
| <b>ip pim hello-holdtime</b>         | Sets the time to wait for hello messages from a neighboring PIM-DM router before declaring it dead | IC        | 1126 |
| <b>ip pim trigger-hello-interval</b> | Sets the maximum time before sending a triggered PIM-DM Hello message                              | IC        | 1127 |
| <b>ip pim join-prune-holdtime</b>    | Configures the hold time for the prune state                                                       | IC        | 1128 |
| <b>ip pim graft-retry-interval</b>   | Configures the time to wait for a Graft acknowledgement before resending a Graft message           | IC        | 1129 |
| <b>ip pim max-graft-retries</b>      | Configures the maximum number of times to resend a Graft message if it has not been acknowledged   | IC        | 1130 |
| <b>show router pim</b>               | Displays the global PIM configuration settings                                                     | NE,<br>PE | 1130 |
| <b>show ip pim interface</b>         | Displays information about interfaces configured for PIM                                           | NE,<br>PE | 1131 |
| <b>show ip pim neighbor</b>          | Displays information about PIM neighbors                                                           | NE,<br>PE | 1132 |

## 7.27.17 **router pim dense-mode**

This command enables Protocol-Independent Multicast - Dense Mode (PIM-DM) globally for the router and enters router configuration mode. Use the **no** form to disable PIM-DM multicast routing.

### **Syntax**

```
[no] router pim dense-mode
```

### **Default Setting**

Disabled

### **Command Mode**

Global Configuration

### **Command Usage**

This command enables PIM-DM globally for the router. PIM-DM also needs to be enabled for each interface that will support multicast routing using the **ip pim dense-mode** command (page 1124), and any changes necessary to the multicast protocol parameters made.

### **Example**

```
Console(config)#router pim dense-mode
Console#show router pim
PIM Dense-Mode Admin Status: Enabled
PIM Sparse-Mode Admin Status: Disabled
Console#
```

## 7.27.18 **ip pim dense-mode**

This command enables PIM-DM on the specified interface. Use the **no** form to disable PIM-DM on this interface.

### **Syntax**

```
[no] ip pim dense-mode
```

### **Default Setting**

Disabled

### **Command Mode**

Interface Configuration (VLAN)

### **Command Usage**

- To fully enable PIM-DM, multicast routing needs to be enabled globally for the router with the **ip multicast-routing** command (page 1104), PIM-DM enabled globally for the router with the **router pim dense-mode** command (page 1123), and also PIM-DM enabled for each interface that will participate in multicast routing with the **ip pim dense-mode** command.
- If PIM is enabled on an interface, IGMP should also be enabled on that interface.
- Dense-mode interfaces are subject to multicast flooding by default, and are only removed from the multicast routing table when the router determines that there are no group members or downstream routers, or when a prune message is received from a downstream router.

## Example

```

Console(config)#interface vlan 1
Console(config-if)#ip pim dense-mode
Console#show ip pim interface
Vlan 1 is up
 PIM is enabled, mode is Dense.
 Internet address is 10.1.0.253.
 Hello time interval is 30 sec, trigger hello time interval is 5
 sec.
 Hello holdtime is 105 sec.
 Join/Prune holdtime is 210 sec.
 Graft retry interval is 3 sec, max graft retries is 2.
 DR Internet address is 10.1.0.253, neighbor count is 0.

Console#

```

### 7.27.19 ip pim hello-interval

This command configures the frequency at which PIM hello messages are transmitted. Use the **no** form to restore the default value.

#### Syntax

**ip pim hello-interval** *<seconds>*

**no pim hello-interval**

*seconds* - Interval between sending PIM hello messages.  
(Range: 1-65535)

#### Default Setting

30 seconds

#### Command Mode

Interface Configuration (VLAN)

## Command Usage

Hello messages are sent to neighboring PIM routers from which this device has received probes, and are used to verify whether or not these neighbors are still active members of the multicast tree.

## Example

```
Console(config-if)#ip pim hello-interval 60
Console(config-if)#
```

## 7.27.20

### ip pim hello-holdtime

This command configures the interval to wait for hello messages from a neighboring PIM router before declaring it dead. Use the **no** form to restore the default value.

#### Syntax

```
ip pim hello-holdtime <seconds>
```

```
no ip pim hello-holdtime
```

*seconds* - The hold time for PIM hello messages. (Range: 1-65535)

#### Default Setting

105 seconds

#### Command Mode

Interface Configuration (VLAN)

#### Command Usage

The **ip pim hello-holdtime** should be 3.5 times the value of **ip pim hello-interval** (section 7.27.19 on page 1125).



## Example

```
Console(config-if)#ip pim hello-holdtime 210
Console(config-if)#
```

### 7.27.21 ip pim trigger-hello-interval

This command configures the maximum time before transmitting a triggered PIM-DM Hello message after the router is rebooted or PIM-DM is enabled on an interface. Use the **no** form to restore the default value.

#### Syntax

```
ip pim trigger-hello-interval <seconds>
```

```
no ip pim trigger-hello-interval
```

*seconds* - The maximum time before sending a triggered PIM-DM Hello message. (Range: 0-65535)

#### Default Setting

5 seconds

#### Command Mode

Interface Configuration (VLAN)

#### Command Usage

- When a router first starts or PIM-DM is enabled on an interface, the hello-interval is set to random value between 0 and the trigger-hello-interval. This prevents synchronization of Hello messages on multi-access links if multiple routers are powered on simultaneously.
- Also, if a Hello message is received from a new neighbor, the receiving router will send its own Hello message after a random delay between 0 and the trigger-hello-interval.

## Example

```
Console(config-if)#ip pim trigger-hello-interval 10
Console(config-if)#
```

### 7.27.22 ip pim join-prune-holdtime

This command configures of the hold time for the prune state. Use the **no** form to restore the default value.

#### Syntax

```
ip pim join-prune-holdtime <seconds>
```

```
no ip pim join-prune-holdtime
```

*seconds* - The hold time for the prune state. (Range: 0-65535)

#### Default Setting

210 seconds

#### Command Mode

Interface Configuration (VLAN)

#### Command Usage

The multicast interface that first receives a multicast stream from a particular source forwards this traffic to all other PIM-DM interfaces on the router. If there are no requesting groups on that interface, the leaf node sends a prune message upstream and enters a prune state for this multicast stream. The prune state is maintained until the join-prune-holdtime timer expires or a graft message is received for the forwarding entry.

## Example

```
Console(config-if)#ip pim join-prune-holdtime 60
Console(config-if)#
```

## 7.27.23 **ip pim graft-retry-interval**

This command configures the time to wait for a Graft acknowledgement before resending a Graft. Use the **no** form to restore the default value.

### Syntax

```
ip pim graft-retry-interval <seconds>
```

```
no ip pim graft-retry-interval
```

*seconds* - The time before resending a Graft. (Range: 0-65535)

### Default Setting

3 seconds

### Command Mode

Interface Configuration (VLAN)

### Command Usage

A graft message is sent by a router to cancel a prune state. When a router receives a graft message, it must respond with an graft acknowledgement message. If this acknowledgement message is lost, the router that sent the graft message will resend it a number of times (as defined by the **ip pim max-graft-retries** command).

### Example

```
Console(config-if)#ip pim graft-retry-interval 9
Console(config-if)#
```

### 7.27.24 **ip pim max-graft-retries**

This command configures the maximum number of times to resend a Graft message if it has not been acknowledged. Use the **no** form to restore the default value.

#### **Syntax**

```
ip pim max-graft-retries <retries>
```

```
no ip pim graft-retry-interval
```

*retries* - The maximum number of times to resend a Graft.  
(Range: 0-65535)

#### **Default Setting**

2

#### **Command Mode**

Interface Configuration (VLAN)

#### **Example**

```
Console(config-if)#ip pim max-graft-retries 5
Console(config-if)#
```

### 7.27.25 **show router pim**

This command displays the global PIM configuration settings.

#### **Command Mode**

Normal Exec, Privileged Exec

## Example

```
Console#show router pim
PIM Dense-Mode Admin Status: Enabled
PIM Sparse-Mode Admin Status: Disabled
Console#
```

### 7.27.26 **show ip pim interface**

This command displays information about interfaces configured for PIM.

#### Syntax

```
show ip pim interface <vlan-id>
 vlan-id - VLAN ID (Range: 1-4094)
```

#### Command Mode

Normal Exec, Privileged Exec

#### Command Usage

This command displays the PIM settings for the specified interface as described in the preceding pages. It also shows the address of the designated PIM router and the number of neighboring PIM routers.

## Example

```
Console#show ip pim interface 1
Vlan 1 is up
 PIM is enabled, mode is Dense.
 Internet address is 10.1.0.253.
 Hello time interval is 30 sec, trigger hello time interval is 5
 sec.
 Hello holdtime is 105 sec.
 Join/Prune holdtime is 210 sec.
 Graft retry interval is 3 sec, max graft retries is 2.
 DR Internet address is 10.1.0.254, neighbor count is 1.

Console#sh ip pim interface 2
Vlan 1 is up
 PIM is enabled, mode is Sparse.
 Internet address is 192.168.1.250.
 Hello time interval is 40 sec, trigger hello time interval is 5
 sec.
 Hello holdtime is 105 sec.
 DR priority is 1.
 DR Internet address is 0.0.0.0, neighbor count is 0.

Console#
```

### 7.27.27 show ip pim neighbor

This command displays information about PIM neighbors.

#### Syntax

```
show ip pim neighbor [ip-address]
```

*ip-address* - IP address of a PIM neighbor.

#### Default Setting

Displays information for all known PIM neighbors.

#### Command Mode

Normal Exec, Privileged Exec

**Example**

```

Console#show ip pim neighbor
 Address VLAN Interface Uptime Expire Mode

 10.1.0.254 1 17:38:16 00:01:25 Dense
Console#

```

*Table 152 show ip pim neighbor - Display Description*

| Field          | Description                                         |
|----------------|-----------------------------------------------------|
| Address        | IP address of the next-hop router.                  |
| VLAN Interface | Interface number that is attached to this neighbor. |
| Uptime         | The duration this entry has been active.            |
| Expire         | The time before this entry will be removed.         |
| Mode           | PIM mode used on this interface.                    |

## PIM-SM Multicast Routing Commands

This section describes commands used to configure PIM-SM dynamic multicast routing on the ECN330-switch.

*Table 153 PIM-SM Multicast Routing Commands*

| Command                                      | Function                                                                                           | Mode | Page |
|----------------------------------------------|----------------------------------------------------------------------------------------------------|------|------|
| <b>router pim<br/>sparse-mode</b>            | Enables PIM-SM globally for the router                                                             | GC   | 1136 |
| <b>ip pim<br/>jp-interval</b>                | Sets the join/prune timer                                                                          | GC   | 1137 |
| <b>ip pim<br/>bsr-candidate</b>              | Configures the ECN330-switch as a Bootstrap Router (BSR) candidate                                 | GC   | 1138 |
| <b>ip pim<br/>rp-candidate</b>               | Configures the ECN330-switch as a Rendezvous Point (RP) candidate                                  | GC   | 1141 |
| <b>ip pim rp-address</b>                     | Sets a static address for the Rendezvous Point                                                     | GC   | 1144 |
| <b>ip pim register-<br/>rate-limit</b>       | Configures the rate at which register messages are sent by the Designated Router (DR)              | GC   | 1146 |
| <b>ip pim<br/>spt-threshold<br/>infinity</b> | Prevents the last-hop PIM router from switching to Shortest Path Source Tree (SPT) mode            | GC   | 1147 |
| <b>ip pim register-<br/>suppression</b>      | Configures the register suppression timer on a DR or the keep alive time on an RP                  | GC   | 1149 |
| <b>ip pim ignore-<br/>rp-set-priority</b>    | Ignores the priority value for RP candidates, and only uses the hashing mechanism for RP selection | GC   | 1150 |
| <b>ip pim crp-prefix</b>                     | Allows the ECN330-switch to be accepted as an RP candidate by a Cisco BSR                          | GC   | 1151 |



| Command                                  | Function                                                                                        | Mode      | Page |
|------------------------------------------|-------------------------------------------------------------------------------------------------|-----------|------|
| <b>ip pim register-checksum-withdata</b> | Calculates the register checksum over the whole packet instead of just the packet header        | GC        | 1153 |
| <b>ip pim sparse-mode</b>                | Enables PIM-SM on the specified interface                                                       | IC        | 1154 |
| <b>ip pim dr-priority</b>                | Sets the priority value for a DR candidate                                                      | IC        | 1155 |
| <b>ip pim hello-interval</b>             | Sets the interval at which periodic hellos are sent out on all interfaces                       | IC        | 1157 |
| <b>ip pim hello-holdtime</b>             | Sets the timer that detects whether a neighbor router is still alive and sending hello messages | IC        | 1158 |
| <b>clear ip pim bsr rp-set</b>           | Clears the RP entries learned through the BSR                                                   | PE        | 1160 |
| <b>show ip pim</b>                       | Shows the global settings for PIM-SM                                                            | PE        | 1161 |
| <b>show ip pim bsr-router</b>            | Displays information about the BSR                                                              | PE        | 1163 |
| <b>show ip pim rp mapping</b>            | Display active RPs and associated multicast routing entries                                     | PE        | 1165 |
| <b>show ip pim rp-hash</b>               | Displays the RP used for the specified multicast group                                          | PE        | 1166 |
| <b>show router pim</b>                   | Displays the global PIM configuration settings                                                  | PE        | 1130 |
| <b>show ip pim interface</b>             | Displays information about interfaces configured for PIM                                        | NE,<br>PE | 1131 |
| <b>show ip pim neighbor</b>              | Displays information about PIM neighbors                                                        | PE        | 1132 |
| <b>show ip mroute</b>                    | Shows the IP multicast routing table                                                            | PE        | 1105 |

## 7.27.28 **router pim sparse-mode**

This command enables Protocol-Independent Multicast - Sparse Mode (PIM-SM) globally for the router and enters router configuration mode. Use the **no** form to disable PIM-SM multicast routing.

### **Syntax**

```
[no] router pim sparse-mode
```

### **Default Setting**

Disabled

### **Command Mode**

Global Configuration

### **Command Usage**

This command enables PIM-SM globally for the router. PIM-SM also needs to be enabled for each interface that will support multicast routing using the **ip pim sparse-mode** command (section 7.27.39 on page 1154), and any changes necessary to the multicast protocol parameters made.

### **Example**

```
Console(config)#router pim sparse-mode
Console#show router pim
PIM Dense-Mode Admin Status: Disabled
PIM Sparse-Mode Admin Status: Enabled
Console#
```

## 7.27.29 ip pim jp-interval

This command sets the join/prune interval. Use the **no** form to restore the default settings.

### Syntax

```
ip pim jp-interval <seconds>
```

```
no ip pim jp-interval
```

*seconds* - The interval at which join/prune messages are sent.  
(Range: 0-65535 seconds)

### Default Setting

60 seconds

### Command Mode

Global Configuration

### Command Usage

- By default, the ECN330-switch sends join/prune messages every 60 seconds to inform other PIM-SM routers about clients who want to join or leave a multicast group.
- Use the same join/prune message interval on all the PIM-SM routers in the same PIM-SM domain, otherwise the routing protocol's performance will be adversely affected.
- The multicast interface that first receives a multicast stream from a particular source forwards this traffic only to those interfaces on the router that have requested to join this group. When there are no longer any requesting groups on that interface, the leaf node sends a prune message upstream and enters a prune state for this multicast stream. The protocol maintains both the current join state and the pending RPT prune state for this (source, group) pair until the jp-interval timer expires.

