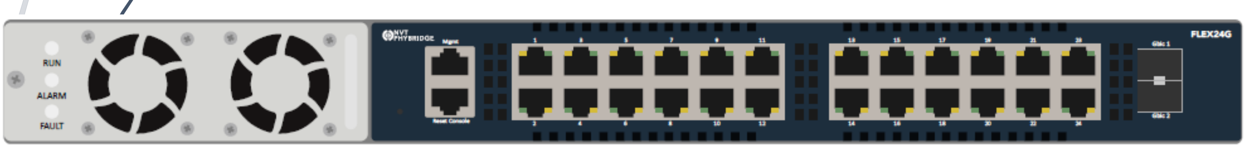
NVT PHYBRIDGE

4/23/2021

FLEX24-10G
Administration Guide



Introduction

The NVT Phybridge FLEX24-10G switch is the most versatile PoE switch on the market, designed to make IP/IoT deployments simple, secure, and cost-effective. The FLEX24-10G switch delivers up to 50 Watts of PoE++ and 10/100/1000 Mbps symmetrical, full-duplex, over 2 or 4 pair UTP (unshielded twisted pairs) cabling with up to 2,000ft (610m) reach.

The FLEX24-10G switch enables Modern LAN principles and comes standard with 2 10Gb uplink ports, 24 10/100/1000 downlink ports, a 1,000 Watt hot-swappable power supply, power sharing, and power redundancy. The FLEX24-10G switch also comes with a new and intuitive GUI interface, ideal for any Cloud or premise-based managed service offering. The new and improved Command Line Interface is very similar to the Cisco offering for ease of use.

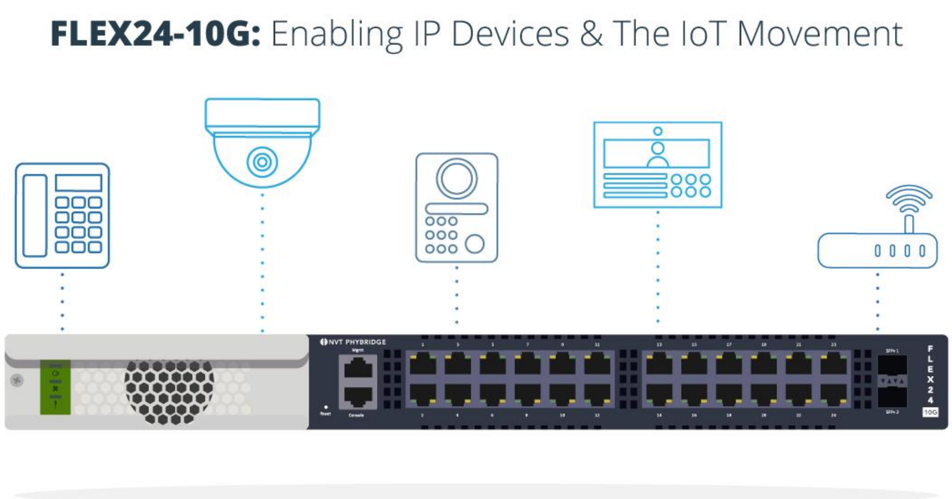
• Accelerate your return on investment by reducing infrastructure costs.

• Simplify your IP modernization, collapsing planning and deployment time.

• Eliminate infrastructure barriers, risks, disruption and costs.

• Create a robust plug-and-play IP platform that is easy to deploy and manage.

• Be environmentally responsible during your IP upgrades.



Chapter 1: Using the FLEX24-10G

Quick Setup

This section outlines how to perform a basic setup on the FLEX24-10G.

Accessing the Command Line

The three methods of accessing the switch's command line interface (CLI) on the FLEX24-10G are via SSH, telnet, and serial console. SSH and telnet are enabled by default and do not require any additional configuration. The default address of VLAN 1 is 192.168.100.1 and the CLI can be accessed from any of the FLEX24-10G's interfaces. The serial console interface uses a speed on 115200 bits per second.

The switch must be powered on and have connectivity to a PC via ethernet or a serial console cable. Once the switch has been powered on and a connection has been made, the computer must be running a terminal emulator. Examples of terminal emulators are TeraTerm or PuTTY for Windows and Minicom for Linux/Mac.

Logging into the Switch

Once a command line session has been created, the user will be greeted with an empty black window. If the username prompt does not appear, press **Enter** to reveal the username prompt.

The default username and password are "admin" and "admin" respectively. When entering the password, no characters will be presented in the terminal.

```
Username: admin
Password:
FLEX24-10G#
```

Once the user has been successfully authenticated, they are operating at privilege level 15. Users with a privilege level of 15 have unrestricted access to the switch's features.

Setting the Hostname

By default, the switch hostname is set to **FLEX24-10G**. This can be changed at the administrator's discretion.

The below CLI snippet changes the switch's hostname to "ThisisaHostname". When the hostname is changed, the change can be seen immediately by the change in the command prompt.

The **configure terminal** command moves the user from Privileged EXEC mode to Global Configuration mode.

```
Username: admin
Password:
FLEX24-10G# configure terminal
FLEX24-10G(config)# hostname ?
    <host_name>    This system's network name
FLEX24-10G(config)# hostname ThisisaHostname
```

```
ThisisaHostname(config)#
```

Resetting the Switch Configuration

If for any reason the switch needs to be reset to its default state, this can be accomplished very easily. Within the CLI the user must be in Privileged EXEC mode. To be sure the user is in Privilege EXEC mode, issue the **end** command or the **CTRL+z** keyboard shortcut.

The **reload defaults** command resets the switch's running-configuration to the default state.

```
ThisisaHostname(config)# end
ThisisaHostname# configure terminal
ThisisaHostname(config)# ^Z
ThisisaHostname# reload defaults
% Reloading defaults. Please stand by.
FLEX24-10G#
```

Running-config and Startup-config

When the switch is first powered on, the contents of the startup-config are loaded from memory. From a factory default state, there are no configuration commands in the startup-config.

As the administrator configures the switch, all the configuration commands are put into the switch's running-config. The running-config is the present state of the switch's configuration.

If the switch were to lose power before the contents of the running-config are saved to the startup-config, all changes made to the switch would be lost.

The running-config can be viewed with the **show running-config** command from Privileged EXEC mode.

```
FLEX24-10G# show running-config
Building configuration...
hostname FLEX24-10G
contact http://www.nvtphybridge.com/support-ticket/_Tel:1-888-901-3633_Mon-Fri_4am-7pm_EST
username admin privilege 15 password encrypted
902b0767a854f248b32aec7f9231d06b731a62d8fec635fb2027fa047fa7909bdc100988b796e5722232b37942fb3a
0202a308c3f0db10188dd347dcea672ad5
!
vlan 1
!
!
!
!
spanning-tree mst name 00-24-63-04-2a-80 revision 0
snmp-server contact http://www.nvtphybridge.com/support-ticket/_Tel:1-888-901-3633_Mon-
Fri_4am-7pm_EST
snmp-server location Oakville
!
voice vlan oui 00-03-6B description Cisco phones
voice vlan oui 00-E0-75 description Polycom phones
voice vlan oui 08-00-0F description Mitel phones
voice vlan oui C8-1F-EA description Avaya phones
!
interface GigabitEthernet 1/1
```

```
!
interface GigabitEthernet 1/2
!
! [. . .]
!
interface GigabitEthernet 1/25
!
interface 10GigabitEthernet 1/1
!
interface 10GigabitEthernet 1/2
!
interface vlan 1
 ip address 192.168.1.1 255.255.255.0
!
!
spanning-tree aggregation
 spanning-tree link-type point-to-point
!
!
line console 0
!
line vty 0
!
line vty 1
!
! [. . .]
!
line vty 14
!
line vty 15
!
!
end
FLEX24-10G#
```

Saving the Running-config to the Startup-config

No configuration changes have been saved until the startup-config has been overwritten with the running-config. To copy the running-config to the startup-config issue the **copy running-config startup-config** command within Privileged EXEC mode.

The syntax of the copy command is *copy <source_file> <destination_file>.*

```
FLEX24-10G# copy running-config startup-config
Building configuration...
% Saving 1940 bytes to flash:startup-config
FLEX24-10G#
```

At this point all changes made to the switch's configuration have been saved. In the event of a system power loss, when the switch reinitializes the startup-config will be loaded from flash. The startup-config contains the contents of the previous running-config.

Backing up the Switch's Configuration to a Remote Device

The FLEX24-10G supports a File Transfer Protocol (FTP), Secure File Transfer Protocol (SFTP), Secure Copy Protocol (SCP), and Trivial File Transfer Protocol (TFTP) client allowing for backing up files to a remote device. Additionally, any file saved to the device's flash can be copied to an FTP, SFTP, SCP, or TFTP server.

Use the **dir** command from Privileged EXEC Mode to view the contents of the switch's flash.

```
FLEX24-10G# dir
Directory of flash:
    r- 2019-11-26 20:02:09      773 default-config
    rw 2019-12-03 11:51:46     1942 startup-config
2 files, 2715 bytes total.

Flash size:        119287808 bytes (113.8 MiB)
Flash free:         64491520 bytes (61.5 MiB)
Flash total free:   89657344 bytes (85.5 MiB) (incl. reserved space)
FLEX24-10G#
```

See below for the syntax of the copy command. The copy command must be executed from Privileged EXEC Mode.

	Command	Explanation
Step 1	copy {<url_file> | running-config | startup-config} {<url_file> | running-config | startup-config}	The copy command requires a source file and a destination file. The first **{<url_file> | running-config | startup-config}** represents the source and the second **{<url_file> | running-config | startup-config}** represents the destination. The source/destination file can either be a file in flash, file on a remote server, the startup-config, or the running-config.
Step 2	copy running-config startup-config	**(Optional)** Copy the contents of the running-config to the startup-config.

The below examples will demonstrate how to back up the startup-config to a computer with an IP address of 192.168.100.2. This computer is running an FTP, SFTP, TFTP, and SCP server.

Backup to FTP Server

	Command	Explanation
Step 1	copy startup-config ftp://<username>[:<password>]@<host>[:<port>]/<path> [ftp-active [syntax-check] | syntax-check [ftp-active]]	Backup the startup config to a remove FTP server.

		The **ftp-active** keyword will use active mode for the FTP transfer. By default, passive mode is used. The **syntax-check** will check the syntax of the source for errors.
Step 2	copy running-config startup-config	**(Optional)** Copy the contents of the running-config to the startup-config.

```
FLEX24-10G# copy startup-config ftp://admin:admin@192.168.100.2/config.txt
% Saving 1942 bytes to server 192.168.100.2: config.txt
FLEX24-10G#
```

Backup to TFTP Server

	Command	Explanation
Step 1	copy startup-config tftp://<username>[:<password>]@<host>[:<port>]/<path> [syntax-check]	Backup the startup config to a remove TFTP server. The **syntax-check** will check the syntax of the source for errors.
Step 2	copy running-config startup-config	**(Optional)** Copy the contents of the running-config to the startup-config.

```
FLEX24-10G# copy startup-config tftp://admin:admin@192.168.100.2/config.txt
% Saving 1942 bytes to server 192.168.100.2: config.txt
FLEX24-10G#
```

Backup to SFTP Server

	Command	Explanation
Step 1	copy startup-config sftp://<username>[:<password>]@<host>[:<port>]/<path> [save-host-key [syntax-check] | syntax-check [save-host-key]]	Backup the startup config to a remove SFTP server. The **save-host-key** keyword will place the SFTP server's host key in the switch's cache. If the server's host key is not in the switch's cache and the **save-host-key** keyword is omitted, the command will fail. The **syntax-check** will check the syntax of the source for errors.

Step 2	copy running-config startup-config	**(Optional)** Copy the contents of the running-config to the startup-config.

```
FLEX24-10G# copy startup-config sftp://admin:admin@192.168.100.2/config.txt
% Saving 1942 bytes to server 192.168.100.2: config.txt
FLEX24-10G#
```

Note: If this is the first time copying to or from a particular SFTP server, the **save-host-key** parameter must be used, otherwise the command will fail. See below CLI snippet:

```
FLEX24-10G# copy startup-config sftp://admin:admin@192.168.100.2/config.txt
% Saving 1942 bytes to server 192.168.100.2: config.txt
% Error saving remote file: Host key not in cache (21)
FLEX24-10G#
```

Backup to SCP Server

	Command	Explanation
Step 1	copy startup-config scp://<username>[:<password>]@<host>[:<port>]/<path> [save-host-key [syntax-check] | syntax-check [save-host-key]]	Backup the startup config to a remove SCP server. The **save-host-key** keyword will place the SCP server's host key in the switch's cache. If the server's host key is not in the switch's cache and the **save-host-key** keyword is omitted, the command will fail. The **syntax-check** will check the syntax of the source for errors.
Step 2	copy running-config startup-config	**(Optional)** Copy the contents of the running-config to the startup-config.

```
FLEX24-10G# copy startup-config scp://admin:admin@192.168.100.2/configscp.txt save-host-key
% Saving 1942 bytes to server 192.168.100.2: configscp.txt
FLEX24-10G#
```

Note: If this is the first time copying to or from a particular SCP server, the **save-host-key** parameter must be used or else the command will fail. See below CLI snippet:

```
FLEX24-10G# copy startup-config scp://admin:admin@192.168.100.2/configscp.txt
% Saving 1942 bytes to server 192.168.100.2: configscp.txt
% Error saving remote file: Host key has changed (22)
```

The CLI snippet above is showing a "`% Error saving remote file: Host key has changed (22)`" error because the switch is currently storing the host key from the SFTP file transfer in the previous example.

Setting the VLAN 1 IP Address

By default, the IP address of VLAN 1 is set to 192.168.100.1. VLAN 1's IP address can be assigned via a DHCP server or statically by the administrator.

Static Configuration - IPv4

The below CLI snippet statically sets the IP address of VLAN 1 to 192.168.200.1/24 and copies the running-config to the startup-config.

<u>Note:</u> ? can be issued at any point during a command to reveal which command parameters are available based on what has already been entered.

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# interface vlan 1
FLEX24-10G(config-if-vlan)# ip address ?
    <ipv4_addr>    IP address
    dhcp           Enable DHCP
FLEX24-10G(config-if-vlan)# ip address 192.168.200.1 255.255.255.0
FLEX24-10G(config-if-vlan)# end
FLEX24-10G# copy running-config startup-config
```

Static Configuration - IPv6

The IP address of VLAN 1 (or any other VLAN) can also be set to an IPv6 address using syntax like the above snippet.

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# interface vlan 1
FLEX24-10G(config-if-vlan)# ipv6 address ?
    <ipv6_subnet>    IPv6 prefix x:x::y/z
    dhcp             Enable DHCPv6 client function
FLEX24-10G(config-if-vlan)# ipv6 address 2001::3/64
FLEX24-10G(config-if-vlan)# end
FLEX24-10G# copy running-config startup-config
Building configuration...
% Saving 2118 bytes to flash:startup-config
FLEX24-10G#
```

DHCP Configuration - IPv4

The below CLI snippet configures VLAN 1 to obtain an IP address from a DHCP server. The switch will send out a DHCP request to obtain a DHCP lease from a server on the network.

An optional fallback IP address can be set if the switch is unable to obtain an IP address from a DHCP server.

```
FLEX24-10G# configure terminal
```

```
FLEX24-10G(config)# interface vlan 1
FLEX24-10G(config-if-vlan)# ip address ?
    <ipv4_addr>    IP address
    dhcp           Enable DHCP
FLEX24-10G(config-if-vlan)# ip address dhcp ?
    client-id    DHCP client identifier
    fallback     DHCP fallback settings
    hostname     DHCP host name
    <cr>
FLEX24-10G(config-if-vlan)# ip address dhcp fallback ?
    <ipv4_addr>    DHCP fallback address
FLEX24-10G(config-if-vlan)# $ dhcp fallback 192.168.200.1 255.255.255.0
FLEX24-10G(config-if-vlan)# end
FLEX24-10G# copy running-config startup-config
Building configuration...
% Saving 1967 bytes to flash:startup-config
FLEX24-10G#
```

DHCP Configuration - IPv6

The IP address of VLAN 1 (or any other VLAN) can also be obtained for a DHCPv6 server on the network.

Rapid-commit is a feature which allows DHCPv6 clients to obtain an IP address via a two message exchange as opposed to the traditional four message exchange. This greatly increases the speed in which clients obtain an address from the DHCPv6 server.

For more information relating to rapid-commit please see *Chapter 23: DHCP*.

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# interface vlan 1
FLEX24-10G(config-if-vlan)# ipv6 address ?
    <ipv6_subnet>    IPv6 prefix x:x::y/z
    dhcp             Enable DHCPv6 client function
FLEX24-10G(config-if-vlan)# ipv6 address dhcp ?
    rapid-commit    Enable DHCPv6 client Rapid-Commit option
    <cr>
FLEX24-10G(config-if-vlan)# ipv6 address dhcp rapid-commit ?
    <cr>
FLEX24-10G(config-if-vlan)# ipv6 address dhcp rapid-commit
FLEX24-10G(config-if-vlan)# end
FLEX24-10G# copy running-config startup-config
Building configuration...
% Saving 2150 bytes to flash:startup-config
FLEX24-10G#
```

Setting a Default Gateway – IPv4

A default gateway or gateway of last result is configured by creating a wildcard IPv4 route. This is done from Global Configuration mode as follows.

	Command	**Explanation**
Step 1	configure terminal	Enter Global Configuration mode.
Step 2	ip route 0.0.0.0 0.0.0.0 <ipv4_address>	Create a wildcard route. **0.0.0.0 0.0.0.0** is a catchall route which will catch all IP traffic which does not match a more specific route in the routing table. **<ipv4_address>** represents the IP address.
Step 3	end	**(Optional)** Return to Privileged EXEC mode.
Step 4	copy running-config startup-config	**(Optional)** Copy the contents of the running-config to the startup-config.

Setting a Default Gateway – IPv6

A default gateway or gateway of last result is configured by creating a wildcard IPv6 route. This is done from Global Configuration mode as follows.

	Command	**Explanation**
Step 1	configure terminal	Enter Global Configuration mode.
Step 2	ipv6 route ::/0 {interface vlan <vlan_id> <ipv6_linklocal> | <ipv6_ucast>}	Create a wildcard route. **::/0** specifies a wildcard route which will catch all traffic which does not match a more specific route in the routing table. The route destination must be a unicast IPv6 address or a vlan interface identifier and a link local IPv6 address.
Step 3	end	**(Optional)** Return to Privileged EXEC mode.
Step 4	copy running-config startup-config	**(Optional)** Copy the contents of the running-config to the startup-config.

Navigating the CLI

Command Line Levels

There are three major CLI levels: EXEC mode, Privileged EXEC mode, and Global Configuration mode. Additionally, there are several sub-modes which exist below Global Configuration mode. Examples of CLI sub-modes are Interface Configuration, VLAN Configuration, etc.

The scope of the commands available at each level varies greatly from level to level. For instance, the commands available to the user within Interface Configuration mode will greatly differ from the commands available within Global Configuration mode.

EXEC Mode

EXEC mode is where all users with a privilege level of 0 or 1 are placed. For a privilege level 0 or 1 user to gain access to Privileged EXEC mode, they must provide additional credentials in the form of an enable password/secret.

The scope of commands available within EXEC mode is extremely limited. No changes to the switch's configuration can be issued from EXEC mode. EXEC mode provides the user with basic connectivity commands (ping, traceroute) as well the ability to execute show commands.

Note: The running-config cannot be displayed from EXEC mode.

To enter Privileged EXEC mode, enter the **enable** command.

EXEC mode is identified with a **FLEX24-10G>** prompt.

Privileged EXEC Mode

Users with a privilege level of two or higher and placed into Privileged EXEC mode when they first log into the switch.

All aspects of the switch's configuration can be examined from Privileged EXEC mode. Privileged EXEC mode can be password protected using an enable password/secret. No aspects of the switch's configuration can be modified in this mode.

The scope of commands available within Privileged EXEC mode is not as limited compared to EXEC mode. Some of the abilities available within Privilege EXEC mode include:

- Clearing switch statistics/counters
- Access to all show commands
- Access to the switch's internal file system
- Firmware upgrade commands
- Etc.

```
FLEX24-10G#  ?
    alarm              alarm
    clear              Clear
    configure          Enter configuration mode
    copy               Copy from source to destination
    delete             Delete one file in flash: file system
    dir                Directory of all files in flash: file system
    disable            Turn off privileged commands
    do                 To run exec commands in the configuration mode
    dot1x              IEEE Standard for port-based Network Access Control
    enable             Turn on privileged commands
    exit               Exit from EXEC mode
    firmware           Firmware upgrade/swap
    help               Description of the interactive help system
    ip                 IPv4 commands
    ipv6               IPv6 configuration commands
    linkdown-count     Reset the link down count
    logout             Exit from EXEC mode
```

```
    more              Display file
    no                Delete trace hunt string
    ping              Send ICMP echo messages
    platform          Platform configuration
    reload            Reload system.
    send              Send a message to other tty lines
    show              show
    terminal          Set terminal line parameters
    traceroute        Send IP Traceroute messages
    traptest          Test SNMP Traps - Remove later
FLEX24-10G#
```

Privileged EXEC mode is identified with a **FLEX24-10G#** prompt.

Privilege EXEC mode grants the user access to Global Configuration mode via the **configure terminal** command.

Global Configuration

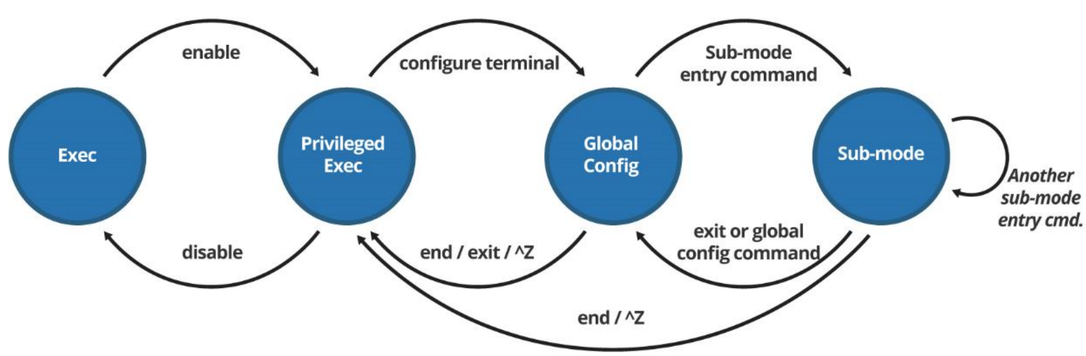
Global Configuration mode is accessed from Privileged EXEC mode via the execution of the **configure terminal** command.

Users require a privilege level of 15 to access Global Configuration mode. Users with a privilege level lower than 15 must provide a privilege level 15 enable password/secret to be granted access.

All switch configuration commands are performed in Global Configuration mode or in one of the sub-modes. Some of the sub-modes available to the user from Global Configuration mode include:

- Interface Configuration mode
- VLAN Configuration mode
- SNMP Host Configuration mode
- IPMC Profile Configuration mode

Global Configuration mode is identified with a **FLEX24-10G(config)#** prompt.



Context Sensitive Help

The switch's CLI contains hundreds of commands, some very simple and others extremely complex. It is required that the switch contains some help system which can aid the user in executing commands.

The FLEX24-10G contains a context sensitive help system which considers what the user has already typed to provide suggestions for which parameter/keyword to include next.

To use the context sensitive help, issue **?** at any point during a command.

<u>For example:</u> If the user would like to configure Rapid Spanning Tree Protocol but does not know the command to do so, the context sensitive help is able to guide the user keyword by keyword until the command is complete.

