Ethernet Switching System

Installation & User Guide

GarrettCom, Inc
25 Commerce Way #1
North Andover, MA 01845
Phone: 978.688.8807
Fax: 978.688.8771

$5.00 USD

Document Part Number and Revision

Provides information about this document.

This document describes the features, functions and configuration parameters for the ***Ethernet Switch System (ESS) product***. For ordering, use kit part number 160-1470-001 for a CD copy of the manual or 160-1470-100 for a paper based manual. The *pdf* file part number is 4-62-1470-01.

Manual Stock Number: 160-1470-001 for CD version
160-1470-100 for paper version

Revision History:

Date	Document Revision	Changes Note
4-28-2003	Preliminary	
6-24-2003	Rev B	Typographical Changes
11-17-2003	Rev C	Formatting and clarifications
1-27-04	Rev D	Full Release
3-30-04	Rev E	Change Company name

This document has been prepared to assist users of equipment manufactured by DYMEC, Inc., and changes are made periodically to the information in this manual. Such changes are published in Software Release Notices. If you have recently upgraded your software, carefully note those areas where new commands or procedures have been added. The material contained in this manual is supplied without any warranty of any kind. DYMEC, Inc. therefore assumes no responsibility and shall incur no liability arising from the supplying or use of this document or the material contained in it.

Table of Contents

Federal Communications Commission (FCC) Compliance Notice:

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his/her own expense.

Changes or modifications could void the user's authority to operate the equipment. The user is cautioned not to change or modify this product.

EN55022 Notice:

Warning

This is a Class A product. In a domestic environment this product may cause radio interference, in which case the user may be required to take adequate measures.

Industry Canada Notice:

This Class A digital apparatus meets all requirements of the Canadian Interference-Causing Equipment Regulations.

Cet appariel numérique de la classe A respecte toutes les exigences du Règlement sur le matérial brouilleur du Canada.

THIS IS A CLASS 1 LASER PRODUCT.

SAFETY NOTICE: CAUTION

This product does not contain field serviceable components.
Risk of explosion if battery is replaced by an incorrect type.
Do not attempt to replace the battery. Contact the factory for further assistance.

1

1. Product Description and Specifications

Ethernet Switch Systems (ESS) are a family of industrial-hardened standalone Ethernet switches that support up to twenty-four 10/100 ports and two Gigabit ports. The 10/100 ports can support 10/100 TX, 10FL or 100FX (single mode or multimode) interfaces, and the optional Gigabit ports can support either copper or fiber optics via SFP modules (small form-factor pluggables).

ESS systems with the standard "hardened" power supplies are specifically designed to operate in harsh environments often found in industrial and utility applications. Extended temperature operation and protection against electrical surge, pulse and Electro-Static Discharge are all elements of the hardened protection built into these systems. ESS systems may optionally be purchased with commercial-rated power supplies for less demanding office or computer room environments.

The ESS is an 802.1D-compliant Ethernet bridge. It has an address table size of up to 8192 MAC addresses. The ESS is based on a silicon switching fabric that can support full wire speed on all ports. Functions such as address learning, packet filtering, ageing and port monitoring are also performed in hardware. Applicable ports support 10/100 auto-detection and MDI/MDIX auto-crossover.

ESS systems are offered in two basic variants, *MANAGED or UNMANAGED*. In the ***unmanaged*** system, units are pre-configured to defined system-wide physical and layer II operations, e.g. fiber port speed, 10/100TX auto-negotiation, and auto-MDIX. The *unmanaged* system is basically a turnkey product that only requires power and physical connectivity to operate. ***Sections 3 through 7 of this user guide are essentially not applicable to an unmanaged ESS.***

In contrast, the ***managed*** systems have an additional management processor and an active management application integrated into the product. This allows additional software-configured functionality including VLANs, port-by-port custom configuration and remote

access to status, diagnostics and configuration commands via the console, Telnet and/or SNMP.

The ESS base module may also be incorporated into a DYMEC Network Integration System (NIS) as an integral Ethernet communications module. The operating software is also unified with the NIS base software in areas such as IP routing and Telnet terminal support. Several NIS advanced features are thus available in the ESS, although with limitations due to physical port and interface considerations.

1.1. Unmanaged Switch Features

- **Wire speed Ethernet switch**
- **Fiber and copper interfaces:**
  - 10/100 TX, 10FL, 100FX and 1000SFP interfaces
- **8192 MAC address table**
- **Half or Full-Duplex operation**
  - When used through-out a network, full-duplex operation reduces Ethernet collisions and improves end-to-end performance
- **Flow control**
  - 802.3x Pause frames on full duplex connections
  - Back pressure enabled for half-duplex
- **Port self-configuration** (as appropriate)
  - 10/100 Auto detection on 10/100TX ports
  - Half/full duplex auto-negotiation
  - Auto-crossover (MDI/MDIX)
- **AC, DC and utility hardened power supplies**

1.2. Managed Switch Features

Managed switches support all the capabilities of the unmanaged switch, with the unmanaged switch settings as defaults. Advanced features supported on the Managed ESS configurations (and not on unmanaged systems) include:

1.2.1. Port Settings Control

Port groups, IP addresses, FDX/HDX, auto negotiation, enable, disable and link loss management are all dynamically configurable on a per port basis.

1.2.2. Spanning Tree Protocol and Rapid Spanning Tree

Spanning Tree Protocol (STP) compliant with IEEE 802.1d, as well as Rapid Spanning Tree Protocol (RSTP) compliant with IEEE 802.1w, can be configured on a port-by-port basis. These protocols prevent unwanted active loops in Ethernet topologies and enable route recovery when a link or node fails in a redundant or ring configuration.

1.2.3. Rapid Port Fail-over (DLL)

Disable TX on Link Loss (DLL) automatically disables the TX port if signal is lost on the corresponding Rx port. This enables very fast recognition of failures and invocation of RSTP recovery procedures to achieve sub-second recovery in redundant configurations.

1.2.4. VLANs

The ESS allows the Ethernet switch to be segmented into groups for port-based VLANs and into tag-based VLANs, compliant with IEEE 802.1Q.

1.2.5. Traffic Prioritization

The ESS prioritizes traffic compliant with IEEE 802.1p, enabling critical applications to maintain superior performance during periods of high network utilization.

1.2.6. BootP and DHCP

The ESS systems support BootP and DHCP helper/server applications to provide automated IP address assignment for attached devices.

1.2.7. IP Routing and Address Filtering

The ESS supports routing of IP traffic on Ethernet ports, building upon the base software from the DYMEC NIS. IP routing supports management applications. It may also support limited inter-VLAN traffic. Appropriate applications include Telnet or SNMP management access to devices attached to the ESS or telemetry, SCADA or alarm surveillance applications. The ESS supports static routing, RIP, RIP-II, RIP-RX and OSPF. The ESS also supports extensive IP address filtering capabilities that can effectively limit the applications and devices that are able to use the IP routing function.

1.2.8. Menu System

The ESS provides a menu-driven configuration system that allows an operator to configure and manage all aspects of the system. This menu system is accessible locally or remotely through an Ethernet port via a Telnet session or via a dedicated RS-232 console port on the unit.

1.2.9. Telnet

Telnet is fully supported on the ESS systems for remote access to configuration menus. An operator can invoke a Telnet session to any network-connected remote ESS unit.

1.2.10. Password Security

The ESS has five operator access levels with password protection. The ESS can also interoperate with a separate RSA SecurID server authentication system.

1.2.11. Remote Access Security

In addition to password security, the ESS provides IP filtering capabilities based on application type, IP address, or MAC address to limit access to ESS management applications.

1.2.12. SNMP

The ESS supports an SNMP client and MIBs to support remote management of the system. This includes Trap generation for alarm notification of the Link status of attached ports.

1.2.13. Port Monitoring

The ESS can monitor the traffic of a port with what is essentially an embedded data-scope. The ESS will capture frames sent and received on a port in real-time and display all or selected elements of this traffic to the console under operator supervision. This feature enhances troubleshooting capability since no special analyzer equipment is needed and the trace capability is accessible remotely via a Telnet session.

1.2.14. Port Mirroring

The ESS supports can replicate (mirror) the traffic on one port onto a second port (in addition to switching this traffic to the normal destination ports). Port mirroring allows an operator to monitor a port's traffic using a monitor attached to the mirror port, locally or remotely.

1.2.15. Event Log

A Flash memory-based event log is provided on all ESS systems. Three different levels of events can be recorded and retrieved either locally or remotely. The levels include SEVERE, WARNING and DIAGNOSTIC. The diagnostic level can be an additional aid to the protocol monitor feature in troubleshooting networking issues.

1.2.16. Operating System and Configuration Updates

The ESS has two copies of the operating systems, one standby and one operating. The operating system can be upgraded remotely via TFTP. Configuration files as well as event logs can also be retrieved and downloaded using TFTP.

1.3. Physical Configuration

1.3.1. Port Configuration Options

The ESS is provided in a number of configurations. 10/100 ports are provided in banks of 8 ports with one base card of 8 ports and then one or two expansion cards, providing a total of 8, 16 or 24 10/100 ports. These ports may be configured in a variety of specified mixes of 10/100 TX, 100 FX MM, 10FL MM, or SFPs for MM or SM (Small Form-factor Pluggables). In addition, the base card optionally supports two Gigabit-ready Ethernet SFP ports with copper or fiber options. "Gigabit ready" means the system has the Gigabit ports with SFP sockets, and the optics or copper transceiver is purchased and installed separately. The pluggables may be purchased and installed as part of the initial order or at a later date.

The **base card** is currently offered in the following port configurations.

10/100 TX	100 FX MM	100 SFP	10FL	1000 SFP
8	-	-	-	-
-	8	-	-	-
6	2	-	-	-
6	-	2	-	-
6	-	2	-	2
8	-	-	-	2

Expansion card options include:

10/100 TX	100 FX MM	100 SFP	10FL	1000 SFP
8	-	-	-	-
-	**8**	-	-	-
-	-	-	**8**	-

One base card is mandatory. Up to two expansion modules can be added to the base model. Due to commercial and logistical factors, certain combinations of cards and power supplies are considered standard configurations; others are considered special configurations. Contact DYMEC sales or customer service representatives for current ordering information.

1.3.2. Fiber Optic Specifications

The following table summarizes specifications for standard fiber optic connectors for the ESS. Long-range lasers are also available for the SFP modules as a special request.

ESS Optical Interface Specifications							
Port Type	**Conn. Type**	**Mode**	**Tx Power (dBm)**		**Rx Sensitivity (dBm)**		**Typical Max Dist.**
			Min	**Max**	**Min**	**Max**	
10FL	MTRJ	MM 850nM	-18	-12	-24	-12	2 km
100FX	LC	MM 1310nM	-20	-14	-31	-14	2 km
100FX Pluggable SFP - MM	LC	MM 1310nM	-19	-14	-28	-8	2 km
100FX Pluggable SFP - SR	LC	SM 1310nM	-15	-8	-34	-10	15 km
100FX Pluggable SFP - MR	LC	SM 1310nM	-5	-0	-34	-10	40 km
GigE Pluggable SFP - SR	LC	SM 1310nM	-9	-3	-20	-3	10 km
GigE Pluggable SFP - MR	LC	SM 1310nM	-7	-3	-24	-3	20 km

"Typical maximum distance" is an estimated projection based on typical fiber installations; actual distance will depend on actual network attenuation.

For all MM (multimode) optics, the recommended fiber cable type is 62.5 / 125 µm fiber. Selected others are supported, including 50 / 125 µm fiber for both 10FL and 100FX and 85/125 µm and 100/140 µm for 100 FX only. For 100FX SM (single mode) optics, the recommended fiber cable type is 9 µm SM fiber.

1.3.3. Power Supply Options

The ESS can be ordered with one of three power supply systems as described in the following table.

ESS Power Supply Options					
Model	**Voltage Nominal (V)**	**Voltage Input Range**	**Power (WATTs)**	**Max Amperage (A)**	**Application**
High Voltage DC	**125 Vdc**	**90-140 Vdc**	**80**	**1.0**	**Utility hardened**
Low Voltage DC	**24/48 Vdc**	**18-60 Vdc**	**80**	**4.5**	**Utility hardened**
Wide input AC	**100-240 Vac**	**90-264 Vac**	**80**	**1.0**	**Commercial**

Note: "Utility hardened" means the power supply is designed to meet C37.90.1, .2 and .3, IEEE 1613 and IEC 61850-3 requirements, including to run without the need for any fans. Note that the overall operating temperature specification for the utility-hardened units is -20° to +75° C. The optional commercial power supply has a narrower operating temperature range of 0°-50° C.

2

2. Installation

This section describes the basic installation of the physical ESS unit, with an emphasis on cabling of power, data and console connections.

Each unit is shipped with the following items:

- Power cord (if AC). (DC power wiring must be supplied by customer)
- CD with documentation in Adobe format

2.1. Rack Mounting

The ESS is based on an industry standard 19 inch, rack-mounted 2U (two rack units) high chassis. The holes in the mounting plates conform to both Telco style rack spacing (multiples of one inch) and standard EIA rack spacing. A unit may be mounted on 19" front, rear or center rails. The mounting ears may also be rotated 90 degrees for secure mounting on walls or rack shelves.

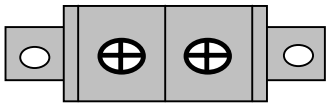
The ESS chassis is designed with all connectors and indicators on the back side. There is a single "power on" LED on the lower right of the front overlay.

The rear of the unit houses all the connections to Ethernet, power and console port. In addition there are Ethernet Link LED indicators for each port and a single LED to the lower right of the second gigabit port that indicates SYSTEM status. The Ethernet Port indicators show OFF for no link activity, SOLID GREEN indicating link, and BLINKING GREEN indicating traffic.

2.2. Power Connections

2.2.1. DC Systems

The ESS provides a hardened DC power supply for industrial applications and/or hostile environments. The power supply connector is located on the rear of the unit on the right-hand side. It is a screw-down terminal with two screws.



DC Input
Unpolarized

Ground Lug

The screws are labeled non-polarized. This means the positive / negative connection is automatically adjusted internally. There is also a grounding lug for connection to a local ground. It is very important that the grounding lug is utilized in all installations, as this is the protective circuit connection to withstand power surges and transients.

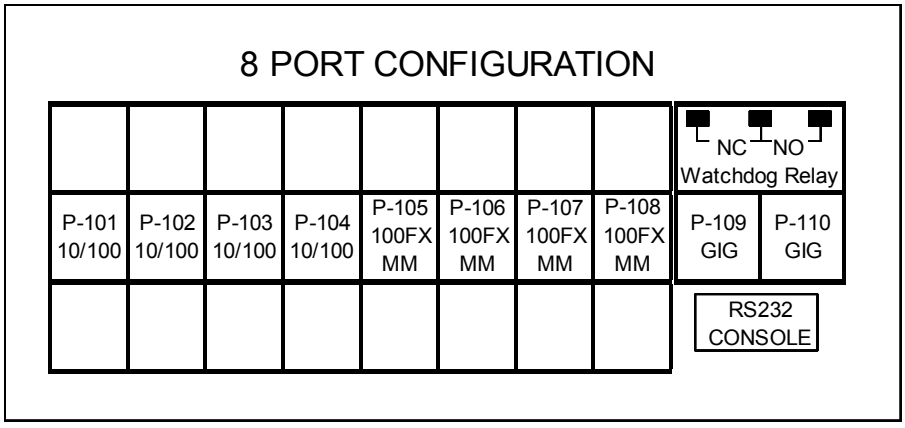
> When installing an ESS unit, an earth ground must be attached to the ground lug prior to connecting power. Failure to do so may result in electric shock to personnel.

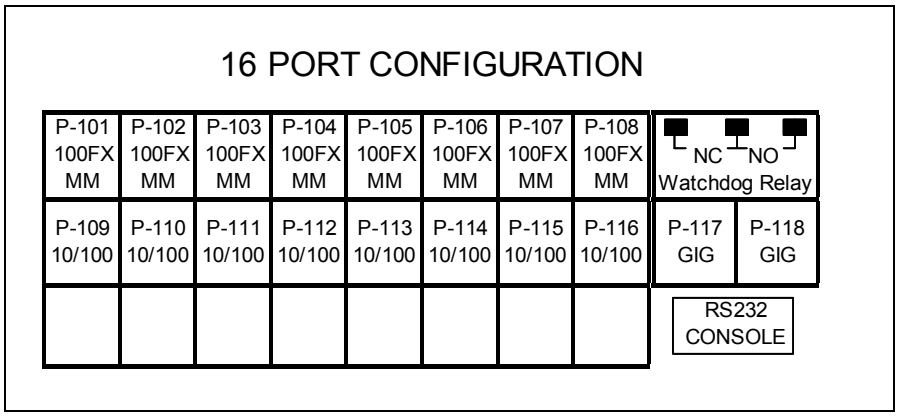
2.2.2. AC Systems

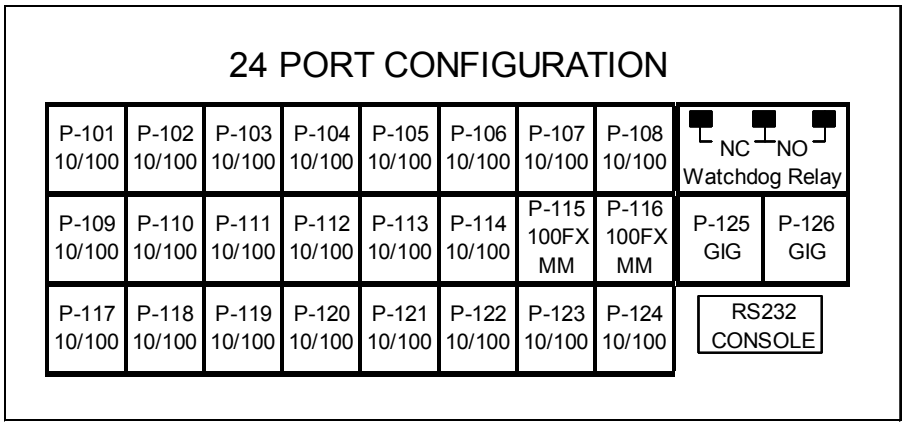
For the commercial AC power systems, the cable connection is to a standard IEC AC socket and connection to it can be made using a standard IEC power cable. The power supply is rated 100-240 Vac auto-ranging and no adjustments are required: just plug it into any properly wired AC source socket.

2.3. Ethernet Port Numbering

The ESS is available in three different basic port configurations: 8-port system, 16-port system or 24 port system, and then with or without Gigabit-ready ports. The port numbering is shown in labels on the face of the ESS next to the ports. 10, 100 and 10/100 Mb ports are assigned port numbers starting at 101 through 1xx, where xx is the number of 10 or 100 Mb ports, and the GE ports (if present) are given the next two numbers. Examples of port labeling and numbering for 8, 16 and 24 port variants is shown below.

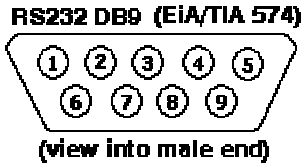






2.4. Console Port Connections

The managed version of the ESS has an asynchronous console port that can be used to access the configuration port. The connector is a standard DB9 male and is pinned out in the standard PC format shown below:



Console Port Connector		
Pin No.	**Name**	**Description**
1	DCD	Data Carrier Detect
2	RD	Receive Data
3	TD	Transmit Data
4	DTR	Data Terminal Ready
5	SGND	Ground
6	DSR	Data Set Ready
7	RTS	Request To Send
8	CTS	Clear To Send
9	RI	Ring Indicator

If you are using this port to connect to a port on a PC running a terminal emulation session such Hyperterm or Procomm, then the interconnecting cable must act as a null modem cable. The wiring for a null modem cable is provided below.

Null Modem Crossover Cable			
DB9	**Signal**	**DB9**	**Signal**
2	RD	3	TD
3	TD	2	RD
4	DTR	6,1	DSR, DCD
6,1	DSR, DCD	4	DTR
7	RTS	8	CTS
8	CTS	7	RTS
5	SGND	5	SGND
9	RI	9	RI

If access to the console port is to be made using an **external dial-up modem** then the following steps should be taken:

- Connect the modem using a straight cable connection to the console port on the ESS.
    - The ESS console port appears as a DTE interface, similar to a PC COM port.
- When the user makes a dialup connection to the modem, they will automatically be connected to the console Supervisor.

For instructions on how to log onto the console port Supervisor software interface and use the menu system, see Section 4, *System Administration* and Section 5, *System Configuration*.

3

3. The ESS Supervisor

This chapter introduces the ESS Supervisor application and describes how to connect to the Supervisor console, log in, enter commands, save changes and move through the Supervisor menus.

The Supervisor application is used to perform the following tasks for Managed Ethernet Switch Systems:

- Configure each port's parameters
- Enable and disable individual ports
- Monitor the status of the ESS
- Monitor individual ports
- Restrict operator access
- Warm or cold start the ESS

3.1. Connecting to the Supervisor

3.1.1. Console Access

After the ESS is installed, a workstation or a remote terminal can be used as the System Operator Console. The system console can be connected to the Supervisor from a workstation on any of the connected LANS, via a dialup connection using an external modem, or via an IP network using Telnet. (See ***Console Port Connections*** in the previous section.) A system administrator can manage multiple ESSs from a single Supervisor Console. Password-based security is provided for all modes of access. Security options are described in Section 7.

- **For terminal mode access to the console:**

  The console terminal device must be set for 9600 Baud, 7 bits, Even parity, and 1 stop bit. For dial connections, call the port and the Supervisor is automatically connected.

- **For access via an IP network:**

  Place a telnet call to the ESS's IP address from a Telnet client on port (socket) 23.

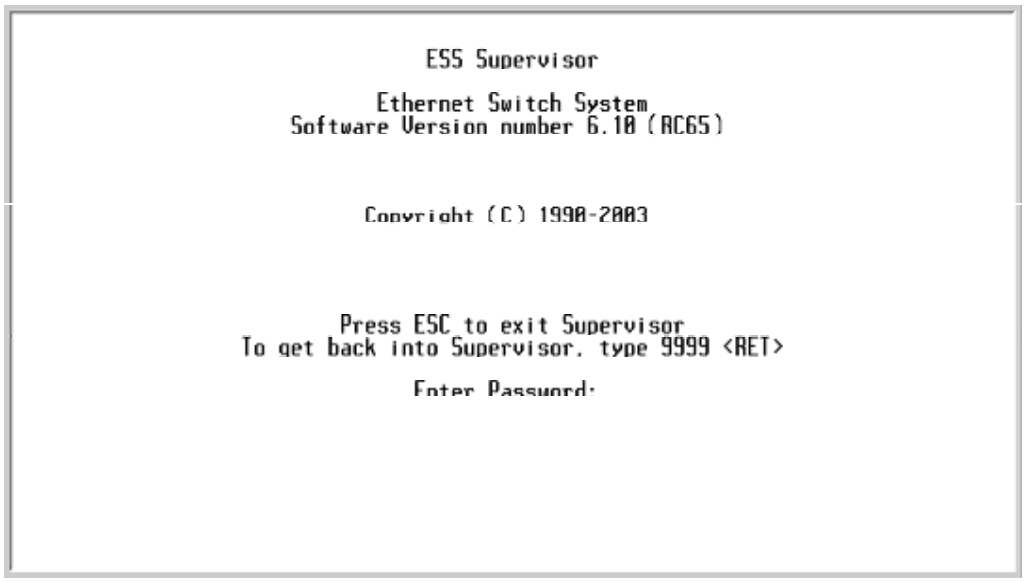
3.1.2. Login Procedures

When the system starts up, the Login menu displays the supervisory herald and the software version number, as shown below. You receive a prompt for the Supervisor's password.

