EOS User Manual

Software Release 4.0.1

April 8, 2009

http://www.aristanetworks.com email:support@aristanetworks.com

Contents

Chapter 1

Upgrade Procedure

UPGRADE/DOWNGRADE PROCEDURES

The active EOS image on an Arista Networks switch can be modified via the **boot system** command. Using this command, you can select an image file and location from flash, allowing the switch to be easily upgraded or downgraded to any desired image.

Modifying the active EOS image on an Arista Networks switch is a four step process:

- Use **copy** to transfer the image file onto the switch (if the image already exists on the switch, this step is not needed)

- Set the active image with **boot system**

- Save the configuration and reload

- Verify the new image is running

1. The desired image must be loaded onto the system. As the flash filesystem is persistent, it is generally recommended to copy any EOS.swi image to the flash and to instruct the switch to load the image from flash on boot. Loading the EOS.swi image file is done with the **copy** command, specifying a file source and a file destination. While the source and destination can change, the syntax is consistent:

- **copy** (image source) (image destination)

Below are examples of the **copy** command in use with various source locations:

COPY USB

```
localhost#copy usb1:/EOS-2.2.0.swi flash:/EOS-2.2.0.swi
localhost#
```

COPY FTP

```
localhost#copy ftp:/user:password@10.0.0.3/EOS-2.2.0.swi flash:/EOS-2.2.0.swi
'EOS-2.2.0.swi' at 13494888 (12%) 1.94M/s eta:47s [Receiving data]
localhost#
```

COPY SCP

```
localhost#copy scp://user:password@172.17.10.21/var/user/EOS-2.2.0.swi flash:/EOS-2.2.0.swi
localhost#
```

COPY HTTP

```
localhost#copy http://10.0.0.10/EOS-2.2.0.swi flash:/EOS-2.2.0.swi
'EOS-2.2.0.swi' at 13647872 (12%) 1.97M/s eta:46s [Receiving data]
localhost#
```

2. Update boot-config

During switch boot-up, the boot-config file is read by the aboot process to determine which .swi image should be loaded. Once you have transferred the desired image file onto the system, update the boot-config file using the **boot system** command:

```
localhost#configure terminal
localhost(config)#boot system flash:/EOS-2.2.0.swi
```

You can verify that the boot-config file has been correctly updated with the **show boot-config** command:

```
localhost(config)#show boot-config
Software image: flash:/EOS-2.2.0.swi
Console speed: (not set)
Aboot password (encrypted): $1$ap1QMbmz$DTqsFYeauuMSa7/Qxbi2l1
```

3. Reload

Once the boot-config file has been updated, the switch must be reloaded to allow the new image to become active. Save the running-configuration and reload the switch:

```
localhost#write memory

localhost#reload
The system is going down for reboot NOW!
```

4. Verify

After the switch has finished reloading, log into the switch and confirm the correct image has been loaded:

```
localhost#show version
Arista DCS-7124S
Hardware version:  02.02
Serial number:     JFL07340036

Software image version: 2.2.0
Architecture:           i386
Internal build version: 2.2.0-59039.EOS2.2.0
Internal build ID:      f34b0734-30ea-4544-b8c2-679b1b6beccf

Uptime:                 1 minute
Total memory:           1036504 kB
Free memory:            777376 kB
```

Chapter 2

CLI Commands

Interface Range Syntax

Name

Interface Range Syntax — syntax for interface ranges

Synopsis

```
localhost#show interfaces Ethernet 5-10,14,18
localhost#show interfaces Et44-48 status
localhost(config)#interface Et5-10
```

Description

An *interface range* specifies a list of interfaces, for configuration or status display purposes. Interface ranges make it more convenient to configure or view several interfaces at once. An interface range is not itself a command, but rather appears as part of a command such as **show interfaces** or **interface**.

The general syntax for an interface range is as follows. The range starts with an interface type keyword such as **Ethernet** or **Vlan**. The type keyword is followed by a comma-separated list of values. Each value in the list may either be an interface number, of a pair of numbers separated by a dash.

The special value **$** means the last port on the system. For example, the range **Ethernet 1-$** represents all Ethernet ports.

See Also

show interfaces, **interface**

aaa authentication enable

Name

aaa authentication enable — Set the authentication method list for the enable command

Synopsis

aaa authentication enable default *method-1* [*method-2*] ... [*method-n*]

no aaa authentication enable default

Description

The enable authentication method list controls which authentication methods are invoked, and in which order, to authenticate the enable command. For example, you may wish to attempt to authenticate against a TACACS+ server, but if that server is unavailable, fall back to the locally configured enable password on the switch. The default configuration is to use only the local enable password.

The supported authentication methods are **local**, **none**, and **group** *group-name*. The *group-name* can either be the special keyword **tacacs+** to indicate the server-group composed of all configured TACACS+ servers, or it can be the name of a group configured by the **aaa group server** command.

The **no aaa authentication enable default** command reverts the authentication method list configuration for the enable command to the default configuration, i.e. **local**.

Mode

Global Configuration

See Also

enable secret, **aaa group server**, **aaa authentication login**

aaa authentication login

Name

aaa authentication login — Set authentication method lists for logins

Synopsis

aaa authentication login { **default** | *service-name* } *method-1* [*method-2*] ... [*method-n*]

no aaa authentication login { **default** | *service-name* }

Description

An authentication method list controls which authentication methods are invoked in which order to authenticate a user for a certain service. For example, you may wish to attempt to authentication against a TACACS+ server, but if that server is unavailable, fall back to the locally configured user database on the switch. The special keyword *default* is used to configure the method list for any service for which no method list has been explicitly configured. The default configuration is to use only the local user database for login authentication for all services.

The supported authentication methods are **local**, **none**, and **group** *group-name*. The *group-name* can either be the special keyword **tacacs+** to indicate the server-group composed of all configured TACACS+ servers, or it can be the name of a group configured by the **aaa group server** command.

The **no aaa authentication login** command reverts the authentication method list configuration for a particular service (or the special keyword **default**) to the default configuration, i.e. **local**.

A separate command, **aaa authentication enable**, configures the authentication method list for the enable command.

Mode

Global Configuration

See Also

username secret, **aaa group server**, **aaa authentication enable**

aaa authorization

Name

aaa authorization — Set authorization method lists

Synopsis

aaa authorization { **exec** | **commands** { *0-15* | **all** } } **default** *method-1* [*method-2*] ... [*method-n*]

no aaa authorization { **exec** | **commands** { *0-15* | **all** } } **default**

Description

An authorization method list controls which authorization methods are invoked in which order to authorize a certain action. For example, you may wish to configure a switch to use a TACACS+ server to authorize all commands entered by a user, but if that server is unavailable, fall back to allowing the commands to be run. The default configuration is to allow all actions, ie. the default contents of all authorization method lists is the single method **none**, which allows all actions.

Actions available for authorization	
exec	Checked when starting a new CLI shell, which happens immedately after login on the console, via ssh, or telnet.
commands 0-15	Checked when executing a CLI command at the specified privilege level. By default a CLI session starts are privilege level 1, and after running **enable** the session privilege level is escalated to 15. The **commands 1** method list controls what sort of authorization is performed by a session with privilege level 1, and **commands 15** controls authorization for a session with privilege level 15, etc.
commands all	Configures the method lists for all command privilege levels with a single command. Using this has the same effect as setting **commands 0** through **commands 15**.

The supported authorization methods are **local**, **none**, and **group** *group-name*. The *group-name* can either be the special keyword **tacacs+** to indicate the server-group composed of all configured TACACS+ servers, or it can be the name of a group configured by the **aaa group server** command.

The **no aaa authorization ...** command reverts the authorization method list configuration for a particular type of action to the default configuration, i.e. **none**.

Mode

Global Configuration

See Also

aaa group server

aaa authorization config-commands

Name

aaa authorization config-commands — Enable authorization of configuration commands

Synopsis

aaa authorization config-commands

no aaa authorization config-commands

Description

Enables authorization of configuration commands, meaning any command in a configuration mode, such as Global Configuration Mode or Interface Configuration Mode. The default setting is to authorize configuration commands using the same policy as for all other commands.

no aaa authorization config-commands disables authorization of configuration commands.

An administrator might want to use this command to simplify their command authorization policy. If an administrator configures a TACACS+ server to deny all commands except for those in a specified whitelist, the number of rules required to allow all necessary configuration commands is large. If the policy is such that any user who may enter Global Configuration Mode is allowed to run any configuration command, then **no aaa authorization config-commands** may allow many fewer rules to be configured on the TACACS+ server.

Mode

Global Configuration

See Also

aaa authorization

aaa group server

Name

aaa group server — Configure an AAA server-group

Synopsis

aaa group server tacacs+ *group-name*

no aaa group server tacacs+ *group-name*

Description

The **aaa group server** command is used to create a named group of servers for use by the Authentication, Authorization, and Accounting (AAA) subsystem. The group can then be specified when configuring an authentication method list, for example when using the **aaa authentication login** or **aaa authentication enable** commands. The only server-group type currently supported is **tacacs+**.

aaa group server tacacs+ *group-name* enters server-group configuration mode for the specified group. You can add a server to the group in this mode using the **server** *hostname-or-address* [**port** *1-65535*]. Remove a server with the **no server** variant of the command used to add the server. Type **exit** to exit server-group configuration mode.

Note that you must separately configure parameters for each server in a group using the **tacacs-server host** host command. No requests will be made to any servers in a TACACS+ server-group that have not also been configured using **tacacs-server host**.

To remove a server-group from the configuration use the **no aaa group server** command and specify the group type (e.g. **tacacs+**) and the group name.

Mode

Global Configuration

See Also

tacacs-server host, **aaa authentication login**, **aaa authentication enable**

banner login

Name

banner login — Configure the login banner

Synopsis

banner login

no banner login

Description

Defines a customized message displayed before the login and password prompts. The login banner applies to console, telnet, and ssh connections.

To configure the login banner, hit enter after the **banner login** command and begin entering the desired message. The login banner may span multiple lines. To end the login banner, type 'EOF' on its own line and hit return.

Certain keywords can be used to display attributes of the switch. The following keywords are supported:

- `$(hostname)`: Displays the host name for the switch

Mode

Global Configuration

See Also

banner motd

banner motd

Name

banner motd — Configure the Message of the Day banner

Synopsis

banner motd

no banner motd

Description

Defines a customized message displayed after login. The motd applies to console, telnet, and ssh connections.

To configure the motd, hit enter after the **banner motd** command and begin entering the desired message. The motd may span multiple lines. To end the motd, type 'EOF' on its own line and hit return.

Certain keywords can be used to display attributes of the switch. The following keywords are supported:

- `$(hostname)`: Displays the host name for the switch

Mode

Global Configuration

See Also

banner login

boot system

Name

boot system — Select system boot software image

Synopsis

boot system *flash:/file-path*

boot system *usb1:/file-path*

Description

The **boot system** command can be used to configure the software image that is loaded at system startup. The image specified can be located on the flash: or on a USB drive, which is mounted as the usb1: device.

You can use *?* to list all available files on the device: e.g: **boot system** *flash:?* will list all available files on flash:. Note that the default extension of the boot images is **.swi**.

Mode

Global Configuration

See Also

show boot-config

cd

Name

cd — Change the current working directory

Synopsis

cd [*url*]

Description

Change the current working directory to *url*. If *url* is omitted, the current working directory is set to the home directory, namely `flash:/`.

The current working directory is the default argument when a complete path is not specified for file related operations.

The **cd** command makes it very convenient to perform file operations such as **copy**, **dir**, etc. By changing the current directory, you do not need to type the complete directory path over and over again.

Mode

Privileged EXEC

See Also

pwd, **dir**, **copy**

channel-group

Name

channel-group — Assign an interface to a port-channel

Synopsis

channel-group *number* **mode** { **on** | **active** | **passive** }

no channel-group

Description

Use the **channel-group** command to assign an interface to a port-channel.

mode on unconditionally assigns the interface to port-channel *number*.

mode active enables LACP on the interface in active mode.

mode passive enables LACP on the interface in passive mode.

To remove an interface from a port-channel, use the **no** form of this command.

Care must be taken when configuring an interface to be in a **channel-group** with **mode on**. If several interfaces in the same port-channel are configured with **mode on**, then it is required that all of these interfaces are physically connected to the same neighboring switch. Further, these interfaces must be configured to belong to a single port-channel on the neighboring switch as well. If these conditions are not met, then the pair of switches are misconfigured.

This unconditional static configuration disables LACP, and so the switch will not verify or negotiate the port-channel membership. Be careful to disable the unconditional port-channel membership before moving any cables connected to these interfaces or changing a static port-channel membership on the remote switch.

Mode

Interface Configuration

See Also

interface port-channel, **show port-channel**, **show port-channel limits**

clear aaa counters tacacs

Name

clear aaa counters tacacs — Clear the TACACS+ status counters

Synopsis

clear aaa counters tacacs

Description

Resets all TACACS+ status counters to zero.

Clearing these counters only affects the values reported by **show tacacs** and does not change interaction between the switch and TACACS+ servers.

Mode

Privileged EXEC

See Also

show tacacs

clear counters

Name — **clear counters** — Clear interface counters (set all counters to 0)

Synopsis — **clear counters** [*interface*] [**session**]

Description — This command clears counters for the specified interface, or for all interfaces if none is specified. With the **session** modifier, the clearing is effective only within the current CLI session, i.e., other CLI sessions are unaffected. This command is useful when looking for small changes in packet or error counters; it in effect establishes a baseline, and future uses of the **show interfaces** or **show interfaces counters** commands will be relative to the baseline.

Mode — Privileged EXEC

See Also — **show interfaces**, **show interfaces counters**

clear mac-address-table dynamic

Name — **clear mac-address-table dynamic** — Clear dynamic entries from the MAC address table

Synopsis — **clear mac-address-table dynamic** [**vlan***vlanId*] [**interface***name*]

Description — Clears the dynamic entries in the MAC address table. The command when used with no arguments clears all the dynamic entries in the MAC address table. The entries to be cleared can also be filtered by specifying the vlanId of the vlan or an interface, for which the entries are to be cleared.

Mode — Priviliged EXEC

See Also — **vlan**, **show mac-address-table**

clear spanning-tree counters

Name — **clear spanning-tree counters** — Clear spanning tree BPDU counters in all CLI sessions

Synopsis — **clear spanning-tree counters** [**interface** *interface*]

Description — The **clear spanning-tree counters** command resets the BPDU counters for the specified interface, or for all interfaces if none is specified, to zero values in all CLI sessions.

Mode — Privileged EXEC

See Also — **clear spanning-tree counters session**, **show spanning-tree counters**

clear spanning-tree counters session

Name — **clear spanning-tree counters session** — Clear all spanning tree BPDU counters in the current CLI session

Synopsis — **clear spanning-tree counters session**

Description — The **clear spanning-tree counter session** command resets the BPDU counters to zero values on all interfaces in the current CLI session. Counters in other CLI sessions are not affected.

Mode — Privileged EXEC

See Also — **clear spanning-tree counters**, **show spanning-tree counters**

clear spanning-tree detected-protocols

Name

clear spanning-tree detected-protocols — Restart the spanning tree protocol migration state machine on the selected interface or all interfaces

Synopsis

clear spanning-tree detected-protocols [**interface** *interface*]

Description

The **clear spanning-tree detected-protocols** command restarts the spanning tree protocol migration state machine on the given interface or all interfaces. This command is used to reset the switch to running the rapid spanning tree protocol on an interface where it has previously detected a bridge running the old version of the protocol.

Mode

Privileged EXEC

clock set

Name

clock set — Set the system date and time

Synopsis

clock set

Description

Set the system clock and time. The system clock needs to be setup so that system generated Syslog messages and other events are recorded accurately.

You can also configure the system to get the current clock using the **ntp server** command from an NTP server. In addition, you can use the **clock timezone** command to configure the correct timezone for your switch.

Mode

Privileged EXEC

See Also

clock timezone, **ntp server**

clock timezone

Name — **clock timezone** — Set the system timezone

Synopsis — **clock timezone** *name*

Description — The **clock timezone** *name* command is used to configure the system timezone. The timezone name can be any from the listed choices.

Mode — Global Configuration

See Also — **show clock**, **ntp server**

configure terminal

Name — **configure terminal** — Change the system configuration

Synopsis — **configure terminal**

Description — This command is used to change the system configuration. Once you enter this command, you can change the global configuration, or enter an interface configuration or some other sub-mode. All changes made in the configuration mode are applied to the running-configuration.

Once within the global configuration mode, you can use the **exit** command, or use **Ctrl-Z**.

Mode — Privileged EXEC

See Also — **enable**

connect

Name

connect — Connect to another host

Synopsis

connect *hostname*

connect *hostname port-number*

Description

Connect to another host using telnet, or any other protocol. The *hostname* can either be the hostname, or the IP address of the host. The second argument - *port-number* is optional, and is the port number for the specific protocol. The common protocols such as telnet, smtp, http are also available as choices. You can use the **connect hostname ?** command to see a complete listing of available protocol choices.