```
FLEX24-10G(config)# spanning-tree ?
    aggregation    Aggregation mode
    edge           Edge ports
    mode           STP protocol mode
    mst            STP bridge instance
    recovery       The error recovery timeout
    transmit       BPDUs to transmit
FLEX24-10G(config)# spanning-tree mode ?
    mstp    Multiple Spanning Tree (802.1s)
    rstp    Rapid Spanning Tree (802.1w)
    stp     802.1D Spanning Tree
FLEX24-10G(config)# spanning-tree mode rstp ?
    <cr>
FLEX24-10G(config)# spanning-tree mode rstp
```

<cr> indicates that the command entered is a valid command and can be executed as such.

Tab Completion and Auto Completion

Tab completion is fully supported on the FLEX24-10G. When the user enters a partial string, which can only match a single keyword, pressing the TAB key will automatically complete the string. If the string is not an exact match to one and only one keyword, pressing the TAB key will list the available keyword possibilities.

<u>Example:</u> Using tab complete on the **configure terminal** command.

```
FLEX24-10G#
FLEX24-10G# co        [TAB KEY IS PRESSED HERE]
configure  copy
FLEX24-10G#
```

In the above snippet "co" is entered and then the TAB key is pressed. The context sensitive help does not know whether the user would like to enter **configure** or **copy** so it lists both options. If the user had entered "con" instead and then pressed TAB, the system would recognize that **configure** is the only Privileged EXEC mode command beginning with the "con" string.

```
FLEX24-10G# con?
    configure    Enter configuration mode
FLEX24-10G# configure t?
```

```
    terminal    Configure from the terminal
    <cr>
FLEX24-10G# configure terminal
FLEX24-10G(config)#
```

When the ability to TAB complete a partial string to a full string is present, TAB completing is not required. Refer to the snipped below:

```
FLEX24-10G#
FLEX24-10G# con t
FLEX24-10G(config)#
```

In essence, **configure terminal** can be shortened to **con t** and the switch will recognize them as being the same command.

Show Commands

Show commands allow the user to verify the switch's configuration and to monitor the switch's performance. All show commands must be entered from either EXEC mode or Privileged EXEC mode.

```
FLEX24-10G# show ?
    aaa                  Authentication, Authorization and Accounting methods
    access               Access management
    access-list          Access list
    aggregation          Aggregation port configuration
    alarm                alarm
    clock                Configure time-of-day clock
    contact              Show Contact information
    ddmi                 DDMI configuration
    dot1x                IEEE Standard for port-based Network Access Control
    history              Display the session command history
    interface            Interface.
    ip                   Interface Internet Protocol configuration commands
    ipmc                 IPv4/IPv6 multicast configuration
    ipv6                 IPv6 configuration commands
    lacp                 LACP configuration/status
    licenses             Display license information.
    line                 TTY line information
    linkdown-count       Show downlink linkdown count
    lldp                 Link Layer Discover Protocol.
    logging              System logging message
    loop-protect         Loop protection configuration
    mac                  Mac Address Table information
    monitor              Monitoring different system events
    mrp                  MRP status
    mvr                  Multicast VLAN Registration configuration
    ntp                  Configure NTP
    platform             Platform configuration
    poe                  Power Over Ethernet
    poe-voltage          Show the current PoE Voltage in deciVolts
    port-security        Show Port Security overview status.
    privilege            Display command privilege
    process              process
    psu-capacity         Show power supply capacity, usage and budget
    psu-current          Show power supply current in A
```

```
    pvlan              PVLAN configuration
    qos                Quality of Service
    radius-server      RADIUS configuration
    rmon               RMON statistics
    running-config     Show running system information
    services           show the services' status
    sflow              Statistics flow.
    snmp               Set SNMP server's configurations
    spanning-tree      STP Bridge
    svl                Shared VLAN Learning configuration
    switchport         Display switching mode characteristics
    system             system
    tacacs-server      TACACS+ configuration
    temperature        Show board temperature and cpu fan speed
    terminal           Display terminal configuration parameters
    thermal-protect    Display thermal protection status.
    udld               Unidirectional Link Detection (UDLD) configurations,
                       statistics and status
    upnp               Display UPnP configuration
    user-privilege     Users privilege configuration
    users              Display information about terminal lines
    version            System hardware and software status
    vlan               VLAN status
    voice              Voice appliance attributes
    web                Web
FLEX24-10G#
```

Using “do” while in a Non-EXEC Mode

Typically, individual commands can only be entered in one CLI mode and one mode only. The one exception to this rule involves the “do” keyword.

The “do” keyword allows Privileged EXEC mode commands to be entered from any CLI mode requiring a higher privilege level. In blatant terms, “do” commands allows Privileged EXEC mode commands to be entered from Global Configuration mode or any sub-mode.

Showing the system clock from Privileged EXEC, Global Configuration, and Interface Configuration:

```
FLEX24-10G# show clock
System Time     : 2019-10-17T00:15:03+00:00

FLEX24-10G# configure terminal
FLEX24-10G(config)# show clock
                    ^
% Invalid word detected at '^' marker.

FLEX24-10G(config)# do show clock
System Time     : 2019-10-17T00:15:12+00:00

FLEX24-10G(config)# interface GigabitEthernet 1/1
FLEX24-10G(config-if)# do show clock
System Time     : 2019-10-17T00:15:59+00:00

FLEX24-10G(config-if)#
```

Notice the CLI mode is different each time **do show clock** is executed.

Banners

Banners and Message of the Days (MOTDs) allow corporations to provide a message to individuals attempting to gain access to the FLEX24-10G. Up to three unique banners can be configured on the switch.

EXEC Banner: EXEC Banners are displayed to the user after they enter Privileged EXEC mode.

Login Banner: Login Banners are displayed to the user before they enter their username and password.

Message of the Day (MOTD): The MOTD is first thing which the use sees when the begin a CLI instance.

Single-line Banner Configuration

A single line banner is just that, a banner which is only one line.

	Command	Explanation
Step 1	configure terminal	Enter Global Configuration mode.
Step 2	banner [exec | login | motd] <string>	Set a system banner. If neither **exec, login,** nor **motd** are specified, the system creates a MOTD. **<string>** must begin and end with a matching delimiting character. The delimiting character should be a special character which is not contained in the banner message. The delimiting character marks the start and finish of the banner message.
Step 3	end	**(Optional)** Return to Privileged EXEC mode.
Step 4	copy running-config startup-config	**(Optional)** Copy the contents of the running-config to the startup-config.

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# banner exec ! This is an EXEC banner. !
FLEX24-10G(config)# banner login ! This is a login banner. !
FLEX24-10G(config)# banner motd ! This is a MOTD for today, October 22nd. !
FLEX24-10G(config)# ^Z
FLEX24-10G# exit

 This is a MOTD for today, October 22nd.

Press ENTER to get started

 This is a login banner.

Username: admin
Password:

 This is an EXEC banner.
```

```
FLEX24-10G#
```

Multi-line Banner Configuration

Multi-line banners are banners which span multiple lines. These are configured in much the same way as single-line banners.

To configure a multi-line banner, press **ENTER** immediately after typing the starting delimiting character.

	Command	Explanation
Step 1	configure terminal	Enter Global Configuration mode.
Step 2	banner [exec | login | motd] <delimiting_character>	Set a system banner. If neither **exec, login,** nor **motd** are specified, the system creates a MOTD. **<delimiting_character>** should be a character not contained within the banner message. Once this command has been executed the prompt will change to FLEX24-10G(multiline-input)#
Step 3	<banner_line1>	Enter first line of banner message.
Step 4	<banner_line2>	Enter second line of banner message. Continue this process for each line in the banner message.
Step 5	<banner_lastline> <delimiting_character>	Enter the last line of the banner message. End the command with a matching delimiting character to signify the end of the banner message.
Step 6	end	**(Optional)** Return to Privileged EXEC mode.
Step 7	copy running-config startup-config	**(Optional)** Copy the contents of the running-config to the startup-config.

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# banner exec !
% Entering multi-line text input mode. Type in text and exit the mode using the delimiting
character '!'. All input after that character will be silently ignored. The effective buffer
size, i.e. excluding the delimiting characters but including any newline characters (e.g. from
multi-line input), cannot be longer than 255.
FLEX24-10G(multiline-input)# EXEC
FLEX24-10G(multiline-input)# Banner !
FLEX24-10G(config)# banner login !
% Entering multi-line text input mode. Type in text and exit the mode using the delimiting
character '!'. All input after that character will be silently ignored. The effective buffer
size, i.e. excluding the delimiting characters but including any newline characters (e.g. from
multi-line input), cannot be longer than 255.
FLEX24-10G(multiline-input)# LOGIN
FLEX24-10G(multiline-input)# Banner !
FLEX24-10G(config)# banner motd !
% Entering multi-line text input mode. Type in text and exit the mode using the delimiting
character '!'. All input after that character will be silently ignored. The effective buffer
```

```
size, i.e. excluding the delimiting characters but including any newline characters (e.g. from
multi-line input), cannot be longer than 255.
FLEX24-10G(multiline-input)# Message
FLEX24-10G(multiline-input)# of
FLEX24-10G(multiline-input)# the
FLEX24-10G(multiline-input)# Day !
FLEX24-10G(config)# ^Z
FLEX24-10G# exit

Message
of
the
Day

Press ENTER to get started

LOGIN
Banner

Username: admin
Password:

EXEC
Banner
FLEX24-10G#
```

Performing a Firmware Upgrade

A firmware upgrade can be performed using the **firmware upgrade** command from Privileged EXEC mode.

The switch software upgrade file must reside on an FTP or HTTP server with network connectivity to the switch.

Upgrade procedure below:

	Command	**Explanation**
Step 1	firmware upgrade <url_file> **Example:** firmware upgrade ftp://testuser:testpw@192.168.100.2/testfirmware.mfi	Upgrade the system firmware with firmware located at **<url_file>.** The syntax of **<url_file>** is as follows: <protocol>://[<username>[:<password>]@]<host>[:<port>][/<path>]/<file_name> If the switch can locate the file and the file is a genuine software image, the firmware upgrade procedure will begin.
Step 2	end	**(Optional)** Return to Privileged EXEC mode.
Step 3	copy running-config startup-config	**(Optional)** Copy the contents of the running-config to the startup-config.

```
FLEX24-10G# firmware upgrade ftp://testuser:testpw@192.168.100.2/testfirmware.mfi
Downloading...
Got 14459628 bytes
Starting flash update - do not power off device!
Erasing flash...done
Programming flash...done
Swapping images...done
Restarting, please wait...

Service "switch_app" of type = "service" with PID = 45 killed by signal Killed (9).
Rebooting...
01:09:46 Rebooting kernel
[21262.749372] reboot: Restarting system
+M25PXX : Init device with JEDEC ID 0xC22019.
phybridge board detected (flex 24).

RedBoot(tm) bootstrap and debug environment [ROMRAM]
Non-certified release, version 1_5-f4c6fba - built 18:44:52, Apr  2 2019

Copyright (C) 2000, 2001, 2002, 2003, 2004, 2005, 2006, 2007, 2008, 2009
Free Software Foundation, Inc.
RedBoot is free software, covered by the eCos license, derived from the
GNU General Public License. You are welcome to change it and/or distribute
copies of it under certain conditions. Under the license terms, RedBoot's
source code and full license terms must have been made available to you.
Redboot comes with ABSOLUTELY NO WARRANTY.

Platform: VCore-III (MIPS32 24KEc) JAGUAR2_C
RAM: 0x80000000-0xa0000000 [0x800365e0-0x9ffd0ffc available]
FLASH: 0x40000000-0x41ffffff, 512 x 0x10000 blocks
== Executing boot script in 3.000 seconds - enter ^C to abort
RedBoot> diag -p
RedBoot> fis load -x linux
MD5 signature validated
Stage1: 0x80100000, length 4907088 bytes
Initrd: 0x80600000, length 204800 bytes
Kernel command line: init=/usr/bin/stage2-loader loglevel=4
RedBoot> exec
Now booting linux kernel:
 Base address 0x80080000 Entry 0x80100000
 Cmdline : init=/usr/bin/stage2-loader loglevel=4
 Active fis: linux
00:00:01 Stage 1 booted. Starting stage2 boot @ 1120 ms
00:00:02 Loading stage2 from NAND file 'fwUopcKv'
00:00:24 Overall: 23305 ms, ubifs = 1730 ms, squash mount: 8 ms, rootfs 12387880 bytes read in
19438 ms (622 KiB/s)
00:00:31 Starting application...
Using existing mount point for /switch/

Press ENTER to get started

Username:
```

Chapter 2: Local User Database, Passwords and Secrets

Introduction

The FLEX24-10G contains a local user database which can contain up to 20 users. Each entry in the user database contains its own username, password, and privilege level. A user's privilege level is used to restrict which features a user has access to once they are authenticated by the switch.

A user's privilege level ranges from 0 to 15. A user with a privilege level of 15 can access all switch features while users with a privilege level of 0 to 14 are restricted to EXEC mode. Users with a privilege level of 0 to 14 are placed into EXEC mode once they are authenticated by the switch. Only users with a privilege level of 15 will be able to access Global Configuration mode.

Traditionally, users with a privilege level of 0 to 14 are placed into EXEC mode. While this is true, there are ways for the user to gain access to Privileged EXEC mode and Global Configuration mode without modifying the user's privilege level. This is accomplished using an enable password or enable secret.

Configuration

Creating a New User Account

User accounts are created from Global Configuration mode. The below configuration will create two user accounts, with privilege levels 0, and 14, respectively.

	<u>**Command**</u>	<u>**Explanation**</u>
Step 1	configure terminal	Enter Global Configuration mode.
Step 2	[no] username <username> privilege <0-15> password {encrypted | none | unencrypted} <password> **Example:** username user1 privilege 0 password unencrypted pass1 **Example:** username usernopass privilege 0 password none	Create a new user account with username **<username>** and password **<password>.** The optional **no** form will delete an already existing user account. **<0-15>** specifies the users privilege level. If the **encrypted** keyword is specified, the switch will expect the encrypted hash as the **<password>** parameter. If the **unencrypted** keyword is specified, the user will enter the desired password in plaintext. The password will be encrypted in the running-config. The **none** keyword configures a user without a password.

		Note: The **username** must be a string less than 32 characters and can contain letters, numbers, and underscores. **Note:** The **password** must be less than 32 characters and can contain any printable character including spaces.
Step 3	end	**(Optional)** Return to Privileged EXEC mode.
Step 4	copy running-config startup-config	**(Optional)** Copy the contents of the running-config to the startup-config.

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# username user1 privilege 0 password ?
    encrypted      Specifies an ENCRYPTED password will follow
    none           NULL password
    unencrypted    Specifies an UNENCRYPTED password will follow
FLEX24-10G(config)# username user1 privilege 0 password unencrypted pass1
FLEX24-10G(config)# username user2 privilege 14 password unencrypted pass2
FLEX24-10G(config)# username user2 privilege 14 password encrypted
faa64e83c78a83facd51657f13e0ca95cb41748fbcb5b74421f18d57df89bbcbe74a6636e5aa87cfab562696a6a69a
eedb0786fc3d6a93ef36dff5ab99b46e26
```

The last line of the above CLI snippet creates user2 using an encrypted hash instead of an unencrypted plaintext password. Both lines beginning with **username user2** create the same user with the same password, the means in which they are created are different.

Logging in with a Privilege Level 0 to 14 User

Above user1 was created with a privilege level of 0. What happens when this user logs into the switch? What kind of permissions will they be given?

```
Press ENTER to get started

Username: user1
Password:
FLEX24-10G> ?
    clear          Clear
    disable        Turn off privileged commands
    do             To run exec commands in the configuration mode
    enable         Turn on privileged commands
    exit           Exit from EXEC mode
    help           Description of the interactive help system
    logout         Exit from EXEC mode
    ping           Send ICMP echo messages
    show           show
    traceroute     Send IP Traceroute messages
FLEX24-10G> enable
% No password set
```

```
FLEX24-10G>
```

```
Press ENTER to get started

Username: user2
Password:
FLEX24-10G# ?
    clear              Clear
    disable            Turn off privileged commands
    do                 To run exec commands in the configuration mode
    enable             Turn on privileged commands
    exit               Exit from EXEC mode
    help               Description of the interactive help system
    linkdown-count     Reset the link down count
    logout             Exit from EXEC mode
    no                 Delete trace hunt string
    ping               Send ICMP echo messages
    show               show
    terminal           Set terminal line parameters
    traceroute         Send IP Traceroute messages
FLEX24-10G#
```

Both users are placed into EXEC mode and only have access to EXEC level commands. If the user attempts to access Privileged EXEC mode, the switch will request an enable password or an enable secret. In the case above neither an enable password nor enable secret have been set.

Logging in with a Privilege Level 15 User

By default, the switch only contains one user account. This user account has a username/password of admin/admin and a privilege level of 15.

```
Press ENTER to get started

Username: admin
Password:
FLEX24-10G# ?
    alarm              alarm
    clear              Clear
    configure          Enter configuration mode
    copy               Copy from source to destination
    delete             Delete one file in flash: file system
    dir                Directory of all files in flash: file system
    disable            Turn off privileged commands
    do                 To run exec commands in the configuration mode
    dot1x              IEEE Standard for port-based Network Access Control
    enable             Turn on privileged commands
    exit               Exit from EXEC mode
```

```
    firmware          Firmware upgrade/swap
    help              Description of the interactive help system
    ip                IPv4 commands
    ipv6              IPv6 configuration commands
    linkdown-count    Reset the link down count
    logout            Exit from EXEC mode
    more              Display file
    no                Delete trace hunt string
    ping              Send ICMP echo messages
    platform          Platform configuration
    reload            Reload system.
    send              Send a message to other tty lines
    show              show
    terminal          Set terminal line parameters
    traceroute        Send IP Traceroute messages
    traptest          Test SNMP Traps - Remove later
FLEX24-10G# configure terminal
FLEX24-10G(config)#
```

Privilege level 15 users have complete unrestricted access to the switch. Global Configuration mode can be reached using **configure terminal** from Privileged EXEC mode.

Enable Passwords and Enable Secrets

Enable passwords and enable secrets give users with a privilege level less than 15 a means to access Privileged EXEC and Global Configuration mode. When a user with a privilege level other than 15 attempts to access Privileged EXEC mode, the switch will prompt them for an enable password/secret (if one has been configured).

By default, an enable password or enable secret has a privilege level of 15 associated with it, however this can be changed at the administrator's discretion.

Creating an Enable Password

	Command	Explanation
Step 1	configure terminal	Enter Global Configuration mode.
Step 2	enable password [level <1-15>] <password>	Create an enable password of **<password>.** An optional privilege level can be associated with the enable password. When a user supplies this password, they will be promoted to the privilege level associated with the enable password for the remainder of the session. By default, the enable password has a privilege level of 15.
Step 3	end	**(Optional)** Return to Privileged EXEC mode.

Step 4	copy running-config startup-config	**(Optional)** Copy the contents of the running-config to the startup-config.

The enable password is stored in the running-config in plaintext.

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# enable password thisisapassword
FLEX24-10G(config)# do show run | include enable password
enable password level 15 thisisapassword
FLEX24-10G(config)# exit
FLEX24-10G# exit

Press ENTER to get started

Username: user1
Password:
FLEX24-10G> enable
Password: ********
FLEX24-10G# configure terminal
FLEX24-10G(config)#
```

Now that an enable password has been configured, user1 will be able to access Privileged EXEC/Global Configuration mode using the enable password.

Creating an Enable Secret

	Command	Explanation
Step 1	configure terminal	Enter Global Configuration mode.
Step 2	enable secret {0 | 5} [level <1-15>] <secret>	Create an enable secret of **<secret>.** **{0 | 5}** specifies the encrypted nature of the secret to follow. • **0** specifies that an unencrypted secret will follow. • **5** specifies that an encrypted secret will follow. An optional privilege level can be associated with the enable secret. When a user supplies this secret, they will be promoted to the privilege level associated with the enable secret for the remainder of the session. By default, the enable secret has a privilege level of 15.
Step 3	end	**(Optional)** Return to Privileged EXEC mode.
Step 4	copy running-config startup-config	**(Optional)** Copy the contents of the running-config to the startup-config.

Note: An enable secret and enable password cannot exist in the running-config at the same time. If an enable password exists in the running-config and an enable secret is later configured, the enable password will be removed from the running-config. This same behavior occurs if an enable password is configured when an enable secret had previously been configured.

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# enable secret 0 level 15 thisisasecret
FLEX24-10G(config)# exit
FLEX24-10G# exit

Press ENTER to get started

Username: user1
Password:
FLEX24-10G> enable
Password: ***************    SUPPLIED ENABLE PASSWORD – LOGIN FAILED
Password: *************      SUPPLIED ENABLE SECRET – LOGIN SUCCESSFULL
FLEX24-10G# configure terminal
FLEX24-10G(config)#
```

In the above CLI snippet, user1 attempts to access Privileged EXEC mode using the enable password. Since the enable secret takes precedence over the enable password, the enable secret must be provided to access Privileged EXEC mode.

Verification

There are no specific show commands to display the contents of the local user database.

All users can be seen from the running-config using the optional **| begin username filter.**

```
FLEX24-10G# show run | begin username
username test privilege 15 password encrypted
e983263b54986f9f80b1c361c68b0325dfa24f31ede665e1480fe79f5a408d77a36b809c56be56a4cce412013457ba
9150fa8a4179b33396ae0513caa6f32c65
username admin privilege 15 password encrypted
902b0767a854f248b32aec7f9231d06b731a62d8fec635fb2027fa047fa7909bdc100988b796e5722232b37942fb3a
0202a308c3f0db10188dd347dcea672ad5
username user1 privilege 0 password encrypted
50011646eb65782aa6e7e3af9f255bbcb87537b88c6b968981bd0811383d3951826296066b94b8b7940744ab756f81
9904a516b1587bccf25f1abc33d0b84aec
username user2 privilege 14 password encrypted
faa64e83c78a83facd51657f13e0ca95cb41748fbcb5b74421f18d57df89bbcbe74a6636e5aa87cfab562696a6a69a
eedb0786fc3d6a93ef36dff5ab99b46e26
username user3 privilege 15 password encrypted
04ddeef11597be753d4f9394261cc07cf77ae73b70921a48a2f189ba7cac6d405996a53ca4c16b3b3860174a983b16
96d8ace71b31a520b6ee9eca9726264164
!
```

show run | include enable: Show the running-config but include only the first line beginning with the "enable" string. This command can be used to display the enable password/secret (if one has been configured).

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# enable password thisisapassword
FLEX24-10G(config)# enable secret 0 thisisasecret
FLEX24-10G(config)# do show run | include enable
enable secret 5 level 15 16ECB5441E89054BBEB13C715CB926D7
FLEX24-10G(config)#
```

Chapter 3: Terminal Lines

Introduction

Whenever a user accesses the switch whether it be via serial console, SSH, or Telnet, they are utilizing one of the several terminal lines contained within the switch.

The FLEX24-10G has support for 17 terminal lines. 16 of these lines are known as VTY (Virtual Teletype) lines and are used for SSH/Telnet sessions. The last terminal line is for the serial console interface.

Because there are multiple VTY lines, multiple SSH/Telnet sessions can exist at the same time. The 17 terminal lines can be configured independently of one another. For example: the user who creates the first SSH instance can be provided a different experience than the user who creates the second SSH session.

Additionally, the VTY lines can be configured separately from the serial console line.

Configuration

Terminal lines can be configured one by one or in bulk. If desired, all 17 terminal lines can be configured at once, all 16 VTY lines can be configured, or individual terminal lines can be configured.

To enter Line Configuration mode, enter **line {<0-16> | console 0 | vty <0-15>}** from Global Configuration mode.

	Command	Explanation
Step 1	configure terminal	Enter Global Configuration mode
Step 2	line {<0-16> | console 0 | vty <0-15>}	Enter Line Configuration mode for the terminal lines to configure. **console 0:** Modify the serial console line. **vty <0-15>:** Edit a single or multiple VTY lines at once. **<0-16>:** Edit any or several of the 17 terminal lines at once.
Step 3	[no] editing	Enable/Disable command line editing.
Step 4	[no] exec-banner	Enable/Disable the EXEC banner. By default, if an EXEC banner is configured, it will be displayed.
Step 5	[no] exec-timeout	Set the EXEC timeout. The EXEC timeout is the amount of time a user can be inactive for before they are logged out. An EXEC timeout of 0 disables the timeout.

Step 6	history size <0-32>	Configure the number of commands stored in the command history. This limits the amounts of previous commands available through the cycling of the UP and DOWN keyboard keys.
Step 7	length <0,3-512>	The length parameter controls the amount of lines to display on the terminal screen before pausing. The effect of this command can be seen when issuing show commands which output multiple lines. **Example:** If **length 3** is issued followed by **do show run**, each successive SPACE press will load three additional lines of the running-config.
Step 8	location <location>	Specify the location of the terminal line.
Step 9	[no] motd-banner	Enable/Disable the MOTD. By default, if an MOTD is configured, it will be displayed.
Step 10	privilege level <0-15>	Configure the default privilege level of the terminal line(s). **Note:** As soon as a user logs into the switch, the privilege level of the session will be equal to the privilege level of the user.
Step 11	width <0,40-512>	Configure the width of the terminal window. The value specified in the command indicates the number of columns to display in the terminal window. Each character represents a column.
Step 12	end	**(Optional)** Exit Line Configuration mode and return to Privileged EXEC mode.
Step 13	copy running-config startup-config	**(Optional)** Copy the contents of the running-config to the startup-config.

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# line 0-16
FLEX24-10G(config-line)# no editing
FLEX24-10G(config-line)# no exec-banner
FLEX24-10G(config-line)# no exec-timeout
FLEX24-10G(config-line)# history size 16
FLEX24-10G(config-line)# length 100
FLEX24-10G(config-line)# location NYC location
FLEX24-10G(config-line)# no motd-banner
FLEX24-10G(config-line)# privilege level 15
FLEX24-10G(config-line)# width 100
FLEX24-10G(config-line)# end
```

```
FLEX24-10G# copy running-config startup-config
Building configuration...
% Saving 2894 bytes to flash:startup-config
FLEX24-10G#
```

Verification

The configuration of the 17 terminal lines can be observed within the running-config.