## Example

```

Console(config)#ip pim jp-interval 80
Console#show ip pim
PIM-DM Admin Status: Disabled
PIM-SM Admin Status: Enabled
Join/Prune-Interval: 80
Register-Suppression: 60
Register-Rate-Limit: 0
Register-Checksum-with Data: Disabled
Ignore RP-Set-Priority: Disabled
CRP-Prefix: Disabled
SPT-Threshold: Disabled
Console#

```

### 7.27.30 ip pim bsr-candidate

This command configures the ECN330-switch as a Bootstrap Router (BSR) candidate. Use the **no** form to remove this router as a BSR candidate.

#### Syntax

```
ip pim bsr-candidate vlan <vlan-id> [hash-mask-length
 <hash-mask-length>] [priority <priority>]
```

```
no ip pim bsr-candidate
```

- *vlan-id* - Identifier of configured VLAN interface. (Range: 1-4094)
- *hash-mask-length* - Hash mask length (in bits) used for RP selection (see “ip pim rp-candidate” on page 1141 and “ip pim rp-address” on page 1144). The portion of the hash specified by the mask length is ANDed with the group address. Therefore, when the hash function is executed on any BSR, all groups with the same seed hash will be mapped to the same RP. If the mask length is less than 32, then only the first portion of the hash is used, and a single RP will be defined for multiple groups. (Range: 0-32; Default: 10)
- *priority* - Priority used by the candidate bootstrap router in the election process. The BSR candidate with the largest priority is preferred. If the priority values are the same, the candidate with the larger IP address is elected to be the BSR. Setting the priority to zero means that this router is not eligible to server as the BSR. At

least one router in the PIM-SM domain must be set to a value greater than zero. (Range: 0-255; Default: 0)

### Default Setting

Hash Mask Length: 10  
Priority: 0

### Command Mode

Global Configuration

### Command Usage

- When the **ip pim bsr-candidate** command is entered, the router starts sending bootstrap messages to all of its PIM-SM neighbors. The IP address of the designated VLAN is sent as the candidate's BSR address. Each neighbor receiving the bootstrap message compares the BSR address with the address from previous messages. If the current address is the same or a higher address, it accepts the bootstrap message and forwards it. Otherwise, it drops the message.
- This router will continue to be the BSR until it receives a bootstrap message from another candidate with a higher priority (or a higher IP address if the priorities are the same).
- To improve failover recovery, it is advisable to select at least two core routers in diverse locations, each to serve as both a candidate BSR and candidate RP. It is also preferable to set up one of these routers as both the primary BSR and RP.

## Example

The following example configures the router to start sending bootstrap messages out of the interface for VLAN 1 to all of its PIM-SM neighbors.

```
Console(config)#ip pim bsr-candidate vlan 1 hash-mask-length 20
priority 200
Console(config)#exit
Console#show ip pim bsr-router
PIMv2 BootStrap Information:
BSR address: 192.168.1.250
BSR priority: 0
BSR hash mask length: 10
Uptime: 0:0:0
Expires: 0:0:5

Candidate BSR: 192.168.1.250 (Vlan1)
Candidate-BSR Priority: 0
Candidate-BSR hash mask length: 10
Console#
```

## Related Commands

**show ip pim bsr-router** (section 7.27.45 on page 1163)

## 7.27.31 **ip pim rp-candidate**

This command configures the ECN330-switch to advertise itself as a Rendezvous Point (RP) candidate to the bootstrap router (BSR). Use the **no** form to remove this router as an RP candidate.

### Syntax

```
ip pim rp-candidate vlan <vlan-id>
 [<group-address mask>] [priority <priority>]
```

```
no ip pim rp-candidate vlan <vlan-id>
 [<group-address mask>]
```

- *vlan-id* - Identifier of configured VLAN interface. (Range: 1-4094)
- *group-address* - An IP multicast group address. If a group address is not specified, the RP is used for all multicast groups.
- *mask* - Subnet mask that is used for the group address.
- *priority* - Priority used by the candidate RP in the election process. The RP candidate with the largest priority is preferred. If the priority values are the same, the candidate with the larger IP address is elected to be the RP. (Range: 0-255; Default: 192)

### Default Setting

Priority: 192

### Command Mode

Global Configuration

### Command Usage

- When the **ip pim rp-candidate** command is entered, the router periodically sends PIMv2 messages to the BSR advertising itself as a candidate RP for the specified group addresses. The IP address of the designated VLAN is sent as the candidate's RP address. The BSR places information about all of the candidate RPs in subsequent bootstrap messages. The BSR uses the RP-election hash algorithm to select an active RP for each group range. The election process is performed by the BSR only for its own use. Each PIM-SM router that

receives the list of RP candidates from the BSR also elects an active RP for each group range using the same election process.

- The election process for each group is based on the following criteria:
  - Find all RPs with the most specific group range.
  - Select those with the highest priority (lowest priority value).
  - Compute hash value based on the group address, RP address, and hash mask included in the bootstrap messages.
  - If there is a tie, use the candidate RP with the highest IP address.
- This distributed election process provides faster convergence and minimal disruption when an RP fails. It also serves to provide load balancing by distributing groups across multiple RPs. Moreover, when an RP fails, the responsible RPs are re-elected on each router, and the groups automatically distributed to the remaining RPs.
- To improve failover recovery, it is advisable to select at least two core routers in diverse locations, each to serve as both a candidate BSR and candidate RP. It is also preferable to set up one of these routers as both the primary BSR and RP.



## Example

The following example configures the router to start advertising itself to the BSR as a candidate RP for the specified multicast groups.

```
Console(config)#ip pim rp-candidate vlan 1 224.0.0.0 255.0.0.0
priority 200
Console(config)#exit
Console#show ip pim bsr-router
PIMv2 BootStrap Information:
This system is the BootStrap Router (BSR)
BSR address: 192.168.1.250
BSR priority: 200
BSR hash mask length: 20
Uptime: 0:14:49
Next BootStrap Message in 0:0:16

Candidate BSR: 192.168.1.250 (Vlan1)
Candidate-BSR Priority: 200
Candidate-BSR hash mask length: 20

Candidate RP: 192.168.1.250 (Vlan1)
Candidate-RP Group/masklen: 224.0.0.0/8
Candidate-RP Priority: 200
Next advisement in 0:0:38
Console#
```

## Related Commands

**show ip pim bsr-router** (section 7.27.45 on page 1163)

## 7.27.32 ip pim rp-address

This command sets a static address for the Rendezvous Point (RP) for a particular multicast group. Use the **no** form to remove an RP address or an RP address for a specific group.

### Syntax

```
ip pim rp-address <rp-address> [<group-address mask>]
[override]
```

```
no ip pim rp-address <rp-address> [<group-address mask>]
```

- *rp-address* - The IP address of the router that will be an RP.
- *group-address* - An IP multicast group address. If a group address is not specified, the RP is used for all multicast groups.
- *mask* - Subnet mask that is used for the group address.
- **override** - If there is a conflict, the static RP configured with this command prevails over a dynamically learned RP.

### Default Setting

None

### Command Mode

Global Configuration

### Command Usage

- The router specified by **ip pim rp-address** command will act as an RP for all multicast groups in the local PIM-SM domain if no group address is specified, or for the specified group or group range (indicated by the mask).
- All routers within the same PIM-SM domain must be configured with the same RP(s). Selecting an RP through the dynamic election process is therefore preferable for most situations. Using the dynamic RP election process also allows a backup RP to automatically take over if the active RP router becomes unavailable.

- Only one RP can be used for each multicast group. However, multiple RPs can be defined for different groups or group ranges using the mask. If a group is matched by more than one group mask, the router will use the RP with the longer prefix length mask. If an **ip pim rp-address** command specifies an IP address that was previously used for an RP, then the older entry is replaced.
- Static definitions for RP addresses may be used together with RP addresses dynamically learned through the bootstrap router (BSR).
- If the **override** parameter is used, a statically configured RP address will take precedence over those learned through the BSR.

### Example

In the following example, the address 192.168.1.1 indicates the RP to use for all multicast groups, and the address 10.1.1.1 indicates the RP to use for groups 224.0.0.0~224.255.255.255.

```

Console(config)#ip pim rp-address 192.168.1.1
Console(config)#ip pim rp-address 10.1.1.1 224.0.0.0 255.0.0.0
 override
Console(config)#exit
Console#show ip pim rp mapping
PIM Group-to-RP Mappings:

Group(s): 224.0.0.0/4, Static
 RP:192.168.1.1, Uptime:0:0:38

Group(s): 224.0.0.0/8, Static
 RP:10.1.1.1, Uptime:0:0:24

Console#

```

### Related Commands

**show ip pim rp mapping** (section 7.27.46 on page 1165)

### 7.27.33 **ip pim register-rate-limit**

This command configures the rate at which register messages are sent by the Designated Router (DR) for each (source, group) entry. Use the **no** form to restore the default setting.

#### **Syntax**

```
ip pim register-rate-limit <rate>
```

```
no pim register-rate-limit
```

*rate* - The maximum number of register packets per second.  
(Range: 1-65535: Default: 0, which means no limit)

#### **Default Setting**

no limit

#### **Command Mode**

Global Configuration

#### **Command Usage**

This command can be used to relieve the load on the Designated Router (DR) and RP. However, because register messages exceeding the limit are dropped, some receivers may experience data packet loss within the first few seconds in which register messages are sent from bursty sources.

## Example

This example sets the register rate limit to 500 pps.

```

Console(config)#ip pim register-rate-limit 500
Console(config)#exit
Console#show running-config
.
.
.
!
router pim sparse-mode
 ip pim register-rate-limit 500
 ip pim rp-candidate vlan 1 224.0.0.0 255.0.0.0 priority 200
 ip pim bsr-candidate vlan 1 hash-mask-length 20 priority 200
 ip pim rp-address 10.1.1.1 224.1.0.0 255.255.0.0
 ip pim rp-address 192.168.1.1 224.0.0.0 240.0.0.0
!
.
.
.
Console#

```

## Related Commands

**show running-config** (section 7.5.3 on page 545)

### 7.27.34 ip pim spt-threshold

This command prevents the last-hop PIM-SM router from switching to Shortest Path Tree (SPT) mode. Use the **no** form to restore the default setting.

## Syntax

```
[no] ip pim spt-threshold infinity
[<group-address mask>]
```

- **group-address** - An IP multicast group address. If a group address is not specified, the shared tree is used for all multicast groups.
- **mask** - Subnet mask that is used for the group address.

## Default Setting

no limit

## Command Mode

Global Configuration

## Command Usage

- The default path for packets from a multicast source to a receiver is through the RP. However, the path through the RP is not always the shortest path. Therefore, the router uses the RP to forward only the first packet from a new multicast group to its receivers. Afterwards, it calculates the shortest path tree (SPT) directly between the receiver and source, and then uses the SPT to send all subsequent packets from the source to the receiver instead of using the shared tree.
- The **ip pim spt-threshold infinity** command forces the router to use the shared tree for all multicast groups, or just for the specified multicast groups.

## Example

This example prevents the ECN330-switch from using the SPT for multicast groups 224.1.0.0~224.1.255.255 .

```
Console(config)#ip pim spt-threshold infinity 224.1.0.0 255.255.0.0
Console(config)#exit
Console#show ip pim
PIM-DM Admin Status: Disabled
PIM-SM Admin Status: Enabled
Join/Prune-Interval: 60
Register-Suppression: 60
Register-Rate-Limit: 500
Register-Checksum-with Data: Disabled
Ignore RP-Set-Priority: Disabled
CRP-Prefix: Disabled
SPT-Threshold: Enabled
 SPT-Threshold Group: 224.1.0.0
 SPT-Threshold Group mask: 255.255.0.0
Console#
```

## Related Commands

**show ip pim** (section 7.27.44 on page 1161)

### 7.27.35 ip pim register- suppression

This command configures the register suppression timer on a DR or the keep alive time on an RP. Use the **no** form to restore the default setting.

#### Syntax

**ip pim register-suppression** <*suppression-time*>

**no ip pim register-suppression**

*suppression-time* - The period during which a DR stops sending register-encapsulated data to the RP after receiving a RegisterStop message. It is also used to calculate the KeepaliveTimer by the RP. (Range: 1-65535 seconds)

#### Default Setting

60 seconds

#### Command Mode

Global Configuration

#### Command Usage

- When the DR receives a register-stop message from the RP, it uses the register suppression time to set the register-stop timer. It then stops sending register messages and starts the register-stop timer for the specified group. Afterwards, the DR periodically sends a null-register message to the RP to determine whether or not the RP wants to start receiving normal register messages for this group.
- When the RP receives a register message for a source for any group, it uses the register suppression time to set the keep-alive timer for that group source.

## Example

This example sets the register suppression time to 500 seconds.

```

Console(config)#ip pim register-suppression 500
Console(config)#exit
Console#show running-config
.
.
!
router pim sparse-mode
 ip pim register-rate-limit 500
 ip pim spt-threshold infinity 224.1.0.0 255.255.0.0
 ip pim register-suppression 500
 ip pim rp-candidate vlan 1 224.0.0.0 255.0.0.0 priority 200
 ip pim bsr-candidate vlan 1 hash-mask-length 20 priority 200
 ip pim rp-address 10.1.1.1 224.1.0.0 255.255.0.0
 ip pim rp-address 192.168.1.1 224.0.0.0 240.0.0.0
!
.
.
Console#

```

## Related Commands

**show running-config** (section 7.5.3 on page 545)

### 7.27.36 ip pim ignore-rp-set-priority

This command ignores the priority value for RP candidates, and only uses the hashing mechanism for RP selection. Use the **no** form to restore the default setting.

#### Syntax

**[no] ip pim ignore-rp-set-priority**

#### Default Setting

Disabled



## Command Mode

### Global Configuration

## Example

This example suppresses the priority bit for RP candidates.

```

Console(config)#ip pim ignore-rp-set-priority
Console(config)#exit
Console#show running-config
.
.
.
!
router pim sparse-mode
 ip pim register-rate-limit 500
 ip pim spt-threshold infinity 224.1.0.0 255.255.0.0
 ip pim register-suppression 500
 ip pim ignore-rp-set-priority
 ip pim rp-candidate vlan 1 224.0.0.0 255.0.0.0 priority 200
 ip pim bsr-candidate vlan 1 hash-mask-length 20 priority 200
 ip pim rp-address 10.1.1.1 224.1.0.0 255.255.0.0
 ip pim rp-address 192.168.1.1 224.0.0.0 240.0.0.0
!
.
.
.
Console#

```

## Related Commands

**show running-config** (section 7.5.3 on page 545)

### 7.27.37 ip pim crp-prefix

This command allows the ECN330-switch to be accepted as an RP candidate by a Cisco BSR. Use the **no** form to restore the default setting.

## Syntax

**[no] ip pim crp-prefix**

## Default Setting

Disabled

## Command Mode

Global Configuration

## Command Usage

Cisco's BSR does not conform to the latest BSR draft. It does not accept candidate RPs with a group prefix of zero. This command is therefore required to make the ECN330-switch an acceptable candidate RP for a Cisco BSR.