Mode

EXEC

See Also

telnet

copy

Name

copy — Copy a file

Synopsis

copy *source-url destination-url*

Description

Copies *source-url* to *destination-url*. If *destination-url* already exists, it is overwritten. If *destination-url* is a directory, *source-url* is copied into that directory with the same name.

Either or both of *source-url* or *destination-url* may be one of the special keywords **running-config** or **startup-config**, which are equivalent to the URLs `system:/running-config` and `flash:/startup-config` respectively.

Mode

Privileged EXEC

See Also

cd, **startup-config**, **running-config**

delete

Name — **delete** — Delete a file or directory tree

Synopsis — **delete** [**/recursive**] *url*

Description — Deletes the file *url*. *url* may be a wildcard, in which case all matching files are deleted.

The command fails if *url* is a directory, unless **/recursive** is specified, in which case *url* and its contents are deleted.

Note that to delete the startup config, you need to use the **erase startup-config** command

Mode — Privileged EXEC

See Also — **rmdir**, **erase startup-config**

description

Name

description — Set an interface's description

Synopsis

description *string*

no description

Description

The **description** command can be used to configure an interface's description. The description is displayed by the **show interfaces** and **show interfaces description** commands.

The **no** form of the command removes the configured description.

Mode

Interface Configuration

See Also

show interfaces, **show interfaces description**

diagnostic

Name — **diagnostic** — Enter diagnostic test mode

Synopsis — **diagnostic**

Description — The **diagnostic** command allows you to enter the diagnostic test mode and run tests. Please work with your support representative to run these tests - they are not yet designed to be run independently.

You can enter **exit** to return to the Privileged EXEC mode.

Mode — Privileged EXEC

See Also — **show diagnostic result**

diff

Name **diff** — Diff two urls

Synopsis **diff** *first-url second-url*

Description Compares two urls and displays the differences in the form of a unified diff.

Mode Privileged EXEC

See Also **startup-config**, **running-config**

dir

Name

dir — List files and directories

Synopsis

dir [**/recursive**] [**/all**] [*url* | **all-filesystems**]

Description

List information about files and directories. Entries are sorted alphabetically.

If *url* is specified, that file is listed, plus its contents if it is a directory. *url* may be a wildcard, in which case all matching files and directories are listed. If **all-filesystems** is specified, the contents of the root directory on all filesystems are listed. If neither *url* nor **all-filesystems** is specified, the contents of the current working directory are listed. If **/recursive** is specified, the contents of any subdirectories are listed recursively. If **/all** is specified, all files will be listed, including hidden files.

For each file or directory, the information presented comprises (in this order) the file's permissions (Directory, Read, Write and eXecute), the file's size (in bytes), the modification time of the file, and its name.

Mode

Privileged EXEC

See Also

pwd, **show file information**

disable

Name

disable — Exit from Privileged EXEC mode

Synopsis

disable 0-15

Description

Once within Privileged EXEC mode, you can use the **disable** command to return to EXEC mode. This way, you can disable all the Privileged commands, say when sharing your session with someone else.

You may specify an optional privilege level from 0 to 15, but the command will fail if the privilege level is greater than your session's current level. If not specified the disable command defaults to reducing the session to privlege level 1. A session with any privilege level greater than 1 is considered to be in Privileged EXEC mode.

Mode

Privileged EXEC

See Also

enable, **show privilege**

echo

Name **echo** — Echo a string

Synopsis **echo** *string*

Description The **echo** command is used to echo a string. This is especially helpful in creating a text file by using the echo command and redirecting the output to a file.

The **echo** command is also useful in putting markers in the output, when connecting to the system through scripts.

Mode Privileged EXEC

enable

Name

enable — Enter the Privileged EXEC mode

Synopsis

enable 0-15

Description

You can use the **enable** command to enter the Privileged EXEC mode.

You may specify an optional privilege level from 0 to 15. If not specified the enable command defaults to authenticating the session to level 15. A session with any privilege level greater than 1 is considered to be in Privileged EXEC mode.

By default EOS is configured to authenticate the enable command using the local database, in which case you must enter the enable password if it has been set. If you have configured EOS to use a different authentication method, the enable command will invoke that other method.

Mode

EXEC

See Also

show aaa, **show privilege**, **enable secret**

enable secret

Name

enable secret — Set password for privileged mode access

Synopsis

enable secret [**0**] *password*

enable secret 5 *encrypted-password*

no enable secret

Description

Set the password required to enter privileged EXEC mode when the enable authentication method list is set to **local**. The first form sets the privileged mode password to the given plaintext password. Use this form when typing a password by hand.

The second form takes a secure hash of the password (known as the "encrypted password") rather than the password itself. There is no known way to compute the password from its secure hash, so this form of the command is more secure. This form is useful primarily when cutting and pasting from a saved configuration file. When the device configuration is saved, only the second form of this command is used, so that the password is protected in the event that the configuration file is lost or stolen.

The third form is used to specify that no password is required to enter privileged EXEC mode.

Mode

Global Configuration

See Also

aaa authentication enable, **username secret**

end

Name

end — Return from any Configuration mode to Privileged EXEC mode

Synopsis

end

Description

You can use the **exit** command to return from any configuration mode to Privileged EXEC mode. Note that the **exit** command only returns you to the previous mode.

As an example, **exit** from Vlan Configuration mode will return the system to the Global Configuration mode. The **end** command however will return the system back from VLAN Configuration mode to Privileged EXEC mode.

Mode

Global Configuration
Interface Configuration
Vlan Configuration

See Also

exit

environment

Name **environment** — Configure environment parameters

Synopsis **environment fan-speed** { **auto** | **override** *percent* }

environment overheat action { **ignore** | **shutdown** }

Description Allows for the configuration of fan-speed settings and switch actions in response to overheat conditions.

Mode Global Configuration

erase startup-config

Name	**erase startup-config** — Erase the contents of the startup configuration
Synopsis	**erase startup-config**
Description	Erase the contents of the startup configuration file `flash:/startup-config`, if it exists.
Mode	Privileged EXEC
See Also	**startup-config**

errdisable recovery cause

Name

errdisable recovery cause — Enable the errdisable recovery for a cause

Synopsis

errdisable recovery cause bpduguard

no errdisable recovery cause bpduguard

default errdisable recovery cause bpduguard

Description

The **errdisable recovery cause** command enables the errdisable recovery timer for the specified cause.

The **no** and **default** forms of the command reverts back the errdisable recovery for the cause, to the default disabled setting.

Mode

Global Configuration

See Also

show errdisable recovery, **show interfaces status errdisabled**, **errdisable recovery interval**

errdisable recovery interval

Name

errdisable recovery interval — Configure the errdisable recovery timer interval

Synopsis

errdisable recovery interval *seconds*

no errdisable recovery interval

default errdisable recovery interval

Description

The **errdisable recovery interval** command configures the errdisable recovery timer interval. The interval value may be between 30 to 86400 seconds.

The **no** and **default** forms of the command reverts the timer interval to the default value of 300 seconds.

Mode

Global Configuration

See Also

errdisable recovery cause, **show errdisable recovery**, **show interfaces status errdisabled**

exit

Name

exit — Exit from current mode

Synopsis

exit

Description

The **exit** command can be used to exit from the current mode. In Global Configuration, or Interface Configuration mode, the **exit** command will return the system to the previous mode.

example: **exit** from Global Configuration mode will return the system to Privileged EXEC mode.

In the Privileged EXEC mode, or EXEC mode, the **exit** command will terminate the user session.

Mode

Privileged EXEC
Global Configuration
Interface Configuration
Vlan Configuration

See Also

configure terminal, **end**

extension

Name

extension — Install or uninstall an EOS extension

Synopsis

extension *extension-name* [*force*]

no extension *extension-name* [*force*]

Description

The **extension** configuration command can be used to install an extension.

Before an extension may be installed the extension must be copied to the EOS extension: filesystem. Use the **copy** command to copy an extension from the local flash filesystem, a USB disk, or a network URL. For example, **copy flash:/Awesome.swix extension:/** will add that extension. Use **delete** to remove an extension.

Note that the extensions filesystem resides on the internal flash disk of an Arista Networks switch, so there must be enough space available on the flash disk to hold the extension. The **dir extension:** command may be used to report available space on this filesystem.

To uninstall an extension use the **no extension** command.

The *force* option can be used to attempt to force the extension to install, ignoring certain errors such as missing dependencies or incorrect digital signatures. Arista Networks does not recommend use of the force option! When an extension fails to install there is typically a good reason, such as required packages not being installed or corruption in the extension file. If an extension fails to install without the force option please contact the developer of that extension for support.

Mode

Global Configuration

See Also

copy, **delete**, **show extensions**, **show loaded-extensions**

hostname

Name

hostname — Configure the system hostname

Synopsis

hostname *string*

no hostname

Description

The **hostname** command can be used to configure the system hostname.

Note that the hostname configured using the **hostname** command can also be used as the *%h* variable in the **prompt** command.

Mode

Global Configuration

See Also

prompt

int

Name

int — Filter configuration lines to include only those for a given interface or set of interfaces

Synopsis

int *pattern* [*pattern...*]

Description

You can use the **int** command as a filter after a '|' on the output of commands such as **show running-config** and **show startup-config** to restrict the output to include only the configuration of interfaces matching one of the given patterns. The name patterns can be full or abbreviated interface names, interface name ranges, or regular expressions.

For example, to display the configuration for interface Ethernet1 use the command:

```
show running-config | int Ethernet1
```

Abbreviated and lower case interface names are accepted as well, and these can be combined with a range to display the configuration for more than one interface. For example, to display the configuration for interfaces Ethernet1 and Ethernet2 in the startup config use the command:

```
show startup-config | int eth1 eth2
```

or

```
show startup-config | int eth1-2
```

You can also use regular expression syntax in the interface name pattern. For example, to display the configuration for interfaces Vlan1, Vlan3, and Vlan5 use the command:

```
show running-config | int vlan[1,3,5]
```

Mode

Privileged EXEC

interface

Name

interface — Configure one or more interfaces

Synopsis

interface *interface*
interface *interface-range*

no interface *interface*

Description

The **interface** configuration command can be used to configure an interface or a range of interfaces. Using this command, you can configure the interface description, flowcontrol configuration if applicable, configure the IP address of the interface, etc. For a complete list of choices, you can type **?** in interface configuration mode.

Note that the single-interface form of the command creates the interface if needed. The multiple-interface form of the command never creates interfaces. Interface ranges may not include interfaces that do not exist.

You can use the **exit** or **end** commands to return from the interface configuration mode.

Mode

Global Configuration

See Also

show interfaces, **Interface Range Syntax**

interface port-channel

Name

interface port-channel — Create or destroy a port-channel

Synopsis

interface port-channel *number*

no interface port-channel *number*

Description

Create port-channel numbered *number*. *number* may be an integer between 1 and 1000, inclusive.

To destroy a port-channel, use the **no** form of this command.

Note that it is not necessary to run **interface port-channel** before assigning a port to this port-channel (see **channel-group** interface configuration command). Port-channel *number* is implicitly created when a port is added to the specified port-channel with the **channel-group** *number* command. **show port-channel** *number* will display the ports that are members of this port-channel.

Mode

Global Configuration

See Also

channel-group, **show port-channel**

ip domain-name

Name

ip domain-name — Configure the IP domain of the system

Synopsis

ip domain-name *string*

no ip domain-name

Description

This configuration command can be used to configure the domain name of the system (such as **aristanetworks.com**). Once the domain name is set, hostnames used in other commands such as copy, or ping, do not need to be fully qualified.

When using this command, you also need a nameserver setup so that name resolution can be performed.

Mode

Global Configuration

See Also

ip name-server

ip igmp snooping

Name

ip igmp snooping - Configure IGMP snooping.

Synopsis

[no] ip igmp snooping

[no | **default] ip igmp snooping vlan** *vlan-range*

Description

This command can be used to enable or disable igmp snooping globally or for a particular vlan or vlan range. The effective snooping state of a vlan is determined by the combination of vlan snooping state and global snooping state.

Mode

Global Configuration

See Also

show ip igmp snooping

ip igmp snooping querier

Name

ip igmp snooping querier - Configure multicast querier properties.

Synopsis

[no] ip igmp snooping querier

[no | **default] ip igmp snooping vlan** *vlan-range* querier

ip igmp snooping querier [**vlan** *vlan-range*] querier **query-interval** *seconds*

no ip igmp snooping querier [**vlan** *vlan-range*] querier **query-interval**

ip igmp snooping querier [**vlan** *vlan-range*] querier **max-response-time** *seconds*

no ip igmp snooping querier [**vlan** *vlan-range*] querier **max-response-time**

ip igmp snooping querier [**vlan** *vlan-range*] querier **address** *ip-address*

no ip igmp snooping querier [**vlan** *vlan-range*] querier **address**

Description

The querier commands can be used to set querier properties for layer 2 querier functionality.

The command '**[no] ip igmp snooping querier**' can be used to enable or disable the querier. The global default setting is 'disabled'. The vlans, by default, follow the global setting, and can override it with vlan specific setting. The 'default' form of the command resets the vlan 'enabled' state to use global setting.

The command '**ip igmp snooping querier query-interval**' can be used to set the querier query-interval. The allowed values are 5-3600 seconds. The global default setting is 125 seconds. The vlans by default, follow the global setting, and can override it with vlan specific setting. The 'no' form of the command resets the property value to its default setting. Note that setting the querier query interval will also cause the switch to configure its membership/querier-timeouts, etc., appropriately.

The command '**ip igmp snooping querier max-response-time**' can be used to set the query-response-interval that the querier uses in the query packets that it sends out. The allowed values are 1-25 seconds. The global default setting is 10 seconds. The vlans, by default, follow the global setting, and can override it with vlan specific setting. The 'no' form of the command resets the property value to its default setting.

The command '**ip igmp snooping querier address**' can be used to set the querier ip address. This address is used for sending query packets, as well as, for participating in querier election. The global default setting is None. The vlans, by default, follow the global setting and can override it with vlan specific setting. The 'no' form of the command resets the property to its default setting.

Mode

Global Configuration

See Also **show ip igmp snooping querier**

ip igmp snooping robustness

Name **ip igmp snooping robustness-variable** - Configure IGMP snooping robustness variable.

Synopsis **[no] ip igmp snooping robustness-variable** {*1-3*}

Description This command can be used to configure robustness variable value. The value indicates the number of query intervals required to age out a port's membership in a group. The default value is 2.

Mode Global Configuration

See Also **show ip igmp snooping**

ip igmp snooping mrouter

Name **ip igmp snooping vlan mrouter** - Configure static multicast router interfaces.

Synopsis **[no] ip igmp snooping vlan** <*vlan range*> **mrouter interface** <*interface*>

Description This command can be used to add or remove the specified interface to/from the multicast router port set for a given vlan or vlan range.

Mode Global Configuration

See Also **show ip igmp snooping mrouter**

ip igmp snooping static

Name

ip igmp snooping vlan static - Configure static multicast group members.

Synopsis

[no] ip igmp snooping vlan <*vlan id*> **static** <*ip-addr*> **interface** <*interface*>

Description

This command can be used to add/remove the specified interface to/from the specified multicast group in the specified vlan. The ip address used with this command must be a valid unreserved IPv4 multicast address.

Mode

Global Configuration

See Also

show ip igmp snooping groups

ip name-server

Name

ip name-server — Specify the name and address resolution server(s)

Synopsis

ip name-server *ip-address* [...] [*ip-address*]

no ip name-server [*ip-address*] [...] [*ip-address*]

Description

This command can be used to configure the IP address of the name server(s) for your network. Up to three IP addresses may be configured.

Mode

Global Configuration

See Also

ip domain-name

ip route

Name

ip route — Configure a static route

Synopsis

ip route { *ip-address mask* | *ip-prefix* } { *interface-name* | *ip-address* } [*metric*]

no ip route { *ip-address mask* | *ip-prefix* }

Description

This command can be used to setup static routes. You can specify an outgoing interface to send packets to, or specify the IP address of the forwarding router.

Mode

Global Configuration

See Also

show ip route

lacp port-priority

Name

lacp port-priority — Set the LACP port priority

Synopsis

lacp port-priority *number*

no lacp port-priority *number*

Description

Set the LACP port priority to *number*. *number* may be an integer between 0 and 65535, inclusive. The default is 32768.

To return the port priority to its default value, use the **no** form of this command.