To view detailed statistics pertaining to the current terminal line issue the following command:

show terminal: Displays terminal statistics relating to the current session.

```
FLEX24-10G# show terminal
Line is con 0.
---------------
    * You are at this line now.
    Location is at NYC location.
    Alive from Console.
    Default privileged level is 15.
    Command line editing is disabled
    Display EXEC banner is disabled.
    Display Day banner is disabled.
    Terminal width is 512.
             length is 100.
             history size is 32.
             exec-timeout is 10 min 0 second.

    Current session privilege is 15.
    Elapsed time is 0 day 0 hour 24 min 45 sec.
    Idle time is 0 day 0 hour 0 min 0 sec.

FLEX24-10G#
```

Chapter 4: Power over Ethernet (PoE)

Introduction

The FLEX24-10G is a PoE capable switch suited to provide power to any endpoint connected to any of the 24 Gigabit interfaces. The amount of PoE emitted from each interface is set from Global Configuration and must be within the range of 48 – 58 Volts. Once the output voltage has been set, all the GigabitEthernet interfaces will output this voltage.

The PoE voltage is set switch wide and cannot be configured on a per-interface basis.

By default, all GigabitEthernet interfaces will auto-negotiate PoE with the endpoint. If the endpoint signals to the switch that PoE is required, the switch will power the endpoint. If the switch detects that the endpoint does not require PoE, no power to the endpoint will be provided.

When the switch is providing PoE to an endpoint, the voltage is consistent, however, the current will vary to match the endpoints PoE requirements.

Configuration

Setting the Switch's Output Voltage

The output voltage is configured from Global Configuration as follows:

	Command	**Explanation**
Step 1	configure terminal	Enter Global Configuration mode.
Step 2	poe <voltage>	Specify the switch's PoE output voltage. **<voltage>** is specified in deciVolts and must be within the range of 480 to 580 (48 to 58 Volts).
Step 3	end	**(Optional)** Return to Privileged EXEC mode.
Step 4	copy running-config startup-config	**(Optional)** Copy the contents of the running-config to the startup-config.

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# poe 100
PoE Voltage should be between 480 and 580 deciVolts

FLEX24-10G(config)# poe 550
FLEX24-10G(config)# end
FLEX24-10G# copy running-config startup-config
Building configuration...
% Saving 2848 bytes to flash:startup-config
FLEX24-10G#
```

Setting an Interface's PoE Mode

Although the default behavior on all GigabitEthernet interfaces is to auto-negotiate PoE with the endpoint, this behavior can be changed from Interface Configuration mode for any of the GigabitEthernet interfaces.

Note: Only GigabitEthernet 1/1 to GigabitEthernet 1/24 can have its PoE mode changed. GigabitEthernet 1/25 does not provide PoE as it is the management interface.

	Command	Explanation
Step 1	configure terminal	Enter Global Configuration mode.
Step 2	interface {*, GigabitEthernet <1/1-24>, 10GigabitEthernet<1/1-2>}	Enter Interface Configuration mode.
Step 3	poe mode [auto | manual | off | semi]	Set the PoE mode. If this command is entered on the management interface, or one of the 10G uplink interfaces, the command will be rejected. **Auto:** The interface will auto-negotiate PoE with the endpoint. **Manual:** The interface will always provide PoE and will not auto-negotiate with the endpoint. **Off:** PoE is disabled on the interface. **Semi:** The interface will determine whether the endpoint requires PoE. If the endpoint requires PoE, the interface will output full power to the endpoint, regardless of the endpoint's power requirements.
Step 4	end	**(Optional)** Return to Privileged EXEC mode.
Step 5	copy running-config startup-config	**(Optional)** Copy the contents of the running-config to the startup-config.

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# interface *
FLEX24-10G(config-if)# poe mode off
Ignoring MGMT port
Ignoring Uplink port
Ignoring Uplink port
FLEX24-10G(config-if)# end
FLEX24-10G# copy running-config startup-config
Building configuration...
% Saving 2862 bytes to flash:startup-config
FLEX24-10G#
```

Verification

show poe status {*, GigabitEthernet <1/1-24>, 10GigabitEthernet<1/1-2>}: Displays the real-time PoE status of certain interfaces on the FLEX24-10G. Output will contain information pertaining to only the interfaces specified in the show command.

```
FLEX24-10G# show poe status *
-------------------------------------------------------------------------------
|    Port no |    Op mode |   Pwr good |      Class | Current(mA) |   Watts(W) |
-------------------------------------------------------------------------------
|          1 |       auto |          0 |          0 |       0.000 |      0.000 |
|          2 |       auto |          0 |          0 |       0.000 |      0.000 |
|          3 |       auto |          0 |          0 |       0.000 |      0.000 |
|          4 |       auto |          0 |          0 |       0.000 |      0.000 |
|          5 |       auto |          0 |          0 |       0.000 |      0.000 |
|          6 |       auto |          0 |          0 |       0.000 |      0.000 |
|          7 |       auto |          0 |          0 |       0.000 |      0.000 |
|          8 |       auto |          0 |          0 |       0.000 |      0.000 |
|          9 |       auto |          0 |          0 |       0.000 |      0.000 |
|         10 |       auto |          0 |          0 |       0.000 |      0.000 |
|         11 |       auto |          0 |          0 |       0.000 |      0.000 |
|         12 |       auto |          0 |          0 |       0.000 |      0.000 |
|         13 |       auto |          0 |          0 |       0.000 |      0.000 |
|         14 |       auto |          0 |          0 |       0.000 |      0.000 |
|         15 |       auto |          0 |          0 |       0.000 |      0.000 |
|         16 |       auto |          0 |          0 |       0.000 |      0.000 |
|         17 |       auto |          0 |          0 |       0.000 |      0.000 |
|         18 |       auto |          0 |          0 |       0.000 |      0.000 |
|         19 |       auto |          0 |          0 |       0.000 |      0.000 |
|         20 |       auto |          0 |          0 |       0.000 |      0.000 |
|         21 |       auto |          0 |          0 |       0.000 |      0.000 |
|         22 |       auto |          0 |          0 |       0.000 |      0.000 |
|         23 |       auto |          0 |          0 |       0.000 |      0.000 |
|         24 |       auto |          0 |          0 |       0.000 |      0.000 |
Ignoring MGMT port 25
Ignoring Uplink port 26
Ignoring Uplink port 27
-------------------------------------------------------------------------------
FLEX24-10G#
```

Chapter 5: VLANs

Introduction

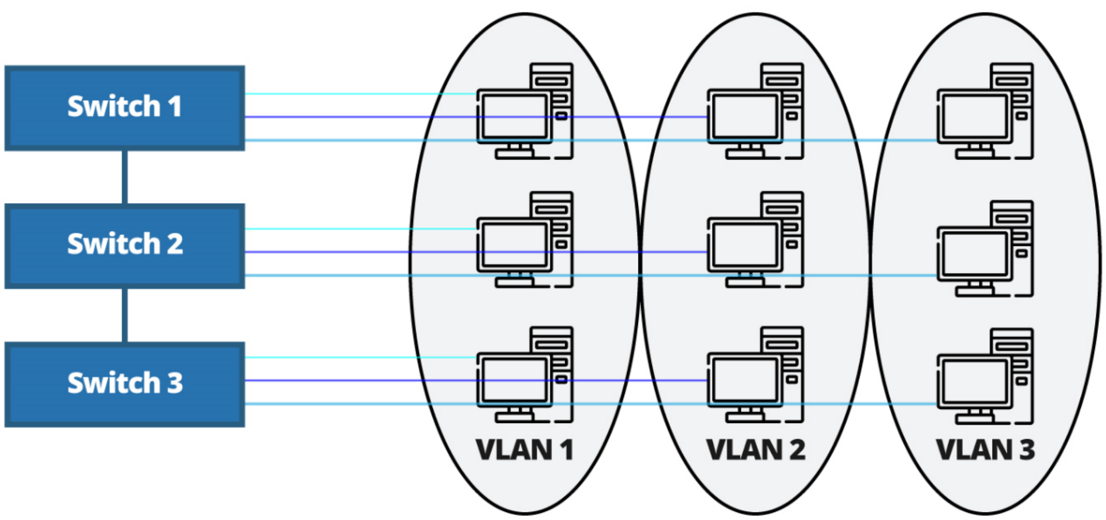
Virtual Local Area Networks (VLANs) are a crucial part of any network. VLANs further divide a network in multiple smaller sub-networks. VLANs create multiple smaller broadcast domains which aid in limiting broadcasts to only hosts which are likely to benefit from them.

By default, only VLAN 1 exists on the FLEX24-10G and all interfaces are members of it. Hence, when the switch broadcasts traffic, all directly connected hosts will receive it. This behavior is often undesirable, for example, as a desktop from the sales department will not likely require the same broadcast traffic as an IP phone in the marketing department.

The ability to segment a network using VLANs can be used to create a different VLAN for each department within a company. With a VLAN created for each department within a company, broadcast traffic is limited to all members of the VLAN and will not reach members of other VLANs.

Since the FLEX24-10G can provide layer-3 routing, an external router is not a requirement for the VLANs to be able to communicate.

A single VLAN can exist on multiple switches. Multiple hosts on multiple switches can be members of the same VLAN. If trunk links are used to connect the switches, broadcast traffic will traverse the trunks and be transmitted to every host in the VLAN.



VLANs on the FLEX24-10G

The FLEX24-10G supports up to 4095 VLANs, ranging 1 through 4095. Traffic belonging to the native VLAN travels across the network unaltered. Traffic not belonging to the native VLAN has a Dot1q tag appended to its ethernet frame. This Dot1q tag, commonly referred to as the VLAN tag, is a 32-bit field which sits between the Source MAC address and EtherType fields of the original frame.

VLAN Tag Format

16 bits	3 bits	1 bit	12 bits
TPID	PCP	DEI	VID

Tag Protocol Identifier (TPID): The TPID field is 16-bits long. This field is used to distinguish the frame from an untagged frame due to its location being identical to the position of the EtherType field in an untagged frame. The TPID field is set to 0x8100. A value of 0x8100 denotes that the frame is an 802.1Q-tagged frame.

Priority Code Point (PCP): The PCP field is a 3-bit field referring to the 802.1p class of service. The PCP value directly maps to the 802.1p priority.

Priority Code Point	Priority	Types of Traffic
000	0	Background
001	1 (default priority)	Best effort
010	2	Excellent effort
011	3	Critical applications
100	4	Video (< 100 ms of latency and jitter)
101	5	Voice (< 10 ms of latency and jitter)
110	6	Internetwork control
111	7	Network control

Drop eligible indicator (DEI): The DEI is a 1-bit field which can work independently or in conjunction with the PCP field. The DEI field marks frames which are eligible to be dropped in the event of network congestion.

VLAN Identifier (VID): The VID is a 12-bit field which indicates which VLAN the frame belongs to. The FLEX24-10G has support for 4095 (1-4095) VLANs.

When the VID has a value of 0x000, this indicates that the frame does not carry a VLAN ID and instead the frame only carries a priority tag.

Frames with a VID of 0x001 are members of the default VLAN.

Port Modes

By default, all interfaces are access ports belonging to VLAN 1 (the default VLAN). Interfaces can also be configured as trunk, or hybrid interfaces.

Access Ports

- Access ports belong to one and only one VLAN. The only instance in which an access port will carry traffic for more than one VLAN is if a voice VLAN is configured.

- It is best practice for all access ports to connect to a single host (PC's, printers, servers, etc). Switch to switch links should never be connected via access ports.
- Access ports can be assigned to any VLAN present on the switch.
- Any access port will drop frames which are not members of the VLAN the interface itself is a member of.
- Access ports will accept C-tagged frames. C-tagged frames are frames containing two Dot1q tags.

Trunk Ports

- By default, trunks ports carry traffic belonging to all VLANs.
- Ports connecting to other switches should always be configured as trunk or hybrid ports.
- All frames which are not members of the trunks native VLAN (VLAN 1 by default) travel across the trunk with a Dot1q tag.
- Egress tagging can be set on trunk ports such that even frames belonging to the trunks native VLAN will receive a Dot1q tag.

Hybrid Ports

Hybrid ports resemble trunk ports while including the following additional features:

- Hybrid ports can be configured to be VLAN tag unaware, C-tag aware, S-tag aware, or S-custom-tag aware.
- Ingress filtering can be controlled.
- Ingress acceptance of frames and configuration of egress tagging can be configured independently.

Creating VLANs, Configuring VLANs, Deleting VLANs

Creating VLANs

In a factory default state, the switch only contains VLAN 1, which all interfaces are a member of. In the below example VLANs 10, 20, and 30 will be created.

	Command	Explanation
Step 1	configure terminal	Enter Global Configuration mode.
Step 2	vlan 10	Create VLAN 10. **Note:** VLANs can be created from any command level below Global Configuration mode.
Step 3	vlan 20	Create VLAN 20. **Note:** VLANs can be created from any command level below Global Configuration mode.
Step 4	vlan 30	Create VLAN 30.

		Note: VLANs can be created from any command level below Global Configuration mode.
Step 5	end	**(Optional)** Return to Privileged EXEC mode.
Step 6	copy running-config startup-config	**(Optional)** Copy the contents of the running-config to the startup-config.

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# vlan 10
FLEX24-10G(config-vlan)# vlan 20
FLEX24-10G(config-vlan)# vlan 30
FLEX24-10G(config-vlan)# end
FLEX24-10G# copy running-config startup-config
Building configuration...
% Saving 2160 bytes to flash:startup-config
FLEX24-10G#
```

Configuring VLANs

Once a VLAN has been created, there are several options which can be configured. For instance, since the FLEX24-10G supports Layer-3 routing, the ability to add an IP address to multiple virtual VLAN interfaces is present. The below example will name VLANs 10, 20, and 30.

Naming VLANs

	Command	**Explanation**
Step 1	configure terminal	Enter Global Configuration mode.
Step 2	vlan 10	Enter VLAN Configuration mode for VLAN 10.
Step 3	name Sales	Name VLAN 10 “Sales”.
Step 4	vlan 20	Enter VLAN Configuration mode for VLAN 20.
Step 5	name Engineering	Name VLAN 20 “Engineering”
Step 6	vlan 30	Enter VLAN Configuration mode for VLAN 30.
Step 7	name Marketing	Name VLAN 30 “Marketing”
Step 8	end	**(Optional)** Exit VLAN Configuration mode and return to Privileged EXEC mode.
Step 9	copy running-config startup-config	**(Optional)** Copy the contents of the running-config to the startup-config.

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# vlan 10
FLEX24-10G(config-vlan)# name Sales
FLEX24-10G(config-vlan)# vlan 20
FLEX24-10G(config-vlan)# name Engineering
FLEX24-10G(config-vlan)# vlan 30
FLEX24-10G(config-vlan)# name Marketing
FLEX24-10G(config-vlan)# end
FLEX24-10G# copy running-config startup-config
Building configuration...
% Saving 2540 bytes to flash:startup-config
FLEX24-10G#
```

Binding an IP Address to a VLANs Switched Virtual Interface

Once a VLAN has been created, a switched virtual interface (SVI) can also be created for each VLAN. These switched virtual interfaces can then have IP addresses bound to them, making Layer-3 routing possible.

	Command	**Explanation**
Step 1	configure terminal	Enter Global Configuration mode.
Step 2	interface vlan 10	Create a switched virtual interface for VLAN 10.
Step 3	**For an IPv4 Address** ip address <ipv4_addr> <subnet_mask> **For an IPv6 Address** ipv6 address <ipv6_address/prefix>	Bind an IP address to the SVI for VLAN 10.
Step 4	end	**(Optional)** Exit VLAN Interface Configuration mode and return to Privileged EXEC mode.
Step 5	copy running-config startup-config	**(Optional)** Copy the contents of the running-config to the startup-config.

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# interface vlan 10
FLEX24-10G(config-if-vlan)# ip address 192.168.200.1 255.255.255.0
FLEX24-10G(config-if-vlan)# end
FLEX24-10G# copy running-config startup-config
Building configuration...
% Saving 2598 bytes to flash:startup-config
FLEX24-10G#
```

Obtaining an SVI's IP Address via DHCP

An alternative to manually setting the IP address of a VLANs SVI would be to allow the SVI to receive an IP address via DHCP.

	Command	**Explanation**
Step 1	configure terminal	Enter Global Configuration mode.
Step 2	interface vlan 10	Create a switched virtual interface for VLAN 10 and enter VLAN Interface Configuration mode.
Step 3	**For an IPv4 Address** ip address dhcp [fallback <ip_address> <subnet_mask>] ip address dhcp [client-id] ip address dhcp [hostname] {domain_name} **For an IPv6 Address** ipv6 address dhcp [rapid-commit]	Configure the SVI for VLAN 10 to receive its IP address from a DHCP server. When configuring DHCP, an optional fallback address can be specified. This fallback address will be assigned to the interface in the event the interface cannot be assigned an address from the DHCP server.

	Command	Explanation
	Rapid-Commit explained below.	The client-id can be configured to be the MAC address of any of the FLEX24-10G's interfaces, a unique ascii string, or a unique hex value.
Step 5	end	**(Optional)** Exit VLAN Interface Configuration mode and return to Privileged EXEC mode.
Step 6	copy running-config startup-config	**(Optional)** Copy the contents of the running-config to the startup-config.

DHCP Rapid Commit:
In a traditional (Normal - Commit) DHCPv6 environment a four-message exchange (SOLICIT -> ADVERTISE -> REQUEST -> REPLY) takes place between the client and the server for the client to obtain an IPv6 address.

With Rapid Commit, a client can successfully obtain an IP address through a two-message exchange (SOLICIT -> REPLY) rather than a four-message exchange. An immediate benefit in using Rapid Commit is that clients obtain their IPv6 address much faster, and there is less overall bandwidth being used.

When only one DHCP server is being used in a network, Rapid Commit provides advantages over the Normal - Commit.

If multiple DHCP servers are in play, when a client requests an IPv6 address, each DHCP server will send an offer to the client. Once the offer has been sent, the lease for any addresses in the offer has begun, regardless of whether the client accepts the offer. This leads to addresses being wasted. In effect, Rapid Commit will waste addresses if multiple DHCP servers are being used. If there are plentiful addresses in the DHCP pool, this is not a problem. If only one DHCP server is being used, Rapid Commit is preferred over Normal – Commit.

Deleting VLANs

	Command	Explanation
Step 1	configure terminal	Enter Global Configuration mode.
Step 2	no vlan 10	Delete VLAN 10.
Step 3	no vlan 20	Delete VLAN 20.
Step 4	no vlan 30	Delete VLAN 30.
Step 5	end	**(Optional)** Return to Privileged EXEC mode.
Step 6	copy running-config startup-config	**(Optional)** Copy the contents of the running-config to the startup-config.

```
FLEX24-10G# show vlan brief
VLAN  Name                              Interfaces
----  --------------------------------  ----------
1     default                           Gi 1/1-25 10G 1/1-2
10    Sales
20    Engineering
30    Marketing
```

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# no vlan 10
FLEX24-10G(config)# no vlan 20
FLEX24-10G(config)# no vlan 30
FLEX24-10G(config)# end
FLEX24-10G# show vlan brief
VLAN  Name                             Interfaces
----  -------------------------------- ----------
1     default                          Gi 1/1-25 10G 1/1-2

FLEX24-10G#
```

Setting the Port Type

	Command	**Explanation**
Step 1	configure terminal	Enter Global Configuration mode.
Step 2	interface {*, GigabitEthernet <1/1-24>, 10GigabitEthernet<1/1-2>}	Enter Interface Configuration mode for the interface(s) to configure.
Step 3	switchport mode {access | trunk | hybrid}	Set the port type to be either an access, trunk, or a hybrid port.
Step 4	end	**(Optional)** Exit Interface Configuration mode and return to Privileged EXEC mode.
Step 5	copy running-config startup-config	**(Optional)** Copy the contents of the running-config to the startup-config.

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# interface GigabitEthernet 1/1-5
FLEX24-10G(config-if)# switchport mode access
FLEX24-10G(config-if)# interface GigabitEthernet 1/6-7
FLEX24-10G(config-if)# switchport mode trunk
FLEX24-10G(config-if)# interface GigabitEthernet 1/8
FLEX24-10G(config-if)# switchport mode hybrid
FLEX24-10G(config-if)# end
FLEX24-10G# copy running-config startup-config
Building configuration...
% Saving 2592 bytes to flash:startup-config
FLEX24-10G#
```

Setting an Interfaces VLAN membership

	Command	**Explanation**
Step 1	configure terminal	Enter Global Configuration mode.
Step 2	interface {*, GigabitEthernet <1/1-24>, 10GigabitEthernet<1/1-2>}	Enter Interface Configuration mode for the interface(s) to configure.
Step 3	switchport mode access	The interface must be configured as an access port for its VLAN membership to be modified.
Step 4	switchport access vlan <vlan_id>	Set the interface(s) to be a member of VLAN **<vlan_id>**.

Step 5	end	**(Optional)** Exit Interface Configuration mode and return to Privileged EXEC mode.
Step 6	copy running-config startup-config	**(Optional)** Copy the contents of the running-config to the startup-config.

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# interface GigabitEthernet 1/1-3
FLEX24-10G(config-if)# switchport access vlan 10
FLEX24-10G(config-if)# interface GigabitEthernet 1/4-5
FLEX24-10G(config-if)# switchport access vlan 20
FLEX24-10G(config-if)# end
FLEX24-10G# copy running-config startup-config
Building configuration...
% Saving 2727 bytes to flash:startup-config
FLEX24-10G#
```

Configuring Trunk Ports

	Command	**Explanation**
Step 1	configure terminal	Enter Global Configuration mode.
Step 2	interface {*, GigabitEthernet <1/1-24>, 10GigabitEthernet<1/1-2>}	Enter Interface Configuration mode for the interface(s) to configure.
Step 3	switchport mode trunk	Set the interface to trunking mode. By default, frames from all VLANs are permitted over trunk ports. **Note:** The interface on the neighboring switch must also be in trunking mode.
Step 4	switchport trunk allowed vlan {<vlan_list> | all | none | add <vlan_list> | except <vlan_list> | remove <vlan_list>}	**(Optional)** Specify exactly which VLANs we would like allowed over the trunk link. **<vlan_list>:** Specifies exact VLAN list to be allowed across the trunk link. **all:** Allows all VLANs to be allowed across the trunk link. This is the default setting. **none:** Removes all VLANs from a trunk port. **add <vlan_list>:** Add a single VLAN or a list of VLANs to the set of already allowed VLANs. **except <vlan_list>:** Configure the trunk to allow all VLANs except **<vlan_list>**.

		remove <vlan_list>: Remove VLANs in **<vlan_list>** from the set of allowed VLANs across the trunk.
Step 5	switchport trunk vlan tag native	**(Optional)** Set the trunk to tag all packets, including those belonging to the native VLAN.
Step 6	switchport trunk native vlan <vlan_id>	**(Optional)** Set the trunks native VLAN. By default, a trunk's native VLAN is VLAN 1. All packets belonging to **<vlan_id>** will travel across the trunk untagged unless **switchport trunk vlan tag native** has been issued.
Step 7	end	**(Optional)** Exit Interface Configuration mode and return to Privileged EXEC mode.
Step 8	copy running-config startup-config	**(Optional)** Copy the contents of the running-config to the startup-config.