*If you are connecting from a LAN, the Telnet connection screen appears before the Login menu. Select <**1**> and press **<return>** on the Telnet connection screen to go to the console and access the login screen.*

To log in:

At the **Enter Password** prompt, type your password and press **<return>**. The password ***is*** case sensitive. *The factory default password is "secret ".*



The first time you log in, type **secret** and press **<return>**. (Instructions for changing the default password are provided in Section 7, Security. Also, instructions are provided for establishing mutliple user levels and different passwords for each level.)

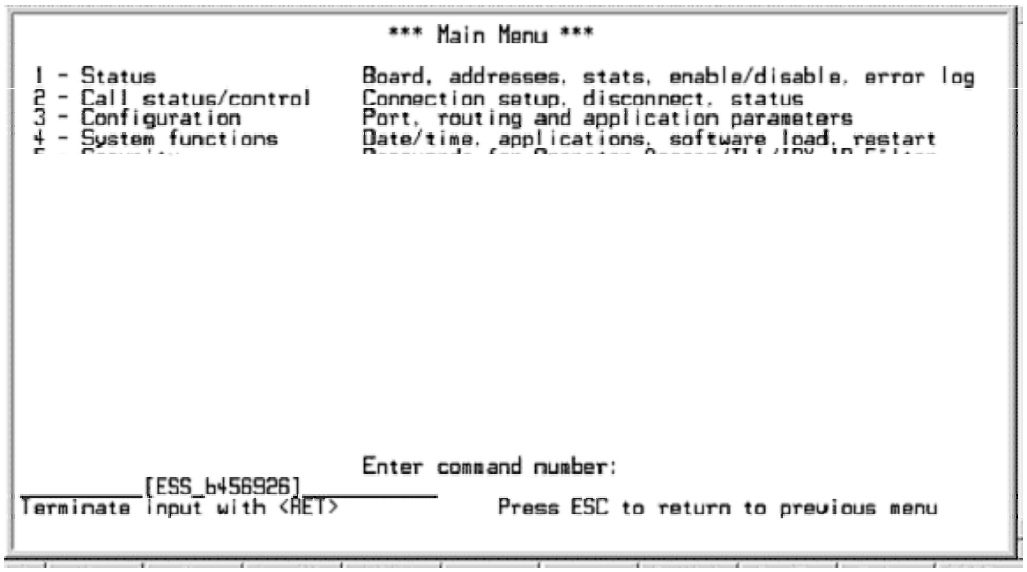
If you do not enter a valid password in three attempts, the connection to the Supervisor is cleared, and you receive the message *CLR PAD*. To be reconnected to the Supervisor, enter **9999** and press **<return>**. Recall that the password is case sensitive. Check Caps Lock setting if a password is failing unexpectedly.

Note: *If the ESS was already booted before the console device was connected, you may see a simple **" * "** prompt and not the supervisory herald as shown above. This indicates the logon screen timed out and the active session was terminated and sent to a pure listening mode. Enter " 9999" and the logon/supervisory herald will be displayed as shown.*

After a successful logon, a screen will appear asking you to identify your console type. Enter your console type and press **<return>**.

- **1** (Wyse 50 or TVI-910/920) or
- **2** (VT100 or ANSI compatible),

The Main menu will appear as shown below.



3.2. Supervisor Basics

3.2.1. Command Notation

Throughout this manual, the following notation is used:

- The names of keys are bold and contained in angle brackets: **<return>**.
- When two keys are pressed simultaneously, they appear in angle brackets separated by a hyphen: **<CTRL-D>**.
- Commands you must enter appear in **boldface**.
- The names of menu fields also appear in **boldface**.
- Representative text in a command line appears in *italics*. For example, the word *file-name* indicates that the actual name of a file is to be entered.
- System messages appear in *italics*.

3.2.2. Universal Commands for Navigating within the Supervisor

The ESS Supervisor is a hierarchical menu system. There are five major sets of menus (the five branches from the Main Menu, above). Each set of menus is a separate hierarchy. Menu navigation procedures refer to moving up or down within this hierarchy. Other universal commands deal with entering commands and saving work.

- **To move down through a set of menus:**

  In the **Enter command number** field, type the number that appears next to the menu you want to display. Press **<return>.**

- **To return to the previous menu in the hierarchy:**

  Press **<ESC>.**

  If you use **<ESC>** to escape from the Login menu, your call to the Supervisor is cleared.

- **To enter new information in menus:**

  Use the **<cursor>** keys (left, right, up, down arrows) or **<tab>** key to move around the fields.

  Note: If the cursor keys do not work correctly (they cause a jump to the previous menu), the cursor keys are not set correctly in the terminal application. For Windows and VT100, select VT100 arrows, not Windows arrows, to correct the problem.

  Depending on the field, enter new information by typing in the new value or by pressing **<return>** to toggle through the available values. The two ways of entering information are mutually exclusive. In fields where you toggle the enter **(cr)** key to enter the values, you must go to the next field by pressing the **<cursor>** or **<tab>** key.

- **To SAVE new changes;**

  - Move the cursor to the **Process selections** field by use of **<tab>** or **<cursor>** keys.

  - Enter **Y** and press **<return>** (or simply press **<return>**) to instruct the Supervisor to process the new information.

    OR

  - Enter **N** and press **<return>** to abort your input and return to the previous menu. This is equivalent to pressing **<ESC>** at any position on the menu.

  NOTE: You can usually move the cursor directly to the **Process Selections** field by positioning it in the leftmost field on a line and pressing the left arrow.

3.2.3. Saving Changes to Flash Memory

The "**Process changes**" command above will activate changes in the current operating software, but not automatically save these changes to Flash Memory such that they will survive a system restart.

As you configure the ESS, you will be reminded to save your changes to Flash Memory by this highlighted message:

Config has changed: use CTRL-W to save.

If you press <**CTRL-W>**, the message "*Saving configuration to Flash"* appears.

Once the save is complete, the message disappears and the ESS console may beep to alert you that changes have been saved.

Note: Be sure to save changes using the **CTRL-W** command before restarting the ESS, *otherwise all changes made will be lost upon a reboot or power cycle.*

3.3. The Supervisor Console Menu Hierarchy

All configuration and system administration is accomplished via a user-friendly menu system. From the top (or Main) menu screen one may branch to numerous sub-menus specifically designed to accomplish the desired configuration or operational function.

The main menu provides access to sub-menus that are titled to indicate the main categories needed for system operation. These are labeled:

- Status
- Call Status & Control
- Configuration
- System Functions
- Security

The primary functions of these sub-areas is summarized:

Status sub-menus are primarily used to:

- View the current status of the ESS or individual ports
- Verify names and other information regarding ports and services
- View statistics at the port or system level
- Enable or disable individual ports
- Activate and view protocol monitoring on specific ports
- View event logs

Call Status and Control sub-menus are primarily used to:

- View the current status of certain bridge port statistics

Configuration sub-menus are primarily used to:

- Configure Ethernet and console ports
- Define Spanning Tree Protocol parameters for bridge operations
- Configure VLANs
- Set optional IP routing, DHCP, BootP and SNMP parameters

System functions sub-menus are primarily used to:

- Initialize date and time system-wide parameters
- Administer system software
- Restart or reinitialize the system
- (Note that the "Systems Administration" section of the manual describes these System functions and also additional initial Boot process and file management functions that bypass the Supervisor menu system.)

Security sub-menus are primarily used to:

- Administer passwords
- Administer multi-level user access permissions
- Define secure IP filtering for Supervisor application access

The following sections of this document generally align to the five main menu areas described above, but in a modified sequence to better reflect the order in which operations are encountered when first configuring an ESS. **System Administration** is presented first as **Section 4**, including a description of the Boot process, followed by **Section 5, System Configuration**. Note that the **"Call Status/Control"** sub-menus along with **Status** commands are combined in **Section 6, Status and Diagnostics.**

4. System Administration

System Administration includes a number of operational functions often reserved to a single authorized 'root' user and encompasses setting initial systems parameters, booting and restarting the system, administering security for all users of the system and administering changes to the operating software.

Many of these functions are supported by the **<4> SYSTEM FUNCTIONS** sub-menus that are accessed from the Main Supervisor menu. Other System Administration functions are supported by sub-menus in other areas of the Supervisor and by Boot time prompts that bypass the Supervisor application

Other sections to note are the system-level configuration capabilities described in **Section 5, System Configuration** and the user access and security administration functions described in **Section 7, Security.**

4.1. Boot Process

The onboard ROM is the source of the BOOT process; this ROM is based on a copy of the full operating system and is normally fixed for the lifetime of the product. With a console port connected, the BOOT process looks like:

```
DYMEC, Inc.
Flash 0 is 4MB AMD top boot [ID = 01f6]
DynaStar 3000 ROM version 4.1B [6.10 (RCxx)]
Serial number dc0038a7
Ethernet address 0020610038a7
*** Press ESC to boot download immediately ***
*** Press CR  to enter LAN monitoring mode ***
Test 8MB RAM addresses
Test 8MB RAM pattern
Monitoring LAN for ROM commands
Cannot find a valid SRAM
Current IP address is 0.0.0.0
```

At this point the boot process is temporarily halted for 20 seconds. The purpose of this feature is the ability to converse with the ESS if no runtime operating system has been loaded, in particular, to set an initial IP address for downloading software and establishing Telnet command sessions. See Section 4.2 *Initializing IP Address* below.

If an operating system already exists, then the boot process can be accelerated by entering **<ESC>,** or simply wait the 20 seconds and the system will boot automatically. The following boot prompts ensue:

Loading DOWNLOAD.BIN
Decompressing 6.10 (RCxx)... Done!

#portVars=102, #link=66, #pad=1, #packet=67
Using SRAM #2, length = 359870, (101 ports)

********* Error Log *********
System reset by Operator
********* Error Log End *********

This completes the boot process. The version number of the Operating system is printed to the console port so the operator can determine the version number along with the CONFIGURATION file memory bank number in use. The current contents of the error log is the last part of the boot process and can be useful in diagnosing boot problems in the unlikely event the system fails to boot.

4.2. Initializing an IP Address

An IP address must be assigned to the "Local/ROM Address" in order for software to be remotely downloaded, for telnet console sessions to be established to the ESS supervisor and/or for SNMP communications with the ESS. If the system is already running under an operating system, then the Local/ROM Address can be assigned through the console command menus. See related topic in *Section 5 – System Configuration – Routing*. To access these commands, from the main menu, select **<3> Configuration**, then in the Configuration Commands menu, select **<2> Router.**

If an operating system does not already exist, then the "Local/ROM Address" must be established during the Boot process. To communicate with the ESS Boot system, execute the Boot process as described above. The Boot process will pause for 20 seconds right after the following message appears:

Current IP address is 0.0.0.0

During this time, the Operator enters **<CR>** at the local console port and the Console will display a prompt to enter an IP address. The IP assignment allows IP applications like TFTP and Telnet to communicate with the ESS from a remote location in order to make configuration changes and/or upgrade the Operating System to a newer version.

Enter different IP address:

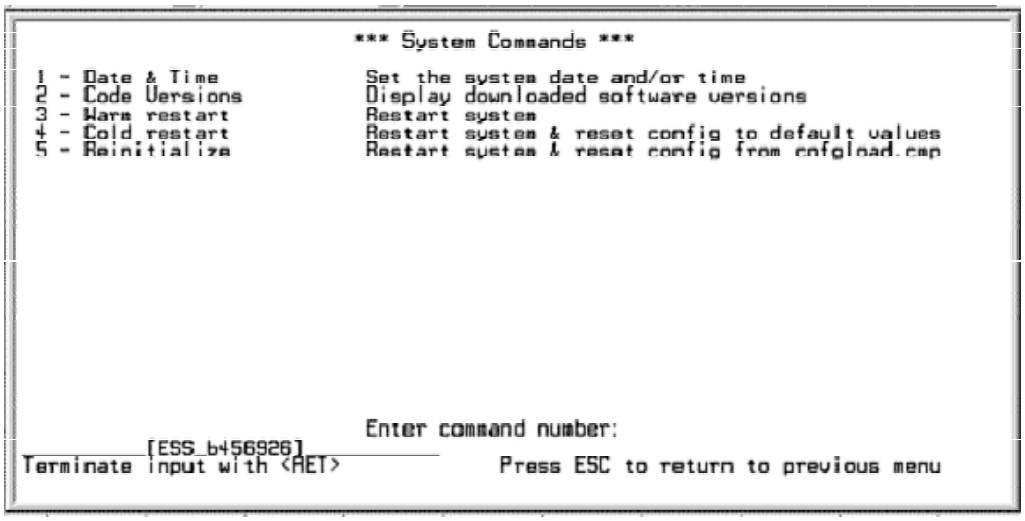
The IP address can be entered in a normal IP address format e.g. ***100.1.1.1 "cr".*** On the display the address will be copied back and another prompt issued.

100.1.1.1 "cr"
Enter different IP address:

The address has been accepted, but not fully processed at this point. You can change the address simply by typing in another IP address, or if the address displayed is acceptable just enter **<CR>** to commit this address to Flash and complete the install process.

4.3. System Functions Commands

The **System Commands** sub-menu can be reached by selecting option **<4> Systems Functions** from the **Main** menu. Within these sub-menus, you can modify the on board Real Time clock, look at software versions that are present in the file system, and initialize the system with WARM and COLD start commands. The sub-menu is shown below:

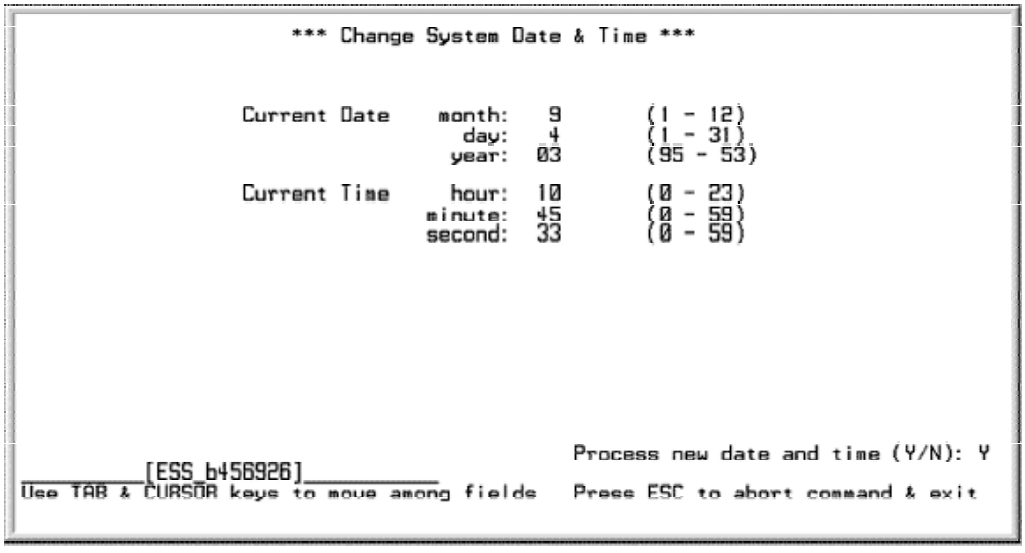


4.3.1. Date & Time

The time and date are preset. To modify the on-board Real Time Clock, select option **<1> Date & Time** from the **System Commands** menu.

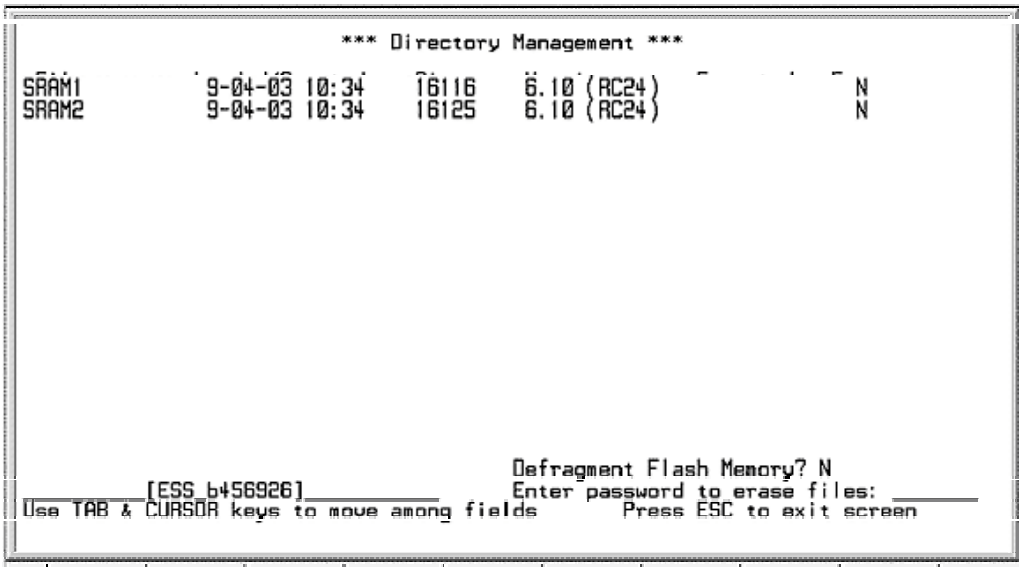
Simply cursor through the fields and overtype the modified values.

Save the new values by exiting through the **Process** command in the bottom right of the screen. The Real Time Clock is battery backed up so this adjustment only needs to be made periodically to compensate for leap years, etc.



4.3.2. Code Versions

This menu option shows the file structure held in memory, including the configuration files. This menu also allows the user to delete files from memory.



The file system can hold multiple copies of the Operating System in the Flash memory. This screen allows an operator to delete unwanted copies of the file system to make space for new ones. It also enables de-fragmentation of the file system. Deleting a file simply marks the file as unusable; de-fragmentation actually re-organizes the memory space and erases files to make space for new. The current ROOT password is required to initiate the **Defragment Flash Memory** process or the erasing of files.

4.3.3. Restarting the ESS

There are three commands for restarting the ESS via the Supervisor. These are reached from the **Systems Commands** menu as the options **<4> Warm Restart**, **<5> Cold Restart** and **<6> Reinitialize**, respectively. All three options have will reboot the ESS and restart active operations. However, the three differ in what source is used for the operating software and active configuration file during and after the restart operation. For all three options, select the desired option from the Systems Commands screen and then enter the Root password to authorize the operation.

Reinitialize

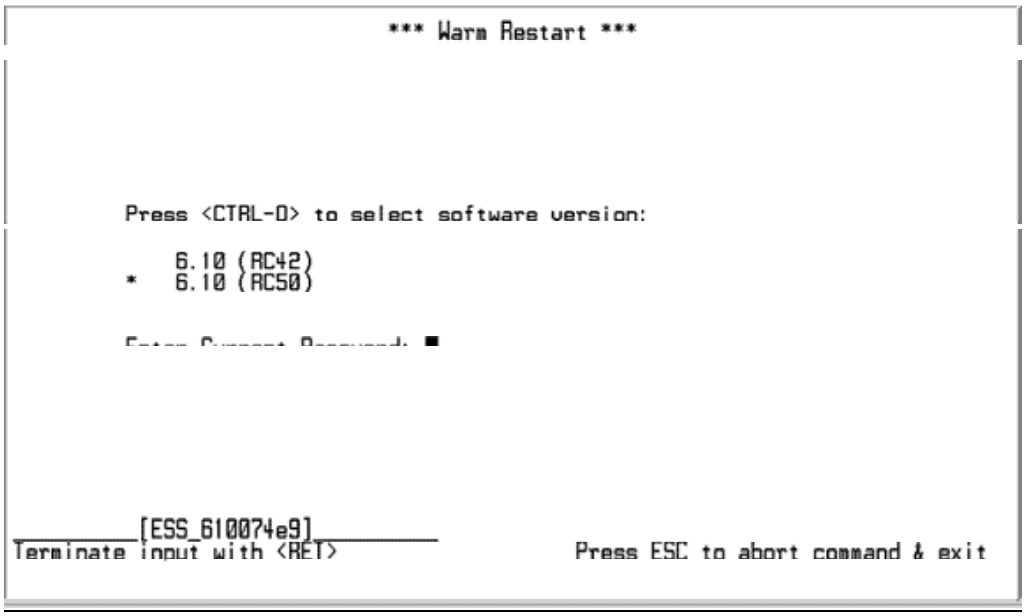
This option is used to re-boot the ESS system, typically from a remote location. The system will re-boot using configuration parameters that are stored in a file named CNFGLOAD.CMP. Other configuration information stored locally will be erased and overwritten. Make sure that the file exists in the file system before invoking this command. The CNFGLOAD.CMP file can be downloaded using TFTP (see description of Software File Management in Section 4.3). Since this affects the system's availability, the command requires the current ROOT password to be entered to ensure authorized usage.

Cold Restart

This option is used to re-boot the ESS system. The system will re-boot using FACTORY DEFAULTS; all pre-configured options will be lost. Use EXTREME CAUTION as invoking this command remotely will cause loss of contact across a network. Since this affects the system's availability, the command requires the correct ROOT password to be entered to ensure authorized usage.

Warm Restart

This option is used to re-boot the ESS system, typically from a remote location. The system will re-boot using configuration parameters that are currently saved in Flash. Since this affects the system's availability, the command requires the current ROOT password to be entered to ensure authorized usage. The command presents a list of all operating system versions presently available in the Flash Memory. The operator may select which version the ESS should use when restarting.



Page intentionally left blank.

5

5. System Configuration

This section describes how **Configuration** sub-menus are used to verify and change system configuration parameters. The main sub-areas for System Configuration include port options, router functions, bridge (STP/RSTP) parameters, other system-wide parameters and SNMP functions.

Note: For initial system configuration, refer also to **Section 4, System Administration**. That section describes the initial Boot process and procedures for initializing the management IP address. Also, **Section 7, Security**, describes how to configure security options including multi-level passwords.

To access the general configuration menu, select **<3> CONFIGURATION** from the Main Menu. The **Configuration Commands** sub-menu is displayed leading to sub-menus for the following functional areas.

Configuration Commands Screen Selections		
Menu Selection	**Command Sub-Menu Name**	**Definition**
1	**Port**	Port options including speed, duplex, flow control, priority, protocol and VLAN membership
2	**Router**	IP addresses and static or dynamic routing parameters for management access and inter-VLAN routing. Also defines BootP and DHCP options.
3	**Bridge**	Parameters for Spanning Tree Protocol and Rapid Spanning Tree Protocol
4	**Server**	Server name and console banners as system-wide parameters
5	**SNMP**	Community strings, trap addresses and authentication parameters for SNMP traps and MIB access.

These command sub-menus areas are each described below.

5.1. Port Configuration

The **Port** configuration sub-menus are used to define the various Ethernet port options and also to configure the console port. To access the port configuration menu, select **<1> PORT** from the **Configurations Commands** menu. The system then prompts for the port or port type to configure. On the ESS, there are two choices:

- **Port 6:** This refers to the RS-232 console port
- **Port 100:** This leads to subsequent screens for configuration of all Ethernet ports.

For provisioning the Console port, enter port **6** and **<CR>.** See provisioning details in **Section 5.1.5,** below.

For Ethernet ports, there are two variants of the provisioning process depending on whether VLAN tagging is enabled or not.

Use "VLANs Not Enabled" provisioning process:

- as the default provisioning model
- if not using 802.1Q VLANs or 802.1p prioritization
- if using the Port Groups and/or port-based traffic prioritization features.

Use "VLANs Enabled" provisioning process if:

- using tagged VLANs based on 802.1Q (Section 5.1.2), and/or
- using traffic prioritization based on 802.1p (Section 5.1.4)

Tagged VLANs, Port Groups and traffic prioritization features are described in more detail within Sections 5.1.1-5.1.4, below.