## Example

This example makes the ECN330-switch an acceptable RP candidate for Cisco BSRs.

```
Console(config)#ip pim crp-prefix
Console(config)#exit
Console#show ip pim
PIM-DM Admin Status: Disabled
PIM-SM Admin Status: Enabled
Join/Prune-Interval: 60
Register-Suppression: 500
Register-Rate-Limit: 500
Register-Checksum-with Data: Disabled
Ignore RP-Set-Priority: Enabled
CRP-Prefix: Enabled
SPT-Threshold: Enabled
 SPT-Threshold Group: 224.1.0.0
 SPT-Threshold Group mask: 255.255.0.0
Console#
```

## Related Commands

**show ip pim** (section 7.27.44 on page 1161)

## 7.27.38 **ip pim register-checksum-withdata**

This command calculates the register checksum over the whole packet instead of just the packet header. Use the **no** form to restore the default setting.

### Syntax

```
[no] ip pim register-checksum-withdata
```

### Default Setting

Disabled - Register checksum is calculated only over the header.

### Command Mode

Global Configuration

### Example

This example makes the ECN330-switch calculate the register checksum over the whole packet.

```
Console(config)#ip pim register-checksum-withdata
Console(config)#exit
Console#show ip pim
PIM-DM Admin Status: Disabled
PIM-SM Admin Status: Enabled
Join/Prune-Interval: 60
Register-Suppression: 500
Register-Rate-Limit: 500
Register-CheckSum-with Data: Enabled
Ignore RP-Set-Priority: Enabled
CRP-Prefix: Enabled
SPT-Threshold: Enabled
 SPT-Threshold Group: 224.1.0.0
 SPT-Threshold Group mask: 255.255.0.0
Console#
```

### Related Commands

**show ip pim** (section 7.27.44 on page 1161)

## 7.27.39 **ip pim sparse-mode**

This command enables PIM-SM on the specified interface. Use the **no** form to disable PM-SM on the selected interface.

### **Syntax**

```
[no] ip pim sparse-mode
```

### **Default Setting**

Disabled

### **Command Mode**

Interface Configuration (VLAN)

### **Command Usage**

- PIM-SM must be enabled on each VLAN interface connected to the PIM Sparse network. Internet Group Management Protocol (IGMP) must also be enabled on each interface using the **ip igmp** command (section 7.21.15 on page 953).
- A PIM-SM interface is used to forward multicast traffic only if a join message is received from a downstream router or if group members are directly connected to the interface. When routers want to receive a multicast flow, they periodically send join messages to the RP, and are subsequently added to the shared path for the specified flow back up to the RP. If routers want to join the source path up through the SPT, they periodically send join messages toward the source. They also send prune messages toward the RP to prune the shared path if they have already connected to the source through the SPT, or if there are no longer any group members connected to the interface.

## Example

This example enables PIM-SM on VLAN 1.

```

Console(config)#interface vlan 1
Console(config-if)#ip pim sparse-mode
Console(config-if)#exit
Console#show ip pim interface 1
Vlan 1 is up
 PIM is enabled, mode is Sparse.
 Internet address is 192.168.1.250.
 Hello time interval is 30 sec, trigger hello time interval is 5 sec.
 Hello holdtime is 105 sec.
 DR priority is 1.
 DR Internet address is 0.0.0.0, neighbor count is 0.

Console#

```

## Related Commands

**show ip pim interface** (section 7.27.26 on page 1131)

### 7.27.40 ip pim dr-priority

This command sets the priority value for a Designated Router (DR) candidate. Use the **no** form to restore the default setting.

#### Syntax

**ip pim dr-priority** <priority-value>

**no ip pim dr-priority**

*priority-value* - Priority advertised by a router when bidding to become the DR. (Range: 0-4294967294)

#### Default Setting

1

## Command Mode

### Interface Configuration (VLAN)

## Command Usage

- More than one PIM-SM router may be connected an Ethernet or other shared-media LAN. If multicast hosts are directly connected to the LAN, then only one of these routers is elected as the DR, and acts on behalf of these hosts, sending periodic Join/Prune messages toward a group-specific RP for each group. A single DR is elected per interface (LAN or otherwise) using a simple election process.
- The router with the highest priority configured on an interface is elected as the DR. If more than one router attached to this interface uses the same priority, then the router with the highest IP address is elected to serve as the DR.
- If a router does not advertise a priority in its hello messages, it is assumed to have the highest priority and is elected as the DR. If more than one router is not advertising its priority, then the router with the highest IP address is elected to server as the DR.

## Example

This example enables PIM-SM on VLAN 1.

```
Console(config)#interface vlan 1
Console(config-if)#ip pim dr-priority 20
Console#show ip pim interface 1
Vlan 1 is up
 PIM is enabled, mode is Sparse.
 Internet address is 192.168.1.250.
 Hello time interval is 30 sec, trigger hello time interval is 5 sec.
 Hello holdtime is 105 sec.
 DR priority is 20.
 DR Internet address is 0.0.0.0, neighbor count is 0.

Console#
```

## Related Commands

**show ip pim interface** (section 7.27.26 on page 1131)

## 7.27.41 **ip pim hello-interval**

This command sets the interval at which periodic hellos are sent out on all interfaces. Use the **no** form to restore the default setting.

### **Syntax**

```
ip pim hello-interval <interval-value>
```

```
no ip pim hello-interval
```

*interval-value* - Interval at which periodic hellos are sent out PIM interfaces. (Range: 1-65535 seconds)

### **Default Setting**

30 seconds

### **Command Mode**

Interface Configuration (VLAN)

### **Command Usage**

- PIM-SM routers send periodic hello messages to inform neighboring routers of their presence, and to determine which router for each LAN segment will serve as the Designated Router (DR).
- When a router is booted or first configured for PIM-SM, it sends an initial hello message, and then sets its Hello timer to the configured value. If a router does not hear from a neighbor for the period specified by the hello-holdtime (set a period of 3.5 times the hello timer by default), that neighbor is dropped. This hold time is included in each hello message received from a neighbor. Also note that hello messages also contain the DR priority of the router sending the message.

## Example

This example sets the hello time on VLAN 1.

```
Console(config)#interface vlan 1
Console(config-if)#ip pim hello-interval 40
Console#show ip pim interface 1
Vlan 1 is up
 PIM is enabled, mode is Sparse.
 Internet address is 192.168.1.250.
 Hello time interval is 30 sec, trigger hello time interval is 40
 sec.
 Hello holdtime is 105 sec.
 DR priority is 20.
 DR Internet address is 0.0.0.0, neighbor count is 0.

Console#
```

## Related Commands

**show ip pim interface** (section 7.27.26 on page 1131)

## 7.27.42

### ip pim hello-holdtime

This command sets the timer that detects whether a neighbor router is still alive and sending hello messages. Use the **no** form to restore the default setting.

#### Syntax

**ip pim hello-holdtime** *<holdtime-value>*

**no ip pim hello-holdtime**

*holdtime-value* - Holdtime for which to keep a neighbor state alive.  
(Range: 1-65535 seconds)

#### Default Setting

3.5 times the hello interval



## Command Mode

### Interface Configuration (VLAN)

## Command Usage

- The hello-holdtime indicates how many seconds the router holds an entry for a neighbor that has stopped sending hello messages.
- The hello-holdtime should be included in each hello message received from a neighbor. Routers on the same subnet may therefore have different hello-holdtimes.
- If the hello interval is set at the default value of 30 seconds, then the default hello-holdtime is 105 seconds. If the hello-holdtime has not been configured, then every time the hello interval is updated (see section 7.27.41 on page 1157), the hello-holdtime is automatically updated. However, if the hello-holdtime has been configured, then it will not be updated when the hello interval changes. Also, note that if a value is set for the hello-holdtime that is less than the hello interval, the command will fail.
- When the **no ip pim hello-holdtime** is entered, the hello-holdtime is set to 3.5 times the current hello interval.

## Example

This example sets the hello-holdtime on VLAN 1.

```
Console(config)#interface vlan 1
Console(config-if)#ip pim hello-holdtime 120
Console#show ip pim interface 1
Vlan 1 is up
PIM is enabled, mode is Sparse.
Internet address is 192.168.1.250.
Hello time interval is 30 sec, trigger hello time interval is 40
sec.
Hello holdtime is 120 sec.
DR priority is 20.
DR Internet address is 0.0.0.0, neighbor count is 0.

Console#
```

## Related Commands

**show ip pim interface** (section 7.27.26 on page 1131)

### 7.27.43 clear ip pim bsr rp-set

This command clears the RP entries learned through the BSR.

## Command Mode

Privileged Exec

## Command Usage

This command can be used to update the entries in the static multicast forwarding table immediately after making configuration changes to the RP.

## Example

This example clears the RP map.

```
Console#clear ip pim bsr rp-set
Console#sh ip pim rp mapping
PIM Group-to-RP Mappings:

Console#
```

## Related Commands

**show ip pim rp mapping** (section 7.27.46 on page 1165)

## 7.27.44 show ip pim

This command shows the global settings for PIM-SM.

### Command Mode

Privileged Exec

### Example

This example displays the global settings for PIM-SM.

```

Console#show ip pim
PIM-DM Admin Status: Disabled
PIM-SM Admin Status: Enabled
Join/Prune-Interval: 60
Register-Suppression: 500
Register-Rate-Limit: 500
Register-Checksum-with Data: Enabled
Ignore RP-Set-Priority: Enabled
CRP-Prefix: Enabled
SPT-Threshold: Enabled
 SPT-Threshold Group: 224.1.0.0
 SPT-Threshold Group mask: 255.255.0.0
Console#

```

**Table 154** show ip pim - Display Description

| Field                | Description                                                                                        |
|----------------------|----------------------------------------------------------------------------------------------------|
| PIM-DM Admin Status  | Shows if PIM-DM is enabled                                                                         |
| PIM-SM Admin Status  | Shows if PIM-SM is enabled                                                                         |
| Join/Prune-Interval  | Frequency at which this router sends Join/Prune messages for the multicast groups it is forwarding |
| Register-Suppression | Value of the register suppression timer on a DR or the keep alive time on an RP                    |

| Field                               | Description                                                                                                       |
|-------------------------------------|-------------------------------------------------------------------------------------------------------------------|
| Register-<br>Rate-Limit             | The rate at which register messages are sent by the Designated Router (DR) for each (source, group) entry         |
| Register-<br>Checksum-<br>with Data | Shows if the register checksum is calculated over the whole packet instead of just the packet header              |
| Ignore RP-<br>Set-Priority          | Shows if the priority value for RP candidates is ignored, and only the hashing mechanism is used for RP selection |
| CRP-Prefix                          | Shows if this router can be accepted as an RP candidate by a Cisco BSR                                            |
| SPT-<br>Threshold                   | Shows if the last-hop PIM-SM router is prevented from switching to Shortest Path Tree (SPT) mode                  |

## 7.27.45 **show ip pim bsr-router**

This command displays information about the bootstrap router (BSR).

### Command Mode

Privileged Exec

### Example

This example displays information about the BSR.

```

Console#show ip pim bsr-router
PIMv2 BootStrap Information:
BSR address: 192.168.1.250
BSR priority: 0
BSR hash mask length: 10
Uptime: 0:0:0
Expires: 0:0:5

Candidate BSR: 192.168.1.250 (Vlan1)
Candidate-BSR Priority: 0
Candidate-BSR hash mask length: 10
Console#

```

**Table 155** *show ip pim bsr-router - Display Description*

| Field                              | Description                                                                                                                                             |
|------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|
| <i>PIMv2 BootStrap Information</i> |                                                                                                                                                         |
| BSR address                        | IP address of interface configured as the BSR                                                                                                           |
| BSR priority                       | Priority assigned to this interface for use in the BSR election process                                                                                 |
| BSR hash mask length               | The number of significant bits used in the multicast group comparison mask. This mask determines the multicast group for which this router can be a BSR |
| Uptime                             | The time this BSR has been up and running                                                                                                               |

| Field                          | Description                                                                                                                                      |
|--------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------|
| Expires                        | The time (hours: minutes:seconds) before the BSR sends its next bootstrap message                                                                |
| <i>Candidate BSR</i>           |                                                                                                                                                  |
| Candidate BSR (address)        | The address of all candidate BSRs attached to this interface                                                                                     |
| Candidate-BSR Priority         | Priority value used by this BSR candidate                                                                                                        |
| Candidate-BSR hash mask length | The number of significant bits used in the multicast group comparison mask by this BSR candidate                                                 |
| <i>Candidate RP</i>            |                                                                                                                                                  |
| Candidate RP (address)         | The address of all candidate RPs attached to this interface                                                                                      |
| Candidate-RP Group/masklen     | The multicast group and mask length for each group for which this candidate RP is bidding                                                        |
| Candidate-RP Priority          | Priority used by the candidate RP in the election process                                                                                        |
| Next advisement in             | Time (hours:minutes:seconds) before the next candidate RP advertisement is sent<br>(This field only displays if the candidate RP is in service.) |

## 7.27.46 **show ip pim rp mapping**

This command display active RPs and associated multicast routing entries.

### **Command Mode**

Privileged Exec

### **Example**

This example displays the RP map.

```

Console#show ip pim rp mapping
PIM Group-to-RP Mappings:

Group(s): 224.0.0.0/8, Static
 RP:10.1.1.1, Uptime:0:0:0
 RP:192.168.1.19, Uptime:0:0:0

Console#

```

**Table 156** *show ip pim rp mapping - Display Description*

| Field                           | Description                                           |
|---------------------------------|-------------------------------------------------------|
| <i>PIM Group-to-RP Mappings</i> |                                                       |
| Group(s)                        | The multicast group address assigned to the listed RP |
| RP                              | IP address of the RP for the listed multicast group   |
| Uptime                          | The time this RP has been up and running              |

## 7.27.47 **show ip pim rp-hash**

This command displays the RP used for the specified multicast group.

### **Syntax**

```
show ip pim rp-hash <group-address>
```

*group-address* - An IP multicast group address. If a group address is not specified, the RP is used for all multicast groups.

### **Command Mode**

Privileged Exec

### **Example**

This example displays the RP used for the specified group, and the method in which this RP was elected (that is , bootstrap or static).

```
Console#show ip pim rp-hash 224.0.1.3
RP: 10.10.11.35
Info source: 10.10.11.35, via bootstrap
Console#sh ip pim rp-hash 224.0.0.0
RP: 192.168.1.19,Static
Console#
```



## 8 Upgrading Firmware

The ECN330-switch contains three firmware components that can be upgraded; the diagnostics (or Boot-ROM) code, runtime operation code and the loader code. For more information, see section 5.1 on page 35. The diagnostics and the loader code can be upgraded only through the ECN330's RS-232 serial console port.

**Note:** The runtime software is upgraded through PEM. Please refer to the *PEM User's Guide* for details.

ECN330-switch firmware can be upgraded by connecting a PC directly to the serial Console port on the ECN330's front panel and using VT100 terminal emulation software that supports the XModem protocol. (See section 5.2.2 on page 38.)