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# interface GigabitEthernet 1/6
FLEX24-10G(config-if)# switchport mode trunk
FLEX24-10G(config-if)# switchport trunk allowed vlan 10,20
FLEX24-10G(config-if)# switchport trunk vlan tag native
FLEX24-10G(config-if)# end
FLEX24-10G# copy running-config startup-config
Building configuration...
% Saving 2798 bytes to flash:startup-config
FLEX24-10G#
```

Configuring Hybrid Ports

Hybrid Ports allow for additional configuration not available with access and trunk ports. With hybrid ports the tagging behavior for ingress and egress traffic can be configured.

Hybrid Port Types

Unaware

On unaware ports, all frames regardless of whether they are carrying a VLAN tag or not are classified to the Port VLAN. For egress traffic, all VLAN tags are preserved.

C-Port

By default, all hybrid ports are configured as C-Ports.

With ports configured as C-Ports, all ingress traffic with a VLAN tag and a TPID = 0x8100, are classified with the VLAN ID embedded in the tag. A TPID value of 0x8100 indicates that the frame is an 802.1Q tagged frame.

All untagged or priority tagged ingress frames are classified with the Port VLAN.

Egress traffic which must be tagged, will be tagged with a C-tag.

S-Port

Ports configured as S-Ports, will classify ingress traffic containing a TPID value of 0x88A8 (double-tagged frames) with the VLAN ID embedded in the tag.

Priority tagged frames are classified to the Port VLAN ID.

For S-Ports configured to accept Tagged Only frames, frames without a TPID of 0x88A8 are dropped.

S-Custom-Port

S-Custom-Ports allow the administrator to specify a custom EtherType value which can be used to modify ingress traffic.

To specify an EtherType for Custom S-Ports issue **vlan ethertype s-custom-port <0x0600-0xfff>** from Global Configuration.

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# vlan ethertype s-custom-port 0x88cc
FLEX24-10G(config)#
```

The above output creates a custom EtherType of 0x88cc (LLDP frames) for S-Custom-Ports.

Ingress frames with a TPID equal to 0x88cc will be classified with the VLAN ID embedded in the tag.

Priority tagged frames are classified to the Port VLAN ID.

If a S-Custom-Port is configured to accept Tagged Only frames, frames without a TPID of 0x88cc will be dropped.

Changing Hybrid Port Types

	Command	Explanation
Step 1	configure terminal	Enter Global Configuration mode.
Step 2	interface {*, GigabitEthernet <1/1-24>, 10GigabitEthernet<1/1-2>}	Enter Interface Configuration mode for the interface(s) to configure.
Step 3	switchport mode hybrid	Set the interface to hybrid mode.
Step 4	switchport hybrid port-type {unaware | c-port | s-port | s-custom-port}	Set the hybrid port type.
Step 5	[no] switchport hybrid ingress-filtering	**(Optional)** By default, access and trunk ports always have ingress filtering enabled. When ingress filtering is enabled, ingress traffic with a VLAN membership different than the port VLAN are dropped.

		If ingress filtering is disabled, all frames which arrive on the interface regardless of their VID will be forwarded to the switch engine.
Step 6	switchport hybrid allowed vlan {<vlan_list> | all | none | add <vlan_list> | except <vlan_list> | remove <vlan_list>}	**(Optional)** Specify exactly which VLANs we would like allowed over the hybrid link. **<vlan_list>:** Specifies exact VLAN list to be allowed across the hybrid link. **all:** Allows all VLANs to be allowed across the hybrid link. This is the default setting. **none:** Removes all VLANs from a hybrid port. **add <vlan_list>:** Add a single VLAN or a list of VLANs to the set of already allowed VLANs. **except <vlan_list>:** Configure the hybrid port to allow all VLANs except **<vlan_list>**. **remove <vlan_list>:** Remove VLANs in **<vlan_list>** from the set of allowed VLANs across the hybrid link.
Step 7	switchport hybrid native vlan <vlan_id>	**(Optional)** Set the hybrid ports native VLAN. By default, the native VLAN is VLAN 1. All packets belonging to **<vlan_id>** will travel across the hybrid link untagged.
Step 8	switchport hybrid acceptable-frame-type {all | tagged | untagged}	**(Optional)** Change which type of frames the hybrid port will accept on ingress. **all:** Both tagged and untagged ingress frames will be accepted on the interface. **tagged:** Only ingress frames containing a VID equal to the ports VLAN are accepted. **untagged:** Only untagged ingress frames are accepted on the interface.
Step 9	switchport hybrid egress-tag {all [except-native] | none}	**(Optional)** Ports in a hybrid or trunking state can control the tagging of egress traffic.

		all except-native: Frames belonging to the native VLAN are transmitted untagged. All other frames contain the correct Dot1q tag. **all:** All frames regardless of their VLAN membership will be transmitted with a Dot1q tag. **none:** No frames regardless of their VLAN membership will be transmitted with a Dot1q tag.
Step 10	end	**(Optional)** Exit Interface Configuration mode and return to Privileged EXEC mode.
Step 11	copy running-config startup-config	**(Optional)** Copy the contents of the running-config to the startup-config.

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# interface GigabitEthernet 1/8
FLEX24-10G(config-if)# switchport mode hybrid
FLEX24-10G(config-if)# switchport hybrid port-type c-port
FLEX24-10G(config-if)# no switchport hybrid ingress-filtering
FLEX24-10G(config-if)# switchport hybrid allowed vlan 20,30
FLEX24-10G(config-if)# switchport hybrid native vlan 20
FLEX24-10G(config-if)# switchport hybrid acceptable-frame-type all
FLEX24-10G(config-if)# switchport hybrid egress-tag all
FLEX24-10G(config-if)# end
FLEX24-10G# copy running-config startup-config
Building configuration...
% Saving 2941 bytes to flash:startup-config
FLEX24-10G#
```

Forbidden VLANs

In certain scenarios it may be desirable to make sure that an interface never becomes a member of a VLAN. Dynamic VLAN protocols such as MVRP and GVRP can dynamically add ports to VLANs. Forbidden VLANs are configured on a per interface basis and will prevent an interface from becoming a member of a VLAN.

By default, no interfaces are configured with Forbidden VLANs.

Configuring an Interface with Forbidden VLANs

	Command	Explanation
Step 1	configure terminal	Enter Global Configuration mode.
Step 2	interface {*, GigabitEthernet <1/1-24>, 10GigabitEthernet<1/1-2>}	Enter Interface Configuration mode for the interface(s) to configure.
Step 3	switchport forbidden vlan add <vlan_list>	Add a list of VLANs to be forbidden on the interface. Any interfaces configured with a forbidden VLAN will be unable to have their VLAN

		membership equal to the VLAN which was made forbidden.
Step 4	switchport forbidden vlan remove <vlan_list>	**(Optional)** Remove a list of forbidden VLANs from the interface.
Step 5	end	**(Optional)** Exit Interface Configuration mode and return to Privileged EXEC mode.
Step 6	copy running-config startup-config	**(Optional)** Copy the contents of the running-config to the startup-config.

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# interface GigabitEthernet 1/15-18
FLEX24-10G(config-if)# switchport forbidden vlan add 10,20,30
FLEX24-10G(config-if)# end
FLEX24-10G# copy running-config startup-config
Building configuration...
% Saving 3101 bytes to flash:startup-config
FLEX24-10G#
```

Verification

The FLEX24-10G supports several different show commands to verify the switch's VLAN configuration.

show vlan [all]: Displays all VLANs on the switch and the interfaces which are members of that VLAN. If **all** is not included, only access VLANs are shown.

```
FLEX24-10G# show vlan all
VLAN  Name                              Interfaces
----  --------------------------------  ----------
1     default                           Gi 1/22-25 10G 1/1-2
10    Sales                             Gi 1/1-2
20    Engineering                       Gi 1/3-4
30    Marketing                         Gi 1/5-7
40    VLAN0040                          Gi 1/8-9
50    VLAN0050                          Gi 1/10-11
60    VLAN0060                          Gi 1/12-13
70    VLAN0070                          Gi 1/14-15
80    VLAN0080                          Gi 1/16-17
90    VLAN0090                          Gi 1/18-19
100   VLAN0100                          Gi 1/20-21

FLEX24-10G#
```

show vlan brief [all]: Displays VLAN summary information. If **all** is not included, only access VLANs are shown.

```
FLEX24-10G# show vlan brief all
VLAN  Name                              Interfaces
----  --------------------------------  ----------
1     default                           Gi 1/22-25 10G 1/1-2
10    Sales                             Gi 1/1-2
20    Engineering                       Gi 1/3-4
30    Marketing                         Gi 1/5-7
```

```
40    VLAN0040                          Gi 1/8-9
50    VLAN0050                          Gi 1/10-11
60    VLAN0060                          Gi 1/12-13
70    VLAN0070                          Gi 1/14-15
80    VLAN0080                          Gi 1/16-17
90    VLAN0090                          Gi 1/18-19
100   VLAN0100                          Gi 1/20-21

FLEX24-10G#
```

show vlan id <vlan_list> [all]: Displays information for only the VLANs included in **<vlan_list>.** If **all** is not included, only access VLANs are shown.

```
FLEX24-10G# show vlan id 10,20
VLAN  Name                              Interfaces
----  --------------------------------  ----------
10    Sales                             Gi 1/1-2
20    Engineering                       Gi 1/3-4

FLEX24-10G#
```

show vlan mac [address <mac_address>]: Displays VLAN MAC entries.

show vlan name <vlan_name>: Displays information for only the VLAN with **<vlan_name>.**

```
FLEX24-10G# show vlan name Marketing
VLAN  Name                              Interfaces
----  --------------------------------  ----------
30    Marketing                         Gi 1/5-7
FLEX24-10G#
```

show vlan protocol [eth2 {<Ethertype> | arp | at | ip | ipx} | llc <DSAP> | snap <snap_oui>]: Displays protocol-based VLAN statuses.

show vlan status: Displays quite verbose information on a per interface basis.

```
FLEX24-10G# show vlan status
GigabitEthernet 1/1 :
---------------------
VLAN User   PortType       PVID  Frame Type     Ing Filter  Tx Tag             UVID  Conflicts
----------  -------------  ----  -------------  ----------  -----------------  ----  ---------
Combined    C-Port         10    All            Enabled     None               10    No
Admin       C-Port         10    All            Enabled     None               10
NAS                                                                                  No
GVRP                                                                                 No
MVR                                                                                  No
Voice VLAN                                                                           No
MSTP                                                                                 No
VCL                                                                                  No
RMirror                                                                              No

GigabitEthernet 1/2 :
---------------------
```

```
VLAN User    PortType      PVID  Frame Type     Ing Filter  Tx Tag             UVID  Conflicts
----------   ------------- ----  -------------  ----------  -----------------  ----  ---------
Combined     C-Port        10    All            Enabled     None               10    No
Admin        C-Port        10    All            Enabled     None               10
NAS                                                                                  No
GVRP                                                                                 No
MVR                                                                                  No
Voice VLAN                                                                           No
MSTP                                                                                 No
VCL                                                                                  No
RMirror                                                                              No

          ------------------------------OUTPUT TRUNCATED------------------------------
```

Chapter 6: MAC Address Table

Introduction

The MAC Address Table (MAC table) is a table which enables the switch to make frame forwarding decisions. Each entry in the MAC address table contains the destination MAC address, VLAN ID, Interface ID, and Entry Type (Static/Dynamic).

Default Entries

```
FLEX24-10G# show mac address-table
Type    VID  MAC Address       Ports
Static  1    00:24:63:04:2a:80  CPU
Static  1    ff:ff:ff:ff:ff:ff GigabitEthernet 1/1-25 10GigabitEthernet 1/1-2 CPU
FLEX24-10G#
```

By default, the MAC address table will contain two entries, one entry for the switch CPU, and the broadcast MAC address. As more clients are connected to the network, more and more entries will be added to the MAC address table.

How Switches Forward Frames

When the switch receives ingress traffic on one of its interfaces, it will examine the source and destination MAC address of each frame. If an entry does not already exist in the MAC address table, an entry will be created with the source MAC address and interface in which the frame was received on. The switch will then look for an entry in its MAC address table matching the destination MAC address of the frame. If an entry is found, the frame will be switched and sent out of the interface indicated in the MAC table entry.

If no entry exists, an ARP request is generated by the switch and broadcast out all interfaces except the one in which the frame was received on. If the ARP request is successful, the destination host will issue an ARP response to the switch indicating their MAC address and the switch will add a new entry to its MAC address table.

Adding Static Entries to the Mac Address Table

A static entry is manually configured by the administrator and will never expire (be removed from the MAC address table).

Example: Create a static entry for MAC 00-14-22-01-23-45, located downstream from GigabitEthernet 1/8, and being a member of VLAN 10.

	Command	**Explanation**
Step 1	configure terminal	Enter Global Configuration mode.
Step 2	mac address-table static 00-14-22-01-23-45 vlan 10 interface GigabitEthernet 1/8	Create a static MAC table entry for 00-14-22-01-23-45 with a VLAN membership of VLAN 10 located downstream from interface GigabitEthernet 1/8.

Step 3	end	**(Optional)** Return to Privileged EXEC mode.
Step 4	copy running-config startup-config	**(Optional)** Overwrite the startup-config with the current entries of the running-config.

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# mac address-table static 00-14-22-01-23-45 vlan 10 interface
GigabitEthernet 1/8
FLEX24-10G(config)# end
FLEX24-10G# copy running-config startup-config
Building configuration...
% Saving 2241 bytes to flash:startup-config
FLEX24-10G#
```

MAC Table Aging Time

When a cable is removed and a host's MAC address is no longer located downstream from an interface, its entry in the MAC table will not be immediately removed. First, the aging time will begin to count down. If no host is connected to the interface in question before the aging time expires, the original entry will be removed from the MAC Table.

By default, the aging time is set to 300 seconds (5 minutes).

The aging time can be changed using the **mac address-table aging-time <0, 10-1000000>** command from Global Configuration. An aging time of 0 disables aging.

MAC Learning

By default, when the switch receives frames with an unknown MAC address, it will begin to populate its MAC table. This behavior can be changed on a per-VLAN basis.

The following example shows how to disable VLAN learning on VLANs 1-5, and 10.

	Command	**Explanation**
Step 1	configure terminal	Enter Global Configuration mode.
Step 2	no mac address-table learning vlan 1-5,10	Disable MAC address learning on VLANs 1-5, and 10. When a new MAC address arrives on VLAN 1-5, and 10, the MAC address will not be learnt. VLAN ranges are specified with commas separating individual VLANs from a range and to separate individual non-consecutive VLANs. Spaces are not accepted when specifying a list of VLANs to disable learning on.
Step 3	end	**(Optional)** Return to Privileged EXEC mode.
Step 4	copy running-config startup-config	**(Optional)** Overwrite the startup-config with the current entries of the running-config.

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# no mac address-table learning vlan 1-5,10
FLEX24-10G(config)# end
FLEX24-10G# copy running-config startup-config
Building configuration...
% Saving 2389 bytes to flash:startup-config
FLEX24-10G#
```

Changing MAC Learning on a Per-Interface Level

MAC learning behavior can also be configured on a per-interface basis. By default, all interfaces will automatically learn the MAC address of any hosts located downstream from that interface.

	Command	Explanation
Step 1	configure terminal	Enter Global Configuration mode.
Step 2	interface {*, GigabitEthernet <1/1-24>, 10GigabitEthernet<1/1-2>}	Enter Interface Configuration mode for the interface(s) to be configured.
Step 3	[no] mac address-table learning [secure]	Applying the "no" form disables MAC learning on the interfaces being configured. **mac address-table learning** configures MAC learning to be done automatically. This is the default behavior. When the "secure" keyword is applied, any present entries in the MAC table for the interface(s) in question will be converted to static entries. If no entry exists, the next host to be connected will be given a static entry in the MAC table. MAC locking can be accomplished using this method. Frames with a source MAC address not matching the entry in the MAC table are dropped.
Step 4	end	**(Optional)** Return to Privileged EXEC mode.
Step 5	copy running-config startup-config	**(Optional)** Overwrite the startup-config with the current entries of the running-config.

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# interface GigabitEthernet 1/1
FLEX24-10G(config-if)# no mac address-table learning secure
FLEX24-10G(config-if)# end
FLEX24-10G# copy running-config startup-config
Building configuration...
% Saving 2464 bytes to flash:startup-config
FLEX24-10G#
```

Viewing the MAC Table

The MAC address table can be viewed by issuing **show mac address-table** from Privileged EXEC mode.

```
FLEX24-10G# show mac address-table
Type    VID  MAC Address       Ports
Static  1    00:24:63:04:2a:80  CPU
Dynamic 1    00:e0:4c:30:0d:65 GigabitEthernet 1/19
Static  1    33:33:00:00:00:01 GigabitEthernet 1/1-25 10GigabitEthernet 1/1-2 CPU
Static  1    33:33:ff:04:2a:80 GigabitEthernet 1/1-25 10GigabitEthernet 1/1-2 CPU
Static  1    ff:ff:ff:ff:ff:ff GigabitEthernet 1/1-25 10GigabitEthernet 1/1-2 CPU
Static  10   00:14:22:01:23:45 GigabitEthernet 1/8
FLEX24-10G#
```

Chapter 7: Port Security

Introduction

Port Security on the FLEX24-10G is a security feature configured at the interface level to limit the amount of MAC addresses allowed access on an interface. How the switch decides which MAC addresses should be allowed is at the discretion of the network administrator. Secure MAC addresses can be learnt dynamically by the switch or configured statically by the administrator. A maximum amount of allowed MAC addresses off a single interface can also be configured, and when this maximum amount is exceeded, a security violation is triggered.

Types of Secure MAC Addresses

Static MAC Address - Static MAC addresses are manually configured by the administrator, not dynamically learnt by the switch.

Configured using the **port-security mac-address <mac_ucast> [sticky]** command.

Dynamic MAC Address - Dynamic MAC addresses are dynamically learnt by the switch. MAC addresses are stored in the switch's MAC address table. Contents of the switch's MAC address table are lost in the event of a system reboot.

Sticky Addresses - Sticky MAC addresses are saved in the running configuration and are not lost in the event of a system reboot. A sticky static MAC address is configured using the **port-security mac-address <mac_ucast> sticky** command.

A sticky dynamic MAC address is configured using the **port-security mac-address sticky** command. This command will convert dynamically learnt MAC Addresses into sticky addresses.

Configuring a Maximum Amount of Allowed MAC Addresses on an Interface

A maximum amount of allowed addresses can be configured on a per interface basis. This feature can be useful when the administrator knows that only a specific number of clients will be connected at one time and would like to eliminate the possibility of unwanted clients gaining access to the network. The maximum amount of MAC addresses is configured using the **port-security maximum <0-1023>** command. When the maximum amount is exceeded, a security violation is triggered.

Violation Types

When the maximum amount of MAC addresses on an interface is exceeded, or an invalid MAC address is detected on an interface configured with port-security, a security violation is triggered.

The switch will take one of three actions: **Protect, Restrict,** or **Shutdown.**

Violation Type	Protect	Restrict*	Shutdown
Frames from offending MAC addresses are dropped	Yes	Yes	Yes
Log messages and SNMP trap(s) are created	No	Yes	Yes
Violation counter is incremented with every violating MAC	No	Yes	Yes
Port is shutdown	No	No	Yes

Setting the Violation Type

port-security violation <protect | restrict | shutdown> must be issued at the interface level to configure the violation type. By default, all interfaces configured with port-security use a violation type of **shutdown**.

*When the violation type is set to Restrict, the default **violation-limit** is set to 4. To manually change the **violation-limit** the **port-security maximum violation <1-1023>** command must be issued.

Configuration

	Command	Explanation
Step 1	configure terminal	Enter Global Configuration mode.
Step 2	interface {*, GigabitEthernet <1/1-24>, 10GigabitEthernet<1/1-2>}	Enter Interface Configuration mode for the interface(s) to configure.
Step 3	switchport mode {access | trunk | hybrid}	Set the switchport type. Port security is compatible with all three switchport types. By default, all interfaces are set to access ports.
Step 4	port-security maximum <0-1023>	Specifies the maximum amount of MAC addressed allowed on the interface. Valid values range from 0 to 1023 inclusive.
Step 5	port-security	Enables port security on the interface(s).
Step 6	port-security mac-address <mac_ucast> [vlan <vlan_id>] [sticky]	**(Optional)** Adds a static MAC address to the port configuration. **Note:** When the **<vlan>** and **<sticky>** parameters are used simultaneously, the **<vlan>** parameter must come first.
Step 7	port-security violation {protect | restrict | shutdown}	**(Optional)** Set the violation type when the switch detects more than the allowed amount of MAC addresses on a single interface. By default, the violation type is set to **shutdown**.

Step 8	port-security maximum-violation <1-1023>	**(Optional)** Only used when the violation type is set to **restrict**. When the violation type is set to restrict the **port-security maximum-violation** command sets the maximum amount of violating MAC addresses. For example: If the **port-security maximum 5**, **port-security violation restrict**, and **port-security maximum-violation 2** are all issued on an interface, the first five MAC addresses will be allowed, the next two will be restricted, and once an eighth MAC is detected the interface will be shutdown.
Step 9	end	**(Optional)** Return to Privileged EXEC mode.
Step 10	copy running-config startup-config	**(Optional)** Overwrite the startup-config with the current entries of the running-config.

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# interface GigabitEthernet 1/1
FLEX24-10G(config-if)# switchport mode access
FLEX24-10G(config-if)# port-security maximum 2
FLEX24-10G(config-if)# port-security
FLEX24-10G(config-if)# port-security mac-address 00-E0-4C-68-07-55 vlan 1
FLEX24-10G(config-if)# port-security violation protect
FLEX24-10G(config-if)# end
FLEX24-10G# copy running-config startup-config
Building configuration...
% Saving 2406 bytes to flash:startup-config
FLEX24-10G#
```

Resetting Port Security Counters

Sometimes it may be desirable to clear the MAC addresses and counters on an interface configured with port-security. This may be useful if a switch is moving from one site to another or perhaps the network topology is changing. To clear any port-security counters on an interface or interfaces issue **clear port-security dynamic** from Privileged EXEC mode.

<u>**Optionally:**</u> **clear port-security dynamic address <mac_addr> [vlan]** - Clears all interfaces configured with port-security which have also learnt **<mac_addr>**. If **[vlan]** is specified, **<mac_addr>** will only be cleared if it is found on an interface which is a member of VLAN **[vlan]**.

clear port-security dynamic interface {*, GigabitEthernet <1/1-24>, 10GigabitEthernet<1/1-2>} - Clears port-security counters/MAC addresses for all interfaces specified.

clear port-security dynamic vlan <vlan_id> - Clears port-security counters/MAC addresses on **<vlan_id>.**

Verification

From Privileged EXEC mode, issuing:

show port-security [address] interface [{*, GigabitEthernet <1/1-24>, 10GigabitEthernet<1/1-2>}] will display port-security information on the specified port(s).