For both the VLANs Enabled and VLANs Not Enabled provisioning processes, enter Port **100** and **<CR>** in the **Port Configuration** menu. The **Ethernet Switch Port Configuration** screen will appear. This screen lists all Ethernet ports of the switch and associated provisioning parameters. In the upper left corner of this screen is "**Port: 100**" (referring to Ethernet ports in general) and below that "**VLAN Enabled: N**" (or "**Y**"). Toggling this "VLAN Enabled" field to **Y** or **N** will bring up differing provisioning screens for the respective provisioning variants.

The following sections provide details for provisioning Ethernet ports with **VLANs Not Enabled (Section 5.1.1)** and for **VLANs Enabled (Section 5.1.2).** Special options that are available when VLANs are enabled include **VLAN Trunk Provisioning (Section 5.1.3)** and **Priority Management using 802.1p (Section 5.1.4).**

5.1.1. Ethernet Port Provisioning – VLANs Not Enabled

Select **Port 100** and enter **<CR>** on the **Configure Port** sub-menu to access the **Ethernet Switch Port Configuration** screen. This leads to a set of screens that configure both global and port-specific Ethernet switching options, including:

- Port speed / negotiation
- Full/half duplex
- DLL (Disable TX on RX Link Loss)
- Flow control: Back pressure for half duplex ports and 802.1x Pause for Full duplex ports
- Ageing time (for the MAC address table)
- Enable/disable IP routing per port
- Port groups (port-based VLANs)
- Traffic prioritization

The default initial setting of the ESS is that VLANs are not enabled. Initially, the following **Ethernet Switch Port Configuration** screen will appear. Note that in the upper left, the parameter "**VLAN Enabled**" is set to "**N**", the default setting. If this field is set to "**Y**", a different version of the provisioning screen will appear. To continue with the "VLANS Not Enabled" mode of provisioning, ensure that this parameter is set to "**N**" and press <TAB>. (To use the "VLANs Enabled: Y" mode, refer to Section 5.1.2.)

```
                *** Ethernet Switch Port Configuration ***
Port: 100                                    Last Changed:   11-11-03 14:32:06
VLAN Enabled: N            Ageing Time (Tog): 5 m    HOX Back Pressure: N


Port  Group  Speed  Duplex  Pause  Pri DLL*  IP BRG
101    100   10FL    half     -    low  Y    Y   N
102    100   10FL    half     -    low  Y    Y   N
103    100   10FL    half     -    low  N    Y   N
104    100   10FL    half     -    low  N    Y   N
105    100   10FL    half     -    low  N    Y   N
106    100   10FL    half     -    low  N    Y   N
107    100   10FL    half     -    low  N    Y   N
108    100   10FL    half     -    low  N    Y   N
109    100   auto    half     -    low  N    Y   N
110    100   auto    half     -    low  N    Y   N
111    100   auto    half     -    low  N    Y   N
112    100   auto    half     -    low  N    Y   N
113    100   auto    half     -    low  N    Y   N
114    100   auto    half     -    low  N    Y   N
*DLL = Disable TX if RX Link Loss

_________[ESS_610074e9]_________          Process selections (Y/N): Y
Use TAB & CURSOR keys to move among fields   Press ESC to abort command & exit
```

The port types that are installed in the ESS and the default parameter settings for the ports are shown in the screen example above. These defaults can be changed by tabbing or cursoring to each field and using **<CR>** to toggle the field's contents to the desired parameter setting. The following tables provide the parameter definitions and options.

Ethernet Port Global Settings: VLANs Not Enabled			
Parameter	**Definition**	**Default**	**Range**
VLAN Enabled	Defines whether Tagged VLANs and traffic prioritization via 802.1Q and 802.1p are being used.	N	Y/N
Ageing Timer	The default ageing (timeout) of learned MAC addresses	5 min	None, 20s, 5m, 15m, 1h, 4h, 1d
HDX Back Pressure	Perform flow control for half duplex ports by inserting collision traffic	Disable (N)	Y/N

Ethernet Port-Specific Parameters: VLANs Not Enabled			
Parameter	**Definition**	**Default**	**Range**
Port Number	The port number corresponds to physical port as labeled 101-126.	Read only	101-126
Group Number	Defines the port group for the port. See note below on Port Groups.	Group 100 (default for all ports)	100 to port count
Speed	Speed is fixed for fiber/gigabit interfaces. Speed may be defined for copper 10/100 interfaces.	Auto-detect	10, 100 or Auto
Duplex	Defines the type of equipment infrastructure as half or full duplex.	Auto-detect	Half, Full or Auto
Pause	For Full Duplex ports only, flow control is optionally implemented using the 802.3x specification for Pause packets. When congested, the switch will send Pause packets to attached devices to request temporary suspension of transmission of further frames.	Enabled (Y) on full duplex ports	Y/N
Priority (Pri)	This parameter sets switch priority of incoming traffic on this port. See note below on traffic priority.	Low (L)	High (H)/ Low (L)
DLL	Disable TX on Link Loss (DLL) feature will immediately deactivate the TX interface of a port when the receive signal is lost. This is useful for automatic link recovery procedures.	Disabled (N)	Y/N
IP	IP parameter allows this port to participate with the internal IP router. The internal Router can be used to	Y	Y/N

	support remote IP access to the Console system or used to route frames between Port groups.	** Enabled	
Bridge (BRG)	This parameter sets how this port participates in Spanning Tree Protocols. See note below.	None: No active STP/RSTP (N)	Y (STP) R(RSTP) L(LAN) E(edge) N(none)

** Note: For IP routing to be active, IP addresses must be assigned. Other restrictions may also apply to IP routing. See Section 5.3 for IP Router configuration options.

Port Groups

With VLANs Not Enabled, a Port Group feature is available that functions essentially as a Port-based VLAN within the single ESS. That is to say, each port can be assigned to a specific Port Group, numbered by the operator as port groups 101-126 (or 101 up to 1xx, where xx is the number of ports on the switch). MAC-layer switching (bridging) will only be allowed between ports that are members of the same port group, essentially the same operation as having the Port Group represent a VLAN. This includes Multicast, Unicast and Broadcast frame types.

By default, all Ports are assigned to Port Group 100 and traffic will be MAC-layer switched among all these ports as long as they remain assigned to the same Port Group number.

Since the ESS also has an integrated IP router, traffic can still cross Port Group boundaries

- if the ports have IP routing enabled (see the IP router parameter described above),
- if an IP address has been assigned to each port group (see IP Router configuration in Section 5.3) and
- if no other IP address filtering is established to block routing between these addresses.

Routing between Port Groups can be prevented in the ESS by any of these techniques, i.e., do not enable IP routing on a port (described above), do not assign an IP address to the Port Group (the default case), or filter out routing using the IP Filter feature described in Section 7.4.

NOTE: The ESS does not allow a port to function as a member of more than one Port Group. Also, the Port Group number only has significance within a given ESS. The Port Group number does not stay with the data frames and does not propagate to other switches or devices in a network. Given these limitations, Port Groups are generally not practical to administer across networks of multiple switches. To extend the Port Group concept beyond a single switch, the operator should consider using tagged VLANs and VLAN trunking as described in sections 5.1.2 and 5.1.3.

Traffic Priority

In the ESS mode of VLANs Not Enabled, the ESS can provide two-level traffic prioritization based upon the port on which specific frames arrive at the switch. Using the Priority field described in the table above, each port is assigned a priority of high or low (the default is Low). Frames are assigned to the output priority based on the ingress port priority setting.

As with Port Groups described above, the Priority has only local significance within a specific ESS. No factors other than input port are considered in assigning the priority. No priority information stays with data frames after they leave the switch, i.e., priority is not propagated to other switches or devices in the network. Network designs that require a more global priority scheme across multiple switches should consider 802.1p-based traffic prioritization described in Section 5.1.4.

Bridging

The Bridging parameter in the **Ethernet Switch Port Configuration** screen defines the mode of Spanning Tree Protocol (STP) or Rapid Spanning Tree Protocol (RSTP) the switch will use on this port. The following table describes the possible port settings for STP/RSTP.

BRG Field Values and Definitions: STP Enabled (See Section 5.2)		
Value	**Stands For:**	**Definition**
Y	Yes - STP	ESS will use Spanning Tree Protocol (STP) compliant with 802.1d on this port and expect that it is communicating with a peer STP switch.
N	None	The ESS will not actively run either STP or RSTP on this port and will not react to BPDUs coming from the device attached to this port. If BPDUs do come into this port, the ESS will attempt to deliver them as data frames, i.e., will initially broadcast the frames to other ESS ports.
BRG Field Values and Definitions: RSTP Enabled (See Section 5.2)		
Value	**Stands For:**	**Definition**
R	RSTP	ESS will use Rapid Spanning Tree Protocol (RSTP) compliant with 802.1w on this port and expect that it is communicating with a peer RSTP switch. This option is not available if the entire ESS is set to legacy STP (802.1d) rather than RSTP.
L	LAN	Use this option for non-point to point connections. ESS will not rapidly transition this connection.
E	Edge	The ESS will expect that the device attached to this port is not running STP or RSTP and will not initiate STP or RSTP BPDUs on this port. However, if the ESS recognizes that the attached device has initiated STP or RSTP BPDUs, then the ESS will become active with STP or RSTP as appropriate.
N	None	The ESS will not actively run either STP or RSTP on this port and will not react to BPDUs coming from the device attached to this port. If BPDUs do come into this port, the ESS will attempt to deliver them as data frames, i.e., will initially broadcast the frames to other ESS ports.

As noted in the definitions, this parameter interacts with the Spanning Tree Protocol parameter of the **Ethernet Spanning Tree Bridge Parameters** screen described in **Section 5.2**. Specifically, if "Normal" (legacy) Spanning Tree Protocol IEEE 802.1d is selected for the entire switch, then RSTP and "Edge" options cannot be specified here.

5.1.2. Ethernet Port Provisioning - VLANs Enabled

Other than VLAN Trunking and a few other advanced options, Ethernet port provisioning with VLANs Enabled is very similar to provisioning with VLANS Not Enabled. Much of the instruction provided above for the VLAN Not Enabled case is repeated here for clarity. Alternative screens are used to provision both the common and unique aspects of the two variants.

To proceed with the VLANs Enabled provisioning process, select **Port 100** and enter **<CR>** on the **Configure Port** sub-menu to access the **Ethernet Switch Port Configuration** screen. This leads to a set of screens that configure both global and port-specific Ethernet switching options.

The default initial setting of the ESS is that VLANs are not enabled. Initially, the **Ethernet Switch Port Configuration** screen shown in Section 5.1.1 will appear. Note that in the upper left of that default screen, the parameter "**VLAN Enabled**" is set to "**N**", the default setting. To provision Ethernet Ports with VLANs Enabled, set the **VLAN Enabled** field to **<Y>** by toggling **(<CR>)** the Y/N values in the screen and entering **<TAB>.** With this field set to "Y", an Ethernet Switch Port Configuration screen similar to the following example will appear.

```
                *** Ethernet Switch Port Configuration ***
Port: 100                                    Last Changed:   11-11-03 14:32:06
VLAN Enabled: Y          Ageing Time (Tag): 5 m    HDX Back Pressure: N
Priority: Ingress tag 0-7: LLLLHHHH  Egress tag L/H: 0/4
                                                          Ingress  Egress
Port  VLAN   Speed  Duplex  Pause  Pri DLL*  IP BRG       Tag Sec   Tag
101      1   10FL   half      -    low  Y     Y   N        opt  Y     N
102      1   10FL   half      -    low  Y     Y   N        opt  Y     N
103      1   10FL   half      -    low  N     Y   N        opt  Y     N
104      1   10FL   half      -    low  N     Y   N        opt  Y     N
105      2   10FL   half      -    low  N     Y   N        opt  Y     N
106      2   10FL   half      -    low  N     Y   N        opt  Y     N
107      2   10FL   half      -    low  N     Y   N        opt  Y     N
108      3   10FL   half      -    low  N     Y   N        opt  Y     N
109      3   auto   half      -    low  N     Y   N        opt  Y     N
110      3   auto   half      -    low  N     Y   N        opt  Y     N
111      1   auto   half      -    low  N     Y   N        opt  Y     N
112      1   auto   half      -    low  N     Y   N        opt  Y     N
113      1   auto   half      -    low  N     Y   N        opt  Y     N
114      1   auto   half      -    low  N     Y   N        opt  Y     N
*DLL = Disable TX if RX Link Loss                                  (*) = Default

_________[ESS_61007de9]_________          Process selections (Y/N): Y
Press Ctrl-U to configure VLAN groups     Press ESC to abort command & exit
```

The port types that are installed in the ESS and the default parameter settings for the ports are shown in the screen example above. These defaults can be changed by tabbing or cursoring to each field and using **<CR>** to toggle the field's contents to the desired parameter setting. The following tables provide the parameter definitions and options.

Ethernet Port Global Settings: VLANs Enabled			
Parameter	**Definition**	**Default**	**Range**
VLAN Enabled	Defines whether Tagged VLANs and traffic prioritization via 802.1Q and 802.1p are being used.	N (must be reset to "Y")	Y/N
Ageing Timer	The default ageing (timeout) of learned MAC addresses	5 minutes	None, 20s, 5m, 15m, 1h, 4h, 1d
HDX Back Pressure	Perform flow control for half duplex ports by inserting collision traffic	Disable (N)	Y/N
Ingress Priority	Defines mapping of the possible values (0-7) of the priority field of incoming frames tagged per 802.1p into the two priority levels of the ESS, L (low) or H (high) (see Section 5.1.4)	LLLLHHHH (for values 0,1,2,…7 respectively)	L (low) or H (high) for each value, as per position, 01234567
Egress Priority	Defines mapping of High or Low priority of ESS into the values (0-7) of previously untagged frames that egress the ESS, per 802.1p. (see Section 5.1.4)	L=0 H=4 (0/4)	L=0-7 H=0-7

Ethernet Port-Specific Parameters: VLANs Enabled			
Parameter	**Definition**	**Default**	**Range**
Port Number	The port number corresponds to physical port as labeled 101-126.	Read only	101-126
VLAN	Defines the VLAN ID that will be assigned to all previously untagged frames that ingress the ESS on this port.	VLAN ID 1 (default for all ports)	1-8192
Speed	Speed is fixed for fiber/gigabit interfaces. Speed may be defined for copper 10/100 interfaces.	Auto-detect	10, 100 or Auto
Duplex	Defines the type of equipment infrastructure as half or full duplex.	Auto-detect	Half, Full or Auto
Pause	For Full Duplex ports, flow control is optionally implemented using the 802.3x specification for Pause packets.	Enabled (Y) on full	Y/N

	When congested, the switch will send Pause packets to attached devices to request temporary suspension of transmission of further frames.	duplex ports	
Priority (Pri)	The ESS has high and low priority queues. Traffic is assigned to high vs. low priority based on the setting of the receive port. This parameter sets the priority of incoming traffic on this port.	Low (L)	High (H)/ Low (L)
DLL	Disable TX on Link Loss (DLL) feature will immediately deactivate its TX interface of a port when the receive signal is lost. This is useful for automatic link recovery procedures.	Disabled (N)	Y/N
IP	IP parameter allows this port to participate with the internal IP router. The internal Router can be used to support remote IP access to the Console system or used to route frames between VLANs.	Y ** Enabled	Y/N
Bridge (BRG)	This parameter sets whether this port actively participates in Spanning Tree Protocols.	None: No active STP/RSTP (N)	Y (STP) R(RSTP) L(LAN) E(edge) N(none)
Ingress Tags Req'd	Indicates whether frames entering the ESS on this port are required to have 802.1Q tags already applied.	Opt (Optional)	Opt or Req (Required)
Ingress Tags Security	Indicates whether the 802.1Q tags should be checked against VLAN membership and non-matching frames should be discarded (not allowed).	Yes (Y) Check membership	Y/N
Egress Tagging	Indicates whether frames leaving this port should have 802.1Q tags left on or stripped before egress.	No (N) Remove tags	Y/N

** Note: For IP routing to be active, IP addresses must be assigned. Other restrictions may also apply to IP routing. See Section 5.3 for IP Router configuration options.

Bridging

The Bridging parameter (BRG) in the **Ethernet Switch Port Configuration** screen defines the mode of Spanning Tree Protocol (STP) or Rapid Spanning Tree Protocol (RSTP) the switch will use on this port. There are five settings that can be established on a port-specific basis. These settings are the same with VLANs Enabled and VLANs Not Enabled. For descriptions of this parameter, see the discussion of Bridging in Section 5.1.1, above.

Basic VLANS

Basic tagged VLANs are very similar to Port Groups described above. In the most basic configuration, devices attached to the ESS are not themselves aware of being a member of a VLAN and do not participate in creating or interpreting VLAN tags. Rather, the ESS port is provisioned to assign a VLAN membership to the device attached to that port, or more specifically to the frames that enter the network on that port. The ESS and other interconnected tagged VLAN switches then create a "VLAN" or Virtual Local Area Network where frames are only MAC-layer switched among ports of the same VLAN. Typically, the devices attached to the ESS have no visibility to devices that are not part of their VLAN except and unless the traffic is routed by an IP router. (Note that unlike most Ethernet switches, the ESS has an embedded IP routing function that can route traffic among VLANs if that is desired. See Section 5.3.)

The main differences between tagged VLANs and Port Groups described in section 5.1.1 is that with Tagged VLANs, the frames are assigned a 'tag' or an additional field in their header per 802.1Q. This tag allows VLAN membership to be associated with a frame rather than a port, and this VLAN membership information can be passed to other devices in an interconnected network. Most commonly, tags are used to allow shared trunks among Ethernet switches to carry traffic for multiple VLANs on a shared basis without compromising the security of the VLANs, i.e., the VLAN traffic is logically separate and the VLAN membership can be screened as required in the downstream Ethernet switch. For more information on configuration of VLAN Trunking, see Section 5.1.3.

As a default mode when using Tagged VLANs, all ports are assigned to VLAN number 1. With all ports in the same VLAN, the ESS behaves as it would with no VLANs, i.e., all traffic is allowed among all ports. Using the Port Configuration screen, each port may be assigned an alternative **VLAN Number**. VLAN numbers assigned to ports may range from 1 to 8192. This VLAN number will be applied to all incoming frames that do not have previously marked 802.1Q tags (which typically is the case for all frames coming into an ESS from a device other than another VLAN-enabled Ethernet switch --- special cases are noted below). All ports that the operator wishes to secure from general traffic should be assigned to a VLAN other than VLAN 1. All ports that the operator wants to participate in a specific VLAN must be assigned the same VLAN number.

VLAN Tagging Options

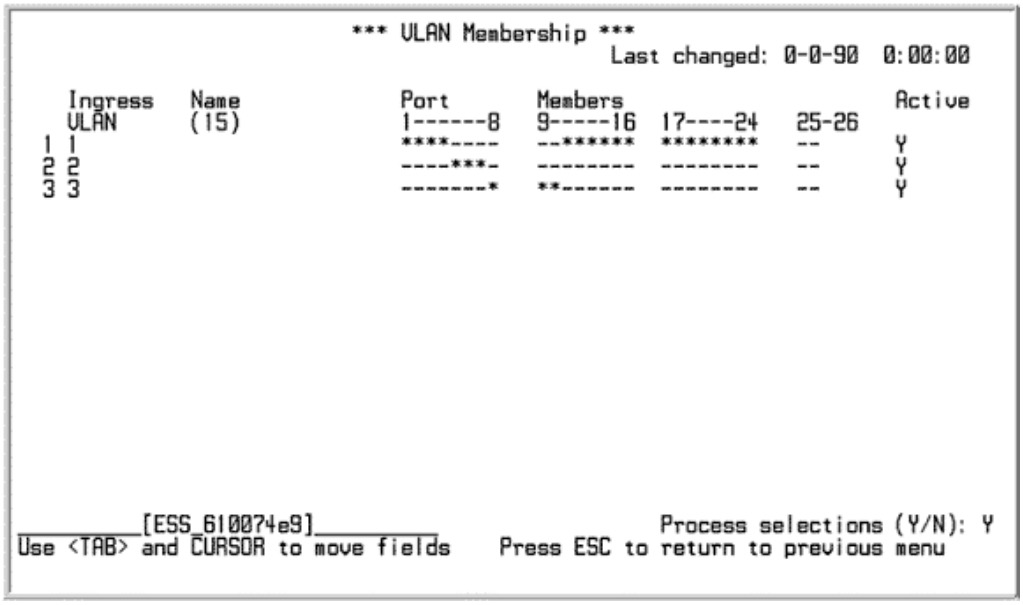
There are three additional configuration parameters associated with VLANs, two dealing with ingress tags and one with egress. The **Ingress Tag Required** parameter indicates whether frames on a given port are required to already have an 802.1Q tag in their header. Similarly, the **Egress Tagging** parameter indicates whether frames leaving a port should contain an 802.1Q tag in their header, or alternatively have any such tag removed by the ESS as the frame leaves the switch. For the case of Basic VLANs, the devices attached to the ESS will not be VLAN-aware (i.e., will not create or expect to see VLAN tags). In these cases, the Ingress and Egress parameters should be left at their default values: "Optional" (rather than "required") for ingress tags and "No" (meaning remove tags) rather than "Yes" (meaning leave tags intact) for Egress Tagging.

The primary use of the Ingress and Egress Tag parameters other than the default settings is to configure VLAN trunks as described in Section 5.1.3, below. In some cases, other devices attached to the ESS may be "VLAN Enabled" and create and interpret 802.1Q tags. In these cases, the Ingress Tagging may be set to either Required or Optional (depending on the application) and Egress Tagging should be set to "Y". Using values other than the default should be done with caution and with some knowledge of the operation of 802.1Q VLANs.

The other related parameter is the **Ingress Security** parameter. This indicates whether the ESS should enforce filtering of frames based on the provisioned VLAN membership. In general, this parameter should always be left at the default setting of "Yes" since VLAN membership should always be enforced. In the case where VLANs are not being actively used, but 802.1Q tagging is still being performed (e.g., when 802.1p traffic prioritization is used, which also depends on tags), then all ports should be assigned to VLAN 1 so that default security will permit all traffic among all ports. (Note: some network operators may find the Security field useful in debugging VLAN configurations or to create other special applications. However, this parameter should be set to "No" only with caution and knowledge of the workings of 802.1Q VLANs.)

VLAN Membership Verification

When using multiple VLANs, it is a good idea to verify that the VLAN membership has been configured correctly by using the **VLAN Membership** screen. This screen is accessed from the **Ethernet Switch Port Configuration** screen (when VLAN Enabled is "Y") by entering **<CNTL-V>.** A screen similar to the following will appear.



All of the VLAN ID numbers that are recognized by the ESS are listed on this screen. Each physical port is listed across the top creating a column per port. (Note that to conserve space, physical port numbers 100-126 correspond to columns numbered 1-26.) An "*" (asterisk) in a column indicates this VLAN is the default VLAN for this port. A "-" (hyphen) indicates that the port is not a member of this VLAN. A "+" (plus sign) indicates that the port is also a member of this VLAN, but not as the primary (default VLAN) for this port. The primary (default) VLAN represents the VLAN number that will be assigned to any unmarked frames entering the ESS on this port (unless Tagging Requiring is set to "Y", in which case untagged frames will be discarded anyway). The other VLANs that a port is assigned to are used as VLAN filters. Assuming VLAN Security is set (parameter is "Y"), then frames for VLANs in which the port is not a member will be discarded. In most cases, ports will belong to their primary (default) VLAN only. The main application for a port belonging to multiple VLANs is for VLAN Trunks, as described in Section 5.1.3.