1. Connect a PC to the ECN330's Console port using a null-modem or crossover RS-232 cable with a female DB-9 connector.
2. Configure the terminal emulation software's communication parameters to 9600 baud, 8 data bits, 1 stop bit, no parity, and set flow control to *none*.
3. Power cycle the ECN330.
4. When the ECN330-switch initialization screen appears, enter firmware-download mode by pressing <Ctrl+u> immediately after power on or rebooting the ECN330-switch.
5. Type **mercury** at the password prompt. Screen text similar to that shown in Figure 239 on page 1168 is displayed:

Figure 239 File Download Menu

```

Image Loader 2.1.0.0

Password : *****
File Name S/Up Type Size Create Time

$logfile_1 0 3 64 1193046:28:15
$logfile_2 0 3 64 1193046:28:15
ECN330-Diag_V2.0.6.1.bix 1 1 810688 00:02:25
ECN330_V1_0_2_21.bix 1 2 2937880 00:07:27
Factory_Default_Config.cfg 1 5 2385 00:00:25
certificate 0 8 31744 00:00:23

Free Space : 8781824
[X]modem Download [D]elete File [S]et Startup File
[C]hange Baudrate [Q]uit
Select>

```

6. Press <C> to change the baud rate of the ECN330's serial connection. Screen text displays as shown in Figure 240.

Figure 240 Changing the Baud Rate

```

Select>
Change baudrate [A]9600 [B]115200
Baudrate set to 115200

```

7. Press <B> to select the option for 115200 baud.
 

There are two baud rate settings available, 9600 and 115200. Using the higher baud rate minimizes the time required to download firmware code files.
8. Set the PC's terminal emulation software to match the 115200 baud rate. Press <Enter> to reset communications with the ECN330-switch.
9. Check that the ECN330-switch has sufficient flash memory space for the new code file before starting the download. From the CLI, use the **dir** command to see how much available flash memory remains. The ECN330-switch has a total of 32 Mbytes of flash memory for system files.

The ECN330-switch can store a maximum of only two runtime and two diagnostic code files in its flash memory. Use the `[D]elete File` command to remove a runtime or diagnostic file.

10. Press `<X>` to start to download the new code file.

If using Windows HyperTerminal, click the “Transfer” button, and then click “Send File...” Select the XModem Protocol and then use the “Browse” button to select the required firmware code file from the PC system. The “Xmodem file send” window displays the progress of the download procedure.

**Note:** The download file must be a valid binary software file for the ECN330-switch.

11. After the file has been downloaded, there is a prompt `Update Image File:` to specify the type of code file. Press `<R>` for runtime code, `<D>` for diagnostic code, or `<L>` for loader code.

---

---

## Caution!

If `<L>` is selected for the loader code, be sure the file is a valid loader code file for the ECN330-switch. If an invalid file is downloaded, the ECN330-switch will not be able to boot. Unless absolutely necessary, do not attempt to download loader code files.

---

---

12. Specify a name for the downloaded code file. File names are case-sensitive, should be 1 to 31 characters, should not contain slashes (`\` or `/`), and the leading letter of the file name should not be a period (`.`). (Valid characters: A-Z, a-z, 0-9, `“.”`, `“-”`, `“_”`)

For example, Figure 241 on page 1170 shows the download procedure for a diagnostic code file:

Figure 241 File Download Procedure

```

Select>x
Xmodem Receiving Start ::
XMODEM, Successful.
Blocks Received = 3159
Bytes Received = 410440
Errors:
 Checksum = 0
 Complement = 0
 Duplicates = 0
Image downloaded to buffer.

 [R]untime
 [D]iagnostic
 [L]oader (Warning: you sure what you are doing?)
Update Image File:d
Runtime Image Filename : diag_v0002
Updating file system.
File system updated.
[Press any key to continue]

```

13. To set the new downloaded file as the startup file, use the [S]et Startup File menu option.
14. When downloading code files has finished, use the [C]hange Baudrate menu option to change the baud rate of the ECN330's serial connection back to 9600 baud.
15. Set the PC's terminal emulation software baud rate back to 9600 baud. Press <Enter> to reset communications with the ECN330-switch.
16. Press <Q> to quit the firmware-download mode and boot the ECN330-switch.

## 9 Troubleshooting

### 9.1 Diagnosing ECN330 Indicators

Table 157 Troubleshooting Chart

| Symptom                   | Cause                                                               | Action                                                                                                                                                                                                                                                                            |
|---------------------------|---------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>PWR</b> LED is off     | DC power is disconnected                                            | <ul style="list-style-type: none"> <li>Check if the DC power supply is connected to the ECN330.</li> <li>Check connections between the ECN330, the power cables, and the DC power circuit.</li> <li>Check the ECN330's fuse condition. Replace the fuse, if necessary.</li> </ul> |
| <b>PWR</b> LED is on red  | The unit's internal power supply is not operating normally          | <ul style="list-style-type: none"> <li>Reboot the ECN330-switch to see if the condition clears.</li> <li>If the condition persists, replace the unit.</li> </ul>                                                                                                                  |
| <b>DIAG</b> LED is on red | The ECN330-switch has detected a fault                              | <ul style="list-style-type: none"> <li>Power cycle the ECN330 to see if the condition is cleared.</li> <li>If the condition persists, replace the unit.</li> </ul>                                                                                                                |
| <b>FAN</b> LED is on red  | One or both cooling fans have a fault, or the ECN330 is overheating | <ul style="list-style-type: none"> <li>Check that there is enough free space around the ECN330 to allow for adequate ventilation</li> <li>Replace the fan tray if required.</li> </ul>                                                                                            |
| <b>CTRL</b> LED is off    | ENC not present                                                     | <ul style="list-style-type: none"> <li>Contact Ericsson.</li> </ul>                                                                                                                                                                                                               |
| <b>CTRL</b> LED is on red | Error in the ENC                                                    | <ul style="list-style-type: none"> <li>Log in to the CLI, check if the ECN330 is in Fallback state. Check the log file for errors. Check the interfaces configuration.</li> <li>If the ECN330 is not in Fallback state, contact Ericsson.</li> </ul>                              |

| Symptom                           | Cause                                                  | Action                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-----------------------------------|--------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| A port status LED is off          | There is no valid link on the port                     | <ul style="list-style-type: none"> <li>• Verify that the ECN330 and attached device are powered on.</li> <li>• Be sure the cable is plugged into both the ECN330 and corresponding device.</li> <li>• If the ECN330 is installed in a rack, check the connections to the punch-down block and patch panel.</li> <li>• Verify that the proper cable type is used and its length does not exceed specified limits.</li> <li>• Check the adapter on the attached device and cable connections for possible defects. Replace the defective adapter or cable if necessary.</li> </ul> |
| A port status LED is flashing red | There is a power overload or short circuit on the port | <ul style="list-style-type: none"> <li>• Remove the connection to the port.</li> <li>• Check the connection cable and connectors for defects and possible short circuits. Replace the network cable if necessary.</li> <li>• If the network cable is verified to be OK, replace the EDA device.</li> </ul>                                                                                                                                                                                                                                                                       |

## 9.2 Power and Cooling Problems

If the power indicator does not turn on when the power cord is plugged in, there may be a problem with the DC power circuit, power cord, or internal power supply. However, if the unit powers off after running for a while, check for loose power connections, power losses or surges from the DC source, and verify that the unit's cooling fans are unobstructed and running prior to shutdown. If the problem still cannot be isolated, the internal power supply may be defective.

## 9.3 Installation

Verify that all system components have been properly installed. If one or more components appear to be malfunctioning (such as the power cord or network cabling), test them in an alternate environment where all the other components are functioning properly.

## 9.4 Problems Accessing the Management Interface

Table 158 Troubleshooting Chart

| Symptom                                                                           | Action                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|-----------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Cannot access the on-board configuration program through a serial port connection | <ul style="list-style-type: none"> <li>Be sure the terminal emulator program is set to VT100 compatible, 8 data bits, 1 stop bit, no parity, and the baud rate set to any of the following (9600, 19200, 38400, 57600, 115200 bps).</li> <li>Check that the null-modem serial cable conforms to the pin-out connections provided in section 2.2.4 on page 9.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Forgot or lost the password                                                       | <ul style="list-style-type: none"> <li>Reinstall the ECN330-switch defaults. Make a direct connection to the ECN330's console port and power cycle the ECN330. Immediately after powering on, press &lt;Ctrl+u&gt; and type the password <b>mercury</b> to access the system file menu. Select &lt;D&gt; to delete all user-defined configuration files. Press &lt;Q&gt; to boot the ECN330-switch.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Cannot connect using Telnet, web browser, or SNMP software                        | <ul style="list-style-type: none"> <li>Be sure the ECN330 is powered up.</li> <li>Check network cabling between the management station and the ECN330.</li> <li>Check that there is a valid network connection to the ECN330 and that the port being using has not been disabled.</li> <li>Be sure the VLAN interface through which the management station is connected is configured with a valid IP address, subnet mask and default gateway.</li> <li>Be sure the management station has an IP address in the same subnet as the ECN330-switch's IP interface to which it is connected.</li> <li>If trying to connect to the ECN330-switch through the IP address for a tagged VLAN group, the management station, and the ports connecting intermediate switches in the network, must be configured with the appropriate tag.</li> <li>If a connection using Telnet fails, the maximum number of concurrent Telnet/SSH sessions permitted may have been exceeded. Try connecting again at a later time.</li> </ul> |

| Symptom                           | Action                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|-----------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Cannot connect using Secure Shell | <ul style="list-style-type: none"> <li>• If a connection using SSH fails, the maximum number of concurrent Telnet/SSH sessions permitted may have been exceeded. Try connecting again at a later time.</li> <li>• Be sure the control parameters for the SSH server are properly configured on the ECN330-switch, and that the SSH client software is properly configured on the management station.</li> <li>• Be sure a public key has been generated on the ECN330-switch and this key exported to the SSH client.</li> <li>• Be sure an account has been set up on the ECN330-switch for each SSH user, including user name, authentication level, and password.</li> <li>• Be sure the client's public key has been imported to the ECN330-switch (if public key authentication is used).</li> </ul> |



# 10 Specifications

## 10.1 Physical Characteristics

|                     |                                                                                                                                                                                                          |
|---------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Ports               | 24 100BASE-TX RJ45 ports<br>2 1000BASE-T/SFP combination ports<br>1 1000BASE-T port                                                                                                                      |
| Network Interface   | 10BASE-T: RJ45 (100-ohm, UTP cable;<br>Category 3 or better)<br><br>100BASE-TX: RJ45 (100-ohm, UTP cable;<br>Category 5 or better)<br><br>1000BASE-T: RJ45 (100-ohm, UTP cable;<br>Category 5, 5e, or 6) |
| Communication Speed | 10, 100, 1000 Mbps                                                                                                                                                                                       |
| Communication Mode  | Full and half duplex                                                                                                                                                                                     |
| Power-over-Ethernet | 23.1 W maximum per port<br>600 mA continuously (maximum, depending on the<br>voltage)<br>700 mA for 75 msec overload limit                                                                               |
| Buffer Architecture | 32 Mbytes per system                                                                                                                                                                                     |
| Aggregate Bandwidth | 10.8 Gbps                                                                                                                                                                                                |
| Switching Database  | 16K MAC address entries                                                                                                                                                                                  |
| LEDs                | System: PWR, DIAG, FAN, CTRL<br>Ports 1-24: Link/Speed/Activity/Overload<br>Ports 25-27: Link/Activity                                                                                                   |
| Weight              | 4.00 kg (8.82 lb)                                                                                                                                                                                        |

|                   |                                                                                                                                        |
|-------------------|----------------------------------------------------------------------------------------------------------------------------------------|
| Size              | 44 x 25 x 4.4 cm (17.4 x 9.8 x 1.7 in.) WxDxH                                                                                          |
| Temperature       | Operating: -40 to 65 °C (-40 to 149 °F)<br>Storage: -40 to 70 °C (-40 to 158 °F)                                                       |
| Humidity          | Operating: 5% to 95%                                                                                                                   |
| Power Supply      | -40.5 – -57 VDC                                                                                                                        |
| Power Consumption | 42 Watts maximum (internally for ECN330)<br>650 Watts maximum (internally for ECN330 and externally for Power-over-Ethernet devices)   |
| Heat Dissipation  | 40.9 BTU/hr (12 W)                                                                                                                     |
| Maximum Current   | 1.1 A @ -40.5 VDC (internally for ECN330)<br>16.0 A @ -40.5 VDC (internally for ECN330 and externally for Power-over-Ethernet devices) |

## 10.2 Compliances

|          |                                                                                                                                                                                                      |
|----------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Emission | GR-63-CORE, Issue 2<br>GR-1089-CORE, Issue 3<br>IMC ICES-003, Class B<br>FCC 47CFR15, Class B<br>EN55022 (CISPR 22) Class B<br>EN 61000-3-2/3<br>VCCI Class B<br>C-Tick - AS/NZS 3548 (1995) Class B |
| Immunity | EN 61000-4-2/3/4/5/6/8/11                                                                                                                                                                            |
| Safety   | CSA/CUS (CSA 22.2. NO 60950 & UL60950)<br>TÜV/GS (EN60950)<br>CB (IEC60950)                                                                                                                          |

## 10.3 Switch Features

|                 |                                                        |
|-----------------|--------------------------------------------------------|
| Forwarding Mode | Store-and-forward                                      |
| Throughput      | Wire speed                                             |
| Flow Control    | Full Duplex: IEEE 802.3x<br>Half Duplex: Back pressure |

## 10.4 Management Features

|                        |                                                                                                                                                                                                                                                                             |
|------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| In-Band Management     | Telnet, SSH, web-based HTTP or HTTPS, SNMP manager, or Secure Shell                                                                                                                                                                                                         |
| Out-of-Band Management | RS-232 DB-9 console port                                                                                                                                                                                                                                                    |
| Software Loading       | TFTP in-band or XModem out-of-band                                                                                                                                                                                                                                          |
| SNMP                   | Management access through MIB database<br>Trap management to specified hosts                                                                                                                                                                                                |
| RMON                   | Groups 1, 2, 3, 9 (Statistics, History, Alarm, Event)                                                                                                                                                                                                                       |
| MIB Support            | Bridge MIB (RFC 1493)<br>DNS Resolver MIB (RFC 1612)<br>DVMRP MIB<br>Differentiated Services MIB (RFC 3289)<br>ECN330-MIB<br>Entity MIB (RFC 2737)<br>EAPS MIB (RFC 3619)<br>Ether-like MIB (RFC 2665)<br>Extended Bridge MIB (RFC 2674)<br>Forwarding Table MIB (RFC 2096) |

|                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| MIB Support<br>(Continued) | IGMP MIB (RFC 2933)<br>Interface Group MIB (RFC 2863)<br>Interfaces Evolution MIB (RFC 2863)<br>IP MIB (RFC 2011)<br>IP Multicasting related MIBs<br>L2MPLS (Martini-draft)<br>MAU MIB (RFC 2668)<br>MIB II (RFC 1213)<br>Notification Log MIB (RFC 3014)<br>OSPF MIB (RFC 1850)<br>PEA_EQUIPMENT<br>PEM-STANDARD<br>PEM-STANDARD-TC<br>PIM MIB (RFC 2934)<br>Port Access Entity MIB (IEEE 802.1X)<br>Port Access Entity Equipment MIB<br>Power over Ethernet MIB (RFC 3621)<br>Private MIB<br>Quality of Service MIB<br>RADIUS Authentication Client MIB (RFC 2621)<br>RIP1 MIB (RFC 1058)<br>RIP2 MIB (RFC 2453)<br>RIP2 Extension (RFC1724)<br>RMON MIB (RFC 2819)<br>RMON II Probe Configuration Group (RFC 2021,<br>partial implementation)<br>QnQ Tunneling (IEEE 802.1ad Provider Bridges)<br>SNMP Framework MIB (RFC 3411)<br>SNMP-MPD MIB (RFC 3412) |
|----------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

|                            |                                                                                                                                                                                                                                                                                          |
|----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| MIB Support<br>(Continued) | SNMP Target MIB, SNMP Notification MIB (RFC 3413)<br>SNMP User-Based SM MIB (RFC 3414)<br>SNMP View Based ACM MIB (RFC 3415)<br>SNMP Community MIB (RFC 3584)<br>TACACS+ Authentication Client MIB<br>TCP MIB (RFC 2012)<br>Trap (RFC 1215)<br>UDP MIB (RFC 2013)<br>VRRP MIB (RFC 2787) |
|----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