Mode

Interface Configuration

See Also

interface port-channel, **lacp system-priority**, **show port-channel**, **show lacp**

lacp rate

Name

lacp rate — Set the LACP requested transmission rate for this interface

Synopsis

lacp rate { **fast** | **slow** }

no lacp rate

Description

The LACP protocol allows a device to request whether its peer should transmit every 30 seconds (**slow**) or every 1 second (**fast**). Since the Arista Networks LACP implementation can detect link failure, the default is **slow**. There is normally no reason to configure this value.

Mode

Interface Configuration

See Also

interface port-channel, **show port-channel**, **show lacp**

lacp system-priority

Name

lacp system-priority — Set the LACP system priority

Synopsis

lacp system-priority *number*

no lacp system-priority

Description

Set the LACP system priority to *number*. *number* may be an integer between 0 and 65535, inclusive. The default is 32768.

To return the system priority to its default value, use the **no** form of this command.

Mode

Global Configuration

See Also

lacp port-priority, **show port-channel**, **show lacp**

load-interval

Name

load-interval — Set the load-interval for interface rate counters

Synopsis

load-interval *interval* - Set the load interval

no load-interval - Reset the load interval to default value of 300s

Description

The load interval determines the how the interface rate counters are calculated. The interface rates are exponentially weighted moving averages such that after 4 load-interval periods, the previous samples count for less than 2load-interval periods, the displayed rate will be within 2stable rate.

Valid values for load-interval are between 5s and 600s.

Mode

EXEC

See Also

show interfaces, **show interface counters**

logging buffered

Name

logging buffered — Configure logging to a system buffer

Synopsis

logging buffered [*buffer-size*] [*severity*]

no logging buffered

Description

This command can be used to enable and/or configure buffered logging. The optional buffer size, a number between 10 and 2147483647, configures the number of messages that are stored, defaulting to 32. You can also set a severity level for buffered logging, which may be specified either as a number between 0 and 7, or as one of the keywords **emergencies**, **alerts**, **critical**, **errors**, **warnings**, **notifications**, **informational** or **debugging**, defaulting to 7 (**debugging**). All system messages equal to, or more severe than the configured value will be logged to the system buffer.

The **[no]** form of the command disables buffered logging.

Mode

Global Configuration

See Also

logging level, **show logging**

logging console

Name

logging console — Configure logging to the console

Synopsis

logging console [*severity*]

no logging console

Description

This command can be used to enable and/or configure logging to the console. You can also set a severity level for console logging, which may be specified either as a number between 0 and 7, or as one of the keywords **emergencies**, **alerts**, **critical**, **errors**, **warnings**, **notifications**, **informational** or **debugging**, defaulting to 2 (**critical**). All system messages equal to or more severe than the configured value will be logged to all terminals on the system.

The **no** form of the command disables console logging.

Mode

Global Configuration

See Also

logging level, **show logging**

logging host

Name

logging host — Configure a syslog server to send system log messages to

Synopsis

logging host { *ip-address* | *hostname* }

no logging host { *ip-address* | *hostname* }

Description

You can use this command in Global Configuration mode to configure the IP address or hostname of your Syslog server. System log messages are then sent to this server, in addition to being logged to the system buffer.

To configure the logging level of messages sent to the Syslog server, please see the **logging trap** command.

Mode

Global Configuration

See Also

logging trap, **show logging**

logging level

Name

logging level — Configure the logging level for a facility

Synopsis

logging level *facility-name severity*

no logging level *facility-name*

Description

You can use this command in Global Configuration mode to configure the logging level of any of the system facilities. The severity may be specified either as a number between 0 and 7, or as one of the keywords **emergencies**, **alerts**, **critical**, **errors**, **warnings**, **notifications**, **informational** or **debugging**. The configured level is passed on to the software objects for the specified facility, and various debug messages can be seen based on the set severity level.

The **no** form of the command reverts the logging level for the facility to the default value of 7 (**debugging**).

Mode

Global Configuration

See Also

show logging

logging on

Name

logging on — Enable logging to all supported destinations

Synopsis

logging on

no logging on

Description

This command can be used to enable logging to all supported destinations — Syslog server and buffered logging.

Mode

Global Configuration

See Also

show logging

logging trap

Name

logging trap — Configure the level of messages sent to Syslog server

Synopsis

logging trap *severity*

no logging trap

Description

This command can be used to configure the level of log messages sent to the Syslog server. The severity may be specified either as a number between 0 and 7, or as one of the keywords **emergencies**, **alerts**, **critical**, **errors**, **warnings**, **notifications**, **informational** or **debugging**.

The **no** form of the command reverts the logging level to the default value of 6 (**informational**).

Mode

Global Configuration

See Also

show logging

logout

Name — **logout** — Exit from current session

Synopsis — **logout**

Description — The **logout** command can be used to exit from the current session. This is the same behavior as using the **exit** command from EXEC mode. However, the **logout** command can be used from any mode to terminate the session.

Mode — EXEC

See Also — **exit**

mac-address-table aging-time

Name

mac-address-table aging-time — Configure the MAC address table aging time

Synopsis

mac-address-table aging-time { *seconds* | *0* }

no mac-address-table aging-time

Description

This commands allows for the configuration of the aging time for MAC address table entries. The duration may be between 10 and 1000000 seconds, or 0 to disable MAC address table aging.

The **no** form of the command reverts the aging time to the default value of 300 seconds.

Mode

Global Configuration

See Also

show mac-address-table aging-time

mkdir

Name	**mkdir** — Create a directory
Synopsis	**mkdir** *url*
Description	Creates the directory *url*. example: **mkdir** *flash:images*
Mode	Privileged EXEC
See Also	**rmdir**

monitor session

Name

monitor session — Configure a mirroring session

Synopsis

monitor session *name* **source** *interface* [*direction*]

monitor session *name* **destination** *interface*

no monitor session *name*

no monitor session *name* **source** *interface* [*direction*]

no monitor session *name* **destination** *interface*

Description

Mirroring can be used to copy packets sent/recieved over the interface (mirror source) to another interface (mirror destination) for monitoring purposes.

The **monitor session** command can be used to configure mirroring. Mirroring is enabled when a session has at least one active mirror source and an active mirror destination. The command takes the session name and the interfaces on which mirroring is to be enabled as arguments.

By default, mirror sources are configured to mirror traffic in both directions. An optional direction argument may be specified to restrict traffic to only one direction.

A mirror source can be a physical interface or a LAG. Once an interface is a LAG member, it inherits the mirroring configuration of its LAG. If a LAG member is configured as a mirror source, the configuration only takes effect when the interface is removed from the LAG.

If a interface is configured as a mirror source or destination in any session, then the interface cannot be configured as a mirror source or destination in any other session.

The **no** forms of the command can be used to change direction of mirror source to both, remove a source, remove the destination or to remove the entire session.

Examples

```
monitor session mon1 source Ethernet1
```

Configures Ethernet1 as a source in mirroring session mon1

```
monitor session mon1 destination Ethernet2
```

Configures Ethernet2 as the destination in mirroring session mon1

```
monitor session mon1 source Ethernet4 rx
```

Configures Ethernet4 as an ingress only mirror source

```
monitor session mon1 source Ethernet1 tx
```

Changes Ethernet1 to be an egress only mirror source

```
no monitor session mon1 source Ethernet1 tx
```

Reverts Ethernet1 to be a bidirectional mirror source (default)

```
no monitor session mon1 source Ethernet4
```

Removes Ethernet4 as a mirror source.

Mode — Global Configuration

See Also — **show monitor session**

more

Name **more** — Display the contents of a file

Synopsis **more** *url*

Description Displays the contents of *url*.

Mode Privileged EXEC

See Also **show file information**

mtu

Name — **mtu** — Configure mtu on specified interface

Synopsis — **mtu** *mtu˙value*

Description — This command configures the MTU for the specified interface. The mtu command is currently supported only for Vlan and Management interfaces. The current MTU value for an interface can be seen via the **show interfaces** command.

Mode — Privileged EXEC

See Also — **show interfaces**

ntp server

Name — **ntp server** — Configure an NTP server

Synopsis — **ntp server** { *ip-address* | *hostname* }

Description — Allows the configuration of a Network Time Protocol server to synchronize the switch clock with an external time source.

Mode — Global Configuration

See Also — **show ntp status**, **show ntp associations**

nz

Name

nz — Filter out show command lines where all counters are 0

Synopsis

nz

Description

You can use the **nz** command as a filter after a '|' on the output of show commands that display tables of counters to leave out lines where all of the counters are zero. Lines that contain no counters, such as table header lines, are not filtered out.

For example, **nz** is often helpful for filtering the output of the **show interface counters** command so that you see only the lines for interfaces that have non-zero counters:

```
so334#show interfaces counters | nz
Port                InOctets     InUcastPkts     InMcastPkts     InBcastPkts
Et1                      320               0               5               0
Et12                     320               0               5               0
Et15                65400630           79836          449879               3
Et17                59834349               0          433533               0
Et19                 9838654               0           27431               0
Ma1                584418602          332230               0         4289539
Po2                 69671947               0          460960               0

Port               OutOctets    OutUcastPkts    OutMcastPkts    OutBcastPkts
Et1                      320               0               5               0
Et12                     320               0               5               0
Et15                 1899920               0           13195               0
Et17                 1933200               0           13425               0
Et19                 1900688               0           13207               0
Ma1                 56281330          327513               0               0
Po2                  3833888               0           26632               0
so334#
```

Mode

Privileged EXEC

ping

Name

ping — Ping another host to test network connectivity

Synopsis

ping *hostname* [**df-bit**] [**repeat** *count*] [**size** *num*] [**timeout** *seconds*]

Description

The **ping** command is similar to the standard ping command in unix. You can specify a hostname, or the IP address of the host you are trying to reach.

The **df-bit** argument can be used to set the do-not-fragment bit.

The **repeat** argument can be used to specify how many times to repeat the echo request. The default is 5 echo packets.

The **size** argument can be used to specify the datagram size. Without this argument, the datagram defaults to 72 bytes.

The **timeout** argument can be used to specify a timeout interval for the echo requests.

You can use **Ctrl-C** to interrupt the ping command. This is helpful when the timeout period is long and the host you are trying to connect to is unreachable.

A summary output is shown at the end of the ping command, showing you the number of packets transmitted, received, roundtrip time, and average latency.

If the destination host is unreachable, and you are certain that there is no problem in the network, you can use the **show ip route** command to see the current routing table of the system.

Mode

Privileged EXEC

See Also

show ip route

prompt

Name

prompt — Set the CLI prompt

Synopsis

prompt *prompt*

no prompt

Description

Sets the Command-Line Interface (CLI) prompt to *prompt*. Any of the following escape sequences may be present in *prompt*.

- **%h** The hostname of the switch up to the first '.'.
- **%H** The hostname of the switch.
- **%p** The prompt string for the current mode, for example ">" in user EXEC mode, "`#`" in privileged EXEC mode, or "`(config)#`" in global configuration mode.
- **%s** A space character.
- **%t** A tab character.
- **%%** A percent character.

The **no** form of the command reverts the prompt to its default value of **%h%p**.

Mode

Global Configuration

See Also

hostname

pwd

Name	**pwd** — Display the current working directory
Synopsis	**pwd**
Description	Display the URL of the current working directory.
Mode	Privileged EXEC
See Also	**cd**

reload

Name

reload — Reset and restart the system

Synopsis

reload [**power**] [**now**]

Description

The **reload** command can be used to reset the system. When the optional **power** argument is specified, the system is power-cycled. Otherwise a soft reset is performed. Unless the optional **now** argument is specified, there is a prompt if there are unsaved changes and a prompt to confirm the reload.

If there are unsaved changes, the prompt will allow saving the **running-confg** and also viewing the differences between **running-config** and **startup-config**.

The power cycle option is a way to reset the system completely, including memory states, and other hardware logic that may not be cleared on a soft reset. While this option is available, the simple **reload** command is sufficient for resetting the system.

Mode

Privileged EXEC

See Also

copy, **startup-config**, **running-config**

rename

Name **rename** — Rename a file

Synopsis **rename** *source-url destination-url*

Description Renames *source-url* to *destination-url*. *source-url* and *destination-url* must be on the same filesystem. If *destination-url* already exists, it is overwritten.

Mode Privileged EXEC

rmdir

Name **rmdir** — Remove a directory

Synopsis **rmdir** *url*

Description Removes the directory *url*. The command fails if the directory is not empty. To remove a non-empty directory, use **delete /recursive**.

Mode Privileged EXEC

See Also **mkdir**, **delete**

service sequence-numbers

Name **service sequence-numbers** — Stamp logger messages with a sequence number

Synopsis **service sequence-numbers**

no service sequence-numbers

Description Adds sequence numbers to logging data.

Mode Global Configuration

See Also **show logging**

show aaa

Name **show aaa** — Display the user database and corresponding encrypted passwords

Synopsis **show aaa**

Description Displays the Aaa user database in the system. The encrypted enable password is shown first, followed by a tabulated output of configured user-ids and their corresponding encrypted password.

Note that for security reasons, the un-encrypted password is never displayed.

Mode Privileged EXEC

show aaa method-lists

Name — **show aaa method-lists** — Display configured AAA method lists

Synopsis — **show aaa method-lists** { **authentication** | **authorization** | **all** }

Description — The policy that controls how the AAA agent authenticates and authorizes actions is defined by several ”method lists”. These method lists can be displayed with the command **show aaa method-lists**, passing the type of method lists that you wish to see, eg. **authentication** or **authorization**, or you may display all method lists with the command **show aaa method-lists all**.

Mode — Privileged EXEC

See Also — **aaa authentication enable**, **aaa authentication login**, **aaa authorization**

show aaa sessions

Name **show aaa sessions** — Display the current login sessions

Synopsis **show aaa sessions**

Description Displays the active AAA login sessions. The information displayed includes username, TTY, state of the session (pending or established), duration, authentication method, and if available, remote host and remote username.

Mode Privileged EXEC

show boot-config

Name

show boot-config — Display the software image that will be loaded at the next system reset

Synopsis

show boot-config

Description

Displays the system configuration showing the software image that will be loaded at bootup. Note that this information is saved separate from the startup-configuration, as the software image needs to be loaded prior to parsing the startup-configuration file.

The boot configuration can point to images in flash: or in usb1:.

Mode

Privileged EXEC

See Also

boot system

show boot-extensions

Name — **show boot-extensions** — Display EOS extension boot configuration

Synopsis — **show boot-extensions**

Description — Displays which extensions will be installed when EOS boots. The extensions are listed in the order in which they will be installed. The **boot-extensions** file has the same format as the output of the **show installed-extensions** command. This makes it possible to install one or more extensions then run the command **copy installed-extensions boot-extensions** to cause the set of currently installed extensions to be reinstalled after a reboot.

Mode — Privileged EXEC

See Also — **show installed-extensions**, **show extensions**

show clock

Name — **show clock** — Display the current time and configured timezone

Synopsis — **show clock**

Description — Displays the current system time and timezone. The system clock is used to generate timestamps for system log messages, and other debugging traces.

Mode — EXEC

See Also — **clock set**, **clock timezone**, **ntp server**

show environment all

Name	**show environment all** — Display all environment status of the system.
Synopsis	**show environment all**
Description	Displays all available environment status.
Mode	EXEC
See Also	**show environment cooling show environment temperature**

show environment cooling

Name **show environment cooling** — Display cooling related status of the system.

Synopsis **show environment cooling**

Description Displays the system fan status, fan speed configuration and ambient temperature.

Mode EXEC

See Also **show environment temperature**

show environment power

Name	**show environment power** — Display cooling related status of the system
Synopsis	**show environment power**
Description	Displays the system fan status, fan speed configuration and ambient temperature.
Mode	EXEC
See Also	**show environment temperature**

show environment temperature

Name	**show environment temperature** — Display the current operating temperature
Synopsis	**show environment temperature**
Description	Displays the current operating temperature of the system.
Mode	EXEC
See Also	**show environment cooling**

show errdisable detect

Name **show errdisable detect** — Display a summary of errdisable detection settings

Synopsis **show errdisable detect**

Description The command displays the errdisable detection setting for the errdisable causes.

Mode EXEC

See Also **show errdisable recovery**

show errdisable recovery

Name

show errdisable recovery — Display a summary of recovery timer settings, and recovery status for errdisabled interfaces

Synopsis

show errdisable recovery

Description

The command displays errdisable recovery timer setting for each errdisable reason (cause), and recovery status for errdisabled interfaces, that have recovery timers. The command shows the errdisable causes, and the time left before the recovery timeout for the errdisabled interfaces. The command does not display status for interfaces that are errdisabled due to causes for which timer recovery is not enabled.

Mode

EXEC

See Also

show interfaces status errdisabled, **errdisable recovery cause**, **errdisable recovery interval**

show error

Name

show error — Display details about a particular system error message

Synopsis

show error *number*

Description

Displays the details of a particular system error message.

The number specified is the error number. All system errors are numbered and start from 0. If the error number passed in has not been generated yet, the command returns a message indicating so.