Example:

The following commands have been issued on GigabitEthernet 1/1, and currently no ethernet cable is connected to the interface:

port-security maximum 2

port-security violation shutdown

port-security

show port-security interface GigabitEthernet 1/1 returns the following output:

```
FLEX24-10G# show port-security interface GigabitEthernet 1/1
Users:
  P = Port Security (Admin)
  8 = 802.1X
  V = Voice VLAN

Interface  Users Limit Current Violating Violation Mode Sticky State
---------- ----- ----- ------- --------- -------------- ------ -------------
Gi 1/1     P--       2       0         0 Shutdown       No     Ready

Aging disabled
Hold time: 300 seconds

FLEX24-10G#
```

Chapter 8: Network Time Protocol (NTP)

Introduction

NTP allows the FLEX24-10G to synchronize its internal clock with an external/internal NTP server. It is often desirable to have every NTP compatible device in a network to be synchronized to the same NTP server. With every device in the network having its clocks synchronized with every other device, this greatly speeds up the troubleshooting process when timestamps from several devices must be examined together.

The FLEX24-10G can only be configured as an NTP client and cannot act as a standalone server.

Configuration

Up to five NTP servers can be configured on the FLEX24-10G at one time. Each configured NTP server is differentiated by its own index number.

	Command	Explanation
Step 1	configure terminal	Enter Global Configuration mode.
Step 2	ntp	Enable NTP.
Step 3	ntp server <index> ip-address {ipv4_address | ipv6_address | domain_name}	Configure the switch to use an external or internal NTP server. **<index>** must be a value from 1 to 5, inclusive. The server can be added in the form of an IPv4 address, IPv6 address, or a hostname. **Note:** If consecutive commands are entered with identical index numbers, only the most recent command will remain in the running-config.
Step 4	end	**(Optional)** Return to Privileged EXEC mode.
Step 5	copy running-config startup-config	**(Optional)** Overwrite the startup-config with the current entries of the running-config.

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# ntp
FLEX24-10G(config)# ntp server 1 ip-address 192.168.100.100
FLEX24-10G(config)# end
FLEX24-10G# copy running-config startup-config
Building configuration...
% Saving 2285 bytes to flash:startup-config
FLEX24-10G#
```

Setting the System’s Date and Time

The system’s date and time can be configured on the FLEX24-10G from Global Configuration as follows:

	Command	Explanation
Step 1	configure terminal	Enter Global Configuration mode.
Step 2	clock timezone <name_of_timezone> <hours_offset_from_UTC> [<minutes_offset_from_UTC>]	**(Optional)** Configure the time zone. Although this command is optional, it is recommended to configure the time zone first. If the switch resides in a locale with UTC +0, the time zone need not be configured. **name_of_timezone** can be any 16-character string but should match the name of the time zone. **hours_offset_from_UTC** must be a value from -23 to 23. **minutes_offset_from_UTC** must be a value from 0 to 59. By default, the switch's time zone is set to UTC +0. **Note:** If the time is set before the time zone, the time will have to be reset as the time zone value will alter the system time.
Step 3	clock set <yyyy/mm/dd> <HH:mm:ss>	Set the system date and time. **yyyy** must be a year within the range of 1970 and 2037. **mm** configures the month and must be a value from 1 to 12. **dd** configures the month and must be a value from 1 to 31. **HH** is specified in 24-hour time. I.e. **HH** must be a value from 0 to 23. The second **mm** indicates the minute value while **ss** indicates the seconds value.
Step 4	clock summer-time <name_of_summer_timezone> {date <month_start> <date_start> <year_start> <time_start> <month_end> <date_end> <year_end> <time_end> [<minute_offset>] | recurring <start_week_number>	**(Optional)** Configure the daylight savings time behavior. When using the **date** keyword, static daylight savings time is configured. A static daylight savings time cycle only occurs once and does not repeat year-after-year.

	<start_weekday> <start_month> <start_time> <end_week_number> <end_weekday> <end_month> <end_time> [<minute_offset>]}	The **recurring** keyword configures the daylight savings time cycle to repeat indefinitely, year-after-year. <u>**Parameters for Static DST**</u> **month_start**, **date_start**, **year_start**, and **time_start** all work in conjunction with each other to determine the exact time when the clock moves back an hour. **month_end**, **date_end**, **year_end**, and **time_end** all work in conjunction with each other to determine the exact time when the clock moves forward an hour. <u>**Parameters for Repeating DST**</u> **start_week_number**, **start_weekday**, **start_month**, and **start_time** all work in conjunction with each other to determine the exact time when the clock moves back an hour. **end_week_number**, **end_weekday**, **end_month**, and **end_time** all work in conjunction with each other to determine the exact time when the clock moves forward an hour. This cycle repeats indefinitely until the commands are removed from the running-config. **minute_offset** can be used to offset the time difference such that the clock with shift one hour + the **minute_offset** value. **minute_offset** can be any value from 1 to 1439.
Step 5	end	**(Optional)** Return to Privileged EXEC mode.
Step 6	copy running-config startup-config	**(Optional)** Overwrite the startup-config with the current entries of the running-config.

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# clock timezone Eastern -5
FLEX24-10G(config)# clock set 2020/01/31 15:15:00
FLEX24-10G(config)# do show clock
System Time     : 2020-01-31T15:15:05-05:00

FLEX24-10G(config)# clock summer-time Central recurring 2 1 3 03:00 1 1 11 02:00
FLEX24-10G(config)# end
FLEX24-10G# copy running-config startup-config
Building configuration...
```

```
% Saving 3482 bytes to flash:startup-config
FLEX24-10G#
```

Verification

The system time can be viewed using the **show clock** command from Privileged EXEC mode. Additionally, all configured NTP servers can be viewed using the **show ntp status** command.

The bellow snippet illustrates how up to 5 NTP servers can be configured.

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# ntp server 1 ip-address 192.168.1.1
FLEX24-10G(config)# ntp server 2 ip-address 192.168.1.2
FLEX24-10G(config)# ntp server 3 ip-address 0.ca.pool.ntp.org
FLEX24-10G(config)# ntp server 4 ip-address time.nist.gov
FLEX24-10G(config)# ntp server 5 ip-address 10.1.1.1
FLEX24-10G(config)# end
FLEX24-10G# show clock
System Time     : 2019-10-15T20:22:16+00:00

FLEX24-10G# show ntp status
NTP mode : disabled
Idx   Server IP host address (a.b.c.d) or a host name string
---   ------------------------------------------------------
1     192.168.1.1
2     192.168.1.2
3     0.ca.pool.ntp.org
4     time.nist.gov
5     10.1.1.1
FLEX24-10G#
```

Chapter 9: Link Aggregation

Introduction

Link Aggregation provides the ability to combine multiple physical switch interfaces into one logical interface. This single logical interface has a combined bandwidth from every individual physical interface involved in the aggregation. All network traffic across the aggregation is load balanced across all links involved in the aggregation. If any links in the aggregation fail, the aggregation itself will remain active; traffic will be load balanced across the remains links.

Link Aggregation is a viable solution when redundant links are present between switches or between a switch and a server. Typically, with redundant links spanning tree would place such links into a blocking state to eliminate the risk of a switching loop from forming. Link Aggregation solves this issue because although multiple physical links are present between two devices, only a single logical link exists. With a single logical link, a switching loop is not possible.

A link aggregation provides redundancy should a physical link go down as well as having the aggregated bandwidth from every interface involved in the aggregation.

Aggregation Modes

Link Aggregation Control Protocol (LACP)

LACP will automatically negotiate a bundling of links with the neighbor switch. This is done by the active sides of the aggregation sending LACP packets to its connected peer.

During the initial detection period LACP packets are sent every second. Once an aggregation is formed, keep-alive packets are sent every 30 seconds. If one link stops sending keep-alive packets, the switch will remove it from the aggregation.

Links configured as active will always send LACP packets while passive links only reply to LACP packets it receives first.

The FLEX24-10G does not support aggregations including more than 16 interfaces.

Configuration

Example: The below example creates a link aggregation across GigabitEthernet 1/1 – 1/5 and 1/7.

	Command	**Explanation**
Step 1	configure terminal	Enter Global Configuration mode.
Step 2	interface GigabitEthernet 1/1-5 GigabitEthernet 1/7	Enter Interface Configuration mode for the specified range of interfaces.
Step 3	aggregation group <group_id> mode {active | on | passive}	**<group_id>** acts as an index number for the aggregation. **<group_id>** must be a value from 1-13 inclusive.

		A single interface can only be a member of one group-id at one time. **Active:** Link Aggregation with LACP. Active links will initiate the aggregation. **Passive:** Link Aggregation with LACP. Passive links will not initiate the aggregation. **On:** Static aggregation. Once this command is executed, a new logical interface named llag <group_id> will be created.
Step 4	end	**(Optional)** Return to Privileged EXEC mode.
Step 5	copy running-config startup-config	**(Optional)** Overwrite the startup-config with the current entries of the running-config.

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# interface GigabitEthernet 1/1-5 GigabitEthernet 1/7
FLEX24-10G(config-if)# aggregation group 1 mode active
FLEX24-10G(config-if)# end
FLEX24-10G# copy running-config startup-config
Building configuration...
% Saving 3012 bytes to flash:startup-config
FLEX24-10G#
```

If the switch on the other side of the aggregation is also a FLEX24-10G, then a similar configuration to the one above will also have to be performed on the neighbor switch.

Additional Aggregation Parameters

LACP Port Priority

LACP Port Priority is configured on a per interface basis. The port-priority enables the switch to decide which interface to choose from the reserve when a link in the bundle goes down. The lower the priority number the greater the priority.

If an active link in the bundle goes down, the switch will choose the highest priority (lowest number) link not in the bundle to then add that link to the bundle.

By default, all interfaces in an LACP aggregation have a port-priority of 32768.

Note: If the **lacp max-bundle** command is not issued in conjunction with **lacp port-priority** for a specific interface in the bundle, changing the port priority will have no effect.

Example: An aggregation exists with five interfaces, a max-bundle of three, and the following port priorities:

Interface	Gig 1/1	Gig 1/2	Gig 1/3	Gig 1/4	Gig 1/5
Port Priority	1	10	1000	10000	65535

Interfaces Gig 1/1, 1/2, and 1/3 will be members of the active bundle since they have the lowest port-priorities. Gig 1/4 and Gig 1/5 are sitting in reserve until a link in the active bundle fails.

If Gig 1/2 goes down, Gig 1/4 will become a member of the active bundle since its port-priority is higher (lower number) than Gig 1/5.

Max Bundle

Note: Max Bundle only applies to LACP aggregations.

A maximum bundle provides additional redundancy should a link or links in the aggregation fail. The max-bundle must be set to a value less than the number of interfaces involved in the aggregation for the value to have any effect. Up to 16 physical links can be members of the max-bundle.

Example: Assume a LACP aggregation is present between two FLEX24-10G switches on their GigabitEthernet 1/1-10 interfaces. Configuration below.

Switch 1 Command Set

	Command	Explanation
Step 1	configure terminal	Enter Global Configuration mode.
Step 2	interface GigabitEthernet 1/1-10	Enter Interface Configuration mode for interfaces GigabitEthernet 1/1 to GigabitEthernet 1/10.
Step 3	aggregation group 1 mode [active | passive]	Either **active** or **passive** can be specified. If **passive** is set, then the second switch must be configured as **active** for the aggregation to form.
Step 4	exit	Return to Global Configuration mode.
Step 5	int llag 1	Enter Interface Configuration mode for the logical link aggregation interface.
Step 6	lacp max-bundle 7	Sets the max-bundle to seven. With a max-bundle of seven, only seven of the ten interfaces will be active in the aggregation, the remaining three are stored in reserve and are used when one of the seven links fail. **Note:** The max-bundle must be set to a value less than the total number of interfaces in the aggregation.
Step 7	lacp failover {non-revertive | revertive}	**(Optional)** The LACP failover command sets the switch's behavior when a link in an aggregation which was previously down becomes restored. **Non-revertive:** When downed links with a higher priority (lower number) become available, the active link(s) with the lower priority (higher number) will remain in the bundle. The links

	Command	Explanation
		which just transitioned from being down to up will remain in reserve until they are needed. **Revertive:** When downed links with a higher priority (lower number) become available the active link(s) with the lower priority (higher number) will be moved into reserve to allow the newly available links to actively become members of the bundle.
Step 8	end	**(Optional)** Return to Privileged EXEC mode.
Step 9	copy running-config startup-config	**(Optional)** Overwrite the startup-config with the current entries of the running-config.

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# interface GigabitEthernet 1/1-10
FLEX24-10G(config-if)# aggregation group 1 mode passive
FLEX24-10G(config-if)# exit
FLEX24-10G(config)# interface llag 1
FLEX24-10G(config-llag)# lacp max-bundle 7
FLEX24-10G(config-llag)# lacp failover revertive
FLEX24-10G(config-llag)# end
FLEX24-10G# copy running-config startup-config
Building configuration...
% Saving 2318 bytes to flash:startup-config
FLEX24-10G#
```

Switch 2 Command Set

	Command	Explanation
Step 1	configure terminal	Enter Global Configuration mode.
Step 2	interface GigabitEthernet 1/1-10	Enter Interface Configuration mode for interfaces GigabitEthernet 1/1 to GigabitEthernet 1/10.
Step 3	aggregation group 1 mode [active | passive]	If **passive** is set on switch 1, **active** must be set on switch 2. If **active** is set on switch 1, ether **active** or **passive** can be set on switch 2.
Step 4	exit	Return to Global Configuration mode.
Step 5	int llag 1	Enter Interface Configuration mode for the logical link aggregation interface.
Step 6	lacp max-bundle 7	Sets the max-bundle to seven. With a max-bundle of seven, only seven of the ten interfaces will be active in the aggregation, the remaining three are stored in reserve and are used when one of the seven links fail. **Note:** The max-bundle must be set to a value less than the total number of interfaces in the aggregation.

Step 7	lacp failover {non-revertive | revertive}	**(Optional)** The LACP failover command sets the switch's behavior when a link in an aggregation which was previously down becomes restored. **Non-revertive:** When downed links with a higher priority (lower number) become available, the active link(s) with the lower priority (higher number) will remain in the bundle. The links which just transitioned from being down to up will remain in reserve until they are needed. **Revertive:** When downed links with a higher priority (lower number) become available the active link(s) with the lower priority will be moved into reserve to allow the newly available links to actively become members of the bundle.
Step 8	end	**(Optional)** Return to Privileged EXEC mode.
Step 9	copy running-config startup-config	**(Optional)** Overwrite the startup-config with the current entries of the running-config.

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# interface GigabitEthernet 1/1-10
FLEX24-10G(config-if)# aggregation group 1 mode active
FLEX24-10G(config-if)# exit
FLEX24-10G(config)# interface llag 1
FLEX24-10G(config-llag)# lacp max-bundle 7
FLEX24-10G(config-llag)# lacp failover revertive
FLEX24-10G(config-llag)# end
FLEX24-10G# copy running-config startup-config
Building configuration...
% Saving 2318 bytes to flash:startup-config
FLEX24-10G#
```

Note: Since the aggregation on Switch 1 was set to passive, the aggregation on Switch 2 must be set to Active for the aggregation to form.

Verification

There are several show commands which can be used to display various information on all configured aggregations.

show aggregation: Displays all aggregation group ID's, and logical interfaces. For each aggregation interface the speed is shown, all ports in the bundle, as well as all ports in the bundle plus those in reserve.

The interfaces listed in the "Configured Ports" column are all interfaces which are a part of the aggregation.

The interfaces listed in the "Aggregated Ports" column are all interfaces which are actively aggregating.

If the max-bundle value is set to a value which is less than the total amount of interfaces in the aggregation then there will be more interfaces listed in the "Configured Ports" column than in the "Aggregated Ports" column.

FLEX24-10G# show aggregation

Aggr ID	Name	Type	Speed	Configured Port	Aggregated Ports
1	LLAG1	LACP_PASSIVE	1G	GigabitEthernet 1/1-10	GigabitEthernet 1/1-10

FLEX24-10G#

show aggregation mode: Displays which elements of the frame header are used to calculate the destination port of frame. The combination of the four settings determine which hash algorithm is used when trying to load balance traffic across the active links in an aggregation. By default, Source MAC, Destination MAC, and Port Number are enabled.

This setting can be changed from Global Configuration with **aggregation mode {dmac | ip | port | smac} [dmac | ip | port | smac] [dmac | ip | port | smac] [dmac | ip | port | smac].**

```
FLEX24-10G#  show aggregation mode
Aggregation mode:

SMAC  : Enabled
DMAC  : Disabled
IP    : Enabled
Port  : Enabled
FLEX24-10G#
```

show lacp internal: Displays all interfaces configured with LACP, their state, and their priority.

```
FLEX24-10G# show lacp internal
Port        State     Key   Priority
----------  --------  ----  --------
Gi 1/1      Active    1     32768
Gi 1/2      Active    1     32768
Gi 1/3      Active    1     32768
Gi 1/4      Active    1     32768
Gi 1/5      Active    1     32768
Gi 1/6      Active    1     32768
Gi 1/7      Active    1     32768
Gi 1/8      Down      1     32768
Gi 1/9      Down      1     32768
Gi 1/10     Down      1     32768
FLEX24-10G#
```

show lacp neighbor: Displays details about the neighbors' system-id, priority, and key. The interfaces and Aggr ID displayed in the **show lacp neighbor** output are the interfaces and Aggr ID on the local switch.

```
FLEX24-10G# show lacp neighbor
Aggr ID  Partner System ID  Partner Prio  Partner Key  Last Changed
-------  -----------------  ------------  -----------  ------------
1        02:00:c1:a3:74:c8  32768         1            00:00:16

Port        State     Aggr ID  Partner Key   Partner Port  Partner Port Prio
----------  --------  -------  ------------  ------------  -----------------
Gi 1/1      Active    1        1             1             32768
Gi 1/2      Active    1        1             2             32768
Gi 1/3      Active    1        1             3             32768
Gi 1/4      Active    1        1             4             32768
Gi 1/6      Active    1        1             6             32768
Gi 1/7      Active    1        1             7             32768
Gi 1/8      Stanbdy   1        1             8             32768
Gi 1/9      Standby   1        1             9             32768
Gi 1/10     Standby   1        1             10            32768
FLEX24-10G#
```

show lacp statistics: Displays transmission and received frame counters for all LACP aggregations.

```
FLEX24-10G# show lacp statistics
Port        Rx Frames   Tx Frames   Rx Unknown  Rx Illegal
----------  ----------  ----------  ----------  ----------
Gi 1/1      5623        5489        0           0
Gi 1/2      5424        5746        0           0
Gi 1/3      4989        5424        0           0
Gi 1/4      5111        5142        0           0
Gi 1/5      5154        5421        0           0
Gi 1/6      5555        5222        0           0
Gi 1/7      5353        5321        0           0
Gi 1/8      0           0           0           0
Gi 1/9      0           0           0           0
Gi 1/10     0           0           0           0
FLEX24-10G#
```

show lacp system-id: Displays the system-id. A system-id allows two interfaces on different switches to behave as though they are a part of the same aggregation. The system-id is comprised of the switch priority as well as the MAC address of the switch CPU.

```
FLEX24-10G# show lacp system-id
System ID: 32768 - 00:24:63:04:2a:80
FLEX24-10G#
```

Chapter 10: Link Layer Discovery Protocol

Introduction

The Link Layer Discovery Protocol (LLDP) is a layer-2 protocol used to discover details about directly connected neighbors. LLDP is a vendor-neutral protocol and is compatible with most modern networking equipment. LLDP is a requirement in a multi-vendor network as it will likely be the only layer-2 discovery protocol found on all network devices.

LLDP must be running on all directly connected neighbors for an exchange of information to take place. The following information can be shared between LLDP neighbors:

- System identity and description
- Device capabilities
- System MAC address and management IP address
- Power requirements
- System holdtime

LLDP information gathered by the switch is stored in the switch's management information base (MIB). The MIB can then by queried by SNMP servers.

By default, the switch will transmit LLDP information from all LLDP-enabled interfaces every 30 seconds. Every 30 seconds, LLDP enabled interfaces send an ethernet frame containing a LLDP data unit (LLDPDU) to its directly connected neighbor. Every LLDPDU contains a sequence of type-length-value (TLV) objects.

Frame Structure

Every LLDPDU contains a minimum of four TLV's. The frame structure for an LLDP frame is as follows:

<table>
<tr><th>7 bytes</th><th>6 bytes</th><th>6 bytes</th><th>2 bytes</th><th colspan="4">Length is Variable</th><th>2 bytes</th><th>4 bytes</th></tr>
<tr><td>Preamble</td><td>Destination MAC</td><td>Source MAC</td><td>Ethertype</td><td>Chassis ID TLV</td><td>Port ID TLV</td><td>TTL TLV</td><td rowspan="2">Optional TLV's</td><td>End of LLDPDU TLV</td><td>FCS</td></tr>
<tr><td colspan="4"></td><td colspan="3">Mandatory TLV's</td><td>Mandatory</td><td></td></tr>
<tr><td colspan="4"></td><td colspan="5">LLDPDU</td><td></td></tr>
</table>

The format of a LLDPDU is essentially a normal Ethernet frame where the payload is the LLDP data unit. The four mandatory TLV's contained in every LLDPDU are as follows:

1. **Chassis ID TLV:** Contains the system Chassis ID, typically the system MAC address.
2. **Port ID TLV:** By default, the port ID will advertise the MAC address of the local interface.
3. **TTL TLV:** Identifies the maximum hop limit of the frame.
4. **End of LLDPDU TLV:** Placeholder TLV which marks the last TLV in the LLDPDU.

LLDP Frames Originating from the FLEX24-10G

LLDP frames originating from the FLEX24-10G will contain the following field properties:

- **Preamble –** The preamble is a set of known bits used for frame synchronization.
- **Source MAC Address** - Contains the MAC address of the local interface in which the frame was sent out of.
- **Destination MAC Address** - Contains one of the three multicast MAC addresses: 01:80:c2:00:00:0e, 01:80:c2:00:00:03, or 01:80:c2:00:00:00. Each of these MAC addresses is a special 802.1D compliant address. These addresses are unique such that frames with one of these addresses are not forwarded by switches.
- **Ethertype** – All LLDP frames contain an Ethertype of 0x88CC.
- **Frame Check Sequence (FCS)** – The FCS is used to determine whether the frame underwent errors during transmission. A function is run on the data in the frame and the output of this function is a number which represents the FCS. The destination host will run an identical function on the frames data and if the result is different than the FCS in the frame, errors took place and the frame is discarded.

Basic LLDP Configuration

Enabling/Disabling LLDP

By default, LLDP is enabled on all switch ports. LLDP can be configured to transmit only, receive only, transmit and receive, or neither transmit nor receive on any switch interface.

	Command	Explanation
Step 1	configure terminal	Enter Global Configuration mode.
Step 2	interface {*, GigabitEthernet <1/1-24>, 10GigabitEthernet<1/1-2>}	Enter Interface Configuration mode for the interface(s) to configure.
Step 3	[no] lldp transmit	Toggle whether the interface should transmit LLDP frames. **Note:** Both **lldp transmit** and **lldp receive** are enabled on all switch ports by default, hence why they are hidden in the running-config.
Step 4	[no] lldp receive	Toggle whether the interface should receive LLDP frames. **Note:** Both **lldp transmit** and **lldp receive** are enabled on all switch ports by default, hence why they are hidden in the running-config.
Step 5	end	**(Optional)** Exit interface Configuration mode and return to Privileged EXEC mode.

Step 6	copy running-config startup-config	**(Optional)** Copy the contents of the running-config to the startup-config.

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# interface GigabitEthernet 1/1
FLEX24-10G(config-if)# no lldp transmit
FLEX24-10G(config-if)# no lldp receive
FLEX24-10G(config-if)# end
FLEX24-10G# copy running-config startup-config
Building configuration...
% Saving 2320 bytes to flash:startup-config
FLEX24-10G#
```

If LLDP is not enabled on all switch interfaces to both transmit and receive, LLDP will have a status of **"Not globally configured"** when **show services** is executed.