## 10.5

## Standards

|                 |                                                                                       |
|-----------------|---------------------------------------------------------------------------------------|
| IEEE 802.3-2002 | Ethernet, Fast Ethernet, Gigabit Ethernet, Link Aggregation, Full-duplex flow control |
| IEEE 802.1p     | Priority tags                                                                         |
| IEEE 802.3ac    | VLAN tagging                                                                          |
| IEEE 802.1D     | Bridging                                                                              |
| IEEE 802.1w     | Rapid Spanning Tree Protocol                                                          |
| IEEE 802.1s     | Multiple Spanning Tree Protocol                                                       |
| IEEE 802.1Q     | VLAN Bridge Management                                                                |
| IEEE 802.1v     | Protocol-based VLANs                                                                  |
| IEEE 802.1X     | Port access control                                                                   |
| ISO/IEC 8802-3  | Carrier sense multiple access with collision detection (CSMA/CD)                      |
| RFC 826         | ARP                                                                                   |
| RFC 2131        | DHCP Client                                                                           |

|                                                                              |                  |
|------------------------------------------------------------------------------|------------------|
| RFC 3046, 951                                                                | DHCP Relay       |
| RFC 2131                                                                     | DHCP Server      |
| RFC 1075, draft-ietf-idmr-dvmrp-v3-11                                        | DVMRP            |
|                                                                              | HTTPS            |
| RFC 792                                                                      | ICMP             |
| RFC 1112                                                                     | IGMP             |
| RFC 2236                                                                     | IGMPv2           |
| RFC 3228                                                                     | IPv4 IGMP        |
| draft-martini-l2circuit-trans-mpls-16, draft-martini-l2circuit-encap-mpls-09 | L2MPLS           |
| RFC 2328, 2178, 1587                                                         | OSPF             |
| RFC 3973                                                                     | PIM-DM           |
| RFC 2362, draft-ietf-pim-sm-v2-new-11                                        | PIM-SM           |
| RFC 2618                                                                     | RADIUS+          |
| RFC 1058                                                                     | RIP              |
| RFC 2453                                                                     | RIPv2            |
| RFC 1724                                                                     | RIPv2, extension |
| RFC 2819<br>(groups 1,2,3,9)                                                 | RMON             |

|                                     |                   |
|-------------------------------------|-------------------|
| RFC 1157                            | SNMP              |
| RFC 1901                            | SNMPv2c           |
| RFC 3414, 3410,<br>2273, 3411, 3415 | SNMPv3            |
| RFC 2030                            | SNTP              |
|                                     | SSH (Version 2.0) |
| RFC 854, 855, 856                   | TELNET            |
| RFC 1350                            | TFTP              |
| RFC 3768                            | VRRP              |





# List of Abbreviations

**3DES**

Triple DES

**ABR**

Area Border Router

**ACL**

Access Control List,  
Access Control List configuration mode

**ARP**

Address Resolution Protocol

**AS**

Autonomous System

**BDR**

Backup Designated Router

**BOOTP**

Boot Protocol

**BPDU**

Bridge Protocol Data Unit

**BSR**

Bootstrap Router

**CIS**

Common and Internal Spanning Tree

**CLI**

Command Line Interface

**CM**

Class Map configuration mode

**CoS**

Class of Service

**CRC**

Cyclic Redundancy Check

**CST**

Common Spanning Tree

**CVLAN**

Control VLAN

**DA**

Destination Address

**DC**

DHCP Server Configuration mode

**DES**

Data Encryption Standard

**DHCP**

Dynamic Host Configuration Protocol

**DiffServ**

Differentiated Services

**DNS**

Domain Name Server

**DR**

Designated Router

**DSA**

Digital Signature Algorithm

**DSCP**

Differentiated Services Code Point

**DSLAM**

Digital Subscriber Line Access Multiplexer

**DVMRP**

Distance Vector Multicast Routing Protocol

**EAN**

Ethernet Access Node

**EAP**

Extensible Authentication Protocol

**EAPOL**

Extensible Authentication Protocol over LANs

**EAPS**

Ethernet Automatic Protection Switching,  
EAPS configuration mode

**EDA**

Ethernet DSL Access

**ENC**

Ethernet Node Controller

**FDB**

Forwarding Database

**FSA**

Flexible Service Access

**FTP**

File Transfer Protocol

**GARP**

Group Address Resolution Protocol

**GC**

Global Configuration mode

**GMRP**

GARP Multicast Registration Protocol

**GMT**

Greenwich Mean Time

**GVRP**

GARP VLAN Registration Protocol

**HTTP**

Hypertext Text Transfer Protocol

**HTTPS**

HTTP over Secure Socket Layer

**IMAP**

Internet Message Access Protocol

**IC**

Interface Configuration mode

**IPX**

Internetwork Packet Exchange

**IST**

Internal Spanning Tree

**Kbps**

Kilobits per second

**LACP**

Link Aggregation Control Protocol

**LACPDU**

LACP Data Unit

**LAG**

Link Aggregation Group

**LAN**

Local Area Network

**LC**

Line Configuration mode

**LED**

Light Emitting Diode

**LLC**

Logical Link Control.

**LS**

Link State

**IEEE**

Institute of Electrical and Electronic Engineers

**IGMP**

Internet Group Management Protocol

**IP**

Internet Protocol

**L2MPLS**

Layer 2 over MPLS

**LDP**

Label Distribution Protocol

**LSA**

Link State Advertisement

**LSR**

Label Switching Router

**MAC**

Media Access Control

**MAN**

Metropolitan Area Network

**MD5**

Message-Digest Algorithm 5

**MDI**

Media Dependent Interface

**MDI-X**

Media Dependent Interface - Crossover

**MIB**

Management Information Base

**MPLS**

Multiprotocol Label Switching

**MST**

Multiple Spanning Tree,  
Multiple Spanning Tree configuration mode

**MSTI**

Multiple Spanning Tree Instance

**MSTP**

Multiple Spanning Tree Protocol

**MTU**

Maximum Transfer Unit

**NE**

Normal Exec configuration mode

**NSSA**

Not-so-stubby Area

**NTP**

Network Time Protocol

**OID**

Object Identifier

**OSPF**

Open Shortest Path First

**PDU**

Protocol Data Unit

**PE**

Provider Equipment,  
Privileged Exec configuration mode

**PEA****PEM**

Public Ethernet Manager

**PIM**

Protocol Independent Multicasting

**PoE**

Power over Ethernet

**POP**

Post Office Protocol

**POST**

Power-on Self-test

**PVID**

Port VLAN ID

**PVLAN**

Protected VLAN

**QinQ**

Queue in Queue (Tunneling)

**QoS**

Quality of Service

**RADIUS**

Remote Authentication Dial-in User Service

**RAM**

Random Access Memory

**RARP**

Reverse Address Resolution Protocol

**RC**

Router Configuration mode

**RIP**

Routing Information Protocol

**RMON**

Remote Monitoring

**RP**

Rendezvous Point

**RPF**

Reverse Path Forwarding

**RPT**

Reverse Path Tree

**RSA**

Ron Rivest, Adi Shamir and Len Adleman  
(Encryption Algorithm)

**RSTP**

Rapid Spanning Tree Protocol

**SA**

Source Address

**SBC**

Single-board Computer

**SHA**

Secure Hash Algorithm

**SNMP**

Simple Network Management Protocol

**SMTP**

Simple Mail Transfer Protocol

**SNTP**

Simple Network Time Protocol

**SFP**

Small Form-Factor Pluggable

**SPF**

Shortest Path First

**SPT**

Shortest Path Tree

**SPVLAN**

Service Provider VLAN

**SSH**

Secure Shell

**SSL**

Secure Socket Layer

**STA**

Spanning Tree Algorithm

**STP**

Spanning Tree Protocol

**TACACS**

Terminal Access Controller Access Control  
System

**TCP**

Transmission Control Protocol

**TFTP**

Trivial File Transfer Protocol

**ToS**

Type of Service

**TPID**

Tag Protocol Identifier

**TTL**

Time To Live

**UDP**

User Datagram Protocol

**UTC**

Coordinated Universal Time

**UTP**

Unshielded Twisted Pair

**VC**

Virtual Channel,  
VLAN Database Configuration mode

**VLAN**

Virtual Local Area Network

**VLSM**

Variable-length Subnet Mask

**VPN**

Virtual Private Network

**VRRP**

Virtual Router Redundancy Protocol

**WFQ**

Weighted Fair Queueing

**WRR**

Weighted Round Robin





# Glossary

## **10BASE-T**

IEEE 802.3 specification for 10 Mbps Ethernet over two pairs of Category 3, 4, or 5 UTP cable.

## **100BASE-FX**

IEEE 802.3u specification for 100 Mbps Fast Ethernet over two strands of 50/125 or 62.5/125 micron core fiber cable.

## **100BASE-TX**

IEEE 802.3u specification for 100 Mbps Fast Ethernet over two pairs of Category 5 UTP cable.

## **1000BASE-LH**

Gigabit Ethernet over two strands of 9/125 micron core fiber cable.

## **1000BASE-LX**

IEEE 802.3z specification for Gigabit Ethernet over two strands of 9/125 micron core fiber cable.

## **1000BASE-SX**

IEEE 802.3z specification for Gigabit Ethernet over two strands of 50/125 or 62.5/125 micron core fiber cable.

## **1000BASE-T**

IEEE 802.3ab specification for Gigabit Ethernet over four pairs of Category 5, 5e, or 6 100-ohm UTP cable.

## **1000BASE-X**

IEEE 802.3 shorthand term for any 1000 Mbps Gigabit Ethernet based on 8B/10B signaling.

## **Access Control List (ACL)**

ACLs can limit network traffic and restrict access to certain users or devices by checking each packet for certain IP or MAC (Layer 2) information.

## **Address Resolution Protocol (ARP)**

ARP converts between IP addresses and MAC (hardware) addresses. ARP is used to locate the MAC address corresponding to a given IP address. This allows the switch to use IP addresses for routing decisions and the corresponding MAC addresses to forward packets from one hop to the next.

## **Auto-negotiation**

Signalling method allowing each node to select its optimum operational mode (for example, 10, 100, or 100 Mbps and half or full duplex) based on the capabilities of the node to which it is connected.

## **Bandwidth**

The difference between the highest and lowest frequencies available for network signals. Also synonymous with wire speed, the actual speed of the data transmission along the cable.

## **BOOTP**

Boot protocol used to load the operating system for devices connected to the network.

## **Class of Service (CoS)**

CoS is supported by prioritizing packets based on the required level of service, and then placing them in the appropriate output queue. Data is transmitted from the queues using weighted round-robin service to enforce priority service and prevent blockage of lower-level queues. Priority may be set according to the port default, the packet's priority bit (in the VLAN tag), TCP/UDP port number, IP Precedence bit, or DSCP priority bit.

## **Collision**

A condition in which packets transmitted over the cable interfere with each other. Their interference makes both signals unintelligible.

## **Collision Domain**

Single CSMA/CD LAN segment.

## **CSMA/CD**

Carrier Sense Multiple Access/Collision Detect is the communication method employed by Ethernet and Fast Ethernet.

## **Differentiated Services (DiffServ)**

DiffServ provides quality of service on large networks by employing a well-defined set of building blocks from which a variety of aggregate forwarding behaviors may be built. Each packet carries information (DS byte) used by each hop to give it a particular forwarding treatment, or per-hop behavior, at each network node. DiffServ allocates different levels of service to users on the network with mechanisms such as traffic meters, shapers/droppers, packet markers at the boundaries of the network.

## **Differentiated Services Code Point Service (DSCP)**

DSCP uses a six-bit tag to provide for up to 64 different forwarding behaviors. Based on network policies, different kinds of traffic can be marked for different kinds of forwarding. The DSCP bits are mapped to the Class of Service categories, and then into the output queues.

## **Domain Name Service (DNS)**

A system used for translating host names for network nodes into IP addresses.

## **Distance Vector Multicast Routing Protocol (DVMRP)**

A distance-vector-style routing protocol used for routing multicast datagrams through the Internet. DVMRP combines many of the features of RIP with Reverse Path Forwarding (RPF).

**Dynamic Host Control Protocol (DHCP)**

Provides a framework for passing configuration information to hosts on a TCP/IP network. DHCP is based on the Bootstrap Protocol (BOOTP), adding the capability of automatic allocation of reusable network addresses and additional configuration options.

**End Station**

A workstation, server, or other device that does not act as a network interconnection.

**Ethernet**

A network communication system developed and standardized by DEC, Intel, and Xerox, using baseband transmission, CSMA/CD access, logical bus topology, and coaxial cable. The successor IEEE 802.3 standard provides for integration into the OSI model and extends the physical layer and media with repeaters and implementations that operate on fiber, thin coax and twisted-pair cable.

**Ethernet Automatic Protection Switching (EAPS)**

EAPS is used to increase the availability and robustness of Ethernet rings used in many Metropolitan Area Networks (MANs) for fibre runs.

**Extensible Authentication Protocol over LAN (EAPOL)**

EAPOL is a client authentication protocol used by this switch to verify the network access rights for any device that is plugged into the

switch. A user name and password is requested by the switch, and then passed to an authentication server (for example, RADIUS) for verification. EAPOL is implemented as part of the IEEE 802.1X Port Authentication standard.

**Fast Ethernet**

A 100 Mbps network communication system based on Ethernet and the CSMA/CD access method.

**Fast Ethernet Switch**

Device that provides a full 100 Mbps bandwidth (or either 10 or 100 Mbps bandwidth with Auto-Negotiation) to each port (LAN segment).

**Full Duplex**

Transmission method that enables switch and network card to transmit and receive concurrently, effectively doubling the bandwidth of that link.

**GARP VLAN Registration Protocol (GVRP)**

Defines a way for switches to exchange VLAN information in order to register necessary VLAN members on ports along the Spanning Tree so that VLANs defined in each switch can work automatically over a Spanning Tree network.

### **Generic Attribute Registration Protocol (GARP)**

GARP is a protocol that can be used by endstations and switches to register and propagate multicast group membership information in a switched environment so that multicast data frames are propagated only to those parts of a switched LAN containing registered endstations. Formerly called Group Address Registration Protocol.

### **Generic Multicast Registration Protocol (GMRP)**

GMRP allows network devices to register endstations with multicast groups. GMRP requires that any participating network devices or endstations comply with the IEEE 802.1p standard.

### **Gigabit Ethernet**

A 1000 Mbps network communication system based on Ethernet and the CSMA/CD access method.

### **Group Attribute Registration Protocol**

*See Generic Attribute Registration Protocol.*

### **IEEE**

Institute of Electrical and Electronic Engineers.

### **IEEE 802.1D**

Specifies a general method for the operation of MAC bridges, including the Spanning Tree Protocol.