Mode

EXEC

show extensions

Name — **show extensions** — Display status of EOS extensions

Synopsis — **show extensions** [*detail*]

Description — Displays status of the EOS extensions that are present in the extensions: filesystem and/or installed. Extensions can add features to EOS, or even modify built-in EOS features. Arista Networks customers and partners may develop their own extensions using the EOS SDK.

Specify the *detail* option to display more information about each installed extension.

Mode — Privileged EXEC

See Also — **show loaded-extensions**

show file information

Name **show file information** — Displays the type of a file

Synopsis **show file information** *url*

Description Displays type of *url*. Type of a file could be directory or a file. You can use the **more** command to display contents of a text file.

Mode Privileged EXEC

See Also **more**

show file systems

Name **show file systems** — List all filesystems

Synopsis **show file systems**

Description Displays information about all local and network filesystems, in alphabetical order.

The information presented for each filesystem comprises (in this order) the capacity of the filesystem (in bytes), the amount of free space on the filesystem (in bytes), the type of the filesystem, the filesystem flags, and the filesystem URL prefix.

Mode Privileged EXEC

show flowcontrol

Name

show flowcontrol — Display the interface flowcontrol information

Synopsis

show flowcontrol [**interface** *interface*]

Description

This command displays the flowcontrol details for the specified interface, or for all interfaces if none is specified. The output shows the configured and operating flowcontrol information for rx and tx directions of the interface(s).

This command is identical to **show interfaces flowcontrol**.

Mode

EXEC

See Also

show interfaces flowcontrol

show history

Name — **show history** — Display history of all commands issued

Synopsis — **show history**

Description — Displays a history of all commands issued during the session.

Mode — EXEC

show installed-extensions

Name **show installed-extensions** — Display installed EOS extensions

Synopsis **show installed-extensions**

Description Displays status of the EOS extensions that have been installed. The extensions are listed in the order in which they were installed. The output of this command is in the same format as the **boot-extensions** file, which determines which extensions are installed during the EOS boot procedure.

Mode Privileged EXEC

See Also **show extensions**

show interfaces

Name

show interfaces — Display details about the status of all interfaces

Synopsis

show interfaces [*interface-range*]

Description

Displays operational status and link related configuration of the specified list of interfaces, or all interfaces if no list is specified. The output includes speed, duplex and flow control information. In addition, basic statistics of the interface(s) are displayed.

The **show interfaces** command is helpful in getting a quick summary of the state of all interfaces. If you are looking for just the link status, you may find the **show interfaces status** command more helpful.

Mode

EXEC

See Also

show interfaces status, **Interface Range Syntax**

show interfaces capabilities

Name **show interfaces capabilities** — Display capabilities of all interfaces

Synopsis **show interfaces** [*interface-range*] **capabilities**

Description Displays capabilities of the specified interfaces, or all interfaces if no range is specified. The output includes speed, duplex and flow control capabilities of the interface(s).

Mode EXEC

See Also **show interfaces status**, **Interface Range Syntax**

show interfaces counters

Name — **show interfaces counters** — Displays interface packet and byte counters

Synopsis — **show interfaces** [*interface-range*] **counters**

Description — Displays the packet and byte counters per interface. The output is more detailed than the summary in **show interfaces** command.

Mode — EXEC

See Also — **show interfaces**, **Interface Range Syntax**

show interfaces counters bins

Name

show interfaces counters bins — Displays interface received packet counters by packet length

Synopsis

show interfaces [*interface-range*] **counters bins**

Description

Displays the received packet counters by packet length per interface. If an interface range is not specified, it displays the counters for all interfaces.

Here is an example of the command output:

```
localhost#show interface Ethernet1-2 counters bins
Port                64 Byte      64-127 Byte     128-255 Byte     256-511 Byte
-------------------------------------------------------------------------------
Et1                        0                0                0                0
Et2                        0                0                0                0

Port           512-1023 Byte   1024-1522 Byte    1523-MAX Byte
-------------------------------------------------------------
Et1                        0                0                0
Et2                        0                0                0
```

Mode

EXEC

See Also

show interfaces counters, **Interface Range Syntax**

show interfaces counters errors

Name — **show interfaces counters errors** — Displays interface error counters

Synopsis — **show interfaces** [*interface-range*] **counters errors**

Description — Displays the error counters per interface. If an interface range is not specified, it displays the error counters for all interfaces.

Here is an example of the command output:

```
localhost#show interface Ethernet1 counters errors
Port               FCS    Align    Symbol       Rx    Runts   Giants       Tx
Et1                  0        0         0        0        0        0        0
```

Mode — EXEC

See Also — **show interfaces counters**, **Interface Range Syntax**

show interfaces description

Name

show interfaces description — Display a summary of all interfaces and their description

Synopsis

show interfaces [*interface-range*] **description**

Description

Displays a summary of all interfaces and their description. This is useful when you want to remember where each interface is connected to, and have described an interface using the **description** command in interface configuration mode.

Mode

EXEC

See Also

description, **Interface Range Syntax**

show interfaces flowcontrol

Name

show interfaces flowcontrol — Display the interface flowcontrol information

Synopsis

show interfaces [*interface-range*] **flowcontrol**

Description

This command displays the flowcontrol details for the specified range of interfaces, or for all interfaces if no range is specified. The output shows the configured and operating flowcontrol information for rx and tx directions of the interface(s).

This command is identical to **show flowcontrol**.

Mode

EXEC

See Also

show flowcontrol, **Interface Range Syntax**

show interfaces status

Name

show interfaces status — Display a summary status of interfaces

Synopsis

show interfaces [*interface-range*] **status**

Description

The command displays status of the specified range of interfaces, or for all interfaces if no interface range is specified. The status shows the interface name, link status, vlan, current speed and duplex.

The output of **show interfaces** is more detailed, and **show interfaces status** is a good way of getting a summary of the operational status.

Mode

EXEC

See Also

show interfaces, **Interface Range Syntax**

show interfaces status errdisabled

Name **show interfaces status errdisabled** — Display a summary status of errdisabled interfaces

Synopsis **show interfaces [***interface***] status errdisabled**

Description The command displays status of the specified errdisabled interface, or for all errdisabled interfaces if no interface is specified. The status shows the interface name, link status, and the errdisable reasons, which are also referred to as errdisable causes.

Mode EXEC

See Also **show errdisable recovery**

show interfaces switchport

Name

show interfaces switchport — Display configured switching properties of interfaces

Synopsis

show interfaces [*interface-range*] **switchport**

Description

show interfaces switchport displays the current configuration of the specified interface range, or of all interfaces if no interface range is specified.

For example, consider the following configuration:

```
vlan 1-20
interface Ethernet1
   switchport access vlan 2
   switchport trunk native vlan 13
   switchport trunk allowed vlan 1-2,7,10-20
   switchport mode trunk
```

The output of the **show interfaces Ethernet1 switchport** command is:

```
localhost#show interfaces eth1 switchport
Name: Et1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Access Mode VLAN: 2 (VLAN0002)
Trunking Native Mode VLAN: 13 (VLAN0013)
Trunking VLANs Enabled: 1-2,7,10-20
```

Mode

EXEC

See Also

switchport mode trunk, **switchport access vlan**, **switchport trunk allowed vlan**, **switchport trunk native vlan**, **Interface Range Syntax**

show interfaces switchport backup

Name

show interfaces switchport backup — Display the running state of backup interface pairs

Synopsis

show interfaces [*interface*] **switchport backup**

Description

show interfaces switchport backup displays the current running state for configured backup interface pairs. When a specific interface argument is given, only the state for the pair containing that interface is displayed. For each pair, the command displays the members of the pair, the role and state of each interface, and the vlans that are currently forwarding on each interface.

For example, consider the following configuration:

```
vlan 1-20
spanning-tree mode backup
interface Ethernet11
   switchport mode trunk
   switchport backup interface Ethernet12 prefer vlan 11-20
interface Ethernet12
   switchport mode trunk
```

With both links up, the output of the **show interfaces switchport backup** command is:

```
localhost#show interfaces switchport backup
Switch backup interface pair: Ethernet11, Ethernet12
Primary Interface: Ethernet11       State:  Up
Backup Interface:  Ethernet12       State:  Up
Ethernet11 forwarding vlans:  1-10
Ethernet12 forwarding vlans:  11-20
```

If the link state of interface Ethernet11 goes down, the output of the command becomes:

```
localhost#show interfaces switchport backup
Switch backup interface pair: Ethernet11, Ethernet12
Primary Interface: Ethernet11       State:  Down
Backup Interface:  Ethernet12       State:  Up
Ethernet11 forwarding vlans:
Ethernet12 forwarding vlans:  1-20
```

If the Spanning Tree protocol mode is changed to something other than **backup**, the output of the command becomes:

```
localhost#show interfaces switchport backup
Switch backup interface pair: Ethernet11, Ethernet12
Primary Interface: Ethernet11       State:  Inactive Configuration
Backup Interface:  Ethernet12       State:  Inactive Configuration
```

Mode	EXEC

show interfaces transceiver properties

Name **show interfaces transceiver properties** — Display speed, duplex and media-type properties of the interface

Synopsis **show interfaces** [*interface-range*] **transceiver properties**

Description Displays the configured and operational speed and duplex of a range of interfaces (or all interfaces if no range is specified). In addition, the media type is displayed. The media type is helpful in distinguishing transceivers based on their capabilities.

Mode EXEC

See Also **show interfaces status**, **show interfaces**, **Interface Range Syntax**

show inventory

Name — **show inventory** — Display hardware inventory with serial numbers

Synopsis — **show inventory**

Description — Displays all hardware and related serial numbers associated with the switch.

Mode — EXEC

show ip igmp snooping

Name — **show ip igmp snooping** - Show IGMP Snooping status.

Synopsis — **show ip igmp snooping** [**vlan** *vlanId*]

Description — This command can be used to see global or per vlan igmp snooping status.

See Also — **ip igmp snooping**

show ip igmp snooping co

Name

show ip igmp snooping counters - Show multicast packet counters.

Synopsis

show ip igmp snooping count [**vlan** *vlanId*] [**detail**]

Description

This command can be used to see the packet counters for multicast control packets going out or coming in on various interfaces. The list can be filtered by specifying a vlanId.

show ip igmp snooping gr

Name

show ip igmp snooping groups - show multicast groups status.

Synopsis

show ip igmp snooping groups [**count** | **dynamic** | **user**] [**detail**]

show ip igmp snooping groups vlan *vlanId* [**count** | *A.B.C.D* | **dynamic** | **user**] [**detail**]

Description

This command can be used to see the status of multicast groups. The list can be filtered according to vlanId and/or group type.

See Also

ip igmp snooping vlan static

show ip igmp snooping mr

Name

show ip igmp snooping mrouter - Show multicast router status.

Synopsis

show ip igmp snooping mrouter [**vlan** *vlanId*] [**detail**]

Description

This command can be used to see the status of multicast routers along with their details. The list can be filtered by specifying a vlanId.

See Also

ip igmp snooping vlan mrouter show ip igmp snooping querier

show ip igmp snooping qu

Name

show ip igmp snooping querier - Show multicast querier status.

Synopsis

show ip igmp snooping querier [**vlan** *vlanId*] [**detail**]

Description

This command can be used to see the multicast queriers along with their details. The list can be filtered by specifying a vlanId.

See Also

show ip igmp snooping mrouter

show ip igmp snooping qu

Name

show ip igmp snooping querier status - Show switch layer-2 querier status.

Synopsis

show ip igmp snooping querier status [**vlan** *vlanId*]

Description

This command can be used to see the configuration and operational status of layer 2 querier on the switch. The list can be filtered by specifying a vlanId.

See Also

ip igmp snooping querier

show ip interface

Name **show ip interface** — Show IP information for an interface

Synopsis **show ip interface** [*interface*]

Description Displays the IP information for an interface. If no interface is specified, IP information for all interfaces is displayed

Mode EXEC

See Also **show ip route**, **ip route**

show ip route

Name — **show ip route** — Display the current routing table entries of the system

Synopsis — **show ip route**

Description — Display the current routing table entries of the system. The displayed entries include all static routes and dynamically learnt routes.

To configure routes statically, you can use the **ip route** configuration command.

Mode — EXEC

See Also — **ip route**

show lacp

Name

show lacp — Display LACP-related information

Synopsis

show lacp [*number*] { **counters** | **internal** | **neighbor** | **sys-id** | **aggregates** } [*detailLevel*] [**all-ports**] — Display LACP related information about port-channels and physical interfaces that are configured to use LACP. When *number* is included, then **show lacp** displays information about members of port-channel *number* only. When *number* is not included, all port-channels are displayed.

show lacp interface *interface* [*detailLevel*] — Display LACP related information about port-channels and interfaces that are configured to use LACP. When *interface* is included, displays information about interface *interface*, otherwise all interfaces are displayed.

The optional *detailLevel* controls what information is displayed for each interface that is chosen.

The **all-ports** option controls which interfaces are chosen for display.

Description

show lacp displays information about all port-channels configured to use LACP.

show lacp *number* displays LACP related information about port-channel *number* and its members.

show lacp interface displays information about all interfaces configured to use LACP.

show lacp interface *interface* displays LACP related information about **interface** *interface*.

When **brief** is specified (the default), then the **show lacp** command prints out basic information about each port in the port-channel.

When **detailed** is specified, then **show lacp** displays far more detailed information about each port.

The **show lacp** command only displays information about port-channels configured to use LACP. When a port is configured to be part of a port-channel, the user can specify the mode. (See **channel-group** interface configuration command to configure an interface to be part of a port-channel). If the mode is "on", then the port-channel is statically configured, and the port-channel does not use LACP, and no information about this port-channel is displayed in the **show lacp** command. If the mode is either "active" or "passive" then the port-channel is configured to use LACP (in either active or passive mode, respectively).

If a physical interface is configured to be part of a port-channel, and the port-channel is configured to use LACP (i.e. the mode is not statically "on"), then the physical interface may be one of the ports considered by LACP. However, LACP only considers a set of "compatible" ports. **show port-channel limits** displays the sets of architecturally mutually compatible ports. Of the set of ports in a compatible set that are configured to be in the same port-channel, LACP will consider only interfaces that have the same attributes (e.g. speed, duplex). Further, LACP considers only active interfaces (for example, those whose link-status is up). **show port-channel** will display information about interfaces that are part of the port-channel, but are not being considered as candidates by LACP.

By default, we only print LACP information about ports that are actually bundled by LACP into the aggregate (such ports have status "Bundled") . If **all-ports** is specified, then we also print

information about ports that are not part of the bundle, but *are* considered as candidates by LACP.

Candidates for LACP aggregation may have status other than "Bundled". If LACP negotiated the port as a standby port, then the status is "Standby". If we are still waiting for the remote LACP to return, then the port status is "In Negotiation". Finally, if LACP negotiated an aggregate for this port which *differs* from the primary aggregate for this port-channel, then there must be some misconfiguration — the aggregates on the two ends do not agree. In such cases the status is displayed as "Mismatched Agg!", and the administrator should investigate the conflicting configuration information on the two switches.

show lacp sys-id displays the System Identifier used by our local LACP when negotiating with remote LACP implementations.

show lacp internal displays the local state of the LACP protocol for each interface. The local state includes the state machines and protocol information described in 802.11.43, as well as some internal state relevant to the Eos implementation of LACP.

show lacp neighbor displays our knowledge of the remote state of the LACP protocol for the neighbor of each interface.

show lacp interface allows the user to specify individual interfaces rather than port-channels. It displays both local and remote information about the LACP state (roughly the combined information of **show lacp internal** and **show lacp neighbor**).

show lacp aggregates displays the aggregates negotiated by LACP for each configured port-channel. The aggregate information includes the aggregate's LAG ID, as well as the member ports.

Mode

EXEC

See Also

channel-group, **show port-channel**, **show port-channel limits**, **lacp system-priority**

show logging

Name — **show logging** — Displays Syslog configuration and buffered log messages

Synopsis — **show logging**

Description — This command displays the current Syslog configuration, and shows the contents of the system logging buffer, if buffered logging is enabled. You can also configure the system to send messages to a Syslog server using the **logging host** configuration command.

Mode — EXEC

See Also — **logging level**, **service sequence-numbers**, **logging buffered**

show mac-address-table

Name

show mac-address-table — Display the contents of the MAC address table

Synopsis

show mac-address-table [**static** | **dynamic**] [**address** *mac-addr*] [**interface** *interface*] [**vlan** *vlanId*]

show mac-address-table multicast [**vlan** *vlanId*] [**user**] [**count**]

show mac-address-table count [**vlan** *vlanId*]

Description

To display entries in the MAC address table, type the command

```
show mac-address-table
```

As shown above, the command prints all addresses known to the switch: static entries, dynamic entries and multicast entries. The entries are shown with the following fields:

`Vlan`	VLAN ID on which this address was learned. The device learns MAC address entries on each VLAN independently.
`MAC address`	The host MAC address, in hexadecimal format.
`Type`	The type of the entry: one of STATIC, DYNAMIC or USER. Multicast addresses seeded by the operator get the USER label.
`Ports`	All ports associated with this host address. For dynamically-learned hosts, this is only a single port. For statically configured hosts this may show more than one port. The port name shown is an abbreviation of the full port name, e.g. 'Et1' for 'Ethernet1'.