5.1.3. VLAN Trunk Provisioning

In general, 'trunks' are Ethernet connections between adjoining Ethernet switches, whether the switches are both DYMEC ESS or other comparable devices. "VLAN Trunks" are Ethernet connections (trunks) from one Ethernet switch to another that support 802.1Q tagged frames and enable multiple VLANs to securely share the trunk and/or support 802.1p frame marking for traffic prioritization. VLAN Trunks require 802.1Q tags, both on frames that enter on a trunk port and egress on a trunk port. This in contrast to Basic VLAN ports described above which typically do not use tagged frames between the ESS and the attached device. With VLAN trunks, the frame tag is how VLAN membership and/or traffic priority regarding the frame is passed on to the next switch in the network.

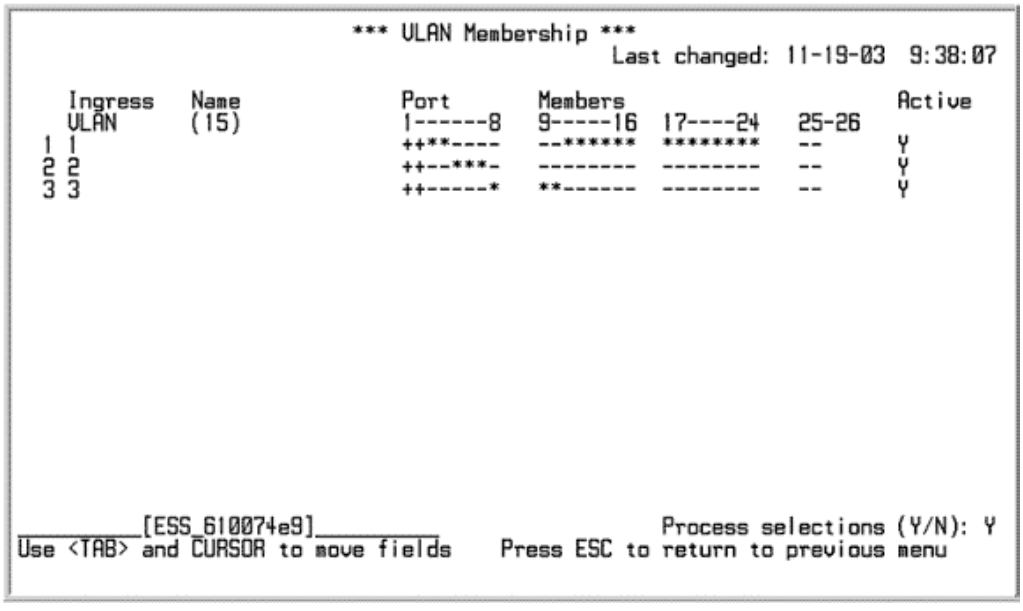
There are two main steps that are required to define VLAN trunks besides general Port Provisioning described above (using the **VLAN Enabled** procedure in Section 5.1.2).

- Enable ingress and egress tags on the port configuration screen
- Set the VLAN Membership for the trunk to include all VLANs

On the **Ethernet Switch Port Configuration** screen (with VLANs Enabled), for the ports that represent VLAN trunks, set:

- Ingress Tagging to "Req" (for required)
- Ingress Security to "Y"
- Egress Tagging to "Y" to propagate tags onto the trunk

Access the **VLAN Membership** screen from the **Ethernet Switch Port Configuration** screen by entering **<CNTL-V>.** A VLAN Membership screen similar to the following will appear. For each Port that represents a VLAN Trunk, toggle the VLAN Membership entries so that there is a "+" (plus sign) in all entries of the column associated with that port, indicating that the trunk port is a member of all VLANs. This is illustrated in the following screen for a switch with three VLANs and two trunks, with Ports 1 and 2 representing the trunks.



Note: ***In some cases it may be necessary to add additional VLANs to the VLAN membership table.*** In a network of several switches, some switches may represent pass-through or transit nodes for VLAN traffic where no members of that VLAN are local ports on that switch. (For example, this could occur in a large ring configuration of several switches.) These distributed VLANs have members on other switches in the network, but not on this particular switch. In order for this VLAN traffic to be switched through the transit switch without being filtered out (discarded), the trunks must be defined as members of these distributed VLANs. To do this, simply type a new line into the VLAN Membership table, starting with the VLAN Number of the distributed VLAN. Then toggle the VLAN membership for the Trunk Ports such that the Trunk Ports are included in this new VLAN. Do not make any of the other local ports members of this new VLAN.

5.1.4. Priority Management using 802.1p

In many ways, traffic prioritization using 802.1p is similar to basic traffic prioritization described in Section 5.1.1. ESS ports are marked as High or Low priority in the **Ethernet Switch Port Configuration** screen and all traffic entering the switch on that port then carries an output queuing priority of either High or Low. However, basic prioritization in 5.1.1 only has meaning within a single switch. By contrast, with 802.1p, frames are marked with a priority tag that can be passed onto other switches (via VLAN tags) or even to other end devices attached to the ESS. The High/Low queuing priority can then be maintained at all points along the network path.

802.1p Port Configuration

To implement traffic prioritization using 802.1p, there are two main requirements:

- Set the Priority parameter for each port to High or Low
- Create VLAN trunks between all Ethernet switches in the network

To set the Priority parameters, use the **Ethernet Switch Port Configuration** screen (with VLANs Enabled = Y) and toggle the Priority column to either H or L for each port, as desired. 802.1p Priority Tags will be internally generated for each frame arriving on these ports.

To pass the priority tags to other switches, configure VLAN Trunks as described in Section 5.1.3. The priority tag is a sub-field of the 802.1Q VLAN tag, so 802.1Q VLANs must be enabled in order for 802.1p prioritization to function. If you are not using VLANs, you must still use VLAN Enabled provisioning and activate 802.1Q. However, you would leave all ports (including the trunk ports) as members of VLAN number 1 (the default VLAN). All traffic would then be allowed among all ports, but VLAN tags will be created within the network to carry the 802.1p priority information.

Global Priority Parameters

On the **Ethernet Switch Port Configuration** screen, there are two global parameters that deal with Priority, both on the fourth row near the top of the screen. These define the mapping between the ingress and egress 802.1p tag values of 0-7 and the internal ESS priority values of high/low. These parameters have recommended default values, but may be customized for specific applications. The 802.1p priority field is a three-bit field with values 0-7 where in general use 0 means “no assigned priority” and the values 1-7 indicate ascending relative priority, with 7 having the highest priority.

The **Priority: Ingress Tag** field controls how the switch treats frames that come into a switch port with an 802.1Q tag (thus having an 802.1p priority field). This generally occurs only with traffic arriving from upstream switches across VLAN trunks, although some other attached

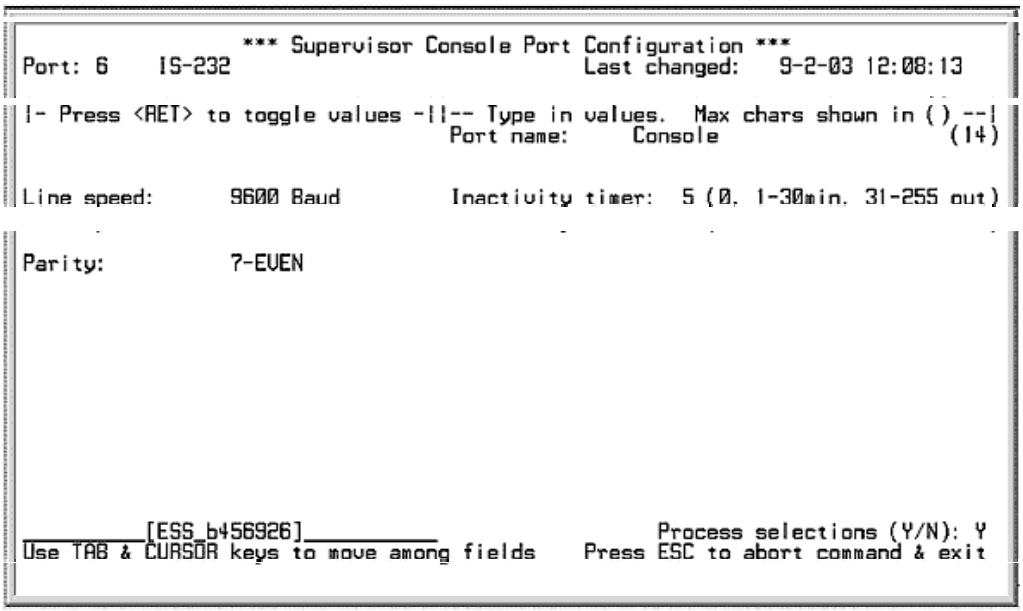
devices may also create tags. (For most locally attached devices, incoming data is not tagged and the priority is taken directly from the High vs. Low Priority parameters set for that associated port in the Ethernet Switch Port Configuration screen.) The 802.1p priority field of incoming frames may have any value from 0 through 7. The **Priority: Ingress Tag** parameters define how these values are mapped into high or low priority within this switch. (Note that if the data is forwarded on to downstream devices that support tags, the 802.1p priority value is forwarded unchanged.)

The **Priority: Ingress Tag** entry on the **Ethernet Switch Port Configuration** screen shows the eight positions corresponding to the values 0-7 (01234567) with a default setting of LLLLHHHH. This indicates that values 0-3 are mapped locally to a Low priority and values 4-7 are mapped locally to a High priority. The operator can modify these defaults by toggling each position to the H/L setting that is desired for the corresponding 802.1p priority field value.

The **Priority: Egress Tag** field defines the 802.1p priority value that will be set on tags created by the ESS. This occurs when the frames enter the ESS without a tag and then egress the switch on a tag-enabled port, most typically a VLAN trunk. (As stated above, frames that both enter and leave the ESS on tag-enabled ports will be forwarded with their tag unchanged.) In the **Ethernet Switch Port Configuration** screen, each port is assigned a priority of Low or High (L/H). The ESS uses these settings to define the priority values of tags the switch creates. The **Priority: Egress Tag** parameter on the **Ethernet Switch Port Configuration** screen shows two values for L/H. The defaults are "0/4" meaning that frames entering on an L (low) port will be marked with a 0 priority and frames from an H (high) priority port will be marked with a "4" value. The operator can change the values set for L and H traffic by toggling each parameter to any value of 0-7.

5.1.5. Console Port

To access the console port configuration, select **Port 6** in the **Configure Port** screen. The following display is shown:



The only configurable options on this menu are described in the following table. This port is always configured for the console and is a fixed DTE interface. Although this port is primarily used for access to the configuration menu, this port can also be used to host Telnet sessions and can be used to PING IP devices.

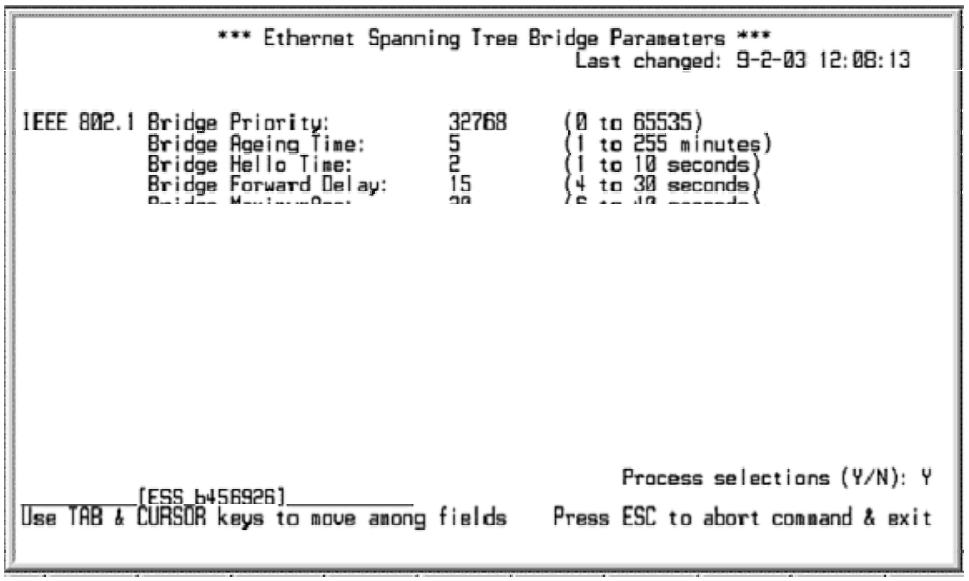
Console Port Parameters			
Parameter	**Definition**	**Default**	**Range**
Port Name	The display name for this port within the Supervisor application menus	Console	14 characters
Speed	Speed of the RS-232 port	9600	Toggle values 600-38.4k bps
Parity	Parity setting for consoles port.	7-EVEN	Toggle values
Inactivity Timer	Timer for inactivity, after which the port will be logged off automatically.	5 minutes	0 (disable), 1-30 min (applies to both Tx and Rx traffic), 31-255 min (applies to Tx traffic only)

5.2. Bridge (STP)

The **<3> Bridge** sub-menu of **Configuration Commands** provides access to parameters associated with the Spanning Tree Protocol (STP). In compliance with IEEE 802.1d or 802.1w (RSTP), the ESS sends and receives data messages called STP Bridge Protocol Data Units (BPDUs) at a regular, user-defined interval and calculates the best loop-free path throughout the network. Switches in the network use the BPDU information to determine if multiple active paths exist between switches and then provide STP settings that block the least desirable redundant paths so loops are not created.

Once STP is enabled on selected ports, the ESS is self-configuring. On power-up, the ESS learns the location of all nodes (e.g., LAN workstations) by examining network traffic and building address tables. It then determines the best loop-free path for sending information across complex network topologies and allows for bridging traffic over all available paths while ensuring that undesirable loops are not created. If a link fails, an automatic reconfiguration function calculates the next best route and unblocks the appropriate path, bridging traffic over another link.

The **<3> Bridge** selection leads to the **Ethernet Spanning Tree Bridge Parameters** screen. This screen allows customization of STP parameters, although the default parameters are usually appropriate. To change parameter values, tab or cursor to the appropriate field and toggle to the desired parameter value. The parameters and their options are defined in the table below.



Spanning Tree Parameters			
Parameter	**Definition**	**Default**	**Range**
Bridge Priority	Used by the IEEE 802.1d spanning tree algorithm to determine the root of the interconnected network. Bridge priority provides a means of assigning a relative priority to each bridge within the set of bridges in the bridged LAN. Enter 1 for the Root node only.	32768	0-65535
Bridge Aging Timer	Value that the bridge uses to automatically remove end stations (i.e., Ethernet addresses) after the last activity from/to the end station. The aging timer allows an end station to move to another LAN or become inactive.	5 min	1-255 minutes
Bridge Hello Time	The amount of time between the transmission of configuration BPDUs on any port.	2 sec	1-10 seconds
Bridge Forward Delay	Controls how long the bridge waits after any state or topology change before forwarding the information to the network.	15 sec	4-30 seconds
Bridge Maximum Age	Specifies the age of STP information learned from the network on any port before it is discarded.	20 seconds	6-40 seconds
Spanning Tree Protocol	Selects protocol to be used, either Spanning Tree Protocol (802.1d) or Rapid Spanning Tree Protocol (802.1w)	Normal (802.1d)	Normal or Rapid

Note: Each STP network requires one Root node for the STP. The Root node is typically selected as one of the nodes most central to the network topology. The Root node is designated by setting the Bridge Priority parameter to 1. In some cases, there may be a specific node designated as the primary alternative node should the Root node fail. This secondary Root may be designated by assigning a different Bridge Priority, greater than 1 and less than the default (e.g., 2).

Except for Root node designation, the default STP settings should work in most environments. The STP algorithm effectively uses the default values and the current state of the network to determine the best STP configuration. Adjusting the timers can affect the speed of topology change convergence throughout the STP network. Care must be taken to avoid loops under any circumstance. Adjustments should be made cautiously and with knowledge of overall network topology and link delays.

5.3. Router (IP)

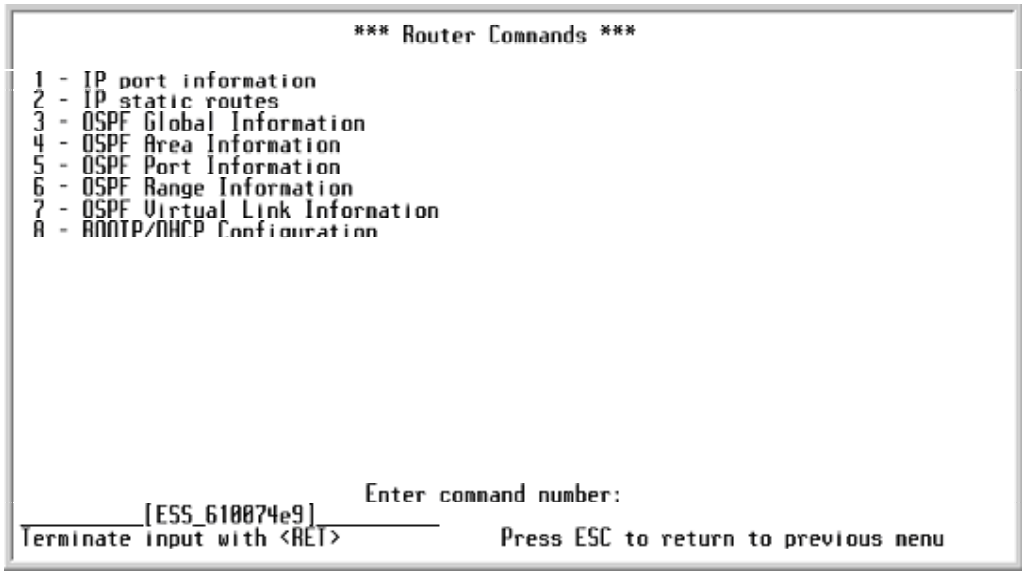
The ESS has an embedded IP router function. This is primarily used for connecting the ESS Supervisor application to an IP network for remote operator access and for remote access to SNMP traps and operating software downloads. The routing function may also be used by the other devices connected to the ESS for routing traffic beyond their specific bridged catenet or VLAN group. The IP routing function is not wire speed at Ethernet port rates, but is useful for networking of telemetry, Telnet and other moderate bit rate applications to/from connected devices. In particular, the routing function may be useful for allowing a single system operator to have Telnet supervisory access to a number of remote devices which otherwise are segregated into different VLANs with no facility for cross-VLAN communications.

One key decision in configuring ESS IP routing is to set the scope of access to the routing function. By default, all Ethernet ports are in one group, share the ESS system IP address and have access to the routing function for routing outside their bridged network. Individual ports may be disabled from the IP routing function by using the **Ethernet Switch Trunk Configuration** screen described above. Routing may be further restricted using the **IP Filter** features described in the Section 7, Security. When Port-based VLAN groups are used and you want these specific groups to participate in IP routing, IP addresses must be assigned separately for each VLAN group, as described below. There are no default IP addresses for VLANs and ports assigned to VLANs will not be able to route (except to the ESS supervisor) until a VLAN IP address is assigned.

A second key decision is to define the routing protocol. By default, routed ports are defined to use RIP as their routing protocol. When RIP is defined, no further routing parameters are required. The other two options are Static Routing and OSPF routing. Each of these require filling in additional configuration screens.

In addition to basic IP routing, the ESS also supports BootP Helper and DHCP Server functions to assist devices that are attached to the ESS in obtaining IP addresses and other parameters required for effective routed operations. BootP and DHCP functions are configured in the ESS as part of this IP Router section.

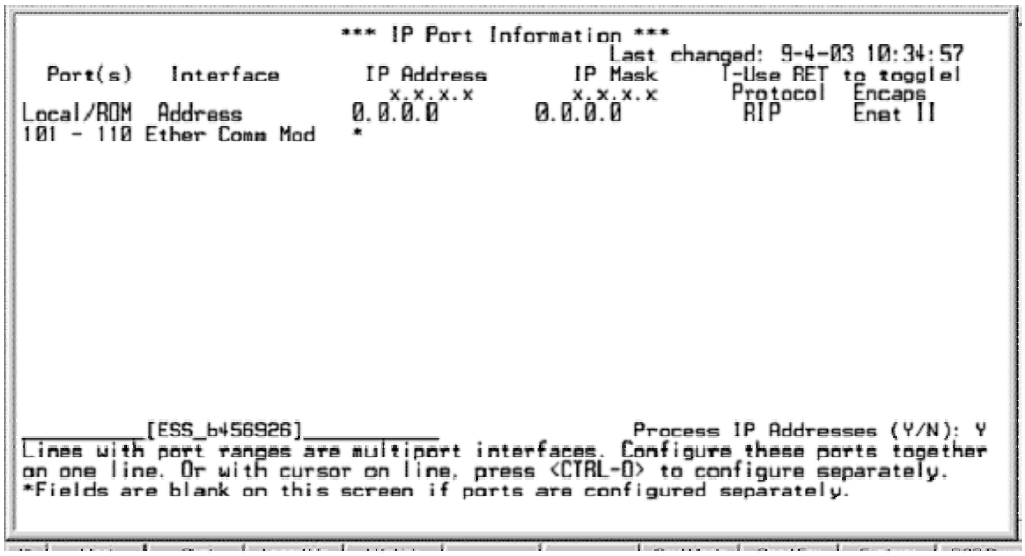
IP router configuration is accessed selecting from the **Main** menu by **<3>** Configuration and then **<2>** Router. The following display shows the various router configuration commands.



The IP addresses and routing protocols are assigned via the **<1> IP Port Information** sub-menu. The **<2> IP Static Routes** and **<3> through <7> OSPF** sub-menus are only required when Static or OSPF routing are used, respectively. These are not used when no routing or default RIP routing is used. **<8> BOOTP/DHCP** sub-menus are also only needed if the respective helper/server tools are to be used. The defaults are that these services are not enabled.

5.3.1. Assign IP Addresses and Protocols

To assign IP addresses to ESS ports that have been enabled for IP support, select option **<1> IP Port Information** from the **Router Commands** menu.



The entry **"Local/ROM Address"** allows configuration of an IP address that the Boot ROM will use during initial Boot sequence. This address can be useful for upgrading an ESS, for remote Telnet access to the console, and for SNMP communications with the ESS.

NOTE: While the IP address may be entered via the initial Boot process (as described in Section 4.2 *Initializing an IP Address),* that process does not permanently save the IP address for the system. This command screen allows the system IP address to be defined and permanently saved.

The second entry **"Ether Comm Mod"** applies to all external Ethernet ports. (The term Ethernet Communications Module refers to the physical hardware of the Ethernet ports.) Providing an IP address for these ports enables Supervisor access via these ports or routed traffic among any of the Ethernet ports that are enabled for IP routing. As described separately below, specific IP addresses may be assigned to individual Port Groups or VLANs.

For each of these entries, cursor to the appropriate entry and enter the designated IP address and sub-net mask.