### **IEEE 802.1Q**

VLAN Tagging—Defines Ethernet frame tags which carry VLAN information. It allows switches to assign endstations to different virtual LANs, and defines a standard way for VLANs to communicate across switched networks.

### **IEEE 802.1p**

An IEEE standard for providing quality of service (QoS) in Ethernet networks. The standard uses packet tags that define up to eight traffic classes and allows switches to transmit packets based on the tagged priority value.

### **IEEE 802.1s**

An IEEE standard for the Multiple Spanning Tree Protocol (MSTP) which provides independent spanning trees for VLAN groups.

### **IEEE 802.1X**

Port Authentication controls access to the switch ports by requiring users to first enter a user ID and password for authentication.

### **IEEE 802.3**

Defines carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications.

### **IEEE 802.3ab**

Defines CSMA/CD access method and physical layer specifications for 1000BASE-T

Gigabit Ethernet. (Now incorporated in IEEE 802.3-2002.)

### **IEEE 802.3ac**

Defines frame extensions for VLAN tagging.

### **IEEE 802.3u**

Defines CSMA/CD access method and physical layer specifications for 100BASE-TX and 100BASE-FX Fast Ethernet. (Now incorporated in IEEE 802.3-2002.)

### **IEEE 802.3x**

Defines Ethernet frame start and stop requests and timers used for flow control on full-duplex links. (Now incorporated in IEEE 802.3-2002.)

### **IEEE 802.3z**

Defines CSMA/CD access method and physical layer specifications for 1000BASE Gigabit Ethernet. (Now incorporated in IEEE 802.3-2002.)

### **IGMP Snooping**

Listening to IGMP Query and IGMP Report packets transferred between IP Multicast Routers and IP Multicast host groups to identify IP Multicast group members.

### **IGMP Query**

On each subnetwork, one IGMP-capable device will act as the querier — that is, the device that asks all hosts to report on the IP multicast groups they wish to join or to which

they already belong. The elected querier will be the device with the lowest IP address in the subnetwork.

### **Internet Control Message Protocol (ICMP)**

A network layer protocol that reports errors in processing IP packets. ICMP is also used by routers to feed back information about better routing choices.

### **Internet Group Management Protocol (IGMP)**

A protocol through which hosts can register with their local router for multicast services. If there is more than one multicast router on a given subnetwork, one of the routers is made the “querier” and assumes responsibility for keeping track of group membership.

### **In-Band Management**

Management of the network from a station attached directly to the network.

### **IP Multicast Filtering**

A process whereby a switch can pass multicast traffic along to participating hosts.

### **IP Precedence**

The Type of Service (ToS) octet in the IPv4 header includes three precedence bits defining eight different priority levels ranging from highest priority for network control packets to lowest priority for routine traffic. The eight values are mapped one-to-one to the Class of Service categories by default, but

may be configured differently to suit the requirements for specific network applications.

### **LAN Segment**

Separate LAN or collision domain.

### **Layer 2**

Data Link layer in the ISO 7-Layer Data Communications Protocol. This is related directly to the hardware interface for network devices and passes on traffic based on MAC addresses.

### **Layer 2 over MPLS (L2MPLS)**

L2MPLS encapsulates Ethernet frames in MPLS packets and uses label stacking to tunnel them across a service provider's network.

### **Layer 3**

Network layer in the ISO 7-Layer Data Communications Protocol. This layer handles the routing functions for data moving from one open system to another.

### **LED**

Light emitting diode used for monitoring a device or network condition.

### **Link Aggregation**

*See Port Trunk.*

### **Link Aggregation Control Protocol (LACP)**

Allows ports to automatically negotiate a trunked link with LACP-configured ports on another device.

### **Link Segment**

Length of twisted-pair or fiber cable joining a pair of repeaters or a repeater and a PC.

### **Local Area Network (LAN)**

A group of interconnected computer and support devices.

### **Media Access Control (MAC)**

A portion of the networking protocol that governs access to the transmission medium, facilitating the exchange of data between network nodes.

### **Management Information Base (MIB)**

An acronym for Management Information Base. It is a set of database objects that contains information about a specific device.

### **MD5 Message-Digest Algorithm**

An algorithm that is used to create digital signatures. It is intended for use with 32 bit machines and is safer than the MD4 algorithm, which has been broken. MD5 is a one-way hash function, meaning that it takes a message and converts it into a fixed string of digits, also called a message digest.

## Modal Bandwidth

Bandwidth for multimode fiber is referred to as modal bandwidth because it varies with the modal field (or core diameter) of the fiber. Modal bandwidth is specified in units of MHz per km, which indicates the amount of bandwidth supported by the fiber for a one km distance.

## Multicast Switching

A process whereby the switch filters incoming multicast frames for services for which no attached host has registered, or forwards them to all ports contained within the designated multicast VLAN group.

## Network Diameter

Wire distance between two end stations in the same collision domain.

## Network Time Protocol (NTP)

NTP provides the mechanisms to synchronize time across the network. The time servers operate in a hierarchical-master-slave configuration in order to synchronize local clocks within the subnet and to national time standards through wire or radio.

## Open Shortest Path First (OSPF)

OSPF is a link-state routing protocol that functions better over a larger network such as the Internet, as opposed to distance-vector routing protocols such as RIP. It includes features such as unlimited hop count, authentication of routing updates, and Variable Length Subnet Masks (VLSM).

## Out-of-Band Management

Management of the network from a station not attached to the network.

## Port Authentication

*See IEEE 802.1X.*

## Port Mirroring

A method whereby data on a target port is mirrored to a monitor port for troubleshooting with a logic analyzer or RMON probe. This allows data on the target port to be studied unobstructively.

## Port Trunk

Defines a network link aggregation and trunking method which specifies how to create a single high-speed logical link that combines several lower-speed physical links.

## Private VLANs

Private VLANs provide port-based security and isolation between ports within the assigned VLAN. Data traffic on downlink ports can only be forwarded to, and from, uplink ports.

## Protocol-Independent Multicasting (PIM)

This multicast routing protocol floods multicast traffic downstream, and calculates the shortest-path back to the multicast source network through reverse path forwarding. PIM uses the router's IP routing table rather than maintaining a separate multicast routing table.

as with DVMRP. PIM - Sparse Mode is designed for networks where the probability of a multicast client is low, such as on a Wide Area Network. PIM - Dense Mode is designed for networks where the probability of a multicast client is high and frequent flooding of multicast traffic can be justified.

### **QinQ Tunneling**

QinQ is designed for service providers carrying traffic for multiple customers across their networks. It is used to maintain customer-specific VLAN and Layer 2 protocol configurations even when different customers use the same internal VLAN IDs..

### **Quality of Service (QoS)**

QoS refers to the capability of a network to provide better service to selected traffic flows using features such as data prioritization, queuing, congestion avoidance and traffic shaping. These features effectively provide preferential treatment to specific flows either by raising the priority of one flow or limiting the priority of another flow.

### **Redundant Power Supply (RPS)**

A backup power supply that automatically takes over in case the primary power supply should fail.

### **Remote Authentication Dial-in User Service (RADIUS)**

RADIUS is a logon authentication protocol that uses software running on a central server to control access to RADIUS-compliant devices on the network.

### **Remote Monitoring (RMON)**

RMON provides comprehensive network monitoring capabilities. It eliminates the polling required in standard SNMP, and can set alarms on a variety of traffic conditions, including specific error types.

### **Rapid Spanning Tree Protocol (RSTP)**

RSTP reduces the convergence time for network topology changes to about 10% of that required by the older IEEE 802.1D STP standard.

### **RJ45 Connector**

A connector for twisted-pair wiring.

### **Routing Information Protocol (RIP)**

The RIP protocol seeks to find the shortest route to another device by minimizing the distance-vector, or hop count, which serves as a rough estimate of transmission cost. RIP-2 is a compatible upgrade to RIP. It adds useful capabilities for subnet routing, authentication, and multicast transmissions.

### **Secure Shell (SSH)**

A secure replacement for remote access functions, including Telnet. SSH can authenticate users with a cryptographic key, and encrypt data connections between management clients and the switch.

### **Simple Mail Transfer Protocol (SMTP)**

A standard host-to-host mail transport protocol that operates over TCP, port 25.



## **Simple Network Management Protocol (SNMP)**

The application protocol in the Internet suite of protocols which offers network management services.

## **Simple Network Time Protocol (SNTP)**

SNTP allows a device to set its internal clock based on periodic updates from a Network Time Protocol (NTP) server. Updates can be requested from a specific NTP server, or can be received through broadcasts sent by NTP servers.

## **Spanning Tree Algorithm (STA)**

A technology that checks the network for any loops. A loop can often occur in complicated or backup linked network systems. Spanning Tree detects and directs data along the shortest available path, maximizing the performance and efficiency of the network.

## **Switched Ports**

Ports that are on separate collision domains or LAN segments.

## **Telnet**

Defines a remote communication facility for interfacing to a terminal device over TCP/IP.

## **Terminal Access Controller Access Control System Plus (TACACS+)**

TACACS+ is a logon authentication protocol that uses software running on a central server to

control access to TACACS-compliant devices on the network.

## **TIA**

Telecommunications Industry Association

## **Transmission Control Protocol/Internet Protocol (TCP/IP)**

Protocol suite that includes TCP as the primary transport protocol, and IP as the network layer protocol.

## **Trivial File Transfer Protocol (TFTP)**

A TCP/IP protocol commonly used for software downloads.

## **Universal Time Coordinate (UTC)**

UTC is a time scale that couples Greenwich Mean Time (based solely on the Earth's rotation rate) with highly accurate atomic time. The UTC does not have daylight saving time.

## **User Datagram Protocol (UDP)**

UDP provides a datagram mode for packet-switched communications. It uses IP as the underlying transport mechanism to provide access to IP-like services. UDP packets are delivered just like IP packets – connection-less datagrams that may be discarded before reaching their targets. UDP is useful when TCP would be too complex, too slow, or just unnecessary.

## **UTP**

Unshielded twisted-pair cable.

## **Virtual LAN (VLAN)**

A Virtual LAN is a collection of network nodes that share the same collision domain regardless of their physical location or connection point in the network. A VLAN serves as a logical workgroup with no physical barriers, and allows users to share information and resources as though located on the same LAN.

## **Virtual Router Redundancy Protocol (VRRP)**

A protocol that uses a virtual IP address to support a primary router and multiple backup routers. The backups can be configured to take over the workload if the master fails or to load share the traffic. The primary goal of VRRP is to allow a host device which has been configured with a fixed gateway to maintain network connectivity in case the primary gateway goes down.

## **XModem**

A protocol used to transfer files between devices. Data is grouped in 128-byte blocks and error-corrected.

# Index

## Numerics

- 1000BASE-T ports 8
- 100BASE-TX ports 7
- 802.1Q tunnel 296, 882
  - address monitor mode 292, 301, 887
  - description 296
  - interface configuration 300, 884–889
  - TPID 292, 301, 885
- 802.1X
  - port authentication 145, 674
  - setting defaults 676

## A

- acceptable frame type 291, 858
- Access Control List *See* ACL
- access levels, CLI 39, 522, 633
- access-list ip 692
- access-list ip mask-precedence 698
- access-list mac 708
- access-list mac mask-precedence 712
- access-list mask-precedence vlan 726
- ACL
  - binding to a port 172, 705, 717
  - displaying basic information 733
  - Extended IP 157, 159, 161, 690, 692, 694
  - MAC 157, 159, 164, 690, 707–711
  - Standard IP 157, 159, 160, 690, 692, 693
  - VLAN 157, 174–182, 690, 719–732
- ACL configuration mode, defined 523
- action, VLAN ACL 723
- address learning, configuring for port 143, 672
- address monitor mode 292, 301, 887

- Address Resolution Protocol *See* ARP
- address table 227, 786
  - aging time 230, 791, 793
  - size 1175
- address-monitor qinq 292, 301, 887
- admin user name 51, 515
- agent, management 6
- aging time, address table 230, 791, 793
- area default-cost, OSPF 444, 1062
- area nssa, OSPF 443, 1068
- area range, OSPF 446, 1061
- area stub, OSPF 442, 1067
- area virtual-link, OSPF 453, 1070
- arguments, CLI 518
- ARP
  - configuration 406, 1023
  - description 405
  - proxy 406, 1027
  - statistics 412, 1034
- arp 1023
- authentication commands 126, 632
- authentication enable 638
- authentication login 637
- authentication traps 110, 618
- authentication, defaults 31
- automatic MDI/MDI-X 8
- auto-negotiation
  - capabilities 185, 188, 741
  - CLI command 740

## B

- baud rate, console default 30
- boot system 568

- bootfile, DHCP client configuration 382, 988
- BOOTP 84, 1016
  - basic setting 43
  - client 81, 1016
  - enabling 81, 1016
- bootstrap router 490, 502, 1138
- BPDU 232, 809
- bridge-ext gvrp 843
- broadcast storm control, configuring 207, 747
- broadcast storm, threshold 207, 747
- buffer size 1175
- buffers, saturation of 8

## C

- calendar set 606
- capabilities 741
- capabilities, auto-negotiation 185, 741
- channel-group 758
- Class Map configuration mode, defined 523
- Class of Service *See* CoS
- class, DiffServ 343, 927
- class-map 923
- clear counters 219, 748
- clear dns cache 973
- clear host 373, 965
- clear ip dhcp binding 386, 995
- clear ip dvmrp route 1117
- clear ip igmp group 960
- clear ip pim bsr rp-set 1160
- clear ip route 423, 1031
- clear log 590
- clear mac-address-table dynamic 788
- clear vrrp interface counters 1014
- clear vrrp router counters 1014
- CLI interface
  - abbreviations 518
  - arguments, defined 518
  - customizing the prompt 536
  - displaying history 521
  - edit keys 526
  - help 519
  - keywords, defined 518
  - login 515
  - modes 521, 525
  - no form, using 521
- client-identifier, DHCP 382, 993
- clock timezone 104, 605
- code files, defined 35
- combo ports
  - explained 8
  - location 5
- commands
  - access levels, CLI 39, 522
  - classes and modes 521
  - entering 518
  - help 519
- community strings 109, 612
  - basic setting 47
  - configuring 109, 612
  - default 31
- compliances, regulatory 1176
- configuration files
  - copy command 89, 561
  - defined 35
  - restoring defaults 560
  - saving 40
  - setting as start-up 91, 568
- configuration modes, defined 522
- configuration settings, saving or restoring 89, 560
- configure, global configuration mode 534
- connections
  - first time 39
  - for remote management 39
  - using console cable 38

- console port
  - basic settings 38
  - connecting 38
  - defaults 30
  - pin assignments 9
- control-vlan 259, 267, 831
- conventions, text 2
- cooling fans
  - access cover 5
- cooling problems 1172
- copy 87, 561

- CoS
  - configuring 324, 897
  - defaults 33
  - DSCP 334, 338, 914
    - DSCP
      - mapping priorities 915
    - IP port priority 340, 910, 911
    - IP precedence 335, 913
    - layer 3/4 priorities 334, 909
    - queue mapping 326, 904
    - queue mode 329, 898
    - traffic class weights 330, 902
- CTRL LED 12

## D

- databits 92, 578
- DB-9 connector, console 38
- default gateway, configuration 82, 401, 1018
- default priority, ingress port 324, 900
- default settings 30
- default-gateway, DVMRP 477, 1114
- default-information originate 440, 1058
- default-router, DHCP 382, 985
- delete public-key 138, 662, 664
- delete, files 88, 565