The MAC address entries can be filtered by a number of options to the **show mac-address-table** command:

- If an entry type is specified, the display shows only entries of that type:

  Just dynamic entries:

  show mac-address-table dynamic

  Just static entries:

  show mac-address-table static

  Just multicast entries:

  show mac-address-table multicast

- Entries corresponding to a specific VLAN are shown with the **vlan** argument:

  show-mac-address-table vlan 1

  This shows all host entries learned on VLAN 1.

- Entries corresponding to a specific port on the device are shown with the **interface** argument:

  show mac-address-table interface Ethernet1

  This shows all hosts learned on Ethernet1.

- Entries corresponding to a specific MAC address are shown with the **address** argument:

  show mac-address-table address 00:11:22:33:44:55

  This shows all instances of the host '00:11:22:33:44:55' being learned on any port or VLAN.

- To show just a summary count of addresses in the table, use the **count** argument:

  show mac-address-table count

Mode EXEC

See Also **vlan**

show mac-address-table aging-time

Name **show mac-address-table aging-time** — Display the configured MAC address table aging time

Synopsis **show mac-address-table aging-time**

Description The **show mac-address-table aging-time** command displays the current aging time for MAC address table entries. The aging time may be configured with the **mac-address-table aging-time** command.

Mode EXEC

See Also **mac-address-table aging-time**

show monitor session

Name

show monitor session — Shows the configured mirror session

Synopsis

show monitor session [*name*]

Description

The **show monitor session** command can be used to show all the mirror sessions currently configured. The command takes an optional argument name which filters the output of the command to only a paricular session.

Here is an example output from the command **show monitor session session1**

```
Session session1
------------------------

Source Ports

  Rx Only:      Et2
  Tx Only:      Et1
  Both:         Et3
  Inactive:     Et4 ( Interface Mode Conflict )

Destination Port: Et6
```

In this output each mirror source is listed with the direction in which it is mirroring. Interfaces that belongs to a channel-group are marked as an inactive mirror source or destination.

See Also

monitor session

show ntp associations

Name	**show ntp associations** — Display the current operating configuration
Synopsis	**show ntp associations**
Description	Displays the current operating configuration of the system as a sequence of configuration commands.
Mode	EXEC
See Also	**show ntp status**

show ntp status

Name	**show ntp status** — Display the current operating configuration
Synopsis	**show ntp status**
Description	Displays the current operating configuration of the system as a sequence of configuration commands.
Mode	EXEC
See Also	**show ntp associations**

show port-channel

Name

show port-channel — Display the members of a port-channel

Synopsis

show port-channel [*number*] [**brief** | **detailed**]

Description

show port-channel displays the members of all port-channels.

show port-channel *number* displays the members of port-channel *number*.

When **brief** is specified (the default) only the currently active members of the port-channel are displayed. When **detailed** is specified *all* configured ports in the port-channel are displayed, whether they are active or not. For inactive ports, **show port-channel** *number* provides a brief reason explaining why the port is inactive.

Note that a port-channel may be configured to contain many ports, but that only a subset may be active at any given time. All active ports in a port-channel must be *compatible*. Compatibility comprises many factors and is specific to a given platform. For example, compatibility may require identical operating parameters such as speed and/or MTU. Compatibility may only be possible between specific ports because of internal organization of the switch. **show port-channel limits** displays the platform specific compatibility requirements (as well as other information that may affect whether ports in a port-channel are currently active.)

A given port-channel may be configured with a set of ports such that more than one subset of the member ports are mutually compatible. Port-channels in EOS are designed to activate the compatible subset of ports with the largest aggregate capacity. A subset with 2 40Gbps ports (aggregate capacity 80Gbps) will be selected in preference to a subset with 5 active 10Gbps ports (aggregate capacity 50Gbps).

Mode

EXEC

See Also

channel-group, **show port-channel limits**

show port-channel limits

Name

show port-channel limits — Displays per-platform limits on how port-channels may be formed from ports

Synopsis

show port-channel limits

Description

show port-channel limits displays groups of ports that are compatible and that may therefore be joined together into port-channels. Each group of compatible ports is called a *LAG group*. For each LAG group, the command also displays "Max interfaces" and "Max ports per interface". "Max interfaces" is a limit that defines the maximum number of active port-channels that may be formed out of these ports. "Max ports per interface" is a limit that defines the maximum number of active ports allowed in a port-channel comprised of ports from this compatibility group at any given time.

Mode

EXEC

See Also

channel-group, **show port-channel**

show privilege

Name — **show privilege** — Display the session's current privilege level

Synopsis — **show privilege**

Description — Displays the current privilege level of the session.

Mode — EXEC

See Also — **enable**, **disable**

show processes

Name

show processes — Show system process and CPU utilization information.

Synopsis

show processes

Description

Displays a one-line summary of how long the system has been up, followed by a list of all processes on the system, sorted by CPU utilization. The first line follows the format of **show uptime**. The columns in the process display consist of:

PID Process ID

%CPU
: Cpu utilization percentage (Cpu time used by this process divided by the time the process has been running)

%MEM
: Memory usage ratio (Process resident memory usage divided by the total physical memory size)

TT Controlling tty (terminal)

STAT
: Process state

  ’D’ Uninterruptible sleep

  ’R’ Running

  ’S’ Sleeping

  ’T’ Traced or stopped

  ’Z’ Zombie

STARTED
: Time the command was started. (HH:MM:SS if less than 24 hours ago, otherwise MMM DD)

TIME
: Cumulative CPU time

CMD
: Command with all its arguments. Note that it is possible for the process to modify this information. If the arguments are not available, the executable name will be shown in brackets.

Mode

EXEC

See Also

show uptime, **show processes top**

show processes top

Name

show processes top — Show a dynamic real-time view of system processes and CPU utilization.

Synopsis

show processes top

Description

Top runs interactively, filling the terminal window with a dynamic display of system process and CPU utilization. A variety of single-character commands are available to modify the output.

Enter '?' while **show processes top** is running for a help screen with all the supported commands.

Enter 'q' or Ctrl-C to exit and return to the Cli prompt.

The default columns in the process display consist of:

PID Process ID

USER
Effective username of the task's owner

PR Priority of the task

NI Nice value of the task

VIRT
Total amount of virtual memory used by the task (kb)

RES Resident size - the non-swapped physical memory used by the task (kb)

SHR Amount of shared memory used by the task (kb)

S Process state

- 'D' Uninterruptible sleep
- 'R' Running
- 'S' Sleeping
- 'T' Traced or stopped
- 'Z' Zombie

%CPU
Cpu utilization percentage (Cpu time used by this process divided by the time the process has been running)

%MEM
Memory usage ratio (Process resident memory usage divided by the total physical memory size)

TIME
Cumulative CPU time for the task

COMMAND
The program name associated with starting the task

Mode EXEC

See Also **show uptime**, **show processes**

show running-config

Name

show running-config — Display the current running configuration of the system

Synopsis

show running-config [**diffs**]

Description

Displays the current operating configuration of the system as a sequence of configuration commands. To save the running-config, you can use the **copy** command: **copy running-config startup-config**.

Specifying **diffs** causes the differences with the startup configuration to be displayed in unified diff format, the same as **diff startup-config running-config**

Mode

Privileged EXEC

See Also

running-config, **show startup-config**, **copy diff**

show running-config interface

Name

show running-config interface — Display the current running configuration of an interface or set of interfaces

Synopsis

show running-config interface *name pattern* [*name pattern*]

Description

This command displays the current operating configuration of interfaces matching the given interface name pattern or patterns. The name patterns can be full or abbreviated interface names, interface name ranges, or regular expressions.

For example, to display the configuration for interface Ethernet1 use the command:

```
show running-config interface Ethernet1
```

Abbreviated and lower case interface names are accepted as well, and these can be combined with a range to display the configuration for more than one interface. For example, to display the configuration for interfaces Ethernet1 and Ethernet2 use the command:

```
show running-config interface eth1 eth2
```

or

```
show running-config interface eth1-2
```

You can also use regular expression syntax in the interface name pattern. For example, to display the configuration for interfaces Vlan1, Vlan3, and Vlan5 use the command:

```
show running-config interface vlan[1,3,5]
```

Mode

Privileged EXEC

show snmp

Name

show snmp — Display high-level status of the SNMP agent

Synopsis

show snmp

Description

Displays high-level status of the SNMP agent. If the SNMP agent is enabled, the output will include SNMP packet and error counters, as well as the SNMP contact and location, if configured.

More detailed information about other aspects of the SNMP agent configuration is available through the **show snmp community**, **show snmp group**, **show snmp host**, **show snmp user**, and **show snmp view** commands.

Mode

EXEC

See Also

show snmp community, **show snmp group**, **show snmp host**, **show snmp user**, **show snmp view**

show snmp community

Name	**show snmp community** — Display details of the configured SNMP communities
Synopsis	**show snmp community**
Description	Displays a listing of the communities that have been configured for the SNMP agent.
Mode	EXEC
See Also	**snmp-server community**

show snmp engineID

Name	**show snmp engineID** — Displays the SNMP agent's engineID
Synopsis	**show snmp engineID**
Description	Displays the SNMP agent's engineID, which is used for SNMPv3 authentication.
Mode	EXEC
See Also	**snmp-server engineID**

show snmp group

Name — **show snmp group** — Display details of the configured SNMP groups

Synopsis — **show snmp group**

Description — Displays a listing of the groups that have been configured for the SNMP agent.

Mode — EXEC

See Also — **snmp-server group**

show snmp host

Name **show snmp host** — Display details of the configured SNMP trap destination hosts

Synopsis **show snmp host**

Description Displays a listing of the hosts that have been configured to receive traps or informs from the SNMP agent.

Mode EXEC

See Also **snmp-server host**

show snmp user

Name **show snmp user** — Display details of the configured SNMP users

Synopsis **show snmp user**

Description Displays a listing of the users that have been configured for the SNMP agent.

Mode EXEC

See Also **snmp-server user**

show snmp view

Name — **show snmp view** — Display details of the configured SNMP views

Synopsis — **show snmp view**

Description — Displays a listing of the access control views that have been configured for the SNMP agent. Listed with each view are the object identifier trees that are included or excluded from that view.

Mode — EXEC

See Also — **snmp-server view**

show spanning-tree

Name

show spanning-tree — Display a summary of the spanning tree protocol state

Synopsis

show spanning-tree

Description

The **show spanning-tree** command displays a summary of the state of the spanning tree protocol running on the switch. For more details, use the **show spanning-tree detail** command.

Here is an example of the command output:

```
Rstp
  Spanning tree enabled protocol rstp
  Root ID    Priority    32768
             Address     001c.7301.0089
             This bridge is the root

  Bridge ID  Priority    32768  (priority 32768 sys-id-ext 0)
             Address     001c.7301.0089
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

Interface        Role       State      Cost      Prio.Nbr Type
---------------- ---------- ---------- --------- -------- --------------------
Et1              designated forwarding 2000      128.1    P2p
Et2              designated forwarding 2000      128.2    P2p
Et3              designated forwarding 2000      128.3    P2p
Et4              designated forwarding 2000      128.4    P2p
Et20             designated forwarding 2000      128.20   P2p
Et24             backup     discarding 2000      128.24   P2p
```

In this output, we first see this switch's information on the root bridge of the network. Next comes information on this switch. Finally, for each interface we see a summary of the current spanning tree state for the interface. Interfaces that are link down are not running the spanning tree protocol and are not shown in the command output.

Mode

EXEC

show spanning-tree blockedports

Name

show spanning-tree blockedports — Display a list of the interfaces in the spanning tree discarding state

Synopsis

show spanning-tree blockedports

Description

The **show spanning-tree blockedports** command displays a list of the interfaces on the switch that are up and running the spanning tree protocol and are in the **discarding** state.

Here is an example of the command output:

```
Name       Blocked Interfaces List
---------- ------------------------------------------------------------------
Rstp       Et1, Et10, Et24

Number of blocked ports (segments) in the system : 3
```

Mode

EXEC

show spanning-tree bridge

Name

show spanning-tree bridge — Display a brief summary of the spanning tree protocol bridge configuration

Synopsis

show spanning-tree bridge

Description

The **show spanning-tree bridge** command displays a list of the spanning tree protocol configuration information for each spanning tree instance running on the switch. The switch currently supports only one instance, so the list is somewhat short.

Here is an example of the command output:

```
                              Bridge ID                      Hello  Max  Fwd
Instance             Priority             MAC addr          Time   Age  Dly
----------   ----------------------------------------      -----  ---  ---
Rstp         32768(32768, sys-id 0   ) 001c.7301.0089        2    20   15
```

Mode

EXEC

show spanning-tree bridge detail

Name

show spanning-tree bridge detail — Display a detailed description of the spanning tree protocol bridge configuration

Synopsis

show spanning-tree bridge detail

Description

The **show spanning-tree bridge detail** command displays a list of the spanning tree protocol configuration information for each spanning tree instance running on the switch. The switch currently supports only one instance, so the list is somewhat short.

Here is an example of the command output:

```
Rstp
  Bridge ID  Priority    32768  (priority 32768 sys-id-ext 0)
             Address     001c.7301.0089
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
```

Mode

EXEC

show spanning-tree counters

Name **show spanning-tree counters** — Display the spanning tree BPDU counters

Synopsis **show spanning-tree counters**

Description The **show spanning-tree counters** command displays the state of the spanning tree BPDU counters.

Here is an example of the command output:

```
port           sent received taggedErr otherErr

Ethernet5       582        0         0        0
Ethernet6       582        0         0        0
Ethernet7       582      381         0        0
Ethernet8       582      381         0        0
Ethernet22      583        2         0        0
Ethernet24        3      582         0        0
```

Mode EXEC

show spanning-tree detail

Name

show spanning-tree detail — Display a detailed description of the spanning tree protocol state

Synopsis

show spanning-tree detail

Description

The **show spanning-tree detail** command displays a detailed listing of the state of the spanning tree protocol running on the switch.

Here is an example of the command output:

```
Rstp is executing the rstp Spanning Tree protocol
 Bridge Identifier has priority 32768, sysid 0, address 001c.7301.0089
 Configured hello time 2, max age 20, forward delay 15, transmit hold-count 6
 We are the root of the spanning tree
 Number of topology changes 1 last change occurred 272586 seconds ago
         from Ethernet20
 Times: hello 2, max age 20, forward delay 15

Port 1 (Ethernet1) of Rstp is designated forwarding
  Port path cost 2000, Port priority 128, Port Identifier 128.1.
  Designated root has priority 32768, address 001c.7301.0089
  Designated bridge has priority 32768, address 001c.7301.0089
  Designated port id is 128.1, designated path cost 0
  Timers: message age 0, forward delay 15, hold 20
  Number of transitions to forwarding state: 1
  Link type is point-to-point by default, Internal
  BPDU: sent 136064, received 0, taggedErr 0, otherErr 0

Port 2 (Ethernet2) of Rstp is designated forwarding
  Port path cost 2000, Port priority 128, Port Identifier 128.2.
  Designated root has priority 32768, address 001c.7301.0089
  Designated bridge has priority 32768, address 001c.7301.0089
  Designated port id is 128.2, designated path cost 0
  Timers: message age 0, forward delay 15, hold 20
  Number of transitions to forwarding state: 1
  Link type is point-to-point by default, Internal
  BPDU: sent 136064, received 0, taggedErr 0, otherErr 0

Port 3 (Ethernet3) of Rstp is designated forwarding
  Port path cost 2000, Port priority 128, Port Identifier 128.3.
  Designated root has priority 32768, address 001c.7301.0089
  Designated bridge has priority 32768, address 001c.7301.0089
  Designated port id is 128.3, designated path cost 0
  Timers: message age 0, forward delay 15, hold 20
  Number of transitions to forwarding state: 1
  Link type is point-to-point by default, Internal
  BPDU: sent 136064, received 0, taggedErr 0, otherErr 0
```

```
Port 4 (Ethernet4) of Rstp is designated forwarding
  Port path cost 2000, Port priority 128, Port Identifier 128.4.
  Designated root has priority 32768, address 001c.7301.0089
  Designated bridge has priority 32768, address 001c.7301.0089
  Designated port id is 128.4, designated path cost 0
  Timers: message age 0, forward delay 15, hold 20
  Number of transitions to forwarding state: 1
  Link type is point-to-point by default, Internal
  BPDU: sent 136064, received 0, taggedErr 0, otherErr 0

Port 20 (Ethernet20) of Rstp is designated forwarding
  Port path cost 2000, Port priority 128, Port Identifier 128.20.
  Designated root has priority 32768, address 001c.7301.0089
  Designated bridge has priority 32768, address 001c.7301.0089
  Designated port id is 128.20, designated path cost 0
  Timers: message age 0, forward delay 15, hold 20
  Number of transitions to forwarding state: 1
  Link type is point-to-point by default, Internal
  BPDU: sent 136065, received 2, taggedErr 0, otherErr 0

Port 24 (Ethernet24) of Rstp is backup discarding
  Port path cost 2000, Port priority 128, Port Identifier 128.24.
  Designated root has priority 32768, address 001c.7301.0089
  Designated bridge has priority 32768, address 001c.7301.0089
  Designated port id is 128.20, designated path cost 0
  Timers: message age 0, forward delay 15, hold 20
  Number of transitions to forwarding state: 0
  Link type is point-to-point by default, Internal
  BPDU: sent 2, received 136065, taggedErr 0, otherErr 0
```

In this output, we first see information on this switch. Then we see the detailed spanning tree state for the interface. Interfaces that are link down are not running the spanning tree protocol and are not shown in the command output.