```
FLEX24-10G# reload defaults
% Reloading defaults. Please stand by.
FLEX24-10G# show services
TELNET    : Enabled
SSH       : Enabled
HTTP      : Enabled
LOG       : Disabled
LLDP      : Enabled
NTP       : Disabled
STP       : Enabled
FLEX24-10G# configure terminal
FLEX24-10G(config)# int GigabitEthernet 1/1
FLEX24-10G(config-if)# no lldp transmit
FLEX24-10G(config-if)# end
FLEX24-10G# show services
TELNET    : Enabled
SSH       : Enabled
HTTP      : Enabled
LOG       : Disabled
LLDP      : Not globally configured
NTP       : Disabled
STP       : Enabled
FLEX24-10G#
```

Configuring LLDP Timers

There are four transmission timers associated with LLDP: the delay, reinitialization time, transmission interval, and holdtime.

- **Delay:** When the switch's configuration is changed, a new LLDP frame is sent with the changes reflected. The new LLDP frame will be sent at least **delay** seconds after the previous. Time between LLDP frames must be at least **delay** seconds. The delay time cannot be greater than 25% of the transmission interval. By default, the delay is 2 seconds. Valid delay values are from 1 to 8192 seconds inclusive.

- **Reinitialization Time:** When LLDP is disabled, the switch is rebooted, or an interface is disabled, LLDP-enabled interfaces will send an LLDP shutdown frame to directly connected neighbors. The reinitialization time is the amount of seconds between the shutdown frame and a new LLDP initialization. By default, the reinitialization time is 2 seconds. Valid reinitialization values are from 1 to 10 seconds inclusive.

- **Transmission Interval:** The transmission interval is how often LLDP frames are sent to directly connected neighbors. By default, LLDP frames are sent every 30 seconds. Valid transmission intervals are from 5 to 32768 seconds inclusive.

- **Holdtime:** The holdtime is the amount of time in which the information in an LLDP frame is considered valid. The holdtime is configured as a multiple of the transmission interval. Valid holdtime values are from 2 to 10 inclusive. By default, the transmission interval is 30 seconds and the holdtime is 4 times. Therefore, LLDP information is considered valid for 120 seconds (30 seconds x 4).

	Command	Explanation
Step 1	configure terminal	Enter Global Configuration Mode.
Step 2	lldp holdtime <2-10>	**(Optional)** Set the LLDP holdtime multiple. The actual holdtime is calculated by multiplying the transmission interval by the specified holdtime multiple.
Step 3	lldp reinit <1-10>	**(Optional)** Set the LLDP reinitialization time.
Step 4	lldp timer <5-32768>	**(Optional)** Set the LLDP transmission interval.
Step 5	lldp transmission-delay <1-8192>	**(Optional)** Set the LLDP transmission delay. **Note:** Transmission delay must not be greater than 25% of the transmission interval.
Step 6	end	**(Optional)** Return to Privileged EXEC mode.
Step 7	copy running-config startup-config	**(Optional)** Copy the contents of the running-config to the startup-config.

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# lldp holdtime 5
FLEX24-10G(config)# lldp reinit 5
FLEX24-10G(config)# lldp timer 10
FLEX24-10G(config)# lldp transmission-delay 300
Note: According to IEEE 802.1AB-clause 10.5.4.2 the transmission-delay must not be larger than
LLDP timer * 0.25. LLDP timer changed to 1200
FLEX24-10G(config)# end
FLEX24-10G#
```

From the above snippet the transmission delay is set to a value greater than 25% of the transmission interval. When this happens, the switch will dynamically modify the transmission interval to be four times the transmission delay.

Configuring TLV's on a Per-Interface Basis

By default, when an LLDP-enabled interface sends LLDP packets to neighbors, the following TLV's are included in the LLDP packet:

- Port Description
- System Name
- System Description
- System Capability
- Management Address

The FLEX24-10G allows the administrator to configure which TLV's to include in LLDP advertisements on a per-interface level.

Example:

a) Interface GigabitEthernet 1/1 will **only** advertise the local switch's System Name.
b) Interface GigabitEthernet 1/3 will advertise all TLV's **except** the local switch's Management address.

The following configuration will satisfy **a)**:

	Command	Explanation
Step 1	configure terminal	Enter Global Configuration mode.
Step 2	interface GigabitEthernet 1/1	Enter Interface Configuration mode for Interface GigabitEthernet 1/1.
Step 3	lldp tlv-select management-address	Disable the management address from being advertised within LLDP frames.
Step 4	lldp tlv-select port-description	Disable the port description from being advertised within LLDP frames.
Step 5	lldp tlv-select system-capabilities	Disable the system capabilities from being advertised within LLDP frames.
Step 6	lldp tlv-select system-description	Disable the system description from being advertised within LLDP frames.
Step 7	end	**(Optional)** Exit Interface Configuration mode and return to Privileged EXEC mode.
Step 8	copy running-config startup-config	**(Optional)** Copy the contents of the running-config to the startup-config.

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# int GigabitEthernet 1/1
FLEX24-10G(config-if)# lldp tlv-select ?
    management-address     Enable/Disable transmission of management address.
    port-description       Enable/Disable transmission of port description.
    system-capabilities    Enable/Disable transmission of system capabilities.
    system-description     Enable/Disable transmission of system description.
    system-name            Enable/Disable transmission of system name.
FLEX24-10G(config-if)# lldp tlv-select management-address
FLEX24-10G(config-if)# lldp tlv-select port-description
FLEX24-10G(config-if)# lldp tlv-select system-capabilities
FLEX24-10G(config-if)# lldp tlv-select system-description
```

```
FLEX24-10G(config-if)# end
FLEX24-10G# copy running-config startup-config
FLEX24-10G#
```

The following configuration will satisfy **b)**:

	Command	Explanation
Step 1	configure terminal	Enter Global Configuration mode.
Step 2	interface GigabitEthernet 1/3	Enter Interface Configuration mode for Interface GigabitEthernet 1/3.
Step 3	lldp tlv-select management-address	Disable the management address from being advertised within LLDP frames.
Step 4	end	**(Optional)** Exit interface configuration and return to Privileged EXEC mode.
Step 5	copy running-config startup-config	**(Optional)** Copy the contents of the running-config to the startup-config.

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# interface GigabitEthernet 1/3
FLEX24-10G(config-if)# lldp tlv-select management-address
FLEX24-10G(config-if)# end
FLEX24-10G# copy running-config startup-config
FLEX24-10G#
```

SNMP Traps and CDP-Aware Interfaces

SNMP Traps

In the situation where the FLEX24-10G suddenly receives new LLDP information on one of its ingress interfaces, an SNMP trap can be emitted. This can be especially useful if an individual achieves unauthorized access of a device and modifies information contained in one of the devices TLV's.

For instance, if an intruder took control over a device directly connected to the FLEX24-10G and changed its management address, the TLV's being sent to the FLEX24-10G would contain a modified management address. The switch's LLDP neighbor table would change, causing an SNMP trap to be sent to the SNMP server (if one is configured).

To enable this feature, the **lldp trap** command must be entered at the interface level.

	Command	Explanation
Step 1	configure terminal	Enter Global Configuration Mode.
Step 2	interface {*, GigabitEthernet <1/1-24>, 10GigabitEthernet<1/1-2>}	Enter Interface Configuration Mode for the interface(s) to configure.
Step 3	lldp trap	Configures an SNMP trap to be emitted when the LLDP table changes for this interface.
Step 4	end	**(Optional)** Exit Interface Configuration mode and return to Privileged EXEC mode.

Step 5	copy running-config startup-config	**(Optional)** Copy the contents of the running-config to the startup-config.

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# interface GigabitEthernet 1/1
FLEX24-10G(config-if)# lldp trap
FLEX24-10G(config-if)# end
FLEX24-10G# copy running-config startup-config
FLEX24-10G#
```

CDP-Aware Interfaces

An interface configured to be CDP-aware will map specific TLV's found in CDP advertisements to appropriate entries in the LLDP neighbor table.

The following mappings will take place on LLDP-enabled CDP-aware interfaces when CDP TLV's are received:

- CDP TLV "Device ID" is mapped to the LLDP "Chassis ID" field.
- CDP TLV "Address" is mapped to the LLDP "Management Address" field. If the CDP TLV contains multiple addresses, only the first address will be shown in the LLDP neighbor table.
- CDP TLV "Port ID" is mapped to the LLDP "Port ID" field.
- CDP TLV "Version and Platform" is mapped to the LLDP "System Description" field.
- CDP TLV "System Capabilities" is mapped to the LLDP "System Capabilities" field. Since CDP covers capabilities which are not a part of LLDP, these capabilities are shown as "Others" in the LLDP neighbor table.

If all interfaces have CDP awareness disabled, the switch will forward CDP frames from connected neighbors. If at least one interface on the switch is configured to be CDP-aware, no CDP frames are forwarded.

If CDP awareness is toggled off on an interface, the CDP information remains in the LLDP neighbor table until the hold time expires.

To enable this feature, the **lldp cdp-aware** command must be entered at the interface level.

	Command	**Explanation**
Step 1	configure terminal	Enter Global Configuration mode.
Step 2	interface {*, GigabitEthernet <1/1-24>, 10GigabitEthernet<1/1-2>}	Enter Interface Configuration mode for the interface(s) to configure.
Step 3	lldp cdp-aware	Configures the interface to accept CDP advertisements. Information in the CDP advertisements are mapped to an appropriate LLDP field based on the rules outlined above.
Step 4	end	**(Optional)** Exit Interface Configuration mode and return to Privileged EXEC mode.
Step 5	copy running-config startup-config	**(Optional)** Copy the contents of the running-config to the startup-config.

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# interface GigabitEthernet 1/1
FLEX24-10G(config-if)# lldp cdp-aware
FLEX24-10G(config-if)# end
FLEX24-10G# copy running-config startup-config
FLEX24-10G#
```

LLDP-MED

LLDP-MED is an extension of LLDP designed to operate between endpoint devices (most commonly IP phones) and network connectivity devices (switches). LLDP-MED endpoints, such as IP phones, determine the capabilities of a connected device, in this case the FLEX24-10G, and whether those capabilities are enabled.

LLDP and LLDP-MED cannot be enabled simultaneously on a switch interface. LLDP-MED conversations always originate from the endpoint device. The FLEX24-10G will initially only send LLDP frames until it receives LLDP-MED frames from the endpoint.

LLDP-MED Policies

LLDP-MED policies are intended for use with applications that have specific real-time network policy requirements, such as interactive voice and/or video services. Up to 32 LLDP-MED policies can be created on the switch. These policies can then be mapped to individual interfaces. There is no limit to the amount of policies mapped to a specific interface.

Each policy contains the following properties:

- **Policy ID:** The Policy ID behaves like an index value. The policy ID has a value of 0 to 31.
- **Application Type:** The Application Type identifies what kind of endpoint is connected to a switch interface. The FLEX24-10G supports eight different application types.
    1. **Voice** – for use by IP phones and other similar application supporting interactive voice services.
    2. **Voice Signaling** – for use in network topologies which require a different policy for voice signaling than for voice media.
    3. **Guest Voice** – for use in networks which include a limited feature-set voice service for guest users and visitors who have their own IP phones.
    4. **Guest Voice Signaling** - for use in network topologies that require a different policy for the guest voice signaling than for the guest voice media.
    5. **Softphone Voice** - for use by applications on data centric devices (PCs, Laptops).
    6. **Video Conferencing** – for use by video conferencing equipment supporting real-time video and audio services.
    7. **Streaming Video** – for use by multicast/broadcast-based video content distribution.
    8. **Video Signaling** - for use in network topologies which require a different policy for video signaling than for video media.
- **Tag:** The Tag property specifies whether traffic pertaining to the specific application type should be on a “tagged” or “untagged” VLAN.
- **VLAN ID:** VLAN Identifier for the interface.

- **L2 Priority:** Quality of Service marking from 0 to 7 as defined in IEEE 802.1D. For more info on Layer-2 priorities see here.
- **DSCP:** Differentiated Services Code Point value ranging for 0 to 63. The DSCP value is used in the IP header for packet classification. DSCP values are removed from frames at a router boundary. However, a router will convert a DSCP value to its associated IP precedence value ensuring that the packets QoS values are preserved.

Common DSCP Values

DSCP Decimal Value	Meaning	Drop Probability	Equivalent IP Precedence Value	Service Class
0	Best Effort	N/A	000 (Routine)	Default DSCP Value
8	CS1		1	Low-Priority Data
10	AF11	Low	001 (Priority)	High-Throughput Data
12	AF12	Medium	001 (Priority)	High-Throughput Data
14	AF13	High	001 (Priority)	High-Throughput Data
16	CS2		2	Operations, Administration, Management (OAM)
18	AF21	Low	010 (Immediate)	Low-Latency Data
20	AF22	Medium	010 (Immediate)	Low-Latency Data
22	AF23	High	010 (Immediate)	Low-Latency Data
24	CS3		3	Broadcast Video
26	AF31	Low	011 (Flash)	Multimedia Streaming
28	AF32	Medium	011 (Flash)	Multimedia Streaming
30	AF33	High	011 (Flash)	Multimedia Streaming
32	CS4		4	Real-Time Interactive
34	AF41	Low	100 (Flash Override)	Multimedia Conferencing
36	AF42	Medium	100 (Flash Override)	Multimedia Conferencing
38	AF43	High	100 (Flash Override)	Multimedia Conferencing
40	CS5		5	Signaling
46	Expedited Forwarding	N/A	101 (Critical)	Telephony
48	CS6		6	Network Control

Creating a Policy and Mapping a Policy to an Interface

Policies are created from Global Configuration mode as follows:

	Command	Explanation
Step 1	configure terminal	Enter Global Configuration mode.
Step 2	lldp med media-vlan-policy <0-31> {guest-voice | guest-voice-signaling | softphone-voice | streaming-video | video-conferencing | video-signaling | voice | voice-signaling} {tagged | untagged} <vlan_id> [l2-priority <0-7>] [dscp <0-63>]	Create an LLDP-MED policy. **<0-31>** indicates the Policy Index. **Note:** If the Layer-2 Priority and DSCP value are both set, the Layer-2

	Example: lldp med media-vlan-policy 0 voice tagged 10 l2-priority 5 dscp 46	priority must precede the DSCP value.
Step 3	interface {*, GigabitEthernet <1/1-24>, 10GigabitEthernet<1/1-2>} **Example:** interface GigabitEthernet 1/1	Enter Interface Configuration mode for the interface in which to apply the policy to.
Step 4	lldp med media-vlan policy-list <range_list> **Example:** lldp med media-vlan policy-list 0	Map a single policy or a list of policies to the interface.
Step 5	end	**(Optional)** Exit Interface Configuration and return to Privileged EXEC mode.
Step 6	copy running-config startup-config	**(Optional)** Copy the contents of the running-config to the startup-config.

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# lldp med media-vlan-policy 0 voice tagged 10 l2-priority 5 dscp 46
FLEX24-10G(config)# interface GigabitEthernet 1/1
FLEX24-10G(config-if)# lldp med media-vlan policy-list 0
FLEX24-10G(config-if)# end
FLEX24-10G# copy running-config startup-config
FLEX24-10G#
```

Connectivity and Endpoint Interfaces

As explained above, LLDP-MED communications always originate from the endpoint device. Although this is true, it should not be taken literally.

By default, all interfaces on the FLEX24-10G are configured with a “Device Type” of **Connectivity.** This means that all interfaces on the switch will not initiate the transmission of LLDP-MED frames. To configure the switch to initiate the transmission of LLDP-MED frames from one or all of its interfaces, those interfaces should be configured with a “Device Type” of **Endpoint.**

	Command	**Explanation**
Step 1	configure terminal	Enter Global Configuration mode.
Step 2	interface {*, GigabitEthernet <1/1-24>, 10GigabitEthernet<1/1-2>}	Enter Interface Configuration mode for the interface(s) to configure.
Step 3	lldp med type {connectivity | end-point}	Set the interface device type to either **connectivity** or **end-point.** Interfaces set as **connectivity** will not initiate the transmission of LLDP-MED frames. Interfaces set as **end-point** will initiate the transmission of LLDP-MED frames. **Note:** By default, all interfaces are set to **connectivity**.

Step 4	end	**(Optional)** Exit Interface Configuration mode and return to Privileged EXEC mode.
Step 5	copy running-config startup-config	**(Optional)** Copy the contents of the running-config to the startup-config.

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# interface GigabitEthernet 1/1
FLEX24-10G(config-if)# lldp med type connectivity
FLEX24-10G(config-if)# end
FLEX24-10G# copy running-config startup-config
Building configuration...
% Saving 2320 bytes to flash:startup-config
FLEX24-10G#
```

Location TLV's

Specific location information can be configured which in turn will be advertised to LLDP-MED neighbors.

For the sake of brevity, the following location information can be set on the switch:

- Coordinates Location
  - Latitude
  - Longitude
  - Altitude (Can be set in floors or meters)
  - Map Datum
- Civic Address Location
  - Country Code
  - City
  - Street
  - Street suffix
  - Landmark
  - Zip Code
  - Floor
  - Postal Community Name
  - Sate
  - City District
  - Leading Street Direction
  - House #
  - Additional Location Information
  - Building
  - Room #
  - P.O Box
  - County
  - Block (Neighborhood)
  - Trailing street suffix
  - House # suffix

- Name
- Apartment
- Place Type
- Additional Code

Note: The total length of the Civic Address Location cannot exceed 250 characters. The two-letter country code is not included in the 250-character limit.

The following configuration will set the coordinates and civic address to the CN Tower in Toronto, Canada:

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# lldp med location-tlv altitude meters 76
FLEX24-10G(config)# lldp med location-tlv latitude north 43
FLEX24-10G(config)# lldp med location-tlv longitude west 79
FLEX24-10G(config)# lldp med location-tlv civic-addr ?
    additional-code            Additional code - Example: 1320300003.
    additional-info            Additional location info - Example: South Wing.
    apartment                  Unit (Apartment, suite) - Example: Apt 42.
    block                      Neighborhood, block.
    building                   Building (structure) - Example: Low Library.
    city                       City, township, shi (Japan) - Example:
                               Copenhagen.
    country                    The two-letter ISO 3166 country code in capital
                               ASCII letters - Example: DK, DE or US.
    county                     County, parish, gun (Japan), district.
    district                   City division, borough, city district, ward,
                               chou (Japan).
    floor                      Floor - Example: 4.
    house-no                   House number - Example: 21.
    house-no-suffix            House number suffix - Example: A, 1/2.
    landmark                   Landmark or vanity address - Example: Columbia
                               University.
    leading-street-direction   Leading street direction - Example: N.
    name                       Name (residence and office occupant) - Example:
                               John Doe.
    p-o-box                    Post office box (P.O. BOX) - Example: 12345.
    place-type                 Place type - Example: Office.
    postal-community-name      Postal community name - Example: Leonia.
    room-number                Room number - Example: 450F.
    state                      National subdivisions (state, canton, region,
                               province, prefecture).
    street                     Street - Example: Oxford Street.
    street-suffix              Street suffix - Example: Ave, Platz.
    trailing-street-suffix     Trailing street suffix - Example: SW.
    zip-code                   Postal/zip code - Example: 2791.
FLEX24-10G(config)# lldp med location-tlv civic-addr country CA.
FLEX24-10G(config)# lldp med location-tlv civic-addr city Toronto
FLEX24-10G(config)# lldp med location-tlv civic-addr landmark CN Tower
FLEX24-10G(config)# lldp med location-tlv civic-addr name John Smith
FLEX24-10G(config)# lldp med location-tlv civic-addr house-no 301
FLEX24-10G(config)# lldp med location-tlv civic-addr street Front
FLEX24-10G(config)# lldp med location-tlv civic-addr street-suffix St
FLEX24-10G(config)# lldp med location-tlv civic-addr trailing-street-suffix W
FLEX24-10G(config)# lldp med location-tlv civic-addr zip-code M5V 2T6
```

```
FLEX24-10G(config)#end
FLEX24-10G# copy running-config startup-config
FLEX24-10G#
```

Emergency Call Service

The Emergency Call Service ELIN identifier is a ten-digit numerical string which is used to identify a caller whenever an emergency call is issued. It is very important that the ELIN identifier is set to a local telephone number corresponding to the physical location of the switch. For instance, if a satellite branch is in Europe but the companies Call Manager is in the North America, the ELIN should be a European phone number, not the company's corporate North American phone number.

If the ELIN is set incorrectly, emergency calls may be routed incorrectly, or the receiver may be displayed the incorrect caller ID.

Setting the ELIN

	Command	**Explanation**
Step 1	configure terminal	Enter Global Configuration mode.
Step 2	lldp med location-tlv elin-addr <elin> **Example:** lldp med location-tlv elin-addr 5555555555	Set the switch's ELIN value. **<elin>** must be a 10-digit numerical string.
Step 3	end	**(Optional)** Return to Privileged EXEC mode.
Step 4	copy running-config startup-config	**(Optional)** Copy the contents of the running-config to the startup-config.

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# lldp med location-tlv elin-addr 5555555555
FLEX24-10G(config)# end
FLEX24-10G# copy running-config startup-config
FLEX24-10G#
```

Fast Start Repeat Count

With frame transmission there is always a risk of frames being lost between neighbors. The Fast Start Repeat Count enables the fast start transmission to be repeated multiple times to ensure that neighbors receive LLDP frames.

The fast start transmission only applies when a LLDP-MED endpoint has been connected to the network. The endpoint will initially advertise itself once and then repeatedly advertise itself. The amount of times the endpoints advertise themselves is equal to the Fast Start Repeat Count.

Configuring the Fast Start Repeat Count

	Command	**Explanation**
Step 1	configure terminal	Enter Global Configuration mode.
Step 2	lldp med fast <1-10>	Configure the Fast Start Repeat Count.

		By default, the Fast Start Repeat Count is set to 4. Valid values are from 1 to 10 inclusive.
Step 3	end	**(Optional)** Return to Privileged EXEC mode.
Step 4	copy running-config startup-config	**(Optional)** Copy the contents of the running-config to the startup-config.

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# lldp med fast 8
FLEX24-10G(config)# end
FLEX24-10G# copy running-config startup-config
Building configuration...
% Saving 2988 bytes to flash:startup-config
FLEX24-10G#
```

Verification

show lldp eee [interface {*, GigabitEthernet <1/1-24>, 10GigabitEthernet<1/1-2>}]: Display LLDP local and neighbor Energy Efficient Ethernet (EEE) information. Output can be modified to only display EEE information for certain interfaces.

```
FLEX24-10G# show lldp eee
Local Interface     : GigabitEthernet 1/1
EEE not supported for this interface

Local Interface     : GigabitEthernet 1/5
EEE not supported for this interface

Local Interface     : GigabitEthernet 1/7
EEE not supported for this interface

FLEX24-10G#
```

show lldp med media-vlan-policy [<policy_number>]: Displays all Media-VLAN-Policies configured on the switch. Output can be restricted to only show an individual LLDP-MED policy.

```
FLEX24-10G# show lldp med media-vlan-policy
Policy Id  Application Type          Tag      Vlan ID  L2 Priority  DSCP
0          Voice                     Tagged   15       0            0
1          Softphone Voice           Tagged   1        0            0
2          Guest Voice               Tagged   1        0            0
3          Voice                     Tagged   1        0            0
4          Video Conferencing        Tagged   1        0            0
5          Video Signaling           Tagged   1        0            0
FLEX24-10G#
```

show lldp med remote-device [interface {*, GigabitEthernet <1/1-24>, 10GigabitEthernet<1/1-2>}]: Display remote device LLDP-MED neighbor information. Output can be filtered to only display remote device LLDP-MED neighbor information for certain interfaces.