- deny
  - Extended ACL 161, 694
  - MAC ACL 164, 709
  - Standard ACL 160, 693
- description, interface 187, 738
- DHCP 81, 84, 1016
  - address pool 380, 983
  - basic setting 43
  - client 81, 963, 974, 1016
  - enabling 81, 1016
  - global enable 379, 981
  - network pool configuration 381, 984
  - next server client configuration 382, 987
  - relay service 376, 977
  - server 378, 980
- DHCP configuration mode, defined 523
- DIAG LED 12
- diagnostic code, defined 35
- Differentiated Services *See* DiffServ
- DiffServ 342, 921
  - binding policy to interface 350, 931
  - class map 343, 923, 927
  - configuring 342, 921
  - policy map 346, 926
  - service policy 350, 931
- dir 566
- disable, privileged exec configuration mode 533
- disconnect, management connection 582
- DNS
  - default domain name 370, 966
  - displaying the cache 374, 972
  - domain name list 370, 964
  - enabling lookup 370, 969
  - name server list 370, 371, 968
  - static entries 372, 964
- dns-server, DHCP client configuration 382, 986
- Domain Name Service *See* DNS

- domain-name, DHCP 382, 986
- dot1x default 676
- dot1x max-req 149, 676
- dot1x operation-mode 148, 678
- dot1x port-control 149, 677
- dot1x re-authenticate 679
- dot1x re-authentication 149, 680
- dot1x system-auth-control 147, 675
- dot1x timeout quiet-period 149, 681
- dot1x timeout re-authperiod 149, 682
- dot1x timeout tx-period 149, 682
- downloading software 87, 561, 1167
- DSCP
  - enabling 334, 914
  - enabling Differentiated Code Point Service
    - See DSCP
  - mapping priorities 338
- DTE serial pinouts 9
- DVMRP
  - configuring 473, 1107
  - enable for interface 479
  - global settings 474, 1107–1114
  - interface settings 479, 1115–1116
  - neighbor routers 481, 1120
  - routing table 482, 1118
- dynamic addresses, displaying 228, 789
- Dynamic Host Configuration Protocol See DHCP

## E

- EAPOL 24
- EAPS 258–271
  - configuration guidelines 260, 824
  - Control VLAN 267, 831
  - description 258
  - domain configuration 265, 826
  - global configuration 264, 835
  - master mode 266, 268, 827

- primary port 267
- Protected VLAN 269, 833
- secondary port 267, 830
- transit mode 266, 268, 827
- EAPS Configuration mode, defined 524
- eaps domain 265, 267, 826
- eaps, global configuration 264, 835
- EDA devices
  - and power management 778
- edge port, STA 246, 249, 813
- edit keys, CLI 526
- enable password 635
- enable, EAPS domain 269, 834
- enable, privileged exec configuration mode 532
- end, return to privileged exec mode 537
- error levels, logging 97, 585
- error message logging 97, 584
- Ethernet Automatic Protection Switching See EAPS
- Exec classes 522
- exec-timeout 575
- exit, returns to previous configuration mode 537

## F

- failtime, EAPS 266, 829
- FAN LED 12
- fan tray access 18
- fast forwarding
  - STA 246, 813, 814
- features
  - management 15, 1177
  - switch 14
- file keyword, using 561
- files
  - boot listing 87, 91, 567
  - copy command 86, 561

- delete command 88, 565
- flash memory listing 566
- managing 86, 560
- name restrictions 36
- setting as start-up 87, 568
- system, defined 35
- filtering management access, IP filter 154, 687
- firmware
  - console port upgrade 560, 1167
  - displaying version 75, 550
  - key features 21
  - setting as start-up 87, 91, 568
  - TFTP save and restore 86, 561
  - upgrading 87, 560
- flash memory, system 35
- flowcontrol 184, 186, 188, 743
- full-duplex
  - auto-negotiation of 185, 187, 740
  - setting 187, 739
  - using 6
- fuse
  - location on switch 9
  - replacing 17

## G

- garp timer 292, 846
- GARP VLAN Registration Protocol *See* GVRP
- gateway, default 82, 402, 1018
- Global Configuration mode, defined 523
- Global Configuration, defined 522
- GVRP 276, 842
  - global setting 276, 843
  - interface configuration 291, 844

## H

- hardware features 7
- hardware version, displaying 75, 550
- hardware-address, DHCP client 382, 994
- hellotime, EAPS 266, 828
- help for CLI 519
- history, CLI 521
- host, DHCP client 382, 992
- hostname 69, 541
- HTTPS 132, 651
- HTTPS, secure server 132, 651
- https-certificate keyword, using 562

## I

- ICMP echo 1021
- IEEE 802.1D 231, 797
- IEEE 802.1s 231, 797
- IEEE 802.1w 231, 797
- IEEE 802.1X 145, 674
- IGMP
  - description of protocol 353
  - explained 935
  - groups, displaying 360, 961
  - Layer 2 354, 935
  - Layer 3 364, 952
  - maximum response time 356, 946, 956
  - multicast router port, configuring 359
  - querier 355, 943
  - query 354, 953
  - query count 356, 944
  - query interval 356, 945, 955
  - query timeout 356, 948, 957
  - query, Layer 2 355, 935
  - query, Layer 3 364, 952
  - report delay 356, 946, 956
  - robustness variable 366, 954

- services, displaying 368, 961
- snooping 354, 935
- snooping, configuring 355, 362, 936
- static port assignment 361
- version, setting 356, 939
- IGMP snooping
  - enabling 355
  - enabling globally 936
  - enabling per interface 362, 937
- indicators, LED 11
- ingress filtering 291, 859
- installation, problems 1172
- interface commands 736
- Interface Configuration mode, defined 524
- interface vlan 856
- interface, CLI configuration mode 737
- ip access-group 705
- IP address
  - BOOTP/DHCP 84, 976, 1016
  - defaults 33
  - dynamic setting 43
  - manual setting 42
  - setting 80, 1016
  - using BOOTP/DHCP 81, 1016
- ip address 80, 1016
- IP commands 1015
- ip default-gateway 82, 1018
- ip dhcp client-identifier 382, 975
- ip dhcp excluded-address 379, 982
- ip dhcp pool 380, 983
- ip dhcp relay server 376, 979
- ip dhcp restart client 976
- ip dhcp restart relay 377, 977
- ip domain-list 371, 967
- ip domain-lookup 371, 969
- ip domain-name 371, 966
- ip dvmrp 1115
- ip dvmrp metric 479, 1116
- ip host 964
- ip http port 650
- ip http secure-port 133, 653
- ip http secure-server 133, 651
- ip http server 650
- ip igmp 952
- ip igmp last-memb-query-interval 957
- ip igmp max-resp-interval 956
- ip igmp query-interval 955
- ip igmp robustval 954
- ip igmp snooping 936, 937
- ip igmp snooping querier 943
- ip igmp snooping query-count 944
- ip igmp snooping query-interval 945
- ip igmp snooping query-max-response-time 946
- ip igmp snooping router-port-expire-time 948
- ip igmp snooping version 939
- ip igmp snooping vlan mrouter 950
- ip igmp snooping vlan static 938
- ip igmp version 958
- ip multicast-routing 1104
- ip name-server 968
- ip ospf authentication 1073
- ip ospf authentication-key 1075
- ip ospf cost 1077
- ip ospf dead-interval 1078
- ip ospf hello-interval 1079
- ip ospf message-digest-key 1076
- ip ospf priority 1080
- ip ospf retransmit-interval 1081
- ip ospf transmit-delay 1082
- ip pim bsr-candidate 1138
- ip pim crp-prefix 1151
- ip pim dense-mode 1124
- ip pim dr-priority 1155
- ip pim graft-retry-interval 1129
- ip pim hello-holdtime 1126, 1158
- ip pim hello-interval 1125, 1157
- ip pim ignore-rp-set-priority 1150



- ip pim join-prune-holdtime 1128
- ip pim jp-interval 1137
- ip pim max-graft-retries 1130
- ip pim register-checksum-withdata 1153
- ip pim register-rate-limit 1146
- ip pim register-suppression 1149
- ip pim rp-address 1144
- ip pim rp-candidate 1141
- ip pim sparse-mode 1154
- ip pim spt-threshold 1147
- ip pim trigger-hello-interval 1127
- IP port priority
  - enabling 340, 910
  - mapping priorities 340, 911
- IP precedence
  - enabling 334, 912
  - mapping priorities 335, 913
- ip proxy-arp 1027
- ip rip authentication key 1047
- ip rip authentication mode 1048
- ip rip receive version, RIP 1043
- ip rip send version, RIP 1044
- ip route 1030
- IP routing 397, 1028
  - configuring interfaces 403, 1030
  - enabling or disabling 401, 1029
  - status 401, 1029
  - unicast protocols 400
- ip routing 1029
- IP settings, default 33
- ip split-horizon 1046
- ip ssh authentication-retries 660
- ip ssh crypto host-key generate 663
- ip ssh crypto zeroize 664
- ip ssh save host-key 665
- ip ssh server 658
- ip ssh server-key size 661
- ip ssh timeout 659
- ip telnet server, TCP port configuration 654

- IP, statistics 413, 1034
- isolated ports 303, 870

## J

- jumbo frame 79, 554

## K

- keywords, CLI 518

## L

- L2MPLS 314, 890
  - binding a VLAN to a tunnel 319, 893
  - description 314
- LACP
  - dynamic trunking 190, 756
  - local parameters 202, 766
  - partner parameters 205, 766
  - protocol message statistics 766
- lacp 759
- lacp *Also see* LACP
- lacp admin-key
  - Ethernet Interface 197, 762
  - Port Channel 196, 763
- lacp port-priority 197, 764
- lacp system-priority 197, 761
- LANs
  - displaying configuration 283
- Layer 2 over MPLS *See* L2MPLS
- lease, DHCP client 382, 991
- LED indicators
  - CTRL 12, 559
  - DIAG 12
  - FAN 12
  - management 6

- problems 1171
- PWR 11
- using 11
- Line Configuration mode, defined 524
- line, console or vty 570
- link aggregation 190, 756
- Link Aggregation Control Protocol *See* LACP
- link type, STA 246, 249, 816
- link-up-down traps 112, 618
- loader code, defined 35
- loader code, upgrading 563, 1169
- logging
  - enabling 97, 584
  - syslog traps 98, 589
  - to syslog servers 98, 587
- logging facility 98, 588
- logging history 585
- logging host 98, 587
- logging on 584
- logging trap 98, 589
- login, CLI
  - first time 40, 515
  - password checking 571
  - screen display 516
  - using Telnet 516
- log-in, Web interface 52
- logon authentication 126, 632
  - RADIUS client 128, 640
  - RADIUS server 128, 640
  - TACACS+ client 128, 646
  - TACACS+ server 128, 646
- logon authentication, sequence 128, 129, 637, 638

## M

- mac access-group 717
- mac-address, for VLAN 864
- mac-address-table aging-time 791
- mac-address-table static 787
- mac-learning 143, 672
- main menu 54, 528
- maintenance, fuse replacement 17
- management
  - agent 6
  - features 15, 1177
  - IP filter 687
  - LEDs 11
  - options 36
  - overview 21
  - remote connections for 39
  - SNMP 6
  - system files 35
- management vlan, configuring 278, 851
- map ip dscp
  - Global Configuration 334, 914
  - Interface Configuration 338, 915
- map ip port
  - Global Configuration 340, 910
  - Interface Configuration 340, 911
- map ip precedence
  - Global Configuration 334, 912
  - Interface Configuration 335, 913
- mask
  - IP ACL 166, 699
  - IP mask for VLAN ACL 178, 727
  - MAC ACL 170, 713
  - MAC mask for VLAN ACL 180, 729
- match, classifying QoS traffic 344, 924
- match, VLAN ACL 175, 722
- max-hops, MSTP 241, 809
- MDI/MDI-X operation 8
- media-type 189, 745
- MIB support 1177
- mirror port, configuring 209, 773
- mirror sessions, configuring 209, 773
- mode, EAPS 266, 268, 827

modes, CLI 521

## MPLS

input label 319, 893

output label 319, 893

tunnel label 320, 891

uplink port 320, 891

VC label 320, 891

mpls 891

mpls l2 893

mpls static binding 893

mst priority 251, 806

mst vlan 251, 805

MSTP 231, 238

assigning VLAN to instance 251, 805

configuring interface settings 256, 817–818

displaying interface settings 254, 821

global configuration 239, 797

global settings 250

maximum hop count 241, 809

priority 251, 806

region revision 241, 808

MTU 321, 554

multicast filtering 352, 935

enabling IGMP snooping 355

enabling IGMP snooping globally 936

enabling IGMP snooping per interface 362, 937

explained 935

router configuration 359, 950

multicast groups 360, 368, 941, 961

displaying 368, 961

static 360, 361, 938, 941

multicast routing 469, 1103

description 469

DVMRP 473, 1107

enabling 469, 1104

general commands 1104

global settings 469, 1104

PIM-DM 484, 1122

PIM-SM 490, 1134

routing table 470, 1105

multicast services

configuring 361, 938

displaying 360, 941

multicast, static router port 359, 950

Multiple Spanning Tree configuration mode, defined 524

## N

name, MSTP region 241, 807

naming the system 69, 541

negotiation 184, 185, 740

neighbor, RIP 434, 1040

netbios-name-server, DHCP client configuration 382, 989

netbios-node-type, DHCP client 382, 990

network area, OSPF 1066

network, DHCP pool configuration 381, 984

network, RIP interface 428, 1039

next-server, DHCP client configuration 382, 987

no keyword, using 521

non-blocking switching 6

Normal Exec mode 522

null-modem console cable 38

## O

operation code, defined 35

OSPF 436, 1053

area border router 439, 1061

AS summary route 458, 1063

authentication key 452, 1075

authentication type 451, 1073

autonomous system boundary router 439, 1059

- backbone 442, 1066
- cost, for interface 451, 1077
- dead interval 451, 1078
- default external route 440, 1058
- general settings 438, 1053
- hello interval 450, 1079
- message digest key 452, 1076
- network area 442, 1066
- normal area 442, 1066
- NSSA 442, 1068
- redistributing external routes 460, 1064
- retransmit interval 450, 1081
- router priority 449, 1080
- stub 442, 1067
- summary address 458, 1063
- transit area 442, 1070
- transmit delay 450, 1082
- virtual link 453, 1070