Mode EXEC

show spanning-tree interface

Name

show spanning-tree interface — Display a summary of the spanning tree protocol state for a given interface

Synopsis

show spanning-tree interface *interface*

Description

The **show spanning-tree interface** command displays a summary of the spanning tree protocol information for the given interface. This is the same information displayed for all interfaces by the **show spanning-tree** command.

Here is an example of the command output:

```
localhost#show spanning-tree interface ethernet1
Instance       Role       State      Cost      Prio.Nbr Type
-------------- ---------- ---------- --------- -------- ------
Et1            designated forwarding 2000      128.1    P2p
```

Mode

EXEC

show spanning-tree interface detail

Name

show spanning-tree interface detail — Display a detailed description of the spanning tree protocol state for a given interface

Synopsis

show spanning-tree interface *interface* **detail**

Description

The **show spanning-tree interface detail** command displays a detailed description of the spanning tree protocol information for the given interface. This is the same information displayed for all interfaces by the **show spanning-tree detail** command.

Here is an example of the command output:

```
localhost#show spanning-tree interface ethernet1 detail
 Port 1 (Ethernet1) of Rstp is designated forwarding
   Port path cost 2000, Port priority 128, Port Identifier 128.1.
   Designated root has priority 32768, address 001c.7301.0089
   Designated bridge has priority 32768, address 001c.7301.0089
   Designated port id is 128.1, designated path cost 0
   Timers: message age 0, forward delay 15, hold 20
   Number of transitions to forwarding state: 1
   Link type is point-to-point by default, Internal
   BPDU: sent 136717, received 0
```

Mode

EXEC

show spanning-tree root

Name

show spanning-tree root — Display a summary of the spanning tree protocol information for the root bridge of the network

Synopsis

show spanning-tree root

Description

The **show spanning-tree root** command displays a summary of the spanning tree protocol information for the current root bridge of the network for each spanning tree protocol instance. The switch currently supports only one instance, so the list is somewhat short.

Here is an example of the command output:

```
localhost#show spanning-tree root
                   Root ID          Root    Hello  Max  Fwd
Instance     Priority    MAC addr   Cost    Time   Age  Dly  Root Port
----------   ------------------- --------- -----  ---  ---  ------------
Rstp         32768 001c.7301.0089 000000000    2    20  15   None
```

Mode

EXEC

show spanning-tree root detail

Name

show spanning-tree root detail — Display a detailed description of the spanning tree protocol information for the root bridge of the network

Synopsis

show spanning-tree root detail

Description

The **show spanning-tree root detail** command displays a detailed description of the spanning tree protocol information for the current root bridge of the network for each spanning tree protocol instance. The switch currently supports only one instance, so the list is somewhat short.

Here is an example of the command output:

```
localhost#show spanning-tree root detail
Rstp
  Root ID    Priority    32768
             Address     001c.7301.0089
             This bridge is the root
```

Mode

EXEC

show spanning-tree topology status

Name

show spanning-tree topology status — Display the forwarding state programmed into the hardware for active vlan/interface combinations

Synopsis

show spanning-tree topology [**vlan** *vlanId*] **status**

Description

The **show spanning-tree topology status** command displays the forwarding state currently programmed into the packet forwarding hardware for active vlan/interface combinations. The output can be limited to the information for a single vlan using the optional **vlan** *vlanId* argument.

Be aware that many vlans can be mapped to a single topology. For example, when the spanning tree mode is configured to **rstp**, all active vlans are mapped to the same topology. Also, be aware that only active port and vlan combinations are included in the output. If a port is link down, it is not active in any topology and will not be show by this command.

Here is an example of the command output when running in **rstp** mode and all ports are forwarding:

```
Topology: Rstp
  Mapped Vlans: 1,10-20
  Ethernet11:        forwarding
  Ethernet12:        forwarding
  Ethernet22:        forwarding
  Ethernet25:        forwarding
  Ethernet26:        forwarding
  Ethernet27:        forwarding
  Ethernet43:        forwarding
  Ethernet44:        forwarding
  Ethernet45:        forwarding
  Ethernet46:        forwarding
```

In this output, we see that vlans 1 and 10 through 20 are all mapped to the Rstp topology. This switch is the root of the network, so all link up ports are forwarding.

Mode

EXEC

show spanning-tree vlan

Name

show spanning-tree vlan — Display a summary of the spanning tree protocol information for the given vlan

Synopsis

show spanning-tree vlan *vlan˙id*

Description

The **show spanning-tree vlan** command displays a summary of the spanning tree protocol information for the given vlan. Currently all vlans are mapped to a single spanning tree instance, so the out put of this command is the same as the **show spanning-tree** command.

Here is an example of the command output:

```
localhost#show spanning-tree vlan 2
Rstp
  Spanning tree enabled protocol rstp
  Root ID    Priority    32768
             Address     001c.7301.0089
             This bridge is the root

  Bridge ID  Priority    32768  (priority 32768 sys-id-ext 0)
             Address     001c.7301.0089
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

Interface        Role       State      Cost      Prio.Nbr Type
---------------- ---------- ---------- --------- -------- --------------------
Et1              designated forwarding 2000      128.1    P2p
Et2              designated forwarding 2000      128.2    P2p
Et3              designated forwarding 2000      128.3    P2p
Et4              designated forwarding 2000      128.4    P2p
Et20             designated forwarding 2000      128.20   P2p
Et24             backup     discarding 2000      128.24   P2p
```

Mode

EXEC

show startup-config

Name

show startup-config — Display the contents of the startup configuration

Synopsis

show startup-config

Description

Displays the contents of the startup configuration file `flash:/startup-config`. You would see the same result by using the **more flash:/startup-config** command. The **show startup-config** command just makes this a bit easier as you do not need to remember the path to the file.

Mode

Privileged EXEC

See Also

startup-config, **show running-config**, **more**

show startup-config interface

Name

show startup-config interface — Display the current startup configuration of an interface or set of interfaces

Synopsis

show startup-config interface *name pattern* [*name pattern*]

Description

This command displays the current contents of the startup configuration for interfaces matching the given interface name pattern or patterns. The name patterns can be full or abbreviated interface names, interface name ranges, or regular expressions.

For example, to display the configuration for interface Ethernet1 use the command:

```
show startup-config interface Ethernet1
```

Abbreviated and lower case interface names are accepted as well, and these can be combined with a range to display the configuration for more than one interface. For example, to display the configuration for interfaces Ethernet1 and Ethernet2 use the command:

```
show startup-config interface eth1 eth2
```

or

```
show startup-config interface eth1-2
```

You can also use regular expression syntax in the interface name pattern. For example, to display the configuration for interfaces Vlan1, Vlan3, and Vlan5 use the command:

```
show startup-config interface vlan[1,3,5]
```

Mode

Privileged EXEC

show tacacs

Name **show tacacs** — Display TACACS+ status

Synopsis **show tacacs**

Description Displays any TACACS+ servers that have been configured, as well as any TACACS+ server-groups and the list of servers in each group.

The following counters that track the interactions between EOS and each TACACS+ server will also be displayed:

- `Connection opens`: Attempts to initiate a new TCP connection to the server.
- `Connections closes`: Connections closed by the client normally after being successfully established.
- `Connection disconnects`: Connections that were closed by the server.
- `Connection failures`: Failed connection attempts, not including timeouts.
- `Connection timeouts`: Connection attempts that failed due to timeout.
- `Messages sent`: Messages sent by the client over established connections.
- `Messages received`: Messages received from the server.
- `Receive errors`: Messages received from the server that resulted in some sort of error. For example: incorrect session id.
- `Receive timeouts`: Timeouts occurred while waiting for a message from the server.
- `Send timeouts`: Timeouts occurred while waiting to send a message while the socket was not writable.

Mode EXEC

See Also **tacacs-server host**

show tech-support

Name **show tech-support** — Displays information needed during troubleshooting

Synopsis **show tech-support**

Description This command is a wrapper around various other commands that are useful when troubleshooting. The output lists all the commands being invoked.

Mode Privileged EXEC

show trace

Name — **show trace** — Displays trace related settings for an Agent

Synopsis — **show trace** *agent-name*

Description — Displays the trace settings for an Agent. An Agent is a task running on the system, and advanced troubleshooting can be done by "tracing" through the Agent software. It is recommended that you use this command with help of a support representative.

Mode — Privileged EXEC

show uptime

Name **show uptime** — Show how long the system has been running.

Synopsis **show uptime**

Description Displays a one line summary with the following information:

- The current time (HH:MM:SS)
- How long the system has been running
- How many users are currently logged in
- System load averages for the past 1, 5, and 15 minutes

Mode EXEC

See Also **show processes**, **show processes top**

show users

Name — **show users** — Displays details about users connected to the system

Synopsis — **show users**

Description — Displays details about users connected to the system, either through the serial console, or through telnet or ssh. The output shows the incoming and outgoing sessions per user, and their idle time.

Mode — Privileged EXEC

See Also — **username secret**, **show aaa sessions**,

show version

Name	**show version** — Display the software and hardware versions
Synopsis	**show version**
Description	Displays the hardware and the current software version. In addition, the serial number of the system, and the uptime are also displayed.
Mode	EXEC
See Also	**show boot-config**

show vlan

Name

show vlan — Display operational status and port membership for configured VLANs

Synopsis

show vlan [**id** *vlanId* | **name** *vlanName*] [**configured-ports** | **active-configuration**]

show vlan summary

Description

This command displays the status of all configured VLANs. The output includes the VLAN id, name, status, and port membership for all configured VLANs. By default the command only displays ports that are part of the active configuration. However, by specifying **configured-ports**, the command will display *all* ports that are members of a configured VLAN. For example, a physical port that is a member of a port-channel inherits the VLAN configuration of the port-channel, and the per-port VLAN configuration is ignored. Such a port will not be displayed in the active configuration, but will be displayed if **configured-ports** is specified.

The system supports VLAN ids from 1 through 4094, and these can be configured using the **vlan** configuration command.

Mode

EXEC

See Also

vlan

shutdown

Name **description** — Disable an interface

Synopsis **shutdown**

no shutdown

Description The **shutdown** command can be used to disable an interface.

The **no** form of the command re-enables the interface.

Mode Interface Configuration

See Also **show interfaces**

snmp-server community

Name

snmp-server community — Create or replace an SNMP community

Synopsis

snmp-server community *community-string* [**ro** | **view** *view-name*]

no snmp-server community *community-string*

Description

The **snmp-server community** configuration command can be used to create an SNMP community or to replace the existing community with the same community string. Optionally, you may specify the name of a view to be used for access control when the agent is accessed with this community string.

The SNMP agent is not enabled until the first community is created. A side-effect of creating a community is to enable the SNMP agent.

SNMP community strings are used when accessing the SNMP agent with SNMPv1 or SNMPv2. For access with SNMPv3, please see the **snmp-server user** and **snmp-server group** commands.

Mode

Global Configuration

See Also

snmp-server group, **snmp-server user**, **snmp-server view**, **show snmp community**

snmp-server engineID

Name

snmp-server engineID — Set the SNMP agent's engineID

Synopsis

snmp-server engineID local *engineid-string*

no snmp-server engineID local

Description

The **snmp-server engineID** configuration command can be used to override the SNMP agent's default engineID. The engineID is specified as a string of hexadecimal characters between 10 and 64 characters long, representing between 5 and 32 octets that compose the engineID. The engineID must be unique within the administrative domain in which the agent is being managed.

It is not common to need to override the engineID. Any SNMPv3 user configured with authentication or privacy options has its passphrase(s) localized using the engineID of the agent at the time the user was configured. If the engineID is changed at a later time, any existing user will cease to function properly due to a mismatch between the engineID used to localize the user's authentication and privacy keys and the newly configured engineID. Thus it is important to reconfigure any users after changing the agent's engineID.

Mode

Global Configuration

snmp-server group

Name

snmp-server group — Create or replace an SNMP group

Synopsis

snmp-server group *group-name* { **v1** | **v2c** | **v3** {**auth** | **noauth** | **priv**} [**read** *view-name* [**notify** *view-name*]]

no snmp-server group *group-name* { **v1** | **v2c** | **v3** }

Description

The **snmp-server group** configuration command can be used to create an SNMP group or to replace an existing group. Each group may optionally be associated with a read view and a notify view for access control. If no read view or notify view is specified, the group has access to all objects provided by the SNMP agent.

To remove a SNMP group use the **no snmp-server group** command.

Mode

Global Configuration

See Also

show snmp group, **show snmp view**, **snmp-server view**

snmp-server host

Name

snmp-server host — Configure the specified host to receive SNMP traps or informs

Synopsis

snmp-server host *hostname-or-address* [**traps** | **informs**] [**version** {**1** | **2c** | **3** [**auth** | **noauth** | **priv**]}] *security-name* [**udp-port** *port*]

Description

The **snmp-server host** configuration command is used to configure the SNMP agent to send traps or informs notifications to an SNMP management station. The host may be specified either by hostname, if the switch has a valid DNS configuration, or by IP address. If neither **traps** nor **informs** are not specified, traps will be sent. Protocol version 1 will be used if no protocol version is specified. Note that SNMPv1 does not support informs, so it is an error to specify informs with protocol version 1.

The *security-name* argument should be a community string for protocol versions **1** or **2c**, and a user name for protocol version **3**. For protocol version 3, the SNMP agent must be separately configured with the remote user's details using the **snmp-server user** command with the **remote** option.

To stop sending traps or informs to a host, use the **no snmp-server host** command and specify the hostname or IP address, and optionally, whether to stop sending traps or informs.

Mode

Global Configuration

See Also

show snmp host

snmp-server user

Name

snmp-server user — Create or replace an SNMP user

Synopsis

snmp-server user *user-name group-name* { **v1** | **v2c** | **v3** [**auth** {**md5** | **sha**} *auth-passphrase* [**priv** {**aes** | **des**} *privacy-passphrase*]] }

Description

The **snmp-server user** configuration command can be used to create an SNMP user or to replace an existing user with the same user name. Each user is a member of a group. The group determines the set of SNMP objects that the user can access.

Each SNMP user is created with a security model of **v1**, **v2c**, or **v3**. A v1 or v2c user is not very different than a community: the user name can be used as a community string when accessing the SNMP agent with version 1 or version 2c of the SNMP protocol. A v3 user is required to access the SNMP agent with version 3 of the SNMP protocol. A v3 user is optionally configured to use MD5 or SHA-1 authentication, and optionally DES or AES encryption.

To remove a SNMP user use the **no snmp-server user** command.

Mode

Global Configuration

See Also

show snmp user, **snmp-server group**

snmp-server view

Name

snmp-server view — Create or update an SNMP view

Synopsis

snmp-server view *view-name object-identifier-tree* {**included** | **excluded**}

no snmp-server view *view-name* [*object-identifier-tree*]

Description

The **snmp-server view** configuration command can be used to create an SNMP view or to update an existing view. If you enter multiple **snmp-server view** commands with the same view name the resulting view will consist of the union of object-identifier trees from all of the commands. Each tree can ether be included or excluded, where included means that access to object identifiers within that subtree is allowed, and excluded means access is denied.

To remove a SNMP view use the **no snmp-server view** command and specify the view name. To remove just one tree from the view, specify the view name and the tree object identifier.

Mode

Global Configuration

See Also

show snmp view

spanning-tree cost

Name

spanning-tree cost — Set the value of the spanning tree protocol path cost parameter for the interface

Synopsis

spanning-tree cost *cost*

no spanning-tree cost

Description

The **cost** parameter defaults to a value determined by the speed of the interface. For 10 gigabit interfaces this default is 2000, and for 1 gigabit interfaces it is 20000. The command accepts a value in the range from 1 to 200,000,000. The **cost** parameter specifies the path cost value used by the spanning tree protocol. Providing a value with this command overrides the interface speed based default value. Lower path cost values make the interface more likely to be used as the root port of the switch.