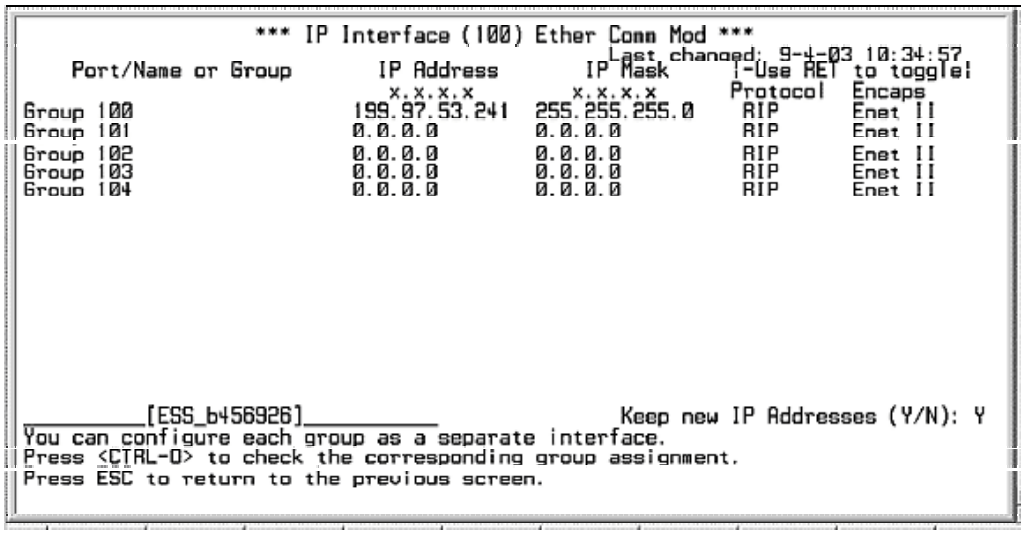
When an address is entered, RIP will appear as the default protocol and Enet II will appear as the default encapsulation. If RIP is the desired routing protocol, no further action is needed.

If RIP is not the desired routing protocol, toggle this field to select the desired entry: RIP, RIP-II, RIP-RX (receive-only RIP) or **"None."**

"None" is the correct entry if no dynamic forwarding of routing information is desired AND if either **Static Routing or OSPF** is desired. No entries exist on this screen to explicitly select either Static or OSPF routing.

If the switch has been segmented into **Port VLANS groups**, then you must access a separate Group IP entry screen from the IP Port Information screen. When in the **IP Port Configuration** screen, place the cursor in the IP Address field of the "Ether Comm Mod" entry and press **<CNTRL O>.** This will bring up an **IP Interface (100) Ether Comm Mod** screen as shown below. This screen has a separate entry for each VLAN group. Group 100 is a default group for all Ethernet ports. The other Groups are those defined in the Ethernet Switch Trunk Configuration screen described in Section 5.1.1.

For VLAN IP address assignments, cursor to the IP address entries that you wish to define and enter the address and mask, as well as the desired routing protocol. Note that different groups may use different routing protocols. However, the ESS only has one instance of each routing protocol, e.g., all groups that use RIP use the same RIP tables; all groups that use Static Routing share the same static routes.



5.3.2. Static Routing

As described above, the IP router can use RIP (the default), RIP-II, RIP-RX, OSPF, Static Routing or no routing protocol. Different VLAN groups can use different routing protocols, including Static Routing, but only a single instance of the routing protocol is used for all groups that share it. Specifically, there is only one Static Routing table for the ESS. This section describes how the ESS Static Routing Table is defined.

To establish Static Routes for IP routing, enter **<2> IP Static Routes** at the **Router Commands** sub-menu. The following screen will appear.

```
                          *** IP Static Routes ***
                                                Last changed: 9-26-03 12:24:33
    IP Address            IP Mask               Next Hop            Hops
     x.x.x.x              x.x.x.x               x.x.x.x           (0 - 15)
 1: 199.97.53.0           255.255.255.0         66.3.22.1           1
 2: 0.0.0.0               0.0.0.0               89.102.1.1          1
 3:
 4:
 5:
 6:
 7:
 8:
 9:
10:
11:
12:
13:
14:
15:
Note: x = 0-255
__________[ESS_b456926]__________          Process Static Routes (Y/N): Y
In IP address field, use UP/DOWN to scroll and LEFT to process selections.
To change or add entry, enter new value      Use <CTRL-D> to delete entry
Use TAB & CURSOR keys to move among fields   Press ESC to abort command & exit
```

This screen is used to define one static route per line of the table. Up to 120 static routes can be configured. For each route, enter the following information on a single line:

- In the **IP Address** column, enter the IP address of the remote network.
  - A default mask appears. If required, modify the IP mask for subnetting.
  - Note: A static route of 0.0.0.0 can be used as a default route for routing any IP address that does not have a match in the routing table.

- Under **Next Hop**, enter the IP address of the remote IP port used to access the IP network specified in this procedure. This will generally be the IP address of a router directly connected to the same switched Ethernet network, but not necessarily directly attached to this ESS.

- In the **Hops** column, enter the number of hops to the remote network using this static route.
  - If the number of hops entered here is greater than the number of hops in a dynamic route (using RIP) to the same IP network, then the dynamic route will be used.

- When you have completed your configuration, enter **Y** in the **Process static routes** field and press **<return>**.

After entering IP routes, it is a good practice to verify the routing information. From the Main menu, select <1> Status Commands, then **<3> Verify Names and Addresses** sub-menu (M,<1>,<3>. These are described in Section 6.3.

In many cases where Static Routes are used, IP Address Filters are also used. **IP Filters** are defined in **Section 7, Security**.

5.3.3. OSPF

OSPF (Open Shortest Path First) is a routing scheme that operates over the IP protocol. It is a link state metric protocol that makes routing decisions based on link capacity, delay and throughput requirements, the number of data units presently in queue for transmission over a particular link, the number of hops required to reach a destination, and the ability to reach gateways and routers along the route. To take network dynamics into account, OSPF includes a weighting factor for each route. OSPF is considered a more robust protocol than RIP, which makes routing decisions based only on the number of hops to a destination.

To improve network efficiency, OSPF selectively limits route status messages and uses network partitioning and subnetting to control the amount of traffic and memory required to update router information. For example, one router can be designated to exchange routing tables with a local gateway, cutting down on the congestion that might occur if all routers exchanged routing information with the gateway. As another example, Link State Advertisements are distributed only when there has been a change to network status. Further, if networks are designed correctly, sub-network status messages can be sent in a single Route Summarization message.

NOTE: These setups require an experienced Network IT Administrator.

OSPF configuration needs to be done in the following order:

1. **IP Address (required)**
2. **OSPF Global Parameters (required)**
3. **OSPF Area Parameters (required)**
4. **OSPF Port Parameters (required)**
5. **OSPF Range Parameters**
6. **OSPF Virtual Link Parameters**

Each of these steps corresponds to a unique selection on the **<3> Router Commands** screen . (M,<2>,<3>) IP addresses are assigned on the **IP Port Information** screen described above. The other five steps have their own **Router Commands.** These will each bring up a screen with parameters that are defined in the corresponding tables provided below. The parameter names and the default and optional values are given on the menu screens. Parameters descriptions are provided in the following tables.

OSPF Global Information			
Parameter	**Description**	**Default**	**Range**
Router ID	OSPF router ID for this ESS distinguishing it from all others in the Autonomous System. This is typically the primary IP address of the ESS.	0.0.0.0	0.0.0.0 - 255.255.255.255 (4 bytes)

Route Sharing	If set to Yes, routing information is exchanged with the ESS's RIP router.	N	Y, N
Automatic V-Link	If set to Yes, enables automatic generation of virtual links. (Virtual links are required to restore backbone connectivity when the Autonomous System is divided into non-contiguous areas.) NOTE: To be able to configure virtual links, the ESS must be an area border router. If this parameter is set to No, all required virtual links must be configured manually.	N	Y, N

OSPF Area Information			
Parameter	**Description**	**Default**	**Range**
AreaID	IP-like address unique to this particular area. The backbone area is typically set for 0.0.0.0	0.0.0.0	0.0.0.0 - 255.255.255.255 (4 bytes
Authentication	If set to None, no password is required. If set to Simple, a password must be defined on the OSPF port configuration menu, and all packets sent on the network must carry this value in the OSPF header.	None	None, Simple
Import AS	If set to Yes, AS (Autonomous System) external advertisements are flooded through this area. The parameter must be set to Yes for the backbone and areas connected to the backbone by a virtual link. Set to No for a Stub area. Routing tables will maintain information for the entire area, regardless of the value of this parameter.	N	Y, N
Stub Metric	Applies to stub areas only. Determines the routing "cost" of the default line. Stub areas are areas into which OSPF does not flood AS (autonomous system) external advertisements. You might want to configure stub areas if much of the topological database consists of AS external advertisements, and you want to minimize the size of the topological databases on an area's routers.	0	1-255

OSPF Port Information			
Parameter	**Description**	**Default**	**Range**
OSPF	Indicate type of OSPF routing enabled on this interface. Set to Broadcast for ESS/LAN ports and Point-Point for WAN ports.	Broadcast	Broadcast Point-Point None
AreaID	Identifier of OSPF area to which the port (interface) belongs, as defined in the Area parameters. 0.0.0.0 is the backbone area.	0.0.0.0	0.0.0.0 - 255.255.255.255 (4 bytes)
Priority	Priority used to determine whether this router will become the network's designated router. 0=this router is ineligible to be the designated router. 255 is the highest priority. 255 means that this router is responsible for sending network link advertisements, which describe all the routers attached to the network. These advertisements are flooded throughout a single area. At least one router on each logical IP network or subnet must be eligible to be the designated router.	0	0-255
The following parameters are toggle fields under the "Parameter" column:			
Transit (Transit Delay)	How often Link State Advertisement packets are sent over this interface. This interval determines the maximum packet transmission rate on an interface, which affects network stability. Because packets are built at the instant of transmission, only the latest information is sent even if the transmission is delayed.	1	1-3600 seconds
Retran (Retransmit Interval)	The time between retransmissions of link state advertisements when an acknowledgment is not received. This parameter is used for adjacencies that belong to this interface and for retransmissions of OSPF Database Description and Link State Request packets. Set this parameter to a value that is higher than the expected round-trip delay between any two routers on the network attached to this port. Otherwise, needless retransmissions will occur. The default value, 5 seconds, is appropriate for a LAN connection. Low-speed links require a higher value.	5	1-3600 seconds
Hello (Hello Interval)	The length of time, in seconds, between Hello packets that the ESS sends on this interface. Must be the same value for all routers connected to this interface. If you set the Hello Interval to a short length of	10	1-3600 seconds

	time, changes to the OSPF topological database will be detected more quickly, but more OSPF routing protocol traffic will be generated. The default value, 10 seconds, is suggested for a LAN connection.		
Dead (Dead Interval)	The length of time, in seconds, before neighboring routers declare a router down when they stop receiving its Hello Packets. The value of the Dead Interval parameter is advertised in Hello Packets sent out from this interface and must be the same on all other routers connected to this interface. Set the Dead Interval to a multiple of the Hello Interval.	40	1-3600 seconds
Metric	Cost, or weight, of sending a packet on this interface. NOTE: The same basis for determining the metric (for example, speed, throughput, or line cost) should be used throughout the network.	1	1-65535
Password	Eight-character authentication: Must be the same for all routers in an area.	No value	0 to 8 ASCII characters
OSPF Range Parameters			
Parameter	**Description**	**Default**	**Range**
Range Net	Together with the Range Mask, identifies a group of subnets in this address range. Routers may belong to multiple areas, depending on their attached networks. When configuring the Range Net values for all address ranges, keep all subnetted networks in the same area. NOTE: Ranges are required only for those areas that connect to the backbone via an area border router.	0.0.0.0	0.0.0.0 - 255.255.255.255 (4 bytes)
Range Mask	Together with Range Net, identifies a group of subnets in this address range.	0.0.0.0	0.0.0.0 - 255.255.255.255 (4 bytes)
AreaID	Unique address as defined for this range.	0.0.0.0	0.0.0.0 - 255.255.255.255 (4 bytes)
Status	If set to Advertise, a single route is advertised for this address range on a summary link advertisement that is external to the area. If set to Hide, no route is advertised for this address range. This setting allows you to hide certain networks from other areas.	Advertise	Advertise, Hide

OSPF Virtual Link Parameters			
Parameter	**Description**	**Default**	**Range**
Transit ID	Unique area identifier for the area that the virtual link passes through.	0.0.0.0	0.0.0.0 - 255.255.255.255 (4 bytes)
Router ID	Router identifier for the other endpoint of the virtual link (neighbor ID)	0.0.0.0	0.0.0.0 - 255.255.255.255 (4 bytes)
The following parameters are toggle fields under the "Parameter" column:			
Transit (Transit Delay)	How often Link State Advertisement packets are sent over this interface. This interval determines the maximum packet transmission rate on an interface, which affects network stability. Because packets are built at the instant of transmission, only the latest information is sent even if the transmission is delayed.	1	1-3600 seconds
Retran (Retransmit Interval)	The time between retransmissions of link state advertisements when an acknowledgment is not received. This parameter is used for adjacencies that belong to this interface and for retransmissions of OSPF Database Description and Link State Request packets. Set this parameter to a value that is higher than the expected round-trip delay between any two routers on the network attached to this port. Otherwise, needless retransmissions will occur. The default value, 5 seconds, is appropriate for a LAN connection. Low-speed links require a higher value.	5	1-3600 seconds
Hello (Hello Interval)	The length of time, in seconds, between Hello packets that the ESS sends on this interface. Must be the same value for all routers connected to this interface. If you set the Hello Interval to a short length of time, changes to the OSPF topological database will be detected more quickly, but more OSPF routing protocol traffic will be generated. The default value, 10 seconds, is suggested for a LAN connection.	10	1-3600 seconds
Dead (Dead Interval)	The length of time, in seconds, before neighboring routers declare a router down when they stop receiving its Hello Packets. The value of the Dead Interval parameter is advertised in Hello Packets sent out from this interface and	40	1-3600 seconds

	must be the same on all other routers connected to this interface. Set the Dead Interval to a multiple of the Hello Interval.		
Autype	Authentication Type. If None, no password is required. If Simple, a password must be defined on the OSPF port configuration menu, and all packets sent on the network must carry this value in the OSPF header.	None	None, Simple
Password	Eight-character authentication: Must be the same for all routers in an area.	No value	0 to 8 ASCII characters

5.3.4. BootP / DHCP

The ESS can act as a BootP Helper and/or DHCP Server in order to provide temporary IP addresses and other IP-related parameters to devices attached to the ESS. From the **Router Commands** menu, **<9> BOOTP/DHCP Configuration** leads to a **BootP/DHCP** screen that prompts you to select either:

<1> Client/Helper Configuration (for BootP)

or

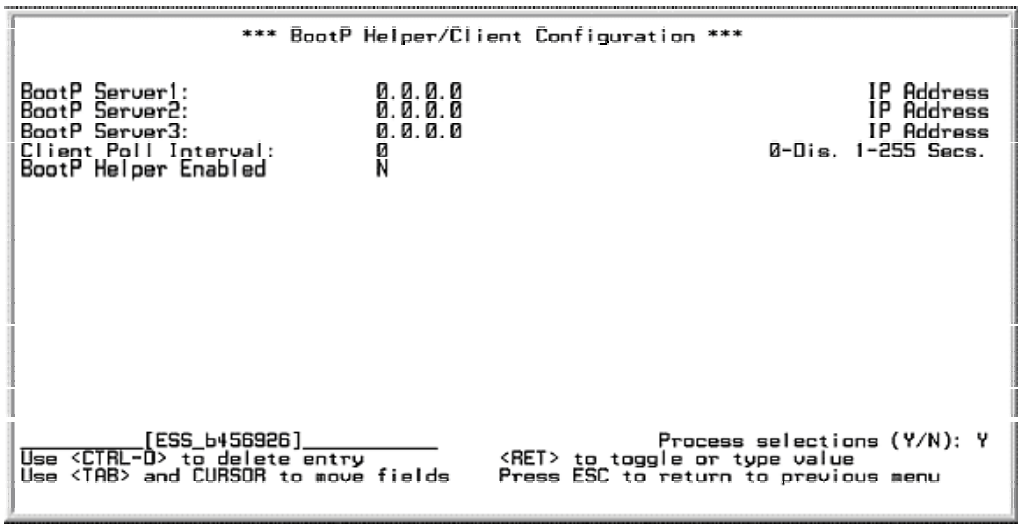
<2> DHCP Server Configuration

These lead to the following two sub-menu areas.

BootP Client/Helper

The ESS can act as a BootP relay agent to transfer BootP messages between clients and servers. BootP (Bootstrap Protocol or Boot Protocol) provides to the requesting device the path and filename of its bootstrap file, as well as its default router, its own IP address, and the BootP server's IP Address. BootP sends its messages in UDP headers enclosed in IP datagrams. In many cases, BootP clients and their associated BootP server(s) do not reside on the same IP network or subnet. The actual BootP server can be several hops away from the BootP client system. In such a case, an ESS can act as a relay agent to transfer BootP messages between clients and servers.

To configure the ESS to act as a BootP relay agent follow the procedure below, select <**1> Client/Helper Configuration** as described above. The following screen will appear. The remote IP addresses of up to three remote BootP servers may be specified. The helper can be enabled/disabled by operator command while keeping Server addresses stored for future use.

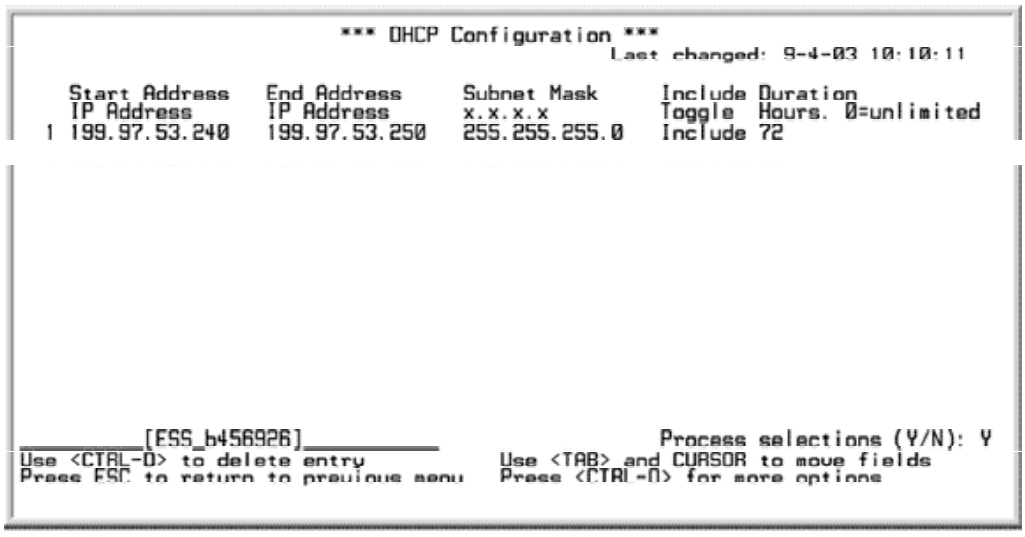


DHCP Server

This feature allows hosts connecting to the network to be automatically configured with an IP address, default route and the addresses of up to three DNS servers. Optionally, an IP address can be statically assigned to a particular MAC address.

Note: *The total number of IP Addresses that the ESS DHCP server will assign is 50. Addresses made available beyond a total of 50 will never be used.* The operator is not prevented from defining additional addresses, but only the first 50 will be assigned.

To configure the DHCP Server, select **<2> DHCP Server Configuration**, as described above. An example of the server screen is shown below:



This screen defines the IP addresses that are held by the ESS DHCP Server and allocated upon request to the devices attached to the ESS.

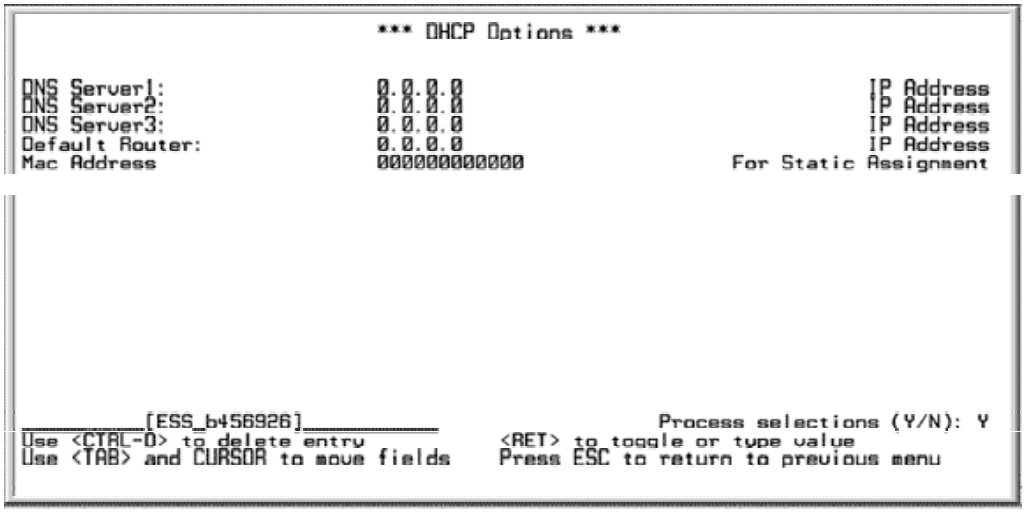
- This table may be populated with up to 15 entries.
    - Each entry may be a single IP address or a range of contiguous IP addresses (defined by the Start Address and End Address of the range.
    - To define a single address, enter the same address as both the Start and End address of a range.
- Each entry may represent addresses to **Include or Exclude**, indicated by toggling the Include field on each line.
    - For example, one line may provide a large range of addresses to be used by the server. Another line may exclude one or more addresses within the range from being assigned.
- The **duration** of the address assignment (lease) is configurable in hours.
    - The default lease is 72 hours.
    - An 'unlimited' lease is specified by entering '0' hours.

For each address or address range, additional parameters can be provided to the requesting device. These include:

- One to three DNS server addresses
- A default router address
- A MAC address for static assignment

These are configured using the **DHCP Options Screen**. This involves:

- Within the DHCP Configuration screen, place the cursor on the IP address range with which you want to associate additional parameters.
    - Note this procedure can be repeated for each address or address range.
- Press **<CNTL O>.** The **DHCP Options** screen will appear (example shown below).
- Enter the IP and MAC addresses as appropriate.



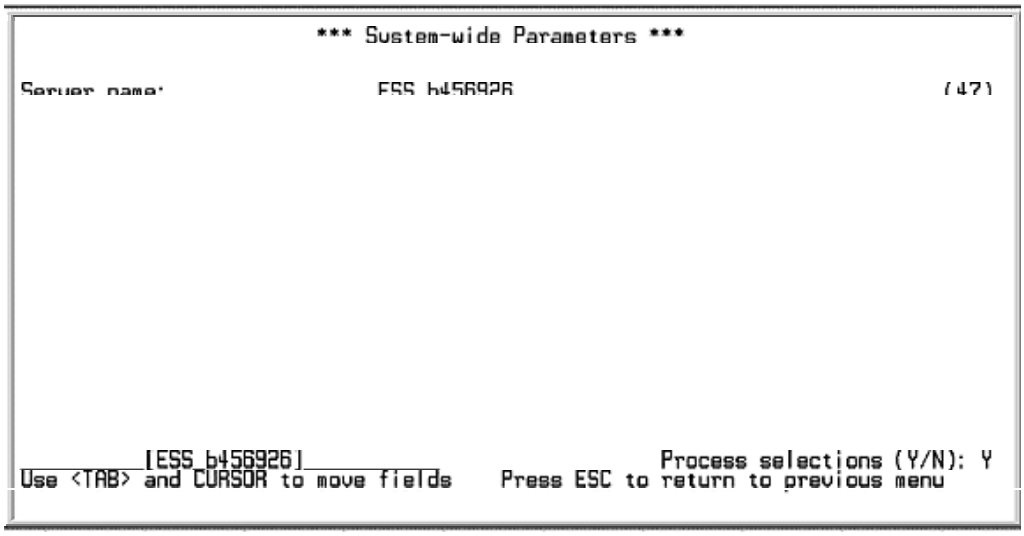
5.4. System Name and Herald

The **<4> Server** selection of the **Configuration Commands** screen allows the operator to change the Console Herald and ESS system name. This can be useful in a network of many systems where the name is modified to represent the equipment location.