## P

- panels, switch front and rear 5
- parity 92, 579
- password, line 573
- passwords
  - administrator setting 126, 633
  - CLI command 633
  - defaults 31
  - recovering lost 1173
  - threshold for wrong entries 576
- password-thresh 576
- path cost 235, 245, 248
  - method 241, 803
  - STA 235, 245, 248, 803
- permit
  - Extended IP ACL 161, 694
  - MAC ACL 164, 709
  - Standard ACL 693
  - Standard IP ACL 160
- PIM-DM 484, 1122, 1123
  - configuring 484, 1122
  - enable on interface 486, 1124
  - global configuration 484, 1123
  - graft retries 487, 1130
  - graft retry interval 486, 1129
  - hello holdtime 486, 1126
  - hello interval 486, 1125
  - interface settings 485, 497
  - jprune holdtime 1128
  - neighbor routers 489, 513, 1132
  - prune holdtime 486
  - trigger hello interval 486, 1127
- PIM-SM 490, 1134, 1136
  - bootstrap router 490, 502, 1138
  - BSR candidate 502, 1138
  - calculate register checksum over entire packet 493, 1153
  - Cisco BSR prefix 493, 1151
  - configuring 490, 1134
  - DR priority 498, 1155
  - enable on interface 497, 1154
  - global configuration 493, 1136
  - hello holdtime 498, 1158
  - hello interval 497, 1157
  - ignore priority of RP candidates 493, 1150
  - interface settings 497, 1154–1158
  - join-prune interval 493, 1137
  - neighbor routers 513, 1132
  - register rate limit for DR 494, 1146
  - register suppression 494, 1149
  - rendezvous point 491, 499, 1141, 1144
  - RP candidate 504
  - RP candidate, advertising 504, 1141
  - shared tree 491
  - shortest path tree 491, 1147
  - SPT threshold 495, 1147
  - static RP, configuring 499, 1144

- pin assignments, console port 9
- ping 1021
- Policy Map configuration mode, defined 524
- policy-map, DiffServ 346, 926
- port aggregation 190, 756
- port authentication 145, 674
- port configuration, defaults 32
- port monitor 210, 773
- port power
  - displaying status 224, 783
  - enabling 225, 780
  - inline 225, 780
  - inline status 224, 783
  - maximum allocation 223, 781
  - priority 226, 782
  - setting a budget 781
  - showing mainpower 223, 785
- port priority
  - configuring 324, 900
  - default ingress 324, 900
  - STA 245, 812
- port priority, STA 248
- port saturation 8
- port security 142, 670
  - configuring 142, 669
- port, EAPS
  - secondary port 267
- port, EAPS primary port 266, 830
- port, statistics 213, 751
- port-channel keyword, defined 737
- ports
  - autonegotiation 188, 740
  - broadcast storm threshold 207, 747
  - capabilities 188, 741
  - combo 5, 8
  - displaying statistics 213, 751
  - displaying status 749, 753
  - duplex mode 187, 739
  - flow control 188, 743
  - forced selection on combo ports 189, 745
  - speed 187, 739
- ports, configuring 184, 736
- ports, mirroring 209, 773
- power budgets
  - port 223, 781
  - port priority 226, 782
  - switch 223, 779
- power inline 780
- power inline maximum allocation 781
- power inline priority 782
- power mainpower maximum allocation 779
- power management
  - explained 778
- Power over Ethernet
  - CLI commands 778
  - description 7
- primary VLAN 304, 306, 870
- priority, default port ingress 324, 900
- private community string 47
- private vlan 303, 870
- private vlan association 871
- private VLANs
  - isolated VLAN 306, 870
  - primary VLAN 306, 870
- private VLANs, configuring 304, 869
- Privileged Exec mode 522
- problems, troubleshooting 1171
- promiscuous ports 303, 869
- prompt, CLI command 536
- prompts, CLI 525
- protect-vlan 833
- protocol migration 249, 820
- protocol-vlan protocol-group
  - configuring groups 312, 878
  - configuring interfaces 313, 879
- proxy ARP 406, 1027
- public community string 47
- public-key keyword, using 562

PVID, setting 291, 860

## PVLAN

- association 307, 871
- interface configuration 309, 873
- isolated ports 303, 870
- primary VLAN 304, 306, 870
- promiscuous ports 303, 869

PWR LED 11

## Q

QoS 342, 921

- configuring 342, 921

Quality of Service *See* QoS

queue bandwidth 330, 902

queue cos-map 326, 904

queue min-bandwidth 332, 903

queue mode 898

- weighted fair queuing (WFQ) 329, 898
- weighted round robin 329, 898

queue weights 330, 902

quit, CLI command 538

## R

RADIUS, logon authentication 128, 640

radius-server host 129, 641

radius-server key 130, 643

radius-server port 129, 642

radius-server retransmit 130, 643

radius-server timeout 130, 644

rate limits, configuring 211, 776

rate-limit 211, 776

redistribute, OSPF external routing information  
460, 1064

reload 535

remote logging 98, 589

remote management 39

rendezvous point 491, 499, 1141, 1144

restarting the system 103, 535

revision, MSTP 241, 808

## RIP

authentication key 432, 1047

authentication type 432, 1048

configuring 424, 1037–1050

description 400

global settings 425, 1037–1038

interface protocol settings 429, 1043–1048

receive version 431, 1043

send version 431, 1044

specifying interfaces 428, 1039

split horizon 431, 1046

statistics 433, 1051, 1052

RJ-45 port LEDs 12, 13

RJ-45 ports, description 7, 8

robustval 954

Router Configuration mode, defined 524

router pim dense-mode 1123

router pim sparse-mode 1136

router redundancy

protocols 387, 998

VRRP 389, 999

router rip 1037

routing table, displaying 422, 1032, 1033

RS-232 serial port connection 38

RSTP 231, 238, 797

global configuration 234, 797

interface settings 247, 810–816

running-config file

copy command 561

explained 36

saving 40

## S

### SBC

- mode selection 557
- sbc ctrlld 559
- sbc power 557
- SBC, mode selection 74
- secure shell 135, 655
- Secure Shell *See* SSH
- serial port
  - configuring 92, 569
  - connection 38
  - XModem downloads 1167
- service dhcp 981
- service-policy, DiffServ 350, 931
- SFP transceivers
  - slots, explained 8
- shared tree 491
- shortest path tree 491, 1147
- show access-group 735
- show access-list 734
- show access-list ip mask-precedence 705
- show access-list mac mask-precedence 716
- show arp 1026
- show bridge-ext 843
- show calendar 607
- show class-map, DiffServ 932
- show commands, displaying 519
- show dns 971
- show dns cache 972
- show dot1q-tunnel 885
- show dot1x 683
- show eaps 836
- show garp timer 847
- show gvrp configuration 845
- show history 534
- show hosts 971
- show interfaces counters 751

- show interfaces protocol-vlan protocol-group 881
- show interfaces status 749
- show interfaces switchport 753
- show ip access-group 706
- show ip access-list 697
- show ip dhcp binding 996
- show ip dvmrp interface 1121
- show ip dvmrp neighbor 1120
- show ip dvmrp route 1118
- show ip host-route 1033
- show ip igmp groups 961
- show ip igmp interface 959
- show ip igmp snooping 940
- show ip igmp snooping mrouter 951
- show ip interface 1019
- show ip mroute 1105
- show ip ospf 1083
- show ip ospf border-routers 1084
- show ip ospf database 1085
- show ip ospf interface 1097
- show ip ospf neighbor 1099
- show ip ospf summary-address 1101
- show ip ospf virtual-links 1101
- show ip pim 1161
- show ip pim bsr-router 1163
- show ip pim interface 1131
- show ip pim neighbor 1132
- show ip pim rp mapping 1165
- show ip pim rp-hash 1166
- show ip redirects 1020
- show ip rip 1050
- show ip route 1032
- show ip ssh 666
- show ip traffic 1034
- show lacp 766
- show line 583
- show logging 591
- show mac access-group 718

- show mac access-list 711
- show mac-address-table 789
- show mac-address-table aging-time 793
- show mac-address-table multicast 941
- show mac-learning 673
- show management 689
- show management vlan 868
- show map ip dscp 919
- show map ip port 916
- show map ip precedence 917
- show mpls l2transport 894
- show policy-map interface, DiffServ 934
- show policy-map, DiffServ 933
- show port monitor 774
- show power inline status 783
- show power mainpower 785
- show protocol-vlan protocol-group 880
- show public-key 668
- show queue bandwidth 906
- show queue cos-map 908
- show queue min-bandwidth 907
- show queue mode 906
- show radius-server 645
- show rip globals 1049
- show router dvmp 1117
- show running-config 545
- show snmp 610
- show snmp engine-id 621
- show snmp group 626
- show snmp user 630
- show snmp view 623
- show snmp 604
- show spanning-tree 821
- show spanning-tree mst configuration 823
- show ssh 666
- show startup-config 542
- show system 548
- show system mode 553
- show system mtu 556
- show tacacs-server 648
- show users 549
- show version 550
- show vlan 866
- show vlan filter 732
- show vlan filter access-map 725
- show vlan mac-address 867
- show vlan private-vlan 876
- show vrrp 1007
- show vrrp all 1010
- show vrrp interface 1011
- show vrrp interface counters 1013
- show vrrp router counters 1012
- shutdown 746
- silent-time 92, 577
- Simple Network Management Protocol *See* SNMP
- SNMP 106
  - basic settings 46
  - CLI commands 608
  - community string 109, 612
  - community strings 47
  - default settings 31
  - enabling traps 110, 618
  - trap manager 110, 615
  - trap receivers 48
  - using 6
- snmp-server community 109, 612
- snmp-server contact 69, 613
- snmp-server enable traps 112, 618
- snmp-server engine-id 115, 619
- snmp-server group 121, 625
- snmp-server host 111, 615
- snmp-server location 69, 614
- snmp-server user 628
- snmp-server view 622
- snmp-server, enabling 108, 609
- SNMPv3
  - client configuration 48, 116, 628



- security models and levels 107
- sntp client 104, 601
- sntp poll 104, 603
- sntp server 104, 602
- software
  - displaying version 75, 550
  - downloading 87, 560, 1167
- software, key features 21
- Spanning Tree *See* STA
- Spanning Tree Protocol *See* STP
- spanning-tree cost 235, 811
- spanning-tree edge-port 249, 813
- spanning-tree forward-time 240, 799
- spanning-tree hello-time 240, 800
- spanning-tree link-type 249, 816
- spanning-tree max-age 240, 801
- spanning-tree mode 239, 797
- spanning-tree mst cost 257, 817
- spanning-tree mst port-priority 256, 818
- spanning-tree mst-configuration 804
- spanning-tree pathcost method 241, 803
- spanning-tree portfast 246, 814
- spanning-tree port-priority 248, 812
- spanning-tree priority 239, 802
- spanning-tree protocol-migration 249, 820
- spanning-tree spanning-disabled 247, 810
- spanning-tree transmission-limit 241, 804
- spanning-tree, global enable 239, 796
- specifications
  - compliances 1176
  - environmental 1176
  - physical 1175
  - power 1176
- speed, console baud rate 580
- speed-duplex, port configuration 739
- SSH
  - authentication retries 141, 660
  - authentication timeout 141, 659
  - clear host key 138, 664
  - configuring 135, 655, 659
  - enabling 140, 658
  - generating host keys 138, 663
  - key size 141, 661
  - save host key to memory 138, 665
- STA 231
  - configuration 231, 794
  - displaying interface settings 243, 821
  - edge port 246, 249, 813
  - fast forwarding 246, 813, 814
  - global settings, configuring 238, 796–804
  - global settings, displaying 234, 821
  - interface settings 243, 810–818
  - link type 246, 249, 816
  - mode 239, 797
  - path cost 235, 245, 248, 811
  - path cost method 241, 803
  - port priority 245, 248, 812
  - protocol migration 249, 820
  - transmission limit 241, 804
- standards
  - compliance 1176
  - IEEE 1179
- startup files
  - creating 90
  - defined 36
  - displaying 87, 567
  - setting 87, 91, 568
- startup-config 562
- static addresses, setting 227, 787
- static routes, configuring 403, 421, 1030
- statistics
  - ARP 412, 1034
  - ICMP 416, 1034
  - IP 413, 1034
  - port 213, 751
  - RIP 433, 1051, 1052
  - TCP 419, 1034
  - UDP 418, 1034

- statistics, clearing counters 219, 748
- status LEDs 11
- stopbits, console port 93, 581
- store-and-forward switching 6
- STP 238, 797
- STP *Also see* STA
- summary-address, OSPF 458, 1063
- switch architecture 6
- switch configuration, saving 40
- switch hardware 7
- switch management, options 36
- switch settings, saving or restoring 560
- switching, method 6
- switchport acceptable-frame-types 858
- switchport allowed vlan 861
- switchport broadcast packet-rate 747
- switchport dot1q-ethertype 885
- switchport forbidden vlan 863
- switchport gvrp 844
- switchport ingress-filtering 859
- switchport mode 857
- switchport mode dot1q-tunnel 884
- switchport mode private-vlan 873
- switchport mtu 889
- switchport native vlan 860
- switchport priority default 900
- switchport private-vlan host-association 875
- switchport private-vlan mapping 874
- syslog servers, configuring 98, 587
- system clock, setting 104, 600
- system defaults 30
- system files
  - defined 35
  - managing 86, 560
  - running-config 36, 40
- system information, displaying 69, 548
- system LEDs 11
- system mode, normal , QinQ or L2MPLS 71, 552

- system mtu 72, 555
- system software, downloading from server 87, 561

## T

- TACACS+, logon authentication 128, 646
- tacacs-server host 130, 646
- tacacs-server key 130, 648
- tacacs-server port 130, 647
- Telnet
  - maximum sessions 39
  - TCP port configuration 94, 654
  - using 94, 516
- terminal emulation, settings 38
- text conventions 2
- tftp keyword, using 562
- TFTP server, uploading and downloading to 86, 87, 561
- time commands 104, 600
- time, setting 104, 600
- timeout login response 92, 94, 574
- timers basic, RIP 426, 1038
- timers spf, OSPF 440, 1060
- TPID 292, 301, 885
- traffic class weights 330, 903
- traffic priority defaults 33, 324, 900
- transceiver slots, SFP 8
- trap manager 110, 615
- trap receivers
  - basic settings 48
  - host configuration 111, 615
- troubleshooting
  - power and cooling problems 1172
  - switch indicators 1171
- trunk
  - configuration 190, 756
  - LACP 193, 756

static 191, 756  
trunking 190, 756

## U

upgrading software 87, 1167  
user account 126, 633  
user password 126, 634  
username 126, 633

## V

version, RIP 431, 1041  
Virtual Router Redundancy Protocol *See* VRRP  
vlan access-map 182, 720  
VLAN Configuration mode, defined 524  
vlan database 849  
vlan filter, binding VLAN ACL 182, 731  
vlan, creating 284, 848, 850  
VLANs  
    adding static members 287, 289, 855  
    creating 284, 848  
    default settings 32  
    description 272  
    displaying basic information 277, 843  
    displaying configuration 843  
    displaying port members 283, 866  
    egress mode 292, 301, 857  
    interface configuration 290, 855–864  
    MAC address configuration 294, 864  
    private 303, 868  
    protocol 311, 877  
VRRP 389, 999  
    authentication 392, 1002  
    configuration settings 389, 999  
    group statistics 395, 1007, 1010  
    preemption 390, 392, 1005

priority 390, 392, 1003  
protocol message statistics 394, 1012  
timers 391, 1004  
virtual address 390, 391, 1000, 1001  
vrrp 1000  
vrrp authentication 1002  
vrrp ip 1001  
vrrp preempt 1005  
vrrp priority 1003  
vrrp timers advertise 1004  
VT100 terminal 38  
Vty prompt 517

## W

Web interface  
    access requirements 51  
    configuration buttons 53  
    home page 52  
    menu list 54  
    panel display 53  
Web server access  
    HTTP, HTTPS 649  
weighted fair queueing  
    minimum bandwidth 332, 903  
weighted fair queueing (WFQ) 329  
weighted fair queueing (WFQ), queue mode 898  
weighted round robin (WRR) 329  
weighted round robin (WRR), queue mode 898  
whichboot 567

## X

XModem downloads 1167