The **no** form of the command reverts the cost to the default value.

Mode

Interface Configuration

spanning-tree forward-time

Name

spanning-tree forward-time — Set the value of the spanning tree protocol forwarding time parameter

Synopsis

spanning-tree forward-time *seconds*

no spanning-tree forward-time

Description

The **forward-time** parameter defaults to 15 seconds. The command accepts a value in the range from 4 to 30 seconds.

The **no** form of the command reverts the forwarding time to the default value.

Mode

Global Configuration

spanning-tree link-type

Name

spanning-tree link-type — Specify whether the interface connects to a shared media network or a point to point link

Synopsis

spanning-tree link-type { **point-to-point** | **shared** }

no spanning-tree link-type

Description

The spanning tree link type defaults to **point-to-point**. If the interface connects to a shared media network, use this command to let the spanning tree protocol know. Certain optimizations within the spanning tree protocol do not work properly if the interface is connected to more than one other device.

The **no** form of the command reverts the link type to the default value.

Mode

Global Configuration

spanning-tree max-age

Name

spanning-tree max-age — Set the value of the spanning tree protocol max age parameter

Synopsis

spanning-tree max-age *seconds*

no spanning-tree max-age

Description

The **max-age** parameter defaults to 20 seconds. The command accepts a value in the range from 6 to 40 seconds. The max age parameter specifies the maximum acceptable value for the max age value in spanning tree protocol information received by the switch from a neighboring switch. The spanning tree protocol information from the neighboring switch is discarded if its max age value exceeds the value specified by this command.

While the max age parameter is specified in seconds, in practice it is implemented in most switches as a hop count rather than a time value. Most switches, including the Arista switches, increment the max age value of the spanning tree information received on the root port by 1 before sending it out in a spanning tree protocol packet on another interface.

The **no** form of the command reverts the max age to the default value.

Mode

Global Configuration

spanning-tree mode

Name

spanning-tree mode — Configure the version of the Spanning Tree Protocol to run

Synopsis

spanning-tree mode { **rstp** | **none** | **backup** }

no spanning-tree mode

Description

The **spanning-tree mode** command configures the version of the spanning tree protocol for the switch to run. The **spanning-tree mode rstp** command configures the switch to run the IEEE spanning tree protocol described in the IEEE 802.1D-2004 specification. This version of the spanning tree protocol is also known as the rapid spanning tree protocol. It was originally specified in the IEEE 802.1w specification.

The **spanning-tree mode none** command configures the switch to disable the spanning tree protocol. In this mode, switchport interfaces immediately forward packets once they are connected, and no spanning tree protocol packets are generated by the switch. Spanning tree protocol packets received by the switch are forwarded within the vlan on which they are received as normal multicast data packets.

The **spanning-tree mode backup** command configures the switch to disable the spanning tree protocol and enable interface pairs configured with the **switchport backup interface** command.

The **no** form of the command reverts the spanning-tree mode to the default of **rstp**.

Mode

Global Configuration

spanning-tree port-priority

Name

spanning-tree port-priority — Set the value of the spanning tree protocol port priority parameter for the interface

Synopsis

spanning-tree port-priority *priority*

no spanning-tree port-priority

Description

The **priority** parameter defaults to 128. The command accepts a value in the range from 0 to 240. The value must be a multiple of 16.

The **no** form of the command reverts the port priority to the default value.

Mode

Interface Configuration

spanning-tree portfast

Name

spanning-tree portfast — Set the value of the spanning tree protocol AdminEdge parameter for the interface

Synopsis

spanning-tree portfast

no spanning-tree portfast

Description

spanning-tree portfast is disabled by default. The command sets the spanning tree protocol AdminEdge parameter to true. This allows the interface to begin forwarding packets immediately when the link comes up. This should only be used on interfaces directly connected to hosts. Enabling **portfast** on an interface connected to another switch in the network can lead to temporary loops in the network. The loops are temporary, because the spanning tree protocol eventually detects another bridge connected to the interface and disables the edge port status initialized by this parameter.

Even if **spanning-tree portfast** is not enabled for an interface, the spanning tree protocol by default attempts to determine if the interface is at the edge of the network. This behavior is controlled by the **spanning-tree portfast auto** command.

Mode

Interface Configuration

spanning-tree portfast auto

Name

spanning-tree portfast auto — Set the value of the spanning tree protocol AutoEdge parameter for the interface

Synopsis

spanning-tree portfast auto

no spanning-tree portfast auto

Description

spanning-tree portfast auto is enabled by default. The command sets the spanning tree protocol AutoEdge parameter to true, and the **no** form of the command sets it to false. When **spanning-tree portfast auto** is enabled, the spanning tree protocol automatically determines whether another bridge running the spanning tree protocol is connected via the interface. If the protocol determines that there is no such bridge, the interface is made an edge port. This is the same whether the **spanning-tree portfast** command has set the AdminEdge interface parameter to true or false.

To disable automatic edge port detection for the interface, use the **no spanning-tree portfast auto** command.

Mode

Interface Configuration

spanning-tree priority

Name

spanning-tree priority — Set the value of the spanning tree protocol bridge priority parameter

Synopsis

spanning-tree priority *priority*

no spanning-tree priority

Description

The **priority** parameter defaults to 32768. The command accepts a value in the range from 0 to 61440 seconds. The value must be a multiple of 4096. The spanning tree protocol specifies that numerically lower bridge priority values are better.

The **no** form of the command reverts the priority to the default value.

Rather than configuring this value directly, we recommend that you use the **spanning-tree root** command instead.

Mode

Global Configuration

spanning-tree root

Name

spanning-tree root — Set the value of the spanning tree protocol bridge priority parameter to a value that makes this switch the root of the spanning tree

Synopsis

spanning-tree root { **primary** | **secondary** }

no spanning-tree root

Description

Use the **spanning-tree root** command to make the switch the primary or secondary root of the network. The **spanning-tree root primary** command sets the **priority** parameter of the switch to 8192. If no other switch is similarly configured, this gives the switch the best priority value in the network. With the best priority value, the switch becomes the root bridge of the network.

The **spanning-tree root secondary** command sets the **priority** parameter of the switch to 16384. If no other switch is similarly configured, this gives the switch the second best priority value in the network. With the second best priority value, the switch becomes the root bridge of the network if the primary root bridge fails.

Mode

Global Configuration

spanning-tree transmit hold-count

Name

spanning-tree transmit hold-count — Set the value of the spanning tree protocol hold count parameter

Synopsis

spanning-tree transmit hold-count *packets*

no spanning-tree transmit hold-count

Description

The **hold-count** parameter defaults to 6 packets. The command accepts a value in the range from 1 to 10 packets. The hold count limits the number of spanning tree protocol packets that the switch can send out on a single interface in a short interval. At most **hold-count** packets are sent out an interface in 1 second.

The **no** form of the command reverts the hold count to the default value.

Mode

Global Configuration

switchport access vlan

Name

switchport access vlan — Configure the VLAN for an interface in access mode

Synopsis

switchport access vlan *vlanId*

no switchport access vlan

default switchport access vlan

Description

The **switchport access vlan** command configures the access VLAN of an interface that is in access mode. The *vlanId* argument must be an integer in the range 1 through 4094. If the specified VLAN doesn't already exist, it is created automatically by this command.

When the interface is in access mode, the access VLAN is the single VLAN of which the interface is a member. Untagged frames received on the interface are associated with the access VLAN. Tagged frames received on the interface are dropped unless they are tagged with the access VLAN.

The **no** and **default** forms of the command both revert the access VLAN to the default value of 1.

Note that the access VLAN only has significance when the interface is in access mode, as configured by the **switchport mode access** command. If the interface is in trunk mode then the configured access VLAN is stored in the running configuration, but has no effect until the interface is put into access mode.

Mode

Interface Configuration

See Also

switchport mode, **show interfaces switchport**

switchport backup interface

Name

switchport backup interface — Set the backup interface for the current interface.

Synopsis

switchport backup interface *interface*

switchport backup interface *interface* **prefer vlan** *vlan-list*

no switchport backup interface

Description

switchport backup interface configures the current interface as a primary interface and the interface given as an argument as its backup. In this configuration, only one of the primary and backup interfaces is allowed to forward traffic for a vlan at any time. When the primary interface is up and running, it forwards traffic for all of the vlans carried by the pair while the backup interface drops all traffic for all of the vlans carried by the pair. If the primary interface fails, the backup interface takes over forwarding for the vlans. When the primary interface comes back up, it takes over forwarding for the vlans again.

Backup interface pairs are usually used in place of the Spanning Tree protocol in an access switch with just a pair of uplinks connecting it to the rest of the network. By allowing only one of the uplinks to be forwarding traffic at a time, the switch prevents forwarding loops just as the Spanning Tree protocol would. For backup interfaces to become active, the Spanning Tree protocol mode must be configured to 'backup' using the **spanning-tree mode backup** command.

Using the **prefer vlan** option to the **backup interface** command allows you to load balance forwarding traffic across both the primary and backup interfaces. The vlans listed with this option are forwarded on the backup interface and not the primary interface when both interfaces are up. They are preferred on the backup. With this option the interfaces act as backups for each other, with each acting as the primary for a subset of the vlans carried by the pair. To check the state of backup interface pairs on the switch, use the **show interfaces switchport backup** command.

For example, configuring interface Ethernet1 as the primary and Ethernet2 as the backup with vlans 1-10 carried on Ethernet1 and 11-20 carried on Ethernet2 you could use the following configuration:

```
localhost(config)#vlan 1-20
localhost(config)#spanning-tree mode backup
localhost(config)#interface Ethernet1
localhost(config-if)#switchport backup interface Ethernet2 prefer vlan 11-20
localhost(config-if)#end
```

With this configuration and both interfaces up, Ethernet1 forwards vlans 1-10 while blocking vlans 11-20. Ethernet2 forwards vlans 11-20 while blocking vlans 1-10. If either of the interfaces goes down, the other takes over forwarding the failed interface's vlans.

The upstream switches connected to the interfaces in the backup interface pair should normally continue to run the Spanning Tree protocol. They can be configured as edge ports or portfast ports to ensure that the interfaces become forwarding quickly when one of the interfaces goes down and then comes back up again.

Mode Interface Configuration

switchport mode

Name

switchport mode — Set the switching mode of an interface

Synopsis

switchport mode { **access** | **trunk** }

no switchport mode

default switchport mode

Description

The **switchport mode** command configures an interface to be in one of the two possible switching modes: **access** or **trunk**.

In **access** mode, the interface is a member of precisely one VLAN, called the access VLAN, which is configured using the **switchport access vlan** command. Untagged frames received on the interface are associated with the access VLAN. Tagged frames received on the interface are dropped unless they are tagged with the access VLAN. Frames sent over the interface are always untagged.

In **trunk** mode, the interface may be a member of many VLANs; the set of VLANs is configured using the **switchport trunk allowed vlan** comand. One VLAN, called the native VLAN of the interface, is used for untagged traffic; it is configured using the **switchport trunk native vlan** command.

Typically, **access** mode is used for interfaces that connect to hosts, whereas **trunk** mode is used for interfaces that connect to other switches.

The **no** and **default** forms of the command both revert the interface to the default switching mode, which is **access** mode.

Mode

Interface Configuration

See Also

switchport access vlan, **switchport trunk allowed vlan**, **switchport trunk native vlan**, **show interfaces switchport**

switchport trunk allowed vlan

Name

switchport trunk allowed vlan — Configure the allowed VLAN set for an interface in trunk mode

Synopsis

switchport trunk allowed vlan [**except**] *vlanSet*

switchport trunk allowed vlan { **add** | **remove** } *vlanSet*

switchport trunk allowed vlan { **all** | **none** }

no switchport trunk allowed vlan

default switchport trunk allowed vlan

Description

The **switchport trunk allowed vlan** command configures the allowed VLAN set of an interface that is in trunk mode. The *vlanSet* argument must be a comma-separated list of individual VLAN IDs and/or hyphen-separated VLAN ID pairs (indicating a range of VLAN IDs), where each VLAN ID is an integer in the range 1 through 4094. The following are all examples of valid *vlanSet* arguments:

- 1234
- 1,3,5,7
- 100-200
- 5,100-1000,99,3000-4094

When the interface is in trunk mode, the allowed VLAN set is the set of VLANs of which the interface is a member, provided that those VLANs have been created with the **vlan** command. Note that, unlike the **switchport access vlan** command, the **switchport trunk allowed vlan** command does not create the VLANs if they don't already exist.

The **switchport trunk allowed vlan** [**except**] *vlanSet* and **switchport trunk allowed vlan** { **all** | **none** } forms of the command completely replace the previously configured allowed VLAN set. The **switchport trunk allowed vlan** { **add** | **remove** } *vlanSet* form of the command modifies the previously configured allowed VLAN set.

The **no** and **default** forms of the command both revert the allowed VLAN set to the default value of **all**.

Note that the allowed VLAN set only has significance when the interface is in trunk mode, as configured by the **switchport mode trunk** command. If the interface is in access mode then the configured allowed VLAN set is stored in the running configuration, but has no effect until the interface is put into trunk mode.

Mode

Interface Configuration

See Also **switchport mode**, **switchport trunk native vlan**, **vlan**, **show interfaces switchport**

switchport trunk native vlan

Name

switchport trunk native vlan — Configure the native VLAN for an interface in trunk mode

Synopsis

switchport trunk native vlan *vlanId*

no switchport trunk native vlan

default switchport trunk native vlan

Description

The **switchport trunk native vlan** command configures the native VLAN of an interface that is in trunk mode. The *vlanId* argument must be an integer in the range 1 through 4094.

When the interface is in trunk mode, the native VLAN is the VLAN used for untagged traffic on the interface. Untagged frames received on the interface are associated with the native VLAN. Frames that are associated with the native VLAN are sent over the interface untagged.

The **no** and **default** forms of the command both revert the native VLAN to the default value of 1.

Note that the native VLAN only has significance when the interface is in trunk mode, as configured by the **switchport mode trunk** command. If the interface is in access mode then the configured native VLAN is stored in the running configuration, but has no effect until the interface is put into trunk mode.

Mode

Interface Configuration

See Also

switchport mode, **switchport trunk allowed vlan**, **show interfaces switchport**

tacacs-server host

Name

tacacs-server host — Set the parameters used to communicate with a TACACS+ server

Synopsis

tacacs-server host *hostname-or-address* [**single-connection**] [**port** *1-65535*] [**timeout** *1-1000*] [**key** *encryption-key*]

no tacacs-server host [*hostname-or-address*] [**port** *1-65535*]

Description

The **tacacs-server host** configuration command sets the options used when communicating with a particular TACACS+ server.

The *hostname-or-address* argument can be either the IP address or the DNS hostname of the TACACS+ server. To use a DNS hostname you must have previously configured a nameserver using the **ip name-server** command. It may be preferable to use an IP address since TACACS+ authentication will fail if the hostname cannot be resolved at the time of a login.

Use the *single-connection* argument to indicate that the TACACS+ server supports multiplexing multiple sessions on the same TCP connection.

Provide the *port* argument if the TACACS+ server is running on a non-standard port. If *port* is not specified the standard TACACS+ port 49 is used. Each server is identified by the combination of its hostname and port, so it is possible to configure multiple servers listening on the same IP address if each server is listening on a different port number.

To use a different timeout value or encryption key than the global values specified using **tacacs-server timeout** or **tacacs-server key** commands you may provide the *timeout* or *key* argument. The globally configured values will be used if these arguments are not provided.

To remove a single TACACS+ server from the configuration use the **no tacacs-server host** *hostname-or-address* command, and also provide a port argument for servers not using the default port number. To remove all TACACS+ servers from the configuration use **no tacacs-server host** without specified a hostname.

Mode

Global Configuration

See Also

tacacs-server key, **tacacs-server timeout**

tacacs-server key

Name

tacacs-server key — Set the shared secret key used to communicate with TACACS+ servers

Synopsis

tacacs-server key *encryption-key*

no tacacs-server key

Description

The **tacacs-server key** configuration command sets the shared secret key used to perform encryption when communicating with any TACACS+ server for which a different key has not been explicitly provided.

To communicate with multiple TACACS+ servers that each have a different key, specify a server-specific key when using the **tacacs-server host** command.

To clear this key from the configuration use the **no tacacs-server key** command.