```
FLEX24-10G# show lldp med remote-device
Local Interface     : GigabitEthernet 1/1
Device Type         : Endpoint Class I
Capabilities        : LLDP-MED Capabilities

Local Interface     : GigabitEthernet 1/5
```

```
Device Type          : Endpoint Class III
Capabilities         : LLDP-MED Capabilities, Network Policy, Extended Power via MDI - PD

Application Type     : Voice
Policy               : Unknown
Tag                  : Untagged
VLAN ID              : -
Priority             : -
DSCP                 : -

Application Type     : Voice Signaling
Policy               : Unknown
Tag                  : Untagged
VLAN ID              : -
Priority             : -
DSCP                 : -

Inventory
Hardware Revision    : PCB Version: 0
Firmware Revision    : Boot 01.06.03.08
Software Revision    : Main 01.06.03.08
Serial Number        :
Manufacturer Name    : Mitel Corporation
model Name           : MITEL 5340 DM
Asset ID             :

Local Interface      : GigabitEthernet 1/7
Device Type          : Endpoint Class III
Capabilities         : LLDP-MED Capabilities, Network Policy, Extended Power via MDI - PD

Application Type     : Voice
Policy               : Unknown
Tag                  : Untagged
VLAN ID              : -
Priority             : -
DSCP                 : -

Application Type     : Voice Signaling
Policy               : Unknown
Tag                  : Untagged
VLAN ID              : -
Priority             : -
DSCP                 : -

Inventory
Hardware Revision    : PCB Version: 0
Firmware Revision    : Boot 01.06.03.08
Software Revision    : Main 01.06.03.08
Serial Number        :
Manufacturer Name    : Mitel Corporation
model Name           : MITEL 5340 DM
Asset ID             :

FLEX24-10G#
```

show lldp neighbors [interface {*, GigabitEthernet <1/1-24>, 10GigabitEthernet<1/1-2>}]: Displays LLDP neighbor information on all LLDP-enabled interfaces. Output can be filtered to only display neighbor information for certain interfaces.

```
FLEX24-10G# show lldp neighbors
Local Interface      : GigabitEthernet 1/1
Chassis ID           : 00-E1-38-00-00-34
Port ID              : 00-E1-38-00-00-34
Port Description     :
System Name          :
System Description   :
System Capabilities  :

Local Interface      : GigabitEthernet 1/5
Chassis ID           : 192.168.100.5
Port ID              : 08-00-0F-35-18-7A
Port Description     : LAN port
System Name          : URL user@192.168.100.5,MITEL 5340 DM
System Description   : URL user@192.168.100.5,MITEL 5340 DM,h/w rev 0,ASIC rev 1,f/w Boot
01.06.03.08,f/w Main 01.06.03.08
System Capabilities : Bridge(+), Telephone(+)
Management Address   : 192.168.100.5 (IPv4)

Local Interface      : GigabitEthernet 1/7
Chassis ID           : 192.168.100.8
Port ID              : 08-00-0F-42-7F-4A
Port Description     : LAN port
System Name          : URL user@192.168.100.8,MITEL 5340 DM
System Description   : URL user@192.168.100.8,MITEL 5340 DM,h/w rev 0,ASIC rev 1,f/w Boot
01.06.03.08,f/w Main 01.06.03.08
System Capabilities : Bridge(+), Telephone(+)
Management Address   : 192.168.100.8 (IPv4)

FLEX24-10G#
```

show lldp preempt [interface {*, GigabitEthernet <1/1-24>, 10GigabitEthernet<1/1-2>}]: Displays LLDP local and neighbor preempt information.

```
FLEX24-10G# show lldp preempt
Local Interface      : GigabitEthernet 1/1

Local Interface      : GigabitEthernet 1/5

Local Interface      : GigabitEthernet 1/7

FLEX24-10G#
```

show lldp statistics interface [{*, GigabitEthernet <1/1-24>, 10GigabitEthernet<1/1-2>}]: Displays LLDP statistics information. Frame counters for all LLDP-enabled interfaces can be shown with this command.

```
FLEX24-10G# show lldp statistics
LLDP global counters
Neighbor entries was last changed at 2019-10-22T13:23:02+00:00  (394 secs. ago).
Total Neighbors Entries Added    21.
Total Neighbors Entries Deleted  18.
Total Neighbors Entries Dropped  0.
Total Neighbors Entries Aged Out 9.

LLDP local counters
                    Rx        Tx        Rx        Rx        Rx TLV    Rx TLV    Rx TLV
Interface           Frames    Frames    Errors    Discards  Errors    Unknown   Organiz.  Aged
---------           ------    ------    ------    --------  ------    -------   --------  ----
GigabitEthernet 1/1 113       2018      0         0         0         0         0         3
GigabitEthernet 1/2 2         0         0         0         0         0         0         0
GigabitEthernet 1/3 2         1         0         0         0         0         0         0
GigabitEthernet 1/4 0         0         0         0         0         0         0         0
```

```
GigabitEthernet 1/5     33          73          0           0           0           0           21          2
GigabitEthernet 1/6     0           0           0           0           0           0           0           0

      -------------------------------------------OUTPUT TRUNCATED-------------------------------------------
```

Chapter 11: TACACS+ and RADIUS

Introduction

The Terminal Access Controller Access Control System Plus (TACACS+) and the Remote Authentication Dial-In User Service (RADIUS) protocols are both Authentication, Authorization, and Accounting (AAA) protocols used to control switch access.

Although both TACACS+ and RADIUS are AAA services, there are some major differences.

On the FLEX24-10G, **TACACS+ supports Authentication, Authorization, and Accounting while RADIUS only supports Authentication.**

For both TACACS+ and RADIUS, a separate TACACS+ or RADIUS server must be configured and have network connectivity to the FLEX24-10G.

TACACS+ and RADIUS allow the switch to use a remote user database to control who is and who is not allowed to gain access to the switch's CLI or WEB GUI. Separate authentication rules can be specified for the various methods in which the switch's management interface can be accessed, i.e. serial console, TELNET, SSH, and WEB GUI. For example, a configuration could be put in place allowing TACACS+/RADIUS users to access the switch's WEB GUI while being denied access to the CLI via serial console, SSH, and TELNET.

Once a TACACS+ user has been successfully authenticated by the TACACS+ server, the user is granted access to the switch's management interface. The scope of commands the user has access to can be configured using Authorization settings. Authorization settings can limit the user such that they are only able to execute commands with a certain privilege level or higher. Authorization can be configured on a serial console, TELNET, and SSH basis.

Accounting settings allow a network administrator to monitor a client's session from the time they are first authenticated to the point the client logs off. Accounting is useful for tracking user activity for a security audit as well as collecting information for user billing in networks which operate on a pay-as-you-go model.

Configuration

The FLEX24-10G only allows the configuration of one TACACS+ or RADIUS server at one time.

Follow the steps below to point the FLEX24-10G to a TACACS+ or RADIUS server.

TACACS+ Server

	Command	**Explanation**
Step 1	configure terminal	Enter Global Configuration mode.
Step 2	tacacs-server host <word1-255>	Specify either the hostname or the IP address of the TACACS+ server.
Step 3	tacacs-server key [unencrypted | encrypted] <line1-63>	Configure the switch with a shared secret matching the secret configured on the TACACS+ server.

		By default, **unencrypted** is implicitly included in the **tacacs-server key** command unless the administrator explicitly supplies the **encrypted** parameter. **Example:** **tacacs-server key unencrypted testing** and **tacacs-server key testing** are recognized as the same command. If **encrypted** is specified, the switch expects an encrypted shared secret to be supplied as a parameter. **Note:** Regardless of whether the user enters the **encrypted** or **unencrypted** parameter, the shared secret will always be displayed as encrypted in the switch's running-configuration. **Note:** If these secrets do not match, authentication packets will not be passed between the switch and TACACS+ server successfully.
Step 4	tacacs-server deadtime <1-1440>	**(Optional)** Configure the deadtime of the TACACS+ server. Default is 0 minutes. The deadtime is specified in minutes and is the amount of time the FLEX24-10G will wait before it stops using a TACACS+ server that does not respond.
Step 6	tacacs-server timeout <1-1000>	**(Optional)** Configure the timeout of the TACACS+ server, in seconds. Default is 5 seconds. The timeout is the number of seconds the FLEX24-10G will wait for a reply from the TACACS+ server before retransmitting the request.

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# tacacs-server host 192.168.100.2
FLEX24-10G(config)# tacacs-server key unencrypted testingsecret
FLEX24-10G(config)# tacacs-server deadtime 1
FLEX24-10G(config)# tacacs-server timeout 10
FLEX24-10G(config)# end
FLEX24-10G#
```

RADIUS Server

	Command	**Explanation**
Step 1	configure terminal	Enter Global Configuration mode.
Step 2	radius-server host <word1-255>	Specify either the hostname or the IP address of the RADIUS server.
Step 3	radius-server key [unencrypted | encrypted] <line1-63>	Configure the switch with a shared secret matching the secret configured on the RADIUS server. By default, **unencrypted** is implicitly included in the **radius-server key** command unless the administrator explicitly supplies the **encrypted** parameter. **Example:** **radius-server key unencrypted testing** and **radius-server key testing** are recognized as the same command. If **encrypted** is specified, the switch expects an encrypted shared secret to be supplied as a parameter. **Note:** Regardless of whether the user enters the **encrypted** or **unencrypted** parameter, the shared secret will always be displayed as encrypted in the switch's running-configuration. **Note:** If these secrets do not match authentication packets will not be passed between the switch and RADIUS server successfully.
Step 4	radius-server deadtime <1-1440>	**(Optional)** Configure the deadtime of the RADIUS server. Default is 0 minutes. The deadtime is specified in minutes and is the amount of time the FLEX24-10G will wait before it stops using a RADIUS server that does not respond.
Step 5	radius-server retransmit <1-1000>	**(Optional)** Configure the retransmit value for the RADIUS server. Default is 3 times. If the FLEX24-10G does not hear a response from the RADIUS server, it will try to send a RADIUS request, by default, 3 more times to the RADIUS server. If the FLEX24-10G does not hear a response to any of these requests, the RADIUS server is marked as dead.

Step 6	radius-server timeout <1-1000>	**(Optional)** Configure the timeout of the RADIUS server, in seconds. Default is 5 seconds. The timeout is the number of seconds the FLEX24-10G will wait for a reply from the RADIUS server before retransmitting the request.

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# radius-server host 192.168.100.2
FLEX24-10G(config)# radius-server key unencrypted radiustestingsecret
FLEX24-10G(config)# radius-server deadtime  1
FLEX24-10G(config)# radius-server retransmit 5
FLEX24-10G(config)# radius-server timeout 10
FLEX24-10G(config)# end
FLEX24-10G#
```

Once the FLEX24-10G has been successfully configured with a TACACS+ or RADIUS server and both the switch and server are able to communicate with each other, authentication, authorization, and accounting can be configured.

Controlling Authentication

Both TACACS+ and RADIUS servers allow for the user to configure a user database within them. This is often preferred as a network can have a centralized user database for the entire IT department rather than having a local user database on every network device. This centralized TACACS+ or RADIUS server would then be configured on every compatible network device.

The FLEX24-10G allows three authentication methods to be configured at once. These authentication methods can also be configured separately for the serial console port, SSH sessions, TELNET sessions, and WEB GUI sessions.

When three different authentication methods are configured the switch will attempt to use the first method, if that should fail, try the second, and finally the third if the second method fails.

	Command	**Explanation**
Step 1	configure terminal	Enter Global Configuration mode.
Step 2	aaa authentication login {console | http | ssh | telnet} {local | radius | tacacs} [local | radius | tacacs] [local | radius | tacacs]	Specify which means of management we would like to control authentication on as well as the order in which to authenticate against a TACACS+ server, RADIUS server, or the local user database. **Example: aaa authentication login ssh radius tacacs local** would control authentication for SSH sessions only. When a user attempts to login during a SSH session, first their credentials will be checked against the RADIUS server's user database.

		If the RADIUS server is offline then the credential will be checked against the TACACS+ server's user database. Finally, if the TACACS+ server is also found to be offline, the switch will fall back to the switch's local user database. A separate command must be entered for each access method for authentication to be configured on.
Step 3	end	**(Optional)** Return to Privileged EXEC mode.
Step 4	copy running-config startup-config	**(Optional)** Copy the contents of the running-config to the startup-config.

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# aaa authentication login ssh radius tacacs local
FLEX24-10G(config)# aaa authentication login telnet tacacs
FLEX24-10G(config)# aaa authentication login http tacacs
FLEX24-10G(config)# aaa authentication login console local
FLEX24-10G(config)# end
FLEX24-10G#
```

Controlling Authorization

With authorization enabled, the scope of commands which are available to the user can be configured. Authorization can be configured for serial console, SSH, and TELNET sessions. Additionally, for each access method a command privilege level can be specified. The user will be given access to all commands with a privilege level higher than or equal to the set privilege level.

	Command	Explanation
Step 1	configure terminal	Enter Global Configuration mode.
Step 2	aaa authorization {console | ssh | telnet} tacacs commands <privilege_level> [config-commands]	Specify which means of management we would like to control authorization on and the privilege level of the commands we would like to permit to the user. Authorization cannot be enabled for WEB GUI sessions, only serial console, SSH, and TELNET sessions. **<privilege_level>** must be a value from 0 to 15, inclusive. The optional **config-commands** parameter enables authorization for configuration commands.

		Example: aaa authorization telnet tacacs commands 0 config-commands enables authorization for telnet sessions permitting commands with a privilege level of 0 and higher (all commands). Authorization is also enabled for configuration commands.
Step 3	end	**(Optional)** Return to Privileged EXEC mode.
Step 4	copy running-config startup-config	**(Optional)** Copy the contents of the running-config to the startup-config.

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# aaa authorization telnet tacacs commands 0 config-commands
FLEX24-10G(config)# end
FLEX24-10G#
```

Configuring Accounting

Accounting allows network administrators to log all activities performed by a user on the FLEX24-10G. From a security perspective it is very desirable to have a record of who accessed the switch, when they accessed the switch, how they accessed the switch (serial console, SSH, TELNET), and what they did on the switch.

With TACACS+ accounting, administrators can receive details on the individual commands which are being executed on the FLEX24-10G.

The ability to only log commands above a privilege level is also present. When this value is set to zero, all commands will be accounted for.

	Command	**Explanation**
Step 1	configure terminal	Enter Global Configuration mode.
Step 2	aaa accounting {console | ssh | telnet} tacacs commands <privilege_level> [exec]	Enable command accounting on all commands with a privilege level of **<privilege level>** and higher. **(Optional)** EXEC (login) accounting is enabled with the **exec** keyword.
	or aaa accounting {console | ssh | telnet} tacacs exec [commands] <privilege_level>	Enable EXEC (login) accounting. **(Optional)** Command accounting is enabled by appending **[commands] <privilege_level>** onto the end of the command. Commands with a privilege level of **<privilege level>** and higher are accounted for.
Step 3	end	**(Optional)** Return to Privileged EXEC mode.
Step 4	copy running-config startup-config	**(Optional)** Copy the contents of the running-config to the startup-config.

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# aaa accounting console tacacs commands 0 exec
FLEX24-10G(config)# aaa accounting ssh tacacs commands 0 exec
```

```
FLEX24-10G(config)# aaa accounting telnet tacacs commands 0 exec
FLEX24-10G(config)# end
FLEX24-10G#
```

Verification Commands

The TACACS+ or RADIUS server configurations can be verified by issuing the **show tacacs-server** or **show radius-server [statistics]** commands respectively.

show tacacs-server: Displays TACACS+ server information such as IP address, timers, hashed shared key, global server key, and port number.

```
FLEX24-10G# show tacacs-server
Global TACACS+ Server Timeout      : 10 seconds
Global TACACS+ Server Deadtime     : 1 minutes
Global TACACS+ Server Key          :
0b3483a9be15461bf46d16b7213306cd3f6e43960916bd52e3ef74c6bea33296dad1490b8b5a1078
ec1d9884a648a066ef14c0186069943ce2ce120d0e1e0d43
TACACS+ Server #1:
  Host name  : 192.168.100.2
  Port       : 49
  Timeout    :
  Key        :
FLEX24-10G#
```

show radius-server: Displays RADIUS server information such as IP address, timers, hashed shared key, global server key, attributes, and authentication/accounting port numbers.

```
FLEX24-10G# show radius-server
Global RADIUS Server Timeout      : 10 seconds
Global RADIUS Server Retransmit   : 5 times
Global RADIUS Server Deadtime     : 1 minutes
Global RADIUS Server Key          :
80bbede0460d3c015e37e7be73712f73e112cf3dabee6c89687bee7491cf74fbbefbec336d94b37c0325e08f2779d5
098e596f830aec3865688a328440edfb260732777285d0b0abb1aa73c2543ca50a
Global RADIUS Server Attribute 4  :
Global RADIUS Server Attribute 95 :
Global RADIUS Server Attribute 32 :
RADIUS Server #1:
  Host name  : 192.168.100.2
  Auth port  : 1812
  Acct port  : 1813
  Timeout    :
  Retransmit :
  Key        :
FLEX24-10G#
```

show radius-server statistics: Displays the same information as **show radius-server** however with more verbose information relating to Authentication and Accounting transmitted and received packet counters.

```
FLEX24-10G# show radius-server statistics
Global RADIUS Server Timeout      : 10 seconds
```

```
Global RADIUS Server Retransmit   : 5 times
Global RADIUS Server Deadtime     : 1 minutes
Global RADIUS Server Key          :
80bbede0460d3c015e37e7be73712f73e112cf3dabee6c89687bee7491cf74fbbefbec336d94b37c0325e08f2779d5
098e596f830aec3865688a328440edfb260732777285d0b0abb1aa73c2543ca50a
Global RADIUS Server Attribute 4  :
Global RADIUS Server Attribute 95 :
Global RADIUS Server Attribute 32 :
RADIUS Server #1:
  Host name  : 192.168.100.2
  Auth port  : 1812
  Acct port  : 1813
  Timeout    :
  Retransmit :
  Key        :

RADIUS Server #1 (192.168.100.2:1812) Authentication Statistics:
Rx Access Accepts:                    0   Tx Access Requests:               0
Rx Access Rejects:                    0   Tx Access Retransmissions:        0
Rx Access Challenges:                 0   Tx Pending Requests:              0
Rx Malformed Acc. Responses:          0   Tx Timeouts:                      0
Rx Bad Authenticators:                0
Rx Unknown Types:                     0
Rx Packets Dropped:                   0
State:                            Ready
Round-Trip Time:                      0 ms

RADIUS Server #1 (192.168.100.2:1813) Accounting Statistics:
Rx Responses:                         0   Tx Requests:                      0
Rx Malformed Responses:               0   Tx Retransmissions:               0
Rx Bad Authenticators:                0   Tx Pending Requests:              0
Rx Unknown Types:                     0   Tx Timeouts:                      0
Rx Packets Dropped:                   0
State:                            Ready
Round-Trip Time:                      0 ms
FLEX24-10G#
```

show aaa: Displays AAA configuration details.

Authentication: The Authentication section of the **show aaa** output lists the order in which the switch will try to authenticate a user who is attempting to access the switch via a console, SSH, Telnet, or WEB GUI session.

Authorization: The Authorization section of the **show aaa** output lists the current authorization configuration on the serial console, SSH, and TELNET lines. If any commands have been disabled/restricted by a privilege level restriction, it will be shown here.

Accounting: The Accounting section of the **show aaa** output lists which, if any, access methods are having their commands accounted for. The privilege level ranges of accounted commands can be found here as well as whether EXEC (login) accounting is enabled.

```
FLEX24-10G# show aaa
Authentication :
  console : local
```

```
  telnet  : tacacs
  ssh     : tacacs radius local
  http    : tacacs
Authorization :
  console : no, commands disabled
  telnet  : no, commands disabled
  ssh     : tacacs, commands 0-15 enabled, config-commands enabled
Accounting :
  console : tacacs, commands 0-15 enabled, exec enabled
  telnet  : tacacs, commands 0-15 enabled, exec enabled
  ssh     : tacacs, commands 0-15 enabled, exec enabled
FLEX24-10G#
```

Chapter 12: 802.1x Port-Based Authentication

Introduction

802.1x Port-Based Authentication is an IEEE standard designed to provide authentication for devices attempting to connect to a network. 802.1x is a subset of the IEEE 802.1 group or protocols and is compatible with both LAN's and WLAN's.

When 802.1x Port-Based Authentication is enabled on a FLEX24-10G's interface, any connected clients will not have network access until their identity has been verified. Both the client and the switch must be 802.1x compatible and have 802.1x authentication enabled for 802.1x authentication to take place. If the endpoint does not have 802.1x authentication enabled, the FLEX24-10G will perform MAC Authentication Bypass.

The FLEX24-10G does not perform the authentication process; the authentication is done by a separate RADIUS server configured to handle 802.1x requests.

Requirements for 802.1x Authentication

- 802.1x enabled on the FLEX24-10G
- 802.1x enabled on client device attempting to access network
- RADIUS server with network connectivity to the FLEX24-10G

Configuration (Pointing FLEX24-10G to RADIUS server)

	Command	**Explanation**
Step 1	configure terminal	Enter Global Configuration mode.
Step 2	radius-server host <word1-255>	Specify either the hostname or the IP address of the RADIUS server.
Step 3	radius-server key [unencrypted | encrypted] <secret>	Configure the switch with a shared secret matching the secret configured on the RADIUS server. By default, **unencrypted** is implicitly included in the **radius-server key** command unless the administrator explicitly supplies the **encrypted** parameter. **Example:** **radius-server key unencrypted testing** and **radius-server key testing** are recognized as the same command. If **encrypted** is specified, the switch expects an encrypted shared secret to be supplied as a parameter.

		Note: Regardless of whether the user enters the **encrypted** or **unencrypted** parameter, the shared secret will always be displayed as encrypted in the switch's running-configuration. **Note:** If these secrets do not match, authentication packets will not be passed between the switch and RADIUS server successfully.
Step 4	radius-server deadtime <1-1440>	**(Optional)** Configure the deadtime of the RADIUS server. Default is 0 minutes. The deadtime is specified in minutes and is the amount of time the FLEX24-10G will wait before it stops using a RADIUS server that does not respond.
Step 5	radius-server retransmit <1-1000>	**(Optional)** Configure the retransmit value for the RADIUS server. Default is 3 times. If the FLEX24-10G does not hear a response from the RADIUS server, it will try to send a RADIUS request, by default, 3 more times to the RADIUS server. If the FLEX24-10G does not hear a response to any of these requests, the RADIUS server is marked as dead.
Step 6	radius-server timeout <1-1000>	**(Optional)** Configure the timeout of the RADIUS server, in seconds. Default is 5 seconds. The timeout is the number of seconds the FLEX24-10G will wait for a reply from the RADIUS server before retransmitting the request.