- The **Server Name** (definable up to 47 alphanumeric characters) appears at the bottom of ESS Supervisor screens as a navigation aid. Spaces are not allowed in this name.

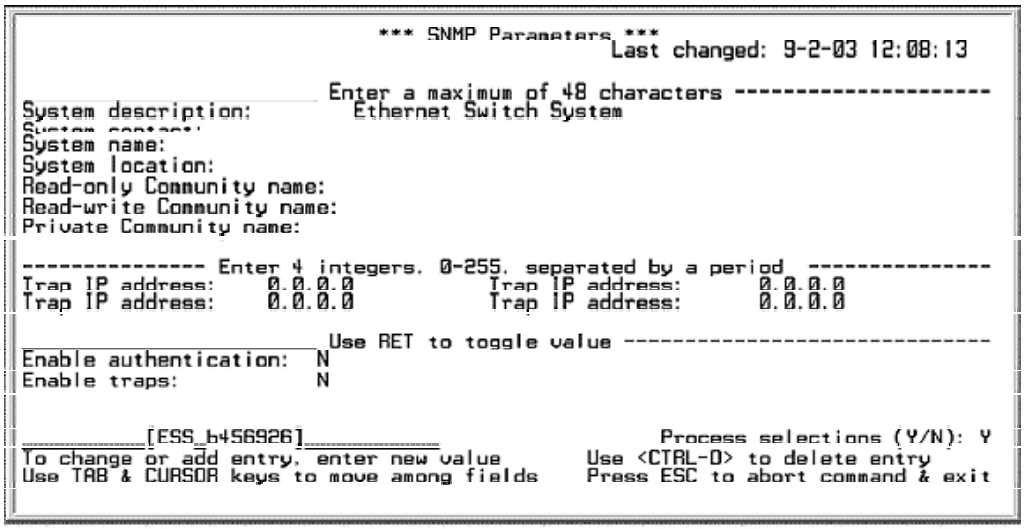
- The **Supervisor Console Herald** appears as a greeting on the initial ESS Supervisor Screen. This may be customized per ESS Supervisor to any alphanumeric name up to 32 characters.

The **<4> Server** selection sub-menu leads to the **System-wide Parameters** screen, shown below. Enter new name and herald text as desired. When done, set **Process Selections** to **<Y>** and enter **<return>.**



5.5. SNMP

This sub-menu allows you to setup the various SNMP parameters associated with this ESS. This setup will be necessary in order to use SNMP to configure the unit remotely or use the SNMP trap generator to report port Link Status changes to a remote network management server. The ESS can send TRAPS (Port status changes) to as many as four remote systems. Enter the IP address of the remote servers and enable the "Enable Trap" field. The Traps generated will include a status of up/down/time and Port Number.



Note: In order to use SNMP, the “Local/ROM Address” must have an assigned IP address as described in Section 5.3.1.

The definitions, defaults and permitted values of the SNMP Parameters screen are provided in the following table.

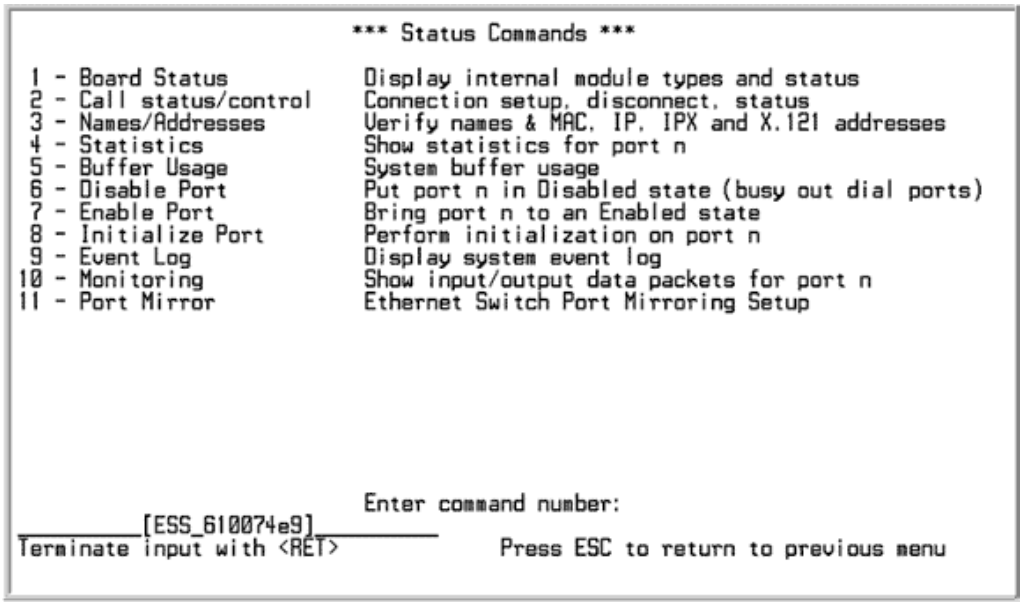
SNMP Parameter Definitions			
Parameter	**Description**	**Default**	**Range**
System Description	A textual description of the system used to set the MIB-II sysDescr variable.	Ethernet Switch System	48 characters
System Contact	The name of a contact person for the ESS, together with information on how to contact this person. It is used by the Supervisor to set the MIB-II sysContact variable.	null	48 characters
System Name	The identifier for the ESS that the Supervisor has used to set the MIB-II sysName variable.	null	48 characters
System Location	The physical location of the ESS (e.g., “telephone closet, 3rd floor”). It is used by the Supervisor to set the MIB-II sysLocation variable.	null	48 characters
Read-Only Community Name	Used by the SNMP agent as a simple authentication mechanism for read-only access to all MIBs. If no string is defined, all standard and private MIB information is read-only, and no authentication failure trap is issued.	null	48 characters
Read-Write Community Name	Used by the SNMP agent as a simple authentication mechanism for read access to all MIBs and write access to standard MIBs. If no string is defined, all MIB information is read-only, and no authentication failure trap is issued.	null	48 characters
Private Community Name	Used by the SNMP agent as a simple authentication mechanism for read and write access to Enterprise MIBs. If no string is defined, all MIB information is read-only, and no authentication failure trap is issued.	null	48 characters
Trap IP Address	When a trap condition occurs, the SNMP agent sends an SNMP trap PDU to this address’s management station. Addresses can be entered for up to four SNMP managers.	0.0.0.0	Valid IP address
Enable Authentication	When set to Y(es), the agent matches the community string on an incoming PDU with community names. If there is no match, no access is allowed. If Enable Traps is also set to Y(es), the agent issues an authentication failure trap. If there is a match, read only or read/write access is allowed, depending on the name matched. When Enable Authentication is set to N(o), no check is made, and read only access to all MIBs is allowed.	N	Y, N
Enable Traps	When set to Y(es) and an error condition occurs, the agent sends an SNMP trap PDU to the IP addresses specified as Trap IP addresses. When Enable Traps is set to N(o), no traps are sent.	N	Y, N

Page intentionally left blank.

6

6. Status and Diagnostics

This section describes a number of tools for verifying, monitoring and diagnosing the configuration and operation of the ESS. In addition to basic LEDs, this section emphasizes the capabilities accessed via the **<1> STATUS** selection of the **Main** menu. The primary **STATUS** sub-menu is:



6.1. Board Status

The **<1> Board Status** screen provides an overview of each port on the ESS system.

This display provides the Port Number and Name, the protocol type, current state (enabled/disabled) and link status (up/down). The information on this screen is automatically refreshed every minute and can also be refreshed on demand by entering **<return>.**

- The **Port Number** is port number 101 to 126. The names and protocol type are always Enet 1xx and Ethernet, respectively.
- The **State** (Enabled vs. Disabled) is set under operator control using the Port Enable/Disable commands described in section 6.6.
- The **Status** indicates the current status of the physical and logical Ethernet connection to another device, either Up or Down. If Spanning Tree or Rapid Spanning Tree protocols are being used on the network, and the port is enabled, then this field

provides the current state of the port within the spanning tree, i.e., Forwarding, Blocking, Listening or Learning.

```
                          *** Board Status ***
                Port Number, Name, Protocol, State, and Status

101        102        103        104        105        106        107        108
Enet 101   Enet 102   Enet 103   Enet 104   Enet 105   Enet 106   Enet 107   Enet 108
Ethernet   Ethernet   Ethernet   Ethernet   Ethernet   Ethernet   Ethernet   Ethernet
Enabled    Enabled    Enabled    Enabled    Enabled    Enabled    Enabled    Enabled
Blocking   Link Up    Link Down  Link Down  Link Down  Link Down  Link Down  Forw'ding

109        110
Enet 109   Enet 110
Ethernet   Ethernet
Enabled    Enabled
Link Down  Link Down

                                                 Press <RET> for update
__________[ESS_b456926]__________                Press ESC to return to previous menu
```

6.2. Call Status/Control

This menu can be accessed from either the Main Menu, <2> or from the Status Menu, (Main,<1>,<2>). This menu selection provides access to status information on current Spanning Tree topology and port states. Access the **Call Status/Control Commands** screen from selection **<2>** of the **Status Commands** menu. Then select option **<2>** of this menu to access the **Bridge Port Status** screen shown below.

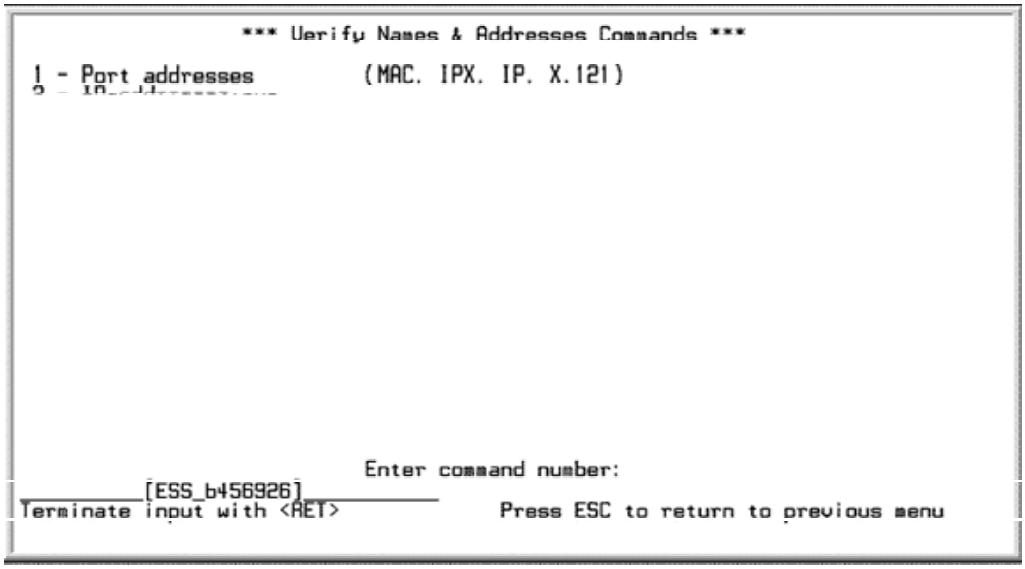
```
                          *** Bridge Port Status ***

Port       State          Role           Network      BPDUs
                                                     TX             RX
101        Listening      Designated     Legacy       7              1
106        Disabled       Designated     Legacy       0              0
107        Disabled       Designated     Legacy       0              0
108        Blocking       Alternate      Legacy       1              7

__________[ESS_b456926]__________
Press <RET> for update              Cursor up/down for more entries
Press <CTRL-D> to clear statistics  Press ESC to return to previous menu
```

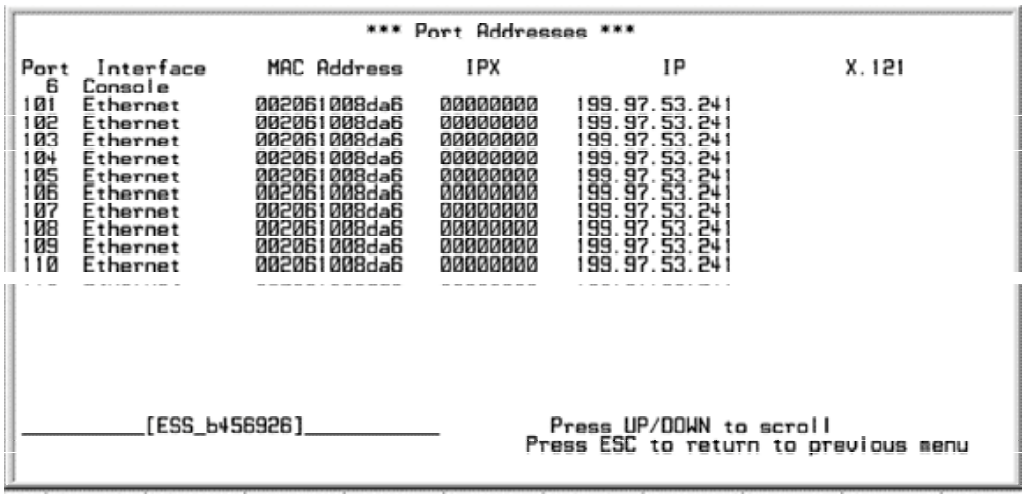
6.3. Verify Names / Addresses

The **<3> Verify Names and Addresses** sub-menu of the **Status Commands** screen provides information on Ports, MAC addresses, IP routing and ARP tables, as well as the DHCP address allocation if the DHCP server has been configured. The screen selection options are shown here. These commands are valuable while performing System Configuration in order to verify correct information entry. The Port, IP address and DHCP display features are described separately below.



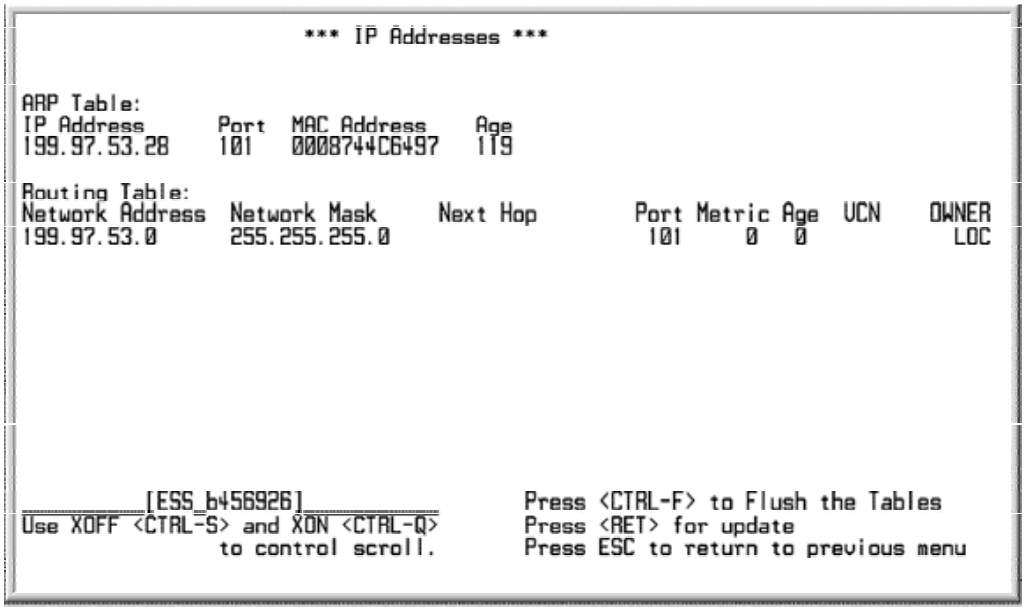
6.3.1. Port Addresses

This **<1> Port Addresses** selection of the **Verify Names & Addresses** menu provides a summary display giving port number, associated MAC address and IP address if assigned. IPX and X.121 addresses are not assigned by the ESS at this time



6.3.2. IP Addresses

The **<2> IP Address** option of the **Verify Names & Addresses** menu provides details of the internal IP router, providing information on learned IP addresses and ARP tables.

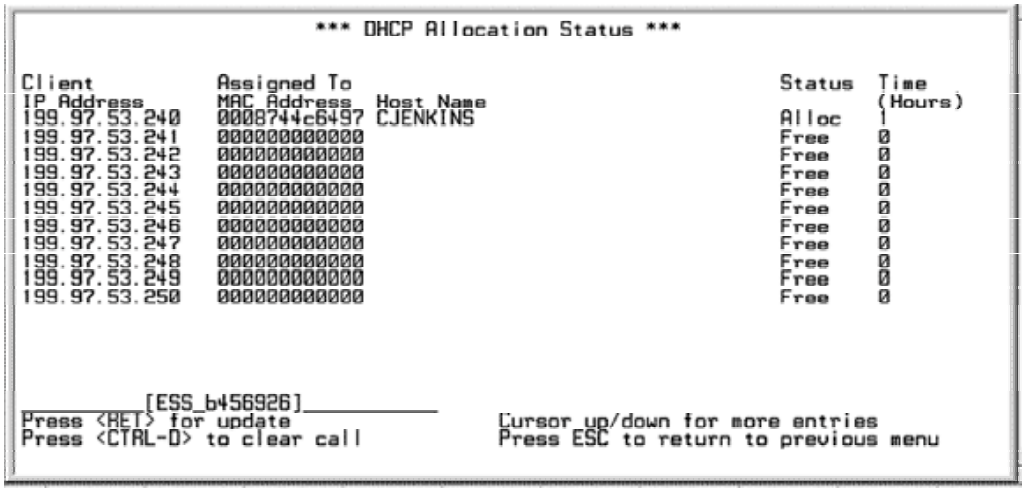


Note: Since routing tables can be extensive, this screen has scrolling options and has the ability to FLUSH the learned tables. Be very careful about flushing tables, as this will empty the routing table and the router will no longer have the ability to ROUTE messages until the routing discovery protocols rebuild the table. RIP discovery typically takes at least 30 seconds. OSPF updates only occur during topology changes.

6.3.3. DHCP allocations

The **<3> DHCP Allocations** option of the **Verify Names and Addresses** menu lists the DHCP Server IP addresses and the MAC addresses to which they have been allocated.

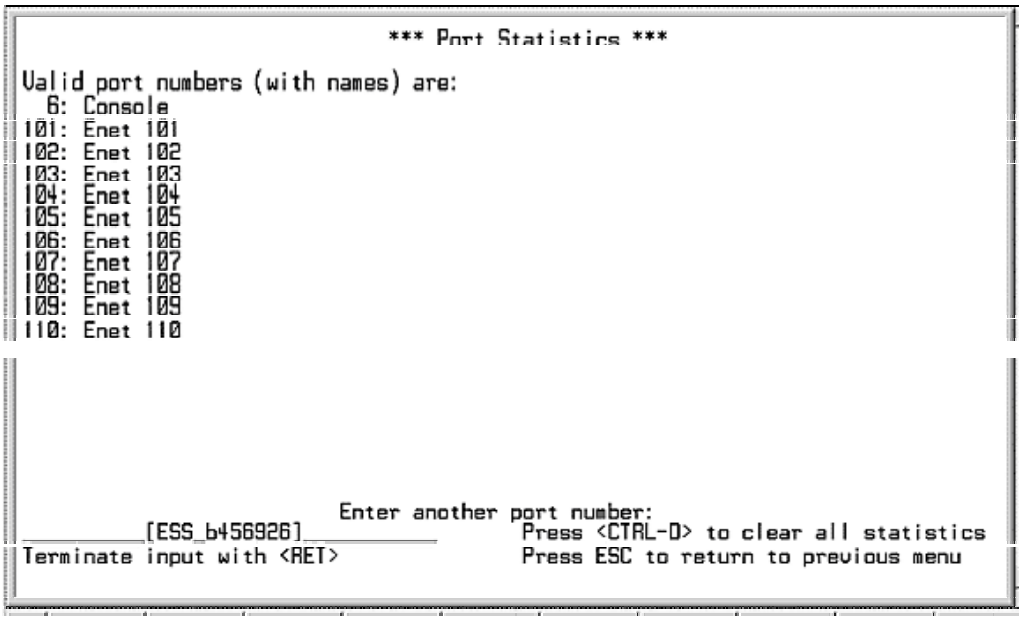
- The **IP Address** will be from the pool of addresses held by the ESS DHCP server and assigned upon request to DHCP clients (see section 5.3.4).
- The **MAC Address** and optional **host name** indicate the device attached to the ESS that made a successful DHCP request.
- **Status** may be Free (unassigned), Expired (timed out) or Assigned (active and current).
- **Time** indicates the time remaining (in hours) in the Lease for the assigned address. At the end of the lease, the assignment times out and the IP address is freed up and the DHCP server may assign it to another client upon request.



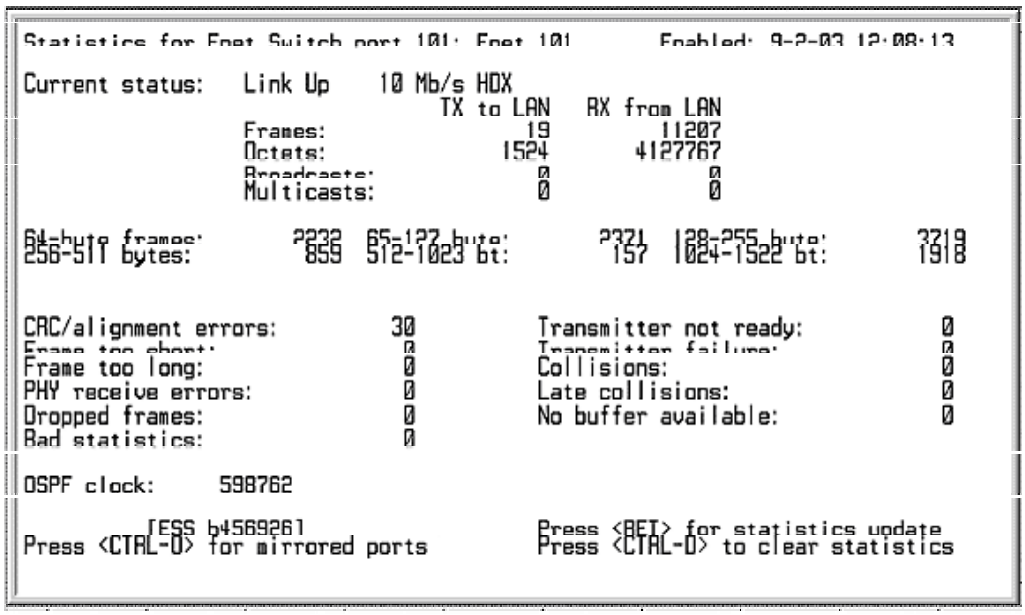
Note: While in this screen, the operator can use **<CTL-D>** to force the release of all addresses assigned by this server. The server may then assign these addresses to new requestors. Note that this action does not release the addresses within the attached devices. Address releases within the attached devices will either occur via time-out or by device operator action.

6.4. Statistics

This feature provides detailed statistics for each port available on the ESS system and is very useful in monitoring network stability. Statistics are reached via selection **<4>** of the **Status Commands** menu. The following port selection menu then appears.



Enter a port number and press **<return>** to obtain detailed statistics for that port. A port-specific screen will appear similar to the one below with the internal port number (e.g., port 101) in the top line.