Mode

Global Configuration

See Also

tacacs-server host

tacacs-server timeout

Name

tacacs-server timeout — Set the maximum time to wait for a TACACS+ response

Synopsis

tacacs-server timeout *1-1000*

no tacacs-server timeout

Description

The **tacacs-server timeout** configuration command sets the timeout used when communicating with any TACACS+ server for which a different timeout has not been explicitly provided. In the case of multiple TACACS+ servers in a redundant configuration the timeout will be used to decide when to fail over and attempt to communicate with another server. If only a single TACACS+ server has been configured, or for the last TACACS+ server in a redundant configuration, the timeout will be used to determine how long to wait before considering the request to have failed.

To communicate with multiple TACACS+ servers that each have a different timeout, specify a server-specific timeout when using the **tacacs-server host** command.

To reset the timeout to the default value (which is 5 seconds) use the **no tacacs-server timeout** command.

Mode

Global Configuration

See Also

tacacs-server host

telnet

Name

telnet — Connect to another host using the Telnet protocol

Synopsis

telnet *hostname*

telnet *hostname port-number*

telnet *hostname keyword*

Description

Connect to another host using the Telnet protocol. The *hostname* can either be the hostname, or the IP address of the host. The second argument - *port-number* is optional, the default being port number 23. You can also specify any of the listed protocol names and the system will Telnet using the corresponding port number.

Mode

EXEC

See Also

connect

terminal length

Name

terminal length — Configure pagination in a terminal

Synopsis

terminal length *lines*

Description

The **terminal length** command configures the pagination length to *lines* for all **show** commands on a terminal. If the output of a **show** command is longer than the configured terminal length, the output will be paused after each screenful of output, prompting the user to continue.

The *lines* argument in an integer between **0** and **32767**, inclusive. A setting of **0** disables pagination for the terminal. By default, all console sessions have pagination disabled.

The pagination settings must be configured for each session.

Users connecting to the switch via ssh may have pagination set automatically by the ssh client. To disable pagination, set **terminal length** to **0**. Note that whenever you adjust the size of the ssh window, pagination may be re-enabled.

Mode

EXEC

traceroute

Name — **traceroute** — Trace packet route to destination

Synopsis — **traceroute** *destination*

Description — Trace packet route to the specified destination. The *destination* can be specified as a hostname or an IP address.

Mode — EXEC

See Also — **show ip route**

username secret

Name

username secret — Set password for a given user account

Synopsis

username *name* **secret** [**0**] *password*

username *name* **secret 5** *encrypted-password*

username *name* **nopassword**

no username *name*

Description

Set the password required to log in using the given username. The first form sets the user's password to the given plaintext password. Use this form when typing a password by hand.

The second form takes a secure hash of the password (known as the "encrypted password") rather than the password itself. There is no known way to compute the password from its secure hash, so this form of the command is more secure. This form is useful primarily when cutting and pasting from a saved configuration file. When the device configuration is saved, only the second form of this command is used, so that the password is protected in the event that the configuration file is lost or stolen.

The third form allows a login for the given username with no password.

The fourth form deletes the given user account.

Mode

Global Configuration

See Also

enable secret

vlan

Name

vlan — Enter vlan configuration mode

Synopsis

vlan *vlanId*

no vlan *vlanId*

default vlan *vlanId*

Description

The vlan configuration command can be used to configure a vlan, or a range of vlans. Using this command, you can configure the vlan settings such as the name and operational state. For a complete list of choices, you can always use ? in vlan configuration mode.

To delete a vlan, use the **no** form of the command. To revert a vlan's settings to their default values, use the **default** form of the command.

Mode

Global Configuration

See Also

show vlan

write

Name

write — Manipulate the running configuration file

Synopsis

write erase

write memory

write network *url*

write terminal

Description

Through this command the running configuration may be deleted, displayed or saved.

The **write erase** command erases the startup configuration file, and is equivalent to the **erase startup-config** command.

The **write memory** command copies the current running configuration to the startup configuration file, and is equivalent to the **copy running-config startup-config** command.

The **write network** command copies the current running configuration to a file over the network, and is equivalent to the **copy running-config** *url* command.

The **write terminal** displays the current running configuration, and is equivalent to the **show running-config** command.

Mode

Privileged EXEC

See Also

erase startup-config, **copy**, **show running-config**

Chapter 3

File Formats

running-config

Name

running-config — Current operation configuration

Description

The **running-config** is a virtual file that contains the current operation configuration of the system, formatted as a sequence of configuration commands.

The **running-config** may be viewed with the command **show running-config**. It is modified every time a configuration command is entered from the CLI. Copying a stored configuration file to the **running-config** with the **copy** command has the effect of updating the operating configuration by executing the commands from the file.

Files

`system:/running-config`
: The running configuration file.

See Also

show running-config, **copy**, **startup-config**

startup-config

Name

startup-config — Startup configuration file

Description

The **startup-config** file contains the configuration that is loaded when the system boots.

The file is formatted as a sequence of configuration commands, exactly as they would be typed in at the CLI. Blank lines and leading and trailing spaces are ignored. Lines whose first non-blank character is an exclamation mark (!) are comments, and are ignored.

The **startup-config** file may be viewed with the command **show startup-config**. It may be erased with the command **erase startup-config** and replaced with the **copy** command.

Files

`flash:/startup-config`
: The startup configuration file.

See Also

show startup-config, **erase startup-config**, **copy**, **running-config**

Chapter 4

Aboot

Introduction

Aboot is the boot loader for Arista Networks switch products. It is a firmware component stored in a small memory on the system board, separate from the internal flash storage device.

When the switch is powered on or rebooted, Aboot reads its configuration from `boot-config` on the internal flash and attempts to boot a software image (SWI) automatically if one is configured.

Aboot provides an interactive command-line interface or "shell," allowing users to boot a SWI manually, recover the internal flash to its factory-default state, run certain hardware diagnostics, and manipulate and copy files.

Terminology

Throughout this chapter, the term "internal flash" refers to the internal storage device, and "USB key" or "USB flash" refers to an external storage device connected to a USB port, regardless of the specific technology, which may change in future switch products.

Connecting to the console

To monitor the automatic boot process or enter the Aboot shell, you need to connect to the system console port.

You can connect a PC or laptop directly to the port and run a terminal emulator to interact with the serial port or access it via a serial concentrator device.

Consult your terminal emulator documentation for instructions on configuring the console port speed and other settings. These settings are stored in `boot-config`; the factory-default settings for Arista Networks products are 9600 baud, no parity, 8 character bits, and 1 stop bit. If you do not know the correct settings, you can perform a full flash recovery to restore the factory-default settings (see section Recovery).

When the console port is connected and the terminal settings are configured properly, you should see the message similar to the following a few seconds after powering up the switch:

```
Aboot 1.0.0

Press Control-C now to enter the Aboot shell
```

Automatic Booting

Aboot attempts to boot the software image (SWI) configured in `boot-config` automatically if you take no action during the boot process.

If the boot process fails for any reason, such as an incorrectly configured SWI, Aboot stops and enters the shell, allowing you to correct the configuration or boot a SWI manually.

Entering the Aboot Shell

To halt the automatic boot process and enter the Aboot shell, press Control-C (ASCII 3 in your terminal emulator) after the `Press Control-C` message appears. Pressing Control-C interrupts the boot process once it has begun, except during the `Starting new kernel` phase which is not interruptible.

If no password has been configured in `boot-config`, the Aboot shell starts immediately. Otherwise, you must enter the correct password at the `Aboot password:` prompt to start the shell. If you enter the wrong password three times, Aboot allows you to perform a full flash recovery to restore the factory-default settings (see the Recovery section).

The Aboot shell starts by printing:

```
Welcome to Aboot.
```

followed by the `Aboot#` prompt.

Manual Booting

To list the contents of the internal flash, enter `ls /mnt/flash` at the `Aboot#` prompt. For example:

```
Aboot# ls /mnt/flash
EOS.swi boot-config startup-config
```

To boot `EOS.swi` on the internal flash, enter `boot flash:EOS.swi` or `boot /mnt/flash/EOS.swi`.

Specifying a Software Image

Aboot's `boot` command supports several ways to specify a SWI.

device`:`*path* - `flash:EOS.swi` - Boots a SWI file from *path* on local storage device *device*; *device* defaults to `flash`

`/mnt/`*device*`/`*path* - `/mnt/flash/EOS.swi` - Boots a SWI file from *path* on local storage device *device*

`http://`*server*`/`*path* - `http://foo.com/images/EOS.swi` - Downloads a SWI file from *path* on the HTTP server on host *server*

`ftp://`*server*`/`*path* - `ftp://foo.com/images/EOS.swi` - Downloads a SWI file from *path* on the FTP server on host *server*

`tftp://`*server*`/`*path* - `tftp://foo.com/EOS.swi` - Downloads a SWI file from *path* on the TFTP server on host *server*

`nfs://`*server*`/`*path* - `nfs://foo.com/images/EOS.swi` - Mounts the parent directory of *path* exported from host *server* and boots the SWI file *path*

Navigating the Aboot Shell

Aboot is based on Linux, and the Aboot shell is similar to the Bourne Shell (`sh`) and Bourne Again Shell (`bash`) on Linux operating systems. If you have used Linux or other flavors of UNIX before, you will find the shell interface familiar.

Some of the most commonly used commands include:

`ls` - Prints a list of the files in the current working directory
`cd` - Changes the current working directory
`cp` - Copies a file
`more` - Prints the contents of a file one page at a time
`vi` - Edits a text file
`boot` - Boots a SWI (see SWI section for information on specifying a SWI)
`swiinfo` - Prints information about a SWI
`recover` - Recovers the factory-default configuration
`reboot` - Reboots the switch
`udhcpc` - Configures a network interface automatically via DHCP
`ifconfig` - Prints or alters network interface settings
`wget` - Downloads a file from an HTTP or FTP server

Many Aboot shell commands are provided by Busybox, an open-source implementation of common UNIX utilities. Busybox command help can be found at http://www.busybox.net/downloads/BusyBox.html. Note that only a subset of the documented commands there are available in Aboot.

Storage Devices

The top level / (root) directory of the Aboot directory hierarchy is a filesystem whose contents are stored in system RAM only; any changes in this filesystem vanish after the Aboot shell exits. The `/mnt` directory contains subdirectories on which the filesystems of storage devices appear; making a storage device available for use is known as mounting.

Aboot mounts the internal flash device on `/mnt/flash`.

On a system with two USB ports, if you insert a USB flash drive into one of the ports, Aboot automatically mounts its filesystem on `/mnt/usb1` or `/mnt/usb2`. The filesystem is automatically unmounted when you remove the USB flash drive from the port. Most USB drives contain an LED that flashes when the system is accessing it; be careful not to remove the drive until the LED stops flashing.

Aboot supports most commonly available models of USB flash drives. The flash drive must be formatted with the FAT or VFAT filesystem (most USB flash drives are sold already formatted with VFAT, but if you use Windows to format the drive, be sure not to select NTFS).

Accessing the Network

Aboot can access networks via the management Ethernet port(s). On a switch with two management ports, Aboot provides network interfaces `mgmt1` and `mgmt2`. These ports are unconfigured by default; you can configure management port settings using Aboot shell commands like `ifconfig` and `udhcpc`.

Once a management interface is configured properly, you can use `wget` to transfer files from an HTTP or FTP server, `tftp` to transfer files from a TFTP server, or `mount` to mount an NFS filesystem.

Configuring Aboot

Aboot reads its configuration from `boot-config` on the internal flash. `boot-config` is a plain (ASCII) text file containing a series of configuration settings, one per line.

Each configuration setting is a line of the form:

NAME=VALUE

where `NAME` is the setting name like `SWI` and `VALUE` is its value. Both `NAME` and `VALUE` may not contain spaces. Blank lines and lines beginning with a `#` character are treated as comments and are ignored.

SWI

Aboot attempts to boot the software image specified by `SWI` automatically. The `SWI` variable encodes a full local or network path, using the same format accepted by the `boot` command.

Aboot accepts a number of SWI path formats:

If `SWI` is not specified in `boot-config`, or an error occurs while booting the SWI (due to an incorrect path or an unavailable HTTP server, for example), Aboot halts the boot process and drops into the shell.

The EOS `boot system` command sets the `SWI` in `boot-config`.

Console Speed

Setting `CONSOLESPEED` to `2400`, `4800`, `9600`, `19200`, or `38400` causes Aboot to configure the console speed to the given baud rate at boot.

Careful! If you set the console speed to a value unsupported by either the switch hardware or by your terminal, you will not be able to interact with the Aboot shell. See the Recovery section for instructions on restoring the factory-default configuration.

The EOS `boot console speed` command sets the `CONSOLESPEED` in `boot-config`.

Password

Normally Aboot allows anyone with access to the switch's console port to enter the Aboot shell. In some environments additional security may be desired. If the `boot-config` contains a `PASSWORD` setting, Aboot requires the user to enter a password before granting access to the Aboot shell. If the wrong password is entered three times, Aboot prompts the user to recover the factory-default configuration; see the Recovery section for details.

The value of the `PASSWORD` setting must be an MD5-encrypted password in the form generated by the UNIX `passwd` program (or the `crypt` library function); plaintext passwords are not understood. Thus it is not recommended to set the value of `PASSWD` manually; use the EOS `boot secret` command to set the Aboot password.

NET Settings

If `NETDEV` is present in `boot-config`, Aboot attempts to configure the specified network interface using the following settings:

`NETDEV` - Name of the network interface configured by Aboot, e.g. `mgmt1`
`NETAUTO` - If set to `dhcp`, Aboot configures the interface automatically via DHCP and ignores the other `NET` settings
`NETIP` - IP address of the network interface, e.g. `1.2.3.4`
`NETMASK` - IP subnet mask, e.g. `255.255.255.0`
`NETGW` - IP address of the default gateway
`NETDOMAIN` - Default domain name, e.g. `mycompany.com`
`NETDNS` - IP address of a DNS server

Recovery

Aboot allows restoring the state of the internal flash to the factory defaults or a customized default state. You can use these recovery methods to:

- restore the factory-default flash contents before transferring the switch to another owner;
- restore Aboot shell access if you lose or forget the Aboot password;
- restore console access if baud rate or other settings are incompatible with your terminal emulator; or
- automatically replace the existing internal flash contents with the `boot-config`, SWI, and other files stored on a USB flash key. This is useful not only for recovery but also for installing a customized configuration on a number of switches or allowing non-technical personnel to set up a switch at a remote site.

Restoring Factory Default State

The Aboot `fullrecover` command erases the internal flash and restores it to the factory-default contents. This command can be accessed from the Aboot shell, or if an Aboot password has been set, and you enter an incorrect password three times in a row while attempting to enter the Aboot shell.

Restoring User Defined State

Aboot can automatically erase the internal flash and repopulate it with the contents of a USB key that has been inserted before powering up or rebooting the switch. This recovery method does not require you to access to the switch console or enter the Aboot password, if one is currently set.

Aboot invokes the recovery mechanism only if two conditions are met:

- the USB key must contain a file called `fullrecover` (the file's contents are ignored; an empty text file is sufficient); and
- if the USB key contains a file called `boot-config`, its timestamp must differ from the timestamp of the `boot-config` file on the internal flash (this prevents Aboot from invoking the recovery mechanism again on every boot if you leave the flash key inserted).

To use this recovery mechanism, set up a USB key with whatever files you want installed on the internal flash—for example, a current EOS SWI and a customized or empty `boot-config`—plus an empty file called `fullrecover`. Check that the timestamp of `boot-config` is current to ensure that tbe above conditions are met.

Chapter 5

Open Source Licenses

Portions of Arista Networks EOS and Aboot are distributed under the terms of the GNU General Public License and other open source licenses. License text for EOS components can be viewed by running **show version license** in the EOS CLI. Complete source code is available from **http://www.aristanetworks.com/en/gpl**, or by contacting **support@aristanetworks.com**.

GNU GENERAL PUBLIC LICENSE
Version 2, June 1991

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Lesser General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE
TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and

you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three

years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent

infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free

Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

> <one line to give the program's name and a brief idea of what it does.>
> Copyright (C) <year> <name of author>
>
> This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.
>
> This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.
>
> You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc.,

```
    51 Franklin Street, Fifth Floor, Boston, MA 02110-1301 USA.

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this
when it starts in an interactive mode:

    Gnomovision version 69, Copyright (C) year name of author
    Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type `show w'.
    This is free software, and you are welcome to redistribute it
    under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate
parts of the General Public License.  Of course, the commands you use may
be called something other than `show w' and `show c'; they could even be
mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your
school, if any, to sign a "copyright disclaimer" for the program, if
necessary.  Here is a sample; alter the names:

  Yoyodyne, Inc., hereby disclaims all copyright interest in the program
  `Gnomovision' (which makes passes at compilers) written by James Hacker.

  <signature of Ty Coon>, 1 April 1989
  Ty Coon, President of Vice

This General Public License does not permit incorporating your program into
proprietary programs.  If your program is a subroutine library, you may
consider it more useful to permit linking proprietary applications with the
library.  If this is what you want to do, use the GNU Lesser General
Public License instead of this License.
```