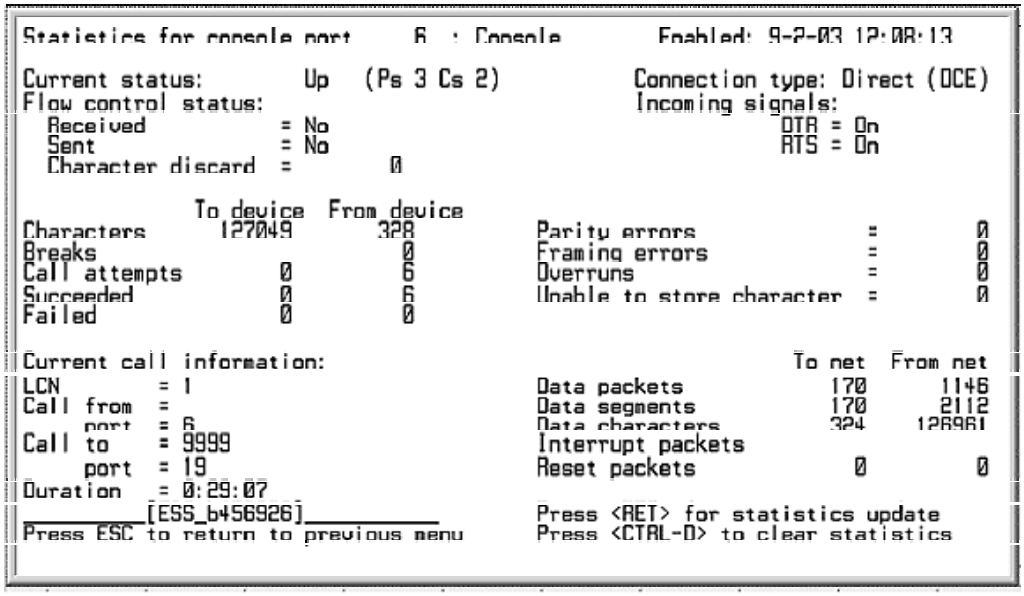


Ethernet port statistics are defined in the following table:

Ethernet Port Statistics	
Statistic	**Meaning**
Port number	The number of the port whose statistics are being displayed.
Enabled	Date and time that the port was enabled.
Current status	Indicates whether a connection is Up or Down. When Spanning Tree is active, shows state in current spanning tree.
Frames	The number of LAN frames sent/received.
Octets	The number of octets (bytes) sent/received in LAN frames.
Broadcasts	The number of LAN broadcast frames sent/received.
Multicasts	The number of LAN multicast frames sent/received
Frame counts	Frame counts by various frame size
CRC/Alignment errors	The number of LAN frames received that are dropped due to CRC error or that frame is not an integral number of octets (LAN error condition).
Frame too short	The number of LAN frames received that were less than 64 bytes (LAN error condition).
Frame too long	The number of LAN frames received that were larger than 1514 bytes (LAN error condition).
PHY Receive errors	Receive errors reported by MAC layer, typically illegal codes

Dropped frames	Frames dropped due to insufficient switch buffer resources
Bad statistics	Counts for when the switch reports a message, but the message itself is corrupted and non interpretable
Transmitter not ready	The number of times the ESS had to wait to transmit a frame (high traffic loads on the LAN).
Transmitter failure	The number of times the LAN was not available to transmit a frame (congestion on the LAN).
Collisions	The number of LAN frames with one or more collisions during transmission (high traffic loads on the LAN).
Late collisions	In half-duplex mode, a collision occurs after the normal collision interval due to misbehavior on the LAN, usually due to some station operating in full duplex
OSPF Clock	OSPF protocol timeout

The console port statistics are also available under the **Port Number 6**.



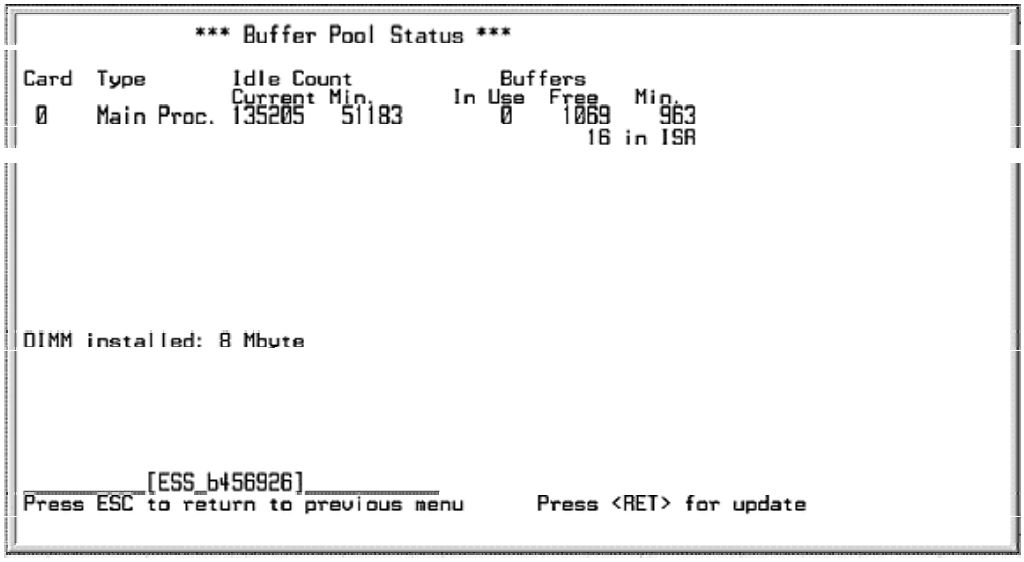
Console port statistics are defined in the following table:

Console Port Statistics	
Statistic	**Meaning**
Port number	The number of the port whose statistics are being displayed.
Enabled	Date and time the port was enabled.
Current status	Indicates whether a connection is Up or Down. Also may show Packet state and Cell state for diagnostic purposes.

Connection type	DCE for Console port.
Flow control status	Indicates whether flow control has been sent (Yes/No) or received (Yes/No) and shows the number of characters discarded after flow control is sent. Flow control can be XON/XOFF or data set signals.
Incoming Signals	Status (On/Off) of incoming data set signals.
Characters	The number of asynchronous characters sent/received.
Breaks	The number of line breaks received.
Call attempts (Succeed, Fail)	The number of calls originated/ received at this port, followed by the number successful and the number failed.
Parity errors	The number of parity errors (line errors).
Framing errors	The number of incorrect stop bits on asynchronous character (line errors).
Overruns	The number of times that an Interrupt service routine cannot process character message has been received from the hardware, indicating there is more traffic than the ESS can handle. Check configuration and verify proper flow control operation.
Unable to store character	The number of times that an Interrupt service routine cannot store character message has been received from the hardware, indicating there is more traffic than the ESS can handle. Check configuration and verify proper flow control operation.
Current Call Information	
LCN	The logical channel number of the active virtual call.
Call From/Port	The address assigned to the local port and the local port's number.
Call To/Port	The destination's address and port in an ESS.
Duration	The call's duration in hours:minutes: seconds.
Data packets	The number of Data packets sent/received.
Data segments	The number of accounting data segments sent/received. That is, a Data packet that is 64 bytes or less. A Data packet of 65 bytes counts as two data segments.
Data characters	The number of data characters sent/received in Data packets.
Interrupt packets	The number of Interrupt packets sent/received.
Reset packets	The number of Reset packets sent/received.

6.5. Buffer Usage (System Indicators)

The **Buffer Pool Status** screen is accessed using the **<5> Buffer Usage** selection of the **Status Commands** menu. This screen provides an overview of internal buffer usage and an indication of processor utilization. The screen also indicates the system memory size. The Idle count is the indication of processor usage. High counts indicate lower processor usage. This screen is automatically updated every 5 seconds and can be updated on demand by entering **<return>.**



6.6. Enable/Disable/Initialize Port

The ESS has the capability of turning on and off remotely individual ports. This function allows (enables) ports to communicate with wired remote terminals, else the ports are not allowed (disabled) to communicate at the link layer and higher layers.

The Status Commands menu provide the operator with the ability to manually:

- **<6> Disable** a port (whether it is operational or not)
- **<7> Enable** a Disabled port
- **<8> Initialize** a specific port.

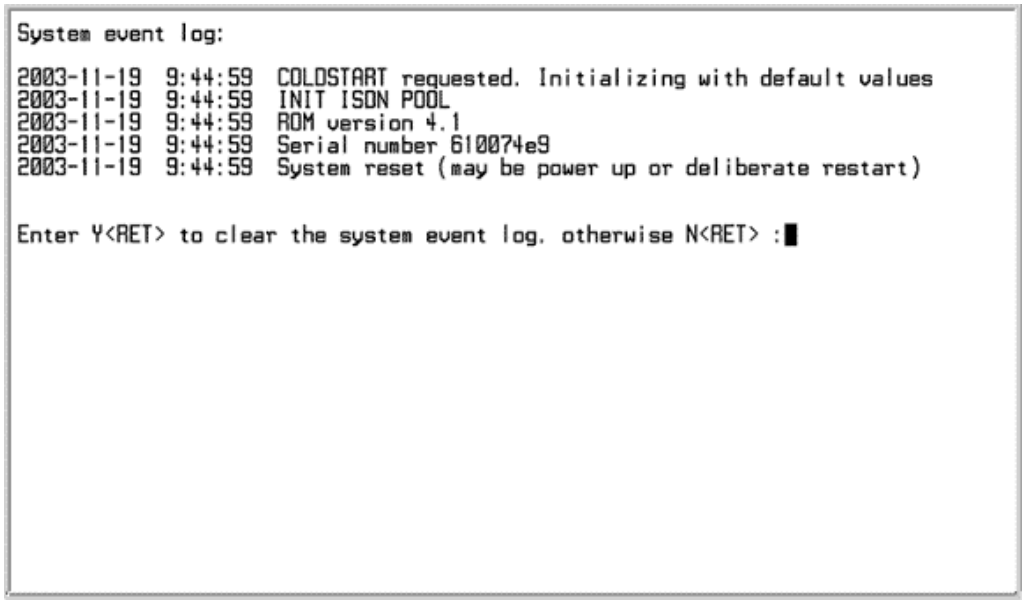
Initializing a port combines the Disable and Enable commands within one command. This is very useful if you are currently accessing the system on the same port you are initializing, where the alternative Disable Port command would lock you out, preventing you from issuing a subsequent Enable command for the same port. This command automatically re-enables the port, allowing the operator to regain access. It essentially represents a rapid resetting of the port.

Disabling a port is prompted as a two-step process, requesting the operator to confirm the action. *Note: The operator should not Disable a port that is being used by the operator to manage the switch,* as the operator will lose the ability to manage the switch, including the ability to Enable the port again.

Enabling a port is similar to the Disable process, above (with opposite effect!).

6.7. Log

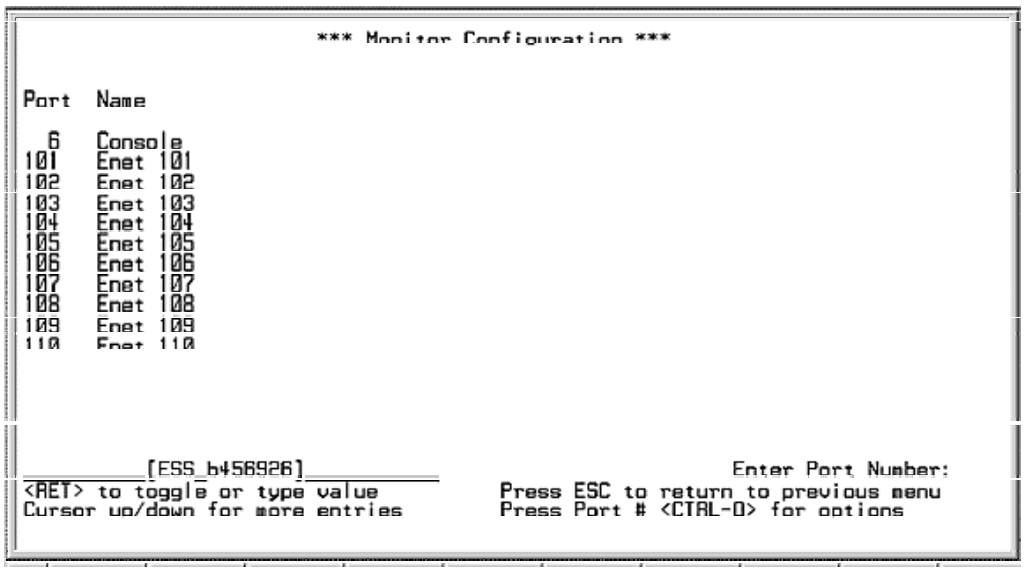
The ESS system has multiple logging features that track various events. These events include normal activities, but in particular the log tracks more serious events and diagnostic information. This can be very useful in tracking down networking problems and configuration errors. The entries are time stamped and stored in FLASH memory and hence survive power outages. The Log is accessed via the **<9> Log** selection of the **Status Commands** menu. A typical log screen is shown here.



6.8. Monitoring

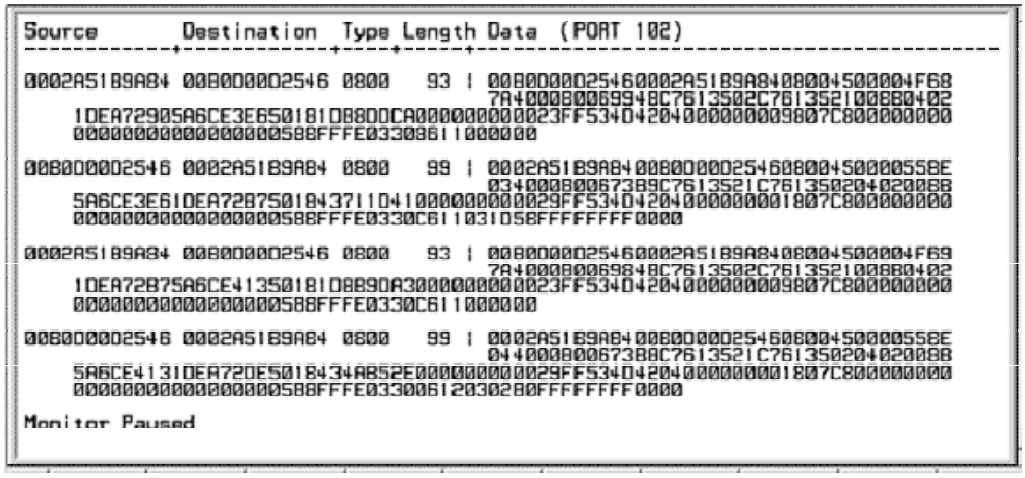
The ESS monitor system allows the operator to retrieve real time traces of traffic flowing on Ethernet ports or on the console connection. Real time protocol level traces from any unit in the field can be seen and/or captured remotely, i.e., at the Network Operations Center. This function will replace the need for a 'data scope' or 'protocol analyzer' for many diagnostic procedures, as well as allowing these traces to be performed from a central console without manual dispatch.

Access the Monitoring feature from the **<10> Monitoring** selection of the **Status Commands** menu.



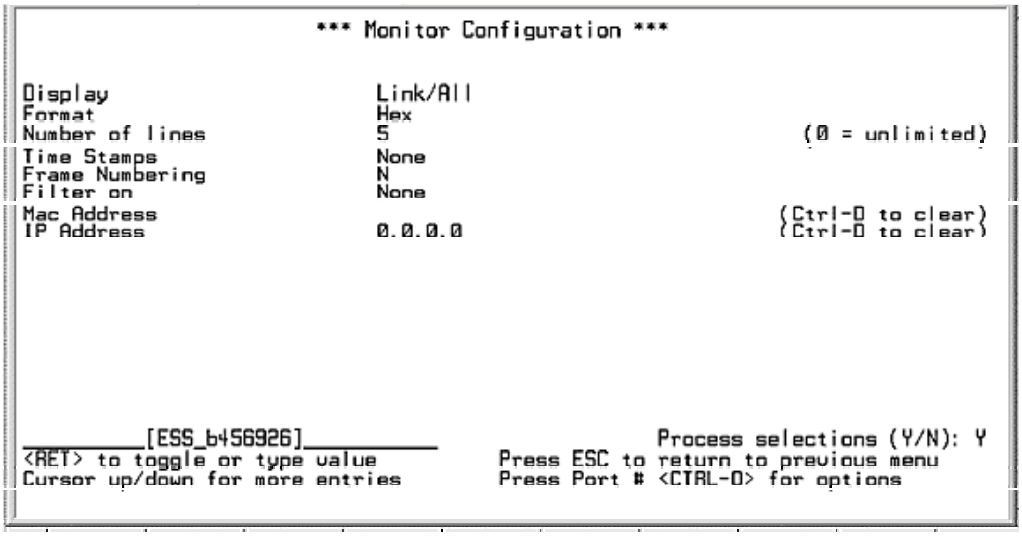
On the initial **Monitor Configuration** screen shown above, enter the **port number** you want to monitor and press **<enter>** to show basic information.

The following display shows a sample basic real time trace of an Ethernet port, Port 102, as displayed to the console port or Telnet session. It provides source and destination addresses, Transmit and Receive data messages and a HEX print out of the data.

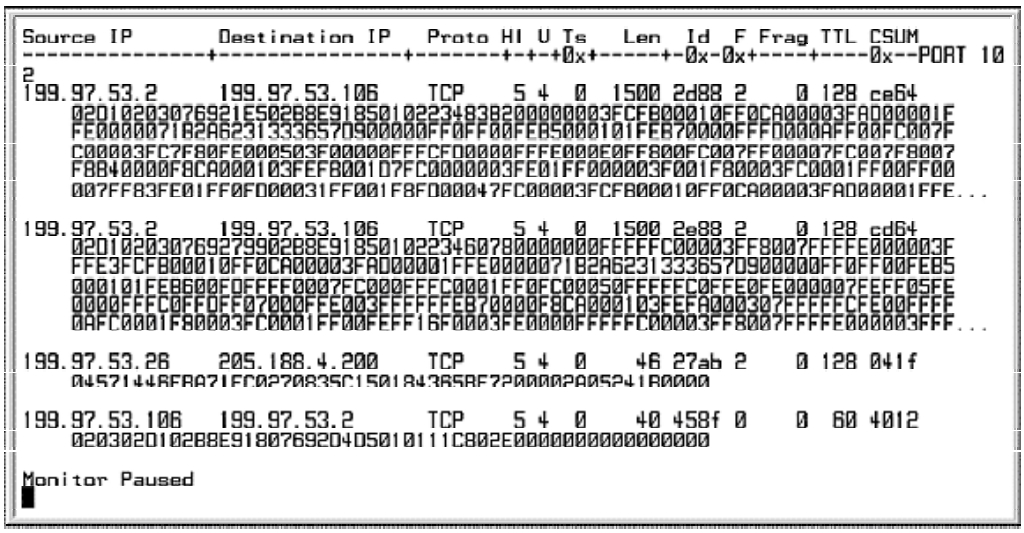


The Monitor displays a notification message in the lower left corner of the screen when the operator pauses and un-pauses the monitor. The indication will be either “Monitor Active” or “Monitor Paused”. Use **<esc>** to quit the monitor. Use **<enter>** to pause or resume the monitor.

Once in the monitor display there are further options to allow the operator to display select parts of the frames, display data in ASCII instead of HEX, display timestamps and filter the information displayed. For example one has the ability to get an IP header decode, or to filter to select only frames from a specific MAC address, an IP addresses or IP address/socket number. This Filter menu is accessible by entering **<CTRL-O>** while in the monitor. The filter display looks like:



To return to the live monitor, enter **Y** to process selections (in the lower right) and enter **<return>.** Enter **<esc>** to exit monitor mode. An example showing the IP breakdown capabilities is shown below:

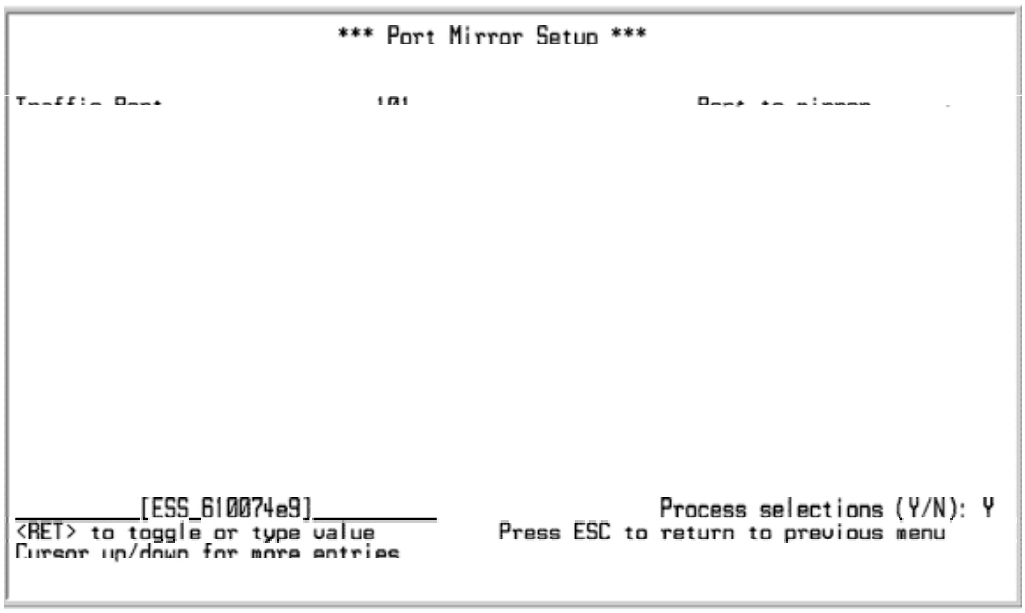


6.9. Port Mirroring

The Port Mirroring feature allows the operator to replicate all the traffic on one switch port onto a second switch port. With a monitoring device attached to this second port, the operator can unobtrusively observe the traffic on the port under study.

Access the Port Mirroring feature from the **<11> Port Mirror** selection of the **Status Commands** menu. The following screen appears. Enter the port number of the port to be studied as the "traffic port" and indicate the port number of the port to which the analysis device will be attached as the "Mirror Port" (the port to which replicated data will be sent).

To cancel mirroring, enter **<CNTL-D>** on each of the port number entries.



6.10. LEDs

The diagnostic visual indicators are on the back side of the ESS, along with all the connections to Ethernet, power and console port. (Exception: The power LED indicator is on the front of the unit.) There are Ethernet Link LED indicators for each port and a single LED to the lower right of the second gigabit port that indicates SYSTEM status. There is also a single "power on" LED on the lower right of the front overlay of the ESS.

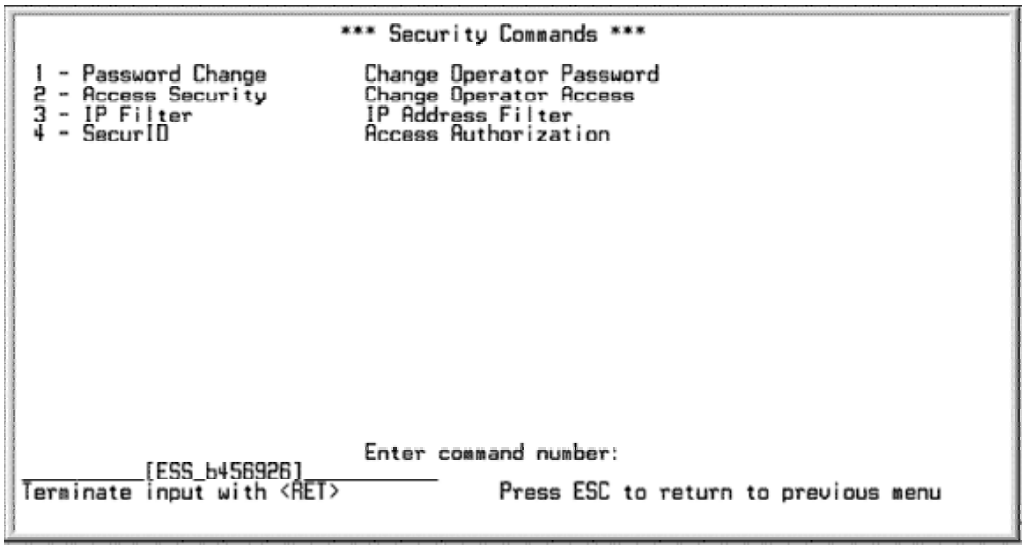
LEDs	Meaning
Ethernet Ports	**Blinking Green**: traffic **Solid Green**: link up but idle **Off:** Link inactive
System	**Green**: 'all is well' **Amber:** in the Boot process **Red**: in a reset state
Power	**Green:** unit is powered

Page intentionally left blank.

7

7. Security

This section describes the security features of the ESS that protect access to the Supervisor and other management functions. Security functions are supported from selection **<5> Security** on the **Main** menu of the Supervisor. The main Security sub-menu is:



Password Change and Access Security are elements of the **Multi-level Operator Access** feature. The **IP Filter** feature is an extension of the IP routing capabilities of the ESS. IP Address Filters can be used to limit access to the Supervisor to only specific remote IP addresses, thus providing an additional level of access protection beyond the ID/password protection.

7.1. Multi-Level Operator Access

In addition to the standard Root access, the ESS supports up to five additional operator authorizations. The Root user defines the additional operators and their access authorizations. Only the Root user can change the names, passwords and access capabilities of these operators.

By default, the Operator_1 through _5 do not have names or passwords assigned to them. These oprators are not active until the Root operator creates names and passwords for them. Each operator must have a unique password. The system will reject any duplicate password and prompt the Root user for another one.

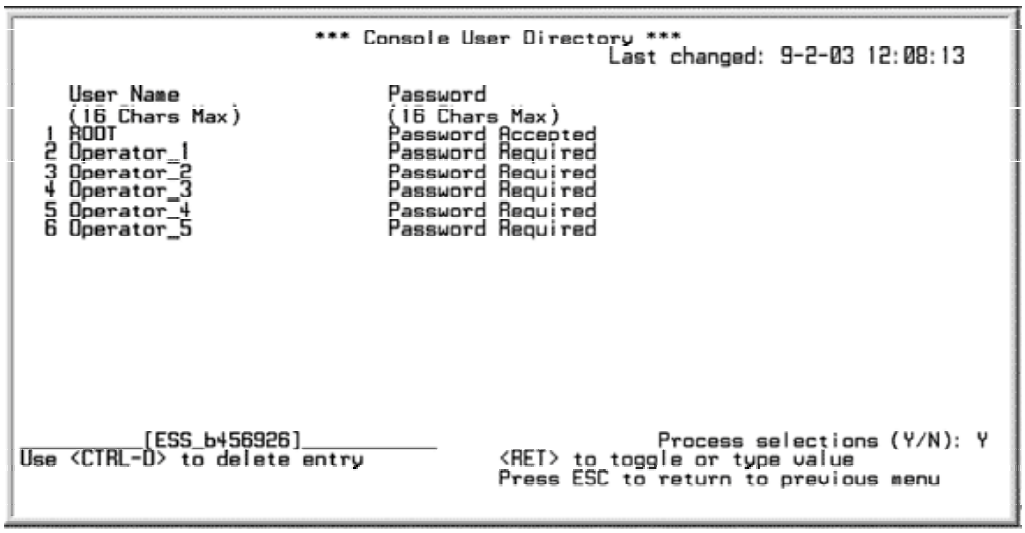
Three levels of access are provided:

No Access (N)	Blocks the operator from accessing a given group of commands	Default for Operator 1-5
Read-only Access (R)	Allows the operator to view parameters but not change them	
Write Access (W)	Provides the ability to read and modify parameters	Default for Root

7.1.1. Password Change

To change the password of the Root user or an individual operator or class of operators, do the following:

From the Security Commands menu, select <**1> Password Change**. A **Console User Directory** screen appears.



To change the user name, move to the operator name you wish to change and type in the new name. New unique names should be assigned to all operators or levels of operators being utilized. Names may be any alphanumeric string up to 16 characters. For example:

Root …..……...might become …..SysAdmin

Operator_1 ….. might become.….NOC Supervisor

Operator_2……might become…..Provisioning

Operator_3……might become…..Net status

Operator_2……might become…..Tech Support

Operator_2……might become…..Field Support

After changing the name use **<Tab>** to move to the **Password Required** (or **Password Accepted)** field, type in the new password and press **Enter**.

Note: Passwords are case sensitive. They may be any alphanumeric string up to 16 characters.

After entering a new password, a message to "Re-enter password" will appear on the screen, just **enter the password and press <enter> one more time**.

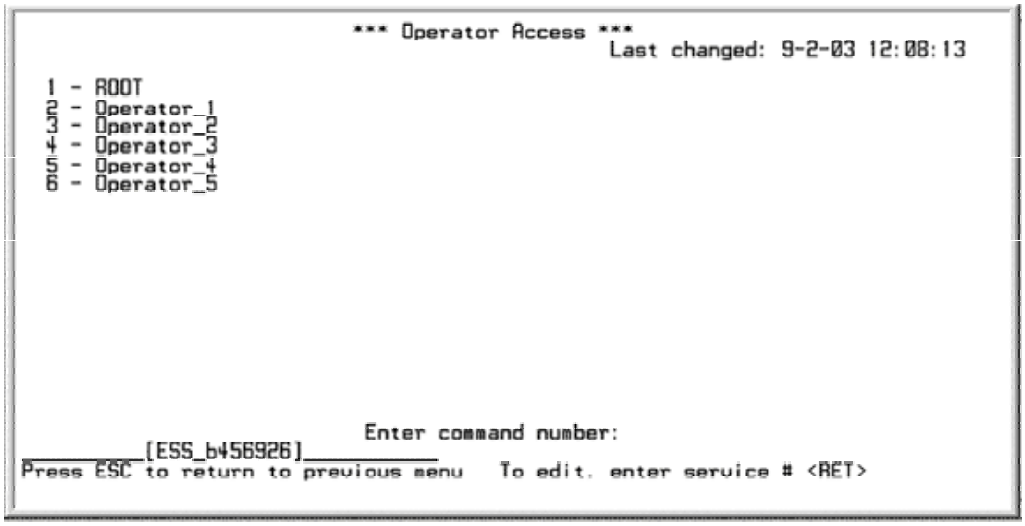
As long as the password was typed in exactly the same both times "**Password Accepted"** is displayed. If not, "**Password Required**" will be displayed and the process must be repeated.

Note: The passwords are not echoed to the screen, so be sure to remember them.

When done editing user names and passwords, enter **<Y>** in the **Process selections** field and press **<enter>**. Be sure to remember the root password and protect it, as it is critical to gaining operator/supervisor access for operation and maintenance purposes.

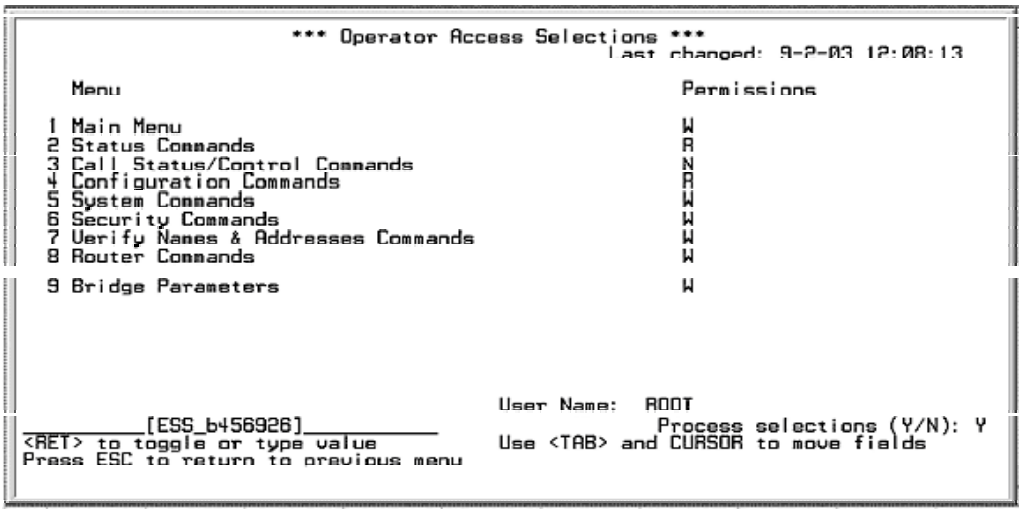
7.1.2. Define Access Permissions

To configure the Supervisor access permissions for different operators, from the Main Menu select **<5> Security Commands then <2> Access Security**. The **Operator Access** menu appears.



The **Operator Access** screen provides a list of the defined users.

To change the access permissions for any given user, enter the number of the operator whose access authorization you want to change. The **Operator Access Selections** menu for the selected operator appears, as shown below:



This screen lists nine categories of menus and commands available in the ESS Supervisor. Each category may have its own rules for operator access. Set the authorizations as required for each available category by toggling W, R or N in the assoociated **Permissions** column. Tab to the selected field and toggle the Permission value using **<CR>.**

As described above:

- **W** represents full access to WRITE and READ,
- **R** represents READ ONLY
- **N** represents NEITHER READ OR WRITE or NO ACCESS.

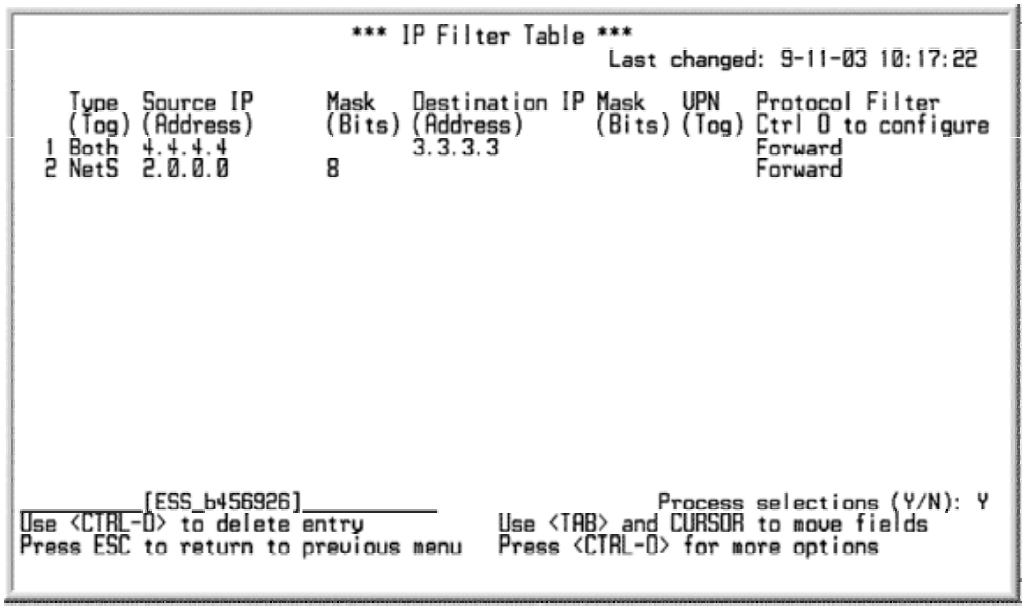
When you have finished configuring the operator access for the operator that was selected, enter **Y** in the **Process selections** field and press **<return>**. Repeat this process for each of the other operators (or class of operators).

7.2. IP Filter

IP filtering allows traffic blocking or forwarding based on specific IP addresses or address masks, as well as on TCP, UDP or ICMP ports or sockets. Subnet mask support is also available.

To set up IP Filters, enter **<3> IP Filter** on the **Security Commands** menu. The IP Filter screen shown below will appear.

Use the IP Filter table to specify up to 60 specific filtering actions and also to designate a default IP action for frames not matching any filter specification. The IP Filter process searches from the top of the table (after a sort process described below) and performs a filtering action based on the first match that it finds for an address. If no match is found for either the source or destination address, the call is blocked or forwarded based on the selection in the **Default filter action** field. This field is initially configured to forward all traffic.



To configure IP Filtering:

- **First,** place the cursor in the **Type** column and press **<enter>** to select the desired type of filter being defined on that line of the filter table:
  - **Both** filters on both the source and destination addresses configured.
  - **Src (Source)** filters on only the specific IP source address configured.
  - **Dest (Destination)** filters on only the specific IP destination address configured.
  - **NetB (Netboth)** filters both the source and destination network addresses based on the masks entered on the same line.
  - **NetS (Netsource)** filters the source network address based on the mask entered on the same line.
  - **NetD (Netdest)** filters the destination network address based on the mask entered on the same line.
- **Next,** tab to the **Source IP, Destination IP**, and/or **Mask** fields as appropriate and enter a complete address or mask as required for the type of filtering you are configuring.
  - The VPN field has reserved meaning and is not utilized at this time.
- Set the Action: cursor to the **Protocol Filter** column and toggle to Forward or Block as desired for this filter
- To set protocol-specific filters or to change the Default action from forward to block, enter **<CNTL-O>** to access the optional **UDP/TCP Filter Table** screen shown below.
  - Toggle the **Action** column settings for the protocols shown, as desired.
  - The **Def** protocol entry refers to the default action for all frames not meeting any of the other filter definitions (i.e., either do not appear in the table or cannot be derived from masks that appear in the table). The default setting is Forward.

- When all of entries are complete, enter **<Y>** in the **Process IP filter table** field and press **<return>.** You will be returned to the Security Commands screen.

- Redisplay the IP Filter table by selecting the IP Filter option to verify the desired actions.

- **Note:** The IP Filter table will have been resorted by class and address according to the following sorting rules:

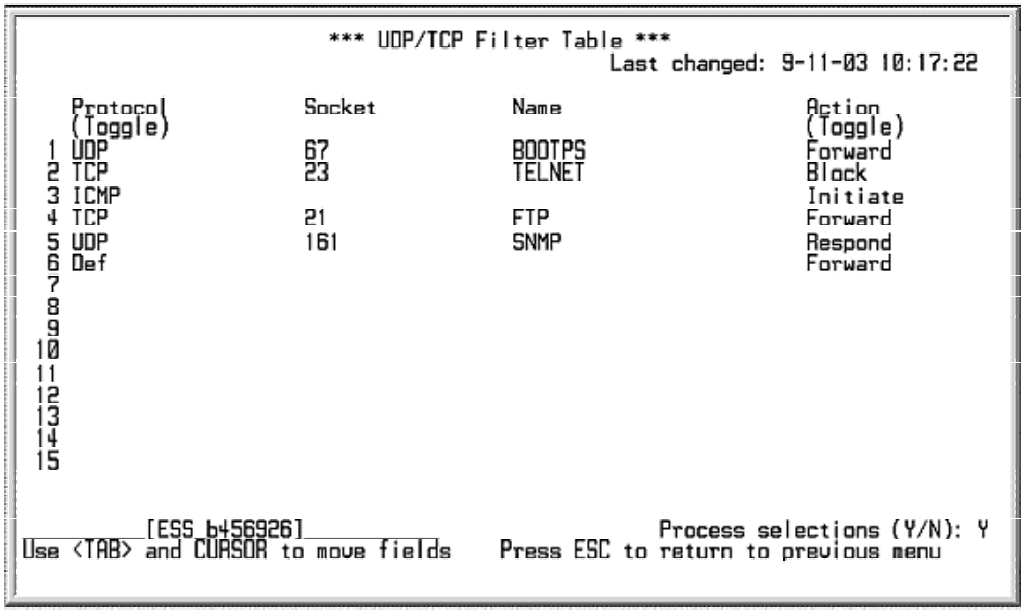
  1. Entries with specific addresses appear before entries with masks.

  2. Addresses and masks are sorted from low to high values.

  3. Actions are sorted (in order of decreasing priority) by class as follows:

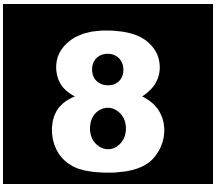
  - BOTH (source and destination address)
  - SOURCE (source address only)
  - DESTINATION (destination address only)
  - NETBOTH (both source and destination network masks)
  - NETSOURCE (source network mask only)
  - NETDESTINATION (destination network mask only)

- **Note:** In the sorted table, an address or mask of *.*.*.* indicates "Don't care" and is not used for filtering.



7.3. SecurID

Use of SecurID requires a SecurID server sold by RSA Security (www.rsasecurity.com). The ESS has the ability to interoperate with this type of authentication server to enhance the inherent ESS username/password login security to the console port. If this functionality is desired please contact your DYMEC sales or customer service representative for assistance.



8. Software File Management

This section describes how to update software files, e.g., the operating system and system configuration files.

The ESS has a flash-based file storage system that contains the operating system, configuration files, and error logs. These files are non-volatile and are not lost ***except for config files and error logs when a system is COLD STARTED***. However, they can be manually erased, updated and/or saved for backup purposes using a TFTP file transfer package from any Workstation or Personal Computer.

The ESS file system can contain up to:

- 2 copies of the run time operating system
- 2 copies of configuration file
- 3 error log files

To verify the current file structure of the ESS, see the System Administration section, Section 4.4.2, Code Versions command.

The operating system is automatically installed when the system is powered up. The boot process includes memory testing and various other activities that test the hardware prior to running the operating system. If a console port is connected to a terminal, then the boot process is displayed on the terminal. At the end of the boot process, the system loads the operating system, prints the current error log and is then operational. The whole process is less then 30 seconds.

8.1. Loading a New Operating System and Configuration File

The same procedure is used for loading a new operating system (OS) or upgrading a current operating system. The operator will require access to a TFTP package from the host machine they intend to use for the download. Most workstations that are UNIX-, LINUX-, or Windows-based come with a TFTP package. Otherwise the operator will have to purchase an application. Some are free on the Internet. The TFTP commands vary between different vendors of TFTP. Here we will choose the standard UNIX commands, and these may need to be modified for other TFTP tools.

The basic steps for loading software from either the BOOT ROM or with the normal system running the Operating System consist of the following steps:

- Make sure that an IP address is configured
- Retrieve the configuration file, if you want this configuration for the new OS
- Erase and/or defragment flash memory segment, where OS is stored

- Download new OS file
- Download configuration file, if the User wants the system to inherit the old system configuration
- Restart or Reinit the system

NOTE: To download files into the ESS, the ESS must have an IP address. This may be set in the Boot process (see Section 4.2 or via the System Configuration process, Section 5.3.1.

8.1.1. Configuration File Management

The operator must save the current configuration options when upgrading the system software. Failure to retrieve this file will default all settings to factory defaults after the upgrade and require a complete manual reconfiguration of the unit. **DO NOT SKIP THIS STEP!**

In UNIX:

- the TFTP package first establishes a connection with the client, using the command sequence: **TFTP <ip address> CR**
- Followed by the Binary Command: **BIN CR**
- To retrieve the configuration file use the TFTP **"GET"** command, to retrieve a file name **"CNFGLOAD.CMP",** e.g.:

GET CNFGLOAD.CMP <sp> <local file name> (sp=SPACE)

In Windows

- For Windows 98, 2000K, XP, and DOS
- GET the cnfgload.cmp file from the ESS:

tftp -i <ip address> get cnfgload.cmp CR

Both:

The ESS will make a compressed copy of the current configuration and send the file to the host application for safekeeping. This file will be downloaded back to the ESS system after the upgrade process, or anytime restoring the entire unit config is deemed necessary. This step is critical because the FLASH memory will be erased in the next step of the process to make space for the new download. The FLASH is also the location of the configuration file, which will be lost during the erase process.

8.1.2. Downloading an Operating System

To download a new operating system, the first step is to make space available in the ESS flash memory.

In UNIX

To do this we send a file to a special location that invokes an erase process, e.g.

PUT <anyfile> <sp> erase/password

where:

<anyfile> is a proper file name on the Host machine that is used to trigger the erase process. You can use the new OS file name.

<erase/password> is the destination file name that invokes the erase procedure followed by the current ESS **Root password** that by default is the word "secret".

Keep in mind that the root password may have been changed. The password is required to ensure proper authorization and for this procedure to work properly

The ESS will respond with a message **"erasing flash."**

The erase process takes about 20 seconds to complete, so wait 20 seconds before taking the next step. Note: TFTP does not support any type of completion notification so one must assume the operation was completed after approximately 20 seconds. Keep in mind that if this procedure is being attempted over a large or slow IP network, considerably more than 20 seconds may be required. A good rule of thumb is to wait 60 seconds when executing this procedure across a network.

The next step is downloading the Operating System file. The file is called ECMLOAD.BIN. This is downloaded to a destination file called DOWNLOAD.BIN. Using the TFTP tool the command is:

PUT ECMLOAD.BIN <sp> DOWNLOAD.BIN

Next send the configuration file that was previously extracted.

PUT CNFGLOAD.CMP <sp> local-filename.CMP

Finally, to restart the system, send a file to a special location "reinit" including the **root password**, as with the erase operation, above**.**

PUT <anyfile><sp> reinit/password.

The system will now re-boot with the new operating system and the information contained in the specified configuration file (e.g., local-filename.CMP).

In Windows

Follow the steps described above for downloading an operating system in Unix command mode, but substitute the following commands for Windows and DOS environments.

- Erase all files on the ESS:

  tftp <ip address> put <anyfile> erase/secret CR

- PUT the new code on the ESS:

  tftp -i <ip address> put ecmload.bin download.bin CR

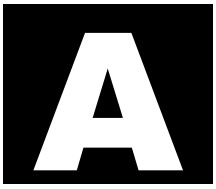
- PUT the configuration file back on the ESS:

  tftp -i <ip address> put cnfgload.cmp CR

- Reinitialize the ESS:

  tftp <ip address> put <anyfile> reinit/secret CR

Page intentionally left blank.



Appendix A: Glossary

802.1D	General IEEE specification for bridged Ethernet
802.1d	IEEE specification for Spanning Tree Protocol (STP)
802.1p	IEEE specification for MAC-layer packet prioritization
802.1q	IEEE specification for bridged VLANs
802.1w	IEEE specification for Rapid Spanning Tree Protocol
802.3x	IEEE specification for full duplex LAN operations
10/100TX	IEEE specification 10/100baseT copper interface
10FL	IEEE specification 10/100baseFL fiber interface
100FX	IEEE specification 10/100baseFX fiber interface
100SFP	100Mbps small form-factor pluggable interface
1000SFP	1000Mbps small form-factor pluggable interface
BOOTP	Bootstrap Protocol
BPDU	Bridge Protocol Data Unit
CRC	Cyclical Redundancy Check
DHCP	Dynamic Host Configuration Protocol
DLL	Disable TX on Link Loss
ESS	DYMEC Ethernet Switching System
FDX	Full duplex
HDX	Half duplex
ICMP	Internet Control Message Protocol
IP	Internet Protocol
LCN	Logical Channel Number
LED	Light Emitting Diode (alarm light)
MAC	Media Access Control (layer of Ethernet interface)
MDI	Media Dependent Interface
MDIX	MDI Crossover
MIB	Management Information Block
MM	Multi-mode fiber optic
MTRJ	RJ-style fiber connector
NIS	DYMEC Network Integration System
OSPF	Open Shortest Path First routing protocol
RAM	Random Access Memory

RIP	Routing Information Protocol
RIP-RX	Routing Information Protocol – receive only mode
ROM	Read Only Memory
RSTP	Rapid Spanning Tree Protocol
RX	Receive port
SFP	Small form-factor pluggable
SCADA	Supervisory Control and Data Acquisition
SM	Single-mode fiber optic
SNMP	Simple Network Management Protocol
STP	Spanning Tree Protocol
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TX	Transmit port
UDP	User Datagram Protocol
VLAN	Virtual Local Area Network