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# radius-server host 192.168.100.2
FLEX24-10G(config)# radius-server key unencrypted testing
FLEX24-10G(config)# radius-server deadtime 1
FLEX24-10G(config)# radius-server retransmit 2
FLEX24-10G(config)# radius-server timeout 10
FLEX24-10G(config)#
```

Port-Based Authentication

During the 802.1x authentication process the user/client is known as the supplicant, the switch is known as the authenticator, and the RADIUS server is known as the authentication server. The switch acts as a middle-man between the supplicant and the authentication server, forwarding requests and responses between them. The switch does not perform any authentication itself; authentication is left entirely in the hands of the RADIUS server.

Frames sent between the supplicant and the authenticator (the switch) are EAPOL (EAP over LAN) frames. Only EAPOL frames are transmitted during the authentication process since the supplicant has yet to receive an IP address.

Frames sent between the authenticator and the authentication server are RADIUS packets. The switch is completely unaware of the authentication details and merely encapsulates the EAP portion of each frame into either an EAPOL packet or a RADIUS packet depending on the packet's destination.

When the authentication process is complete, the RADIUS server sends a special packet containing a success or failure indication. Besides forwarding this decision to the supplicant, the switch uses it to allow or block traffic on the switchport connected to the supplicant.

Enabled 802.1x Authentication

	Command	Explanation
Step 1	configure terminal	Enter Global Configuration mode.
Step 2	dot1x system-auth-control	Enables 802.1x authentication globally on the switch.
Step 3	interface {*, GigabitEthernet <1/1-24>, 10GigabitEthernet<1/1-2>}	Enter Interface Configuration mode for the interface(s) to configure.
Step 4	no spanning-tree	Spanning Tree Protocol must be disabled before 802.1x authentication can be enabled.
Step 5	dot1x port-control <auto | force-authorized | force-unauthorized | mac-based | multi | single>	Set the port-security state: **Auto:** Port-based authentication is enabled when the **auto** keyword is specified. Before the client is authenticated by the RADIUS server, only EAPOL frames are switched. The client will not be assigned an IP address until its identity is verified by the RADIUS server. The switch acts as a middle-man between the client and the RADIUS server, and will encapsulate the EAP portion of the frames from the server/client into RADIUS or EAPOL frames before sending it. **Force Authorized:** Any client downstream from this interface is granted network access without authentication. **Force Unauthorized:** Any client downstream from this interface is refused network access. **Mac-Based:** Mac-Based authentication does not follow the 802.1x standard. With Mac-based authentication the client's MAC address is used as both the username and password

		during the authentication process with the RADIUS server. No software is required on the client for Mac-based authentication to be successful. **Multi:** Multi 802.1x authentication allows one or more clients to be authenticated at the same time. The number of clients which can be authenticated at once can be directly controlled using port-security. **Single:** With Single 802.1x authentication, only one client is authenticated at one time. Once one client has been successfully authenticated, only that client is allowed access. Additional clients who attempt to authenticate will not be granted access.
Step 6	dot1x re-authenticate	**(Optional)** If authentication fails for whatever reason, **dot1x re-authenticate** can be issued to restart the authentication process.
Step 7	end	**(Optional)** Exit Interface Configuration mode and return to Privileged EXEC mode.
Step 8	copy running-config startup-config	**(Optional)** Copy the contents of the running-config to the startup-config.

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# dot1x system-auth-control
FLEX24-10G(config)# interface GigabitEthernet 1/1
FLEX24-10G(config-if)# no spanning-tree
FLEX24-10G(config-if)# dot1x port-control auto
FLEX24-10G(config-if)# dot1x re-authenticate
FLEX24-10G(config-if)# end
LEX24-10G# copy running-config startup-config
Building configuration...
% Saving 2442 bytes to flash:startup-config
FLEX24-10G#
```

Additional 802.1x Interface Commands

	Command	Explanation
Step 1	configure terminal	Enter Global Configuration mode.
Step 2	interface {*, GigabitEthernet <1/1-24>, 10GigabitEthernet<1/1-2>}	Enter Interface Configuration mode for the interface(s) to configure.
Step 3	no spanning-tree	Spanning Tree Protocol must be disabled before 802.1x authentication can be enabled.
Step 4	dot1x guest-vlan	**(Optional)** Enables/disables guest VLAN. The guest VLAN is a VLAN where 802.1x unaware clients are placed following a network administrator-defined timeout.

		Note: dot1x feature guest-vlan must also be issued from Global Configuration.
Step 5	dot1x radius-qos	**(Optional)** Enables/disables per-port state of RADIUS assigned QoS. The switch will react to QoS Class Information carried in the Accept-Accept packet sent by the RADIUS server when a client is successfully authenticated. **Note: dot1x feature radius-qos** must also be issued from Global Configuration. **Note:** This option is only available when **dot1x port-control auto** or **dot1x port-control single** is issued.
Step 6	dot1x radius-vlan	**(Optional)** Enables/disables per-port state of RADIUS-assigned VLAN. The switch will react to VLAN ID Information carried in the Accept-Accept packet sent by the RADIUS server when a client is successfully authenticated. If the VLAN ID is present and valid, the port's VLAN ID will be dynamically changed to match the VLAN ID of the Accept-Accept packet. **Note: dot1x feature radius-vlan** must also be issued from Global Configuration. **Note:** This option is only available when **dot1x port-control auto** or **dot1x port-control single** is issued.

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# interface GigabitEthernet 1/1
FLEX24-10G(config-if)# no spanning-tree
FLEX24-10G(config-if)# dot1x guest-vlan
FLEX24-10G(config-if)# dot1x radius-qos
FLEX24-10G(config-if)# dot1x radius-vlan
FLEX24-10G(config-if)#
FLEX24-10G(config-if)# end
FLEX24-10G# copy running-config startup-config
Building configuration...
% Saving 2497 bytes to flash:startup-config
FLEX24-10G#
```

Additional 802.1x Parameters

Reauthentication: When enabled, successfully authenticated clients are reauthenticated once the reauthentication period expires.

Reauthentication is enabled with the **dot1x reauthentication** command from Global Configuration.

The reauthentication period is set with the **dot1x authentication timer re-authenticate <1-3600>** command from Global Configuration.

The maximum reauthentication count can be configured. The maximum reauthentication count configures the number of times the switch transmits an EAPOL Request Identity frame without response before entering the Guest VLAN.

Note: If the Guest VLAN is not globally enabled, the maximum reauthentication count cannot be configured.

The maximum reauthentication count is configured with the **dot1x max-reauth-req <1-255>** command from Global Configuration.

EAPOL Timeout: The EAPOL timeout determines the time for retransmission of Request Identity EAPOL frames. Valid values are from 1 to 65535 seconds, inclusive.

EAPOL Timeout is configured from Global Configuration using **dot1x timeout tx-period <1-65535>.**

Hold Time: Hold Time applies to interfaces configured with:

- Single 802.1x
- Multi 802.1x
- MAC-Based Authentication

If a client who is trying to authenticate is denied access by the RADIUS server, or the server requests timeout, the client must wait until the Hold Time expires before they are given another opportunity to authenticate with the RADIUS server. The default Hold Time is 10 seconds.

During the Hold Time, the client is put on hold in the Unauthorized state.

The Hold Time is configured from Global Configuration using the **dot1x timeout quiet-period <10-1000000>** command**.**

Aging Time: Aging Time applies to interfaces configured with:

- Single 802.1x
- Multi 802.1x
- MAC-Based Authentication

When the port-security module checks for activity on an interface's MAC address, the frequency of these checks is determined by the Aging Time. By default, the Aging Time is set to 300 seconds.

If no activity is seen on an interface's MAC address within *aging time* seconds, the switch will free resources which were previously allocated to that MAC address, for example, removing the MAC entry from the switch's MAC address table.

The Aging Time is set using the **dot1x authentication timer inactivity <10-1000000>** command from Global Configuration.

Guest VLAN: The guest VLAN is a VLAN where 802.1x unaware clients are placed following a network administrator-defined timeout.

To enable the Guest VLAN: **dot1x feature guest-vlan** from Global Configuration.

To set the Guest VLAN: **dot1x guest-vlan <vlan_id>** from Global Configuration.

Allow Guest VLAN if EAPOL Seen: The switch remembers if an EAPOL frame has been received on the port for the lifetime of the port.

Once the switch considers whether to enter the Guest VLAN, it will first check if this option is enabled or disabled.

If disabled, the switch will only enter the Guest VLAN if an EAPOL frame has not been received on the port for the lifetime of the port.

If enabled, the switch will consider entering the Guest VLAN even if an EAPOL frame has been received on the port for the lifetime of the port.

By default, this setting is disabled.

To enable this setting, issue **dot1x guest-vlan supplicant** from Global Configuration.

Verification

show dot1x status [brief | interface {*, GigabitEthernet <1/1-24>, 10GigabitEthernet<1/1-2>}]: Displays the all interfaces and their 802.1x port state.

```
FLEX24-10G# show dot1x status
Interface  Admin Port State      Last Src          Last ID           QOS VLAN Guest
---------- ----- --------------- ----------------- ----------------- --- ---- -----
Gi 1/1     Port  Down            -                 -                 -   -    -
Gi 1/2     Auth  Down            -                 -                 -   -    -
Gi 1/3     Auth  Down            -                 -                 -   -    -
Gi 1/4     Auth  Down            -                 -                 -   -    -
Gi 1/5     Auth  Down            -                 -                 -   -    -
Gi 1/6     Auth  Down            -                 -                 -   -    -
Gi 1/7     Auth  Down            -                 -                 -   -    -
Gi 1/8     Auth  Down            -                 -                 -   -    -
Gi 1/9     Auth  Down            -                 -                 -   -    -
Gi 1/10    Auth  Down            -                 -                 -   -    -
Gi 1/11    Auth  Down            -                 -                 -   -    -
Gi 1/12    Auth  Down            -                 -                 -   -    -
Gi 1/13    Auth  Down            -                 -                 -   -    -
Gi 1/14    Auth  Down            -                 -                 -   -    -
Gi 1/15    Auth  Down            -                 -                 -   -    -
```

```
Gi 1/16    Auth  Down          -               -               -   -    -
Gi 1/17    Auth  Down          -               -               -   -    -
Gi 1/18    Auth  Down          -               -               -   -    -
Gi 1/19    Auth  Down          -               -               -   -    -
Gi 1/20    Auth  Down          -               -               -   -    -
Gi 1/21    Auth  Down          -               -               -   -    -
Gi 1/22    Auth  Down          -               -               -   -    -
Gi 1/23    Auth  Down          -               -               -   -    -
Gi 1/24    Auth  Down          -               -               -   -    -
Gi 1/25    Auth  Down          -               -               -   -    -
10G 1/1    Auth  Down          -               -               -   -    -
10G 1/2    Auth  Down          -               -               -   -    -
FLEX24-10G#
```

show dot1x statistics {all | eapol | radius} [interface {*, GigabitEthernet <1/1-24>, 10GigabitEthernet<1/1-2>]: Displays more granular dot1x statistics on a per-interface basis. Output can be filtered to only display dot1x statistics for a particular interface.

```
FLEX24-10G#  show dot1x statistics all
Gi 1/1 EAPOL Statistics:
Rx Total:                       0   Tx Total:                       0
Rx Response/Id:                 0   Tx Request/Id:                  0
Rx Response:                    0   Tx Request:                     0
Rx Start:                       0
Rx Logoff:                      0
Rx Invalid Type:                0
Rx Invalid Length:              0

Gi 1/1 Backend Server Statistics:
Rx Access Challenges:           0   Tx Responses:                   0
Rx Other Requests:              0
Rx Auth. Successes:             0
Rx Auth. Failures:              0

Gi 1/2 EAPOL Statistics:
Rx Total:                       0   Tx Total:                       0
Rx Response/Id:                 0   Tx Request/Id:                  0
Rx Response:                    0   Tx Request:                     0
Rx Start:                       0
Rx Logoff:                      0
Rx Invalid Type:                0
Rx Invalid Length:              0

Gi 1/2 Backend Server Statistics:
Rx Access Challenges:           0   Tx Responses:                   0
Rx Other Requests:              0
Rx Auth. Successes:             0
Rx Auth. Failures:              0
 -------------------------------------OUTPUT TRUNCATED -------------------------------------
```

Chapter 13: Logging

Introduction

Logs are a key part of any troubleshooting process. Having the ability to view a history of major switch events from a centralized syslog server can greatly accelerate the troubleshooting process when multiple network devices are involved.

The FLEX24-10G supports linking the switch with an external syslog server. Once the switch has been configured to utilize a syslog server and a connection has been established, all system logs will be sent to the server.

A traditional network will have several switches, routers, etc. utilizing a single syslog server. This centralized approach allows for very efficient troubleshooting as logs from multiple devices may be cross-referenced at a single time.

Configuration

To make use of a syslog server, logging must be enabled globally on the FLEX24-10G and the syslog servers IP must be provided.

	Command	Explanation
Step 1	configure terminal	Enter Global Configuration mode.
Step 2	logging on	Enable the transmission of system logs to an external syslog server.
Step 3	logging host <domain_name> <ipv4_ucast>	Specify the IPv4 address or domain name of the syslog server.
Step 4	logging level {error | warning | notice | informational}	**(Optional)** Specify the which category of logs to send to the syslog server. The various severity levels are: 0. Emergency (Highest Priority) 1. Alert 2. Critical 3. Error 4. Warning 5. Notification 6. Informational 7. Debugging (Lowest Priority) All logs of priority equal to and higher than the configured value will be sent to the syslog server. The default logging level is **notification.** **Example:** If the logging level is set to **error,** only log messages with a severity level of error, critical, alert, and emergency will be sent to the syslog server.

Step 5	logging notification listen <identifying_name> level {error | warning | notice | informational} <identification>	**(Optional)** Create a custom notification when a log is generated which matches the details of the parameters in the command.
Step 6	end	**(Optional)** Return to Privileged EXEC mode.
Step 7	copy running-config startup-config	**(Optional)** Copy the contents of the running-config to the startup-config.

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# logging on
FLEX24-10G(config)# logging host 192.168.100.50
FLEX24-10G(config)# logging level warning
FLEX24-10G(config)# end
FLEX24-10G# copy running-config startup-config
Building configuration...
% Saving 2381 bytes to flash:startup-config
FLEX24-10G#
```

Verification

show logging [<logging_id> | error | informational | notice | warning]: Displays the entire system log as well as any syslog server configuration details. Output can be filtered to only display logs messages of a specific type or types. Also, if the **logging_id** of a specific log message is known, only that log can be displayed using the **show logging <logging_id>** command.

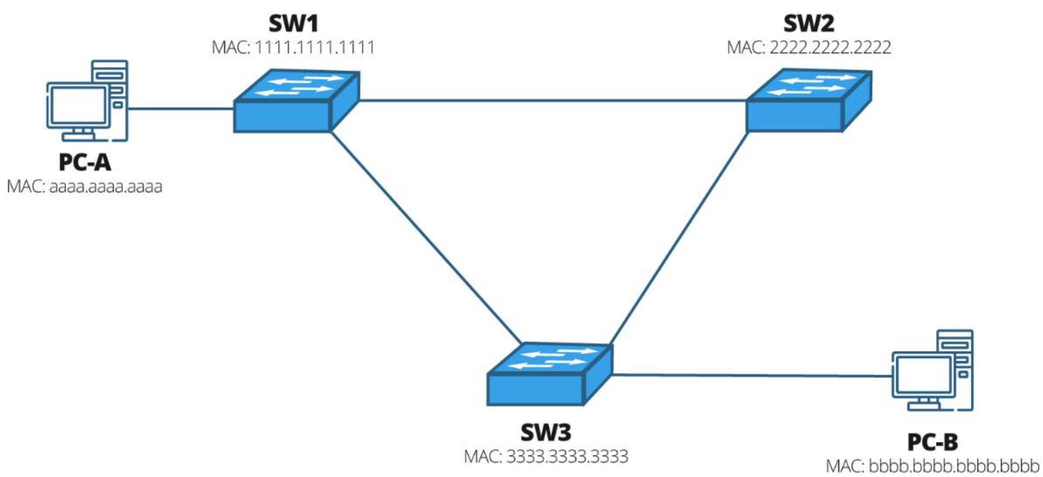
```
FLEX24-10G# show logging
Switch logging host mode is disabled
Switch logging host address is 192.168.100.2
Switch logging level is informational

Number of entries on Switch 1:
Error        : 0
Warning      : 0
Notice       : 44
Informational: 1
All          : 45

ID          Level          Time & Message
----------  -------------  --------------
         1  Informational  2019-11-20T20:43:03+00:00
                           SYS-BOOTING: Switch just made a cold boot.

         2  Notice         2019-11-20T20:43:04+00:00
                           LINK-UPDOWN: Interface Vlan 1, changed state to down.

         3  Notice         2019-11-20T20:43:04+00:00
-- more --, next page: Space, continue: g, quit: ^C
```

Chapter 14: Spanning Tree Protocol

Introduction

In a Layer-2 network environment there is a desire to create redundant links between switches. With redundant links there is no single point of failure in a cabling topology. Problems can arise however when broadcast traffic is introduced into a network with a physical cabling loop. A cabling or switching loop occurs when there is more than one path between two endpoints.

Consider the example three switch network below. Each switch is connected to each of the other two switches.



If all three switches have an empty MAC address table and PC-A attempts to transmit traffic to PC-B, SW1 will not have an entry in its MAC address table for bbbb.bbbb.bbbb. Since no entry exists, SW1 will broadcast the traffic for PC-B's MAC address in an attempt to find the interface in which PC-B is located. This broadcast traffic is sent out all interfaces except the interface where PC-A is located.

This broadcast traffic will be then sent to SW2 and SW3. SW2 and SW3 will also not have any entry in their MAC address tables for PC-B and will broadcast the traffic out all interfaces except the one which it was received on.

This is where the underlying problem lies. When SW2 and SW3 broadcast the traffic, SW1 will receive a copy of the traffic which it originally broadcasted but since it also has no idea where PC-B is located the data will continue to be bounced between SW1, SW2, and SW3.

This is how a switching loop occurs. Every time additional broadcasts are sent between the switches, the switches which receive them will update their MAC address tables based on the source MAC of the unknown unicast frames.

Throughout this process the MAC address tables of all three switches are continuously changing and the total amount of traffic is growing rapidly. This is how a broadcast storm is created. A broadcast storm has the potential to slow the entire network to a halt.

Spanning Tree Protocol (STP) was designed as a solution to switching loops while allowing redundant links to remain present. STP in essence, blocks certain interfaces which have the potential to create a switching loop. These blocked interfaces make it impossible for there to be more than one path between two endpoints.

Spanning Tree Root Bridge, Bridge ID and Bridge Priority

By default, all switches in an STP environment have a bridge priority of 32768. The bridge priority must be in increments of 4096. The bridge priority is used between the switches to elect a root bridge. The root bridge in an STP topology is the switch with the lowest Bridge ID (BID). The BID is comprised of the switch's bridge priority and MAC address.

For example: A switch with a priority of 32768 and a MAC address of aaaa.aaaa.aaaa will have a BID of 32768.aaaa.aaaa.aaaa.

In the event of a tiebreaker between two switches with identical priorities, the switch with the lowest MAC address will win the election.

There can only be one root bridge for each STP instance. Many factors should be considered when deciding which switch should be the root bridge. The root bridge should generally be a core switch with high bandwidth links to the distribution layer. If there are redundant core switches, then a backup root bridge can be designated. The root bridge should not be an edge switch or a switch with a problematic operating history.

If the root bridge is not set by the administrator, the switch with the lowest MAC address will win the election becoming the root bridge. Leaving the root bridge election down to chance is not recommended.

All switches will calculate their best path to the root bridge. If more than one path to the root bridge exists, an interface or interface(s) on the less desirable path will be put into a blocking state.

Spanning Tree Port States

Every Layer-2 interface on a switch running spanning tree (STP) exists in one of the following states.

STP Port State Process

1. **Blocking:** This is the first stage of the election process. An interface in the blocking state does not forward frames and will discard all frames from the attached network segment (except for BPDUs).
2. **Listening:** If spanning tree determines that the interface should participate in frame forwarding, the interface will transition into the Listening state. A *listening* interface still only accepts BPDU's which are sent to the switch system module for processing. After 15 seconds, the switch transitions to the Learning State.
3. **Learning:** A switch in the learning state is listening for and processing BPDUs. *Learning* ports drop incoming frames and begin to update the switch's MAC address table. An interface remains in the learning state for 15 seconds.

4. **Forwarding:** Forwarding ports forward frames normally and continue to listen for BPDUs. This is the normal operating state.
5. **Disabled:** A disabled port is not participating in spanning tree or frame forwarding. A port could be disabled because of a shutdown port, no data link, or spanning tree has been disabled on the interface in question.

The interface on any non-root bridge with the lowest cost to the root bridge is known as a root port. Root ports are always in a forwarding mode and each switch can only have one root port.

A designated port is a non-root port on a LAN segment with the lowest cost to the root. If the other end of the designated port is not a root port, it is a Non-Designated Port. Designated ports are always forwarding while Non-Designated ports are always blocking.

All interfaces on the root bridge are designated ports. There cannot be any root ports on the root bridge.

Spanning Tree Election Process

When STP is enabled within a network topology. All switches running the same STP mode participate in a Root Bridge Election. In the initial stage of the election all switches will advertise themselves as the root bridge using BPDU's. These BPDU's advertise the switches' BID and are sent to other STP switches in the topology.

If a switch receives a BPDU containing a lower BID than its own, it will stop advertising itself as the root and will begin to advertise the switch with the lower BID as the root.

STP BPDUs are encapsulated inside of Ethernet Frames. An STP BPDU contains the following information:

1. **Protocol ID (2 bytes):** Contains "0x0000" for 802.1D.
2. **Version ID (1 byte):** Contains "0" for STP, "2" for RSTP, "3" for MST, "4" for SPT BPDU.
3. **BPDU Message Type (1 byte):** Contains "0x00" for configuration BPDU, "0x80" for TCN BPDU, and "0x02" for RST/MST Config BPDU.
4. **Flags (1 byte):**
    a. Bit 1
        i. "0" or "1" for Topology Change
    b. Bit 2
        i. "0" (unused)
        ii. "1" for Proposal in RST/MST/SPT BPDU
    c. Bits 3-4
        i. "00" (unused)
        ii. "01" for Port Role Alternate/Backup in RST/MST/SPT BPDU
        iii. "10" for Port Role Root in RST/MST/SPT BPDU
        iv. "11" for Port Role Designated in RST/MST/SPT BPDU
    d. Bit 5
        i. "0" (unused)
        ii. "1" for Learning in RST/MST/SPT BPDU

   e. Bit 6
      i. "0" (unused)
      ii. "1" for Forwarding in RST/MST/SPT BPDU
   f. Bit 7
      i. "0" (unused)
      ii. "1" for Agreement in RST/MST/SPT BPDU
   g. Bit 8
      i. "0" or "1" for Topology Change Acknowledgement
5. **Root ID (8 bytes):**
   a. Bits 1-4
      i. Bridge Priority
   b. Bits 5-16
      i. Bridge System ID Extension
   c. Bits 17-64
      i. Bridge MAC Address
6. **Root Path Cost (4 bytes):** External Path Cost in MST/SPT BPDU
7. **Bridge ID (8 bytes):** Regional Root ID in MST/SPT BPDU
8. **Port ID (2 bytes):** Identifies the port in which the message originated.
9. **Message Age (2 bytes):** Amount of time which has elapsed since the root bridge sent the message.
10. **Max Age (2 bytes):** Specifies when the current message should be deleted.
11. **Hello Time (2 bytes):** Frequency in which the root bridge sends configuration messages.
12. **Forward Delay (2 bytes):** Period switches should wait before changing to new STP port state.

Once all switches agree on which switch should be the root, and all switchports are placed in the correct port state, STP is said to have *converged.*

The switches can determine what the best path to the root is by using the Root Path Cost field within configuration BPDUs. The Root Path Cost is used to determine the port state of each interface running STP.

Topology Change Notification (TCN) BPDU's are used by non-root switches to inform other switches of interface changes. **TCN BPDU's only contain fields 1-3 from the list above.** TCN BPDU's are propagated throughout the network until they reach the root. Once the root receives the TCN BPDU, the root will set the TCN flag in its normal BPDUs which are then sent to every switch in the STP instance. Upon receipt of the root switch's BPDU with the TCN flag, all non-root switches age out their MAC address tables.

Path/Port Costs

Interface Bandwidth	STP Path Cost	RSTP Path Cost
4 Mbit/s	250	5000000
10 Mbit/s	100	2000000
16 Mbit/s	62	1250000
100 Mbit/s	19	200000
1 Gbit/s	4	20000

2 Gbit/s	3	10000
10 Gbit/s	2	2000
100 Gbit/s	N/A	200
1 Tbit/s	N/A	20

STP uses bandwidth as the basis to calculate path costs. Obviously, higher bandwidth links are preferred over lower bandwidth links. A trunk links path cost can be manipulated by the administrator to allow spanning tree to favor paths which would typically have a higher cost.

By default, all GigabitEthernet interfaces on the FLEX24-10G have an STP and RSTP cost of 4 and 20000 respectively. The below configuration shows how to manually set an interface's port cost to a non-default value. Both ends of the side should be configured with a matching port cost.

	Command	**Explanation**
Step 1	configure terminal	Enter Global Configuration mode.
Step 2	interface {*, GigabitEthernet <1/1-24>, 10GigabitEthernet<1/1-2>}	Enter Interface Configuration mode for the interface to configure.
Step 3	spanning-tree mst <0-7> cost {auto | <1-200000000>}	Set the port cost of the interface to a value from 1 to 200000000 inclusive. **<0-7>** represents the spanning tree instance. The **auto** parameter allows a port's cost to change dynamically when the interface is running with a non-default speed.
Step 4	end	**(Optional)** Exit Interface Configuration mode and return to Privileged EXEC mode.
Step 5	copy running-config startup-config	**(Optional)** Copy the contents of the running-config to the startup-config.

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# interface GigabitEthernet 1/1
FLEX24-10G(config-if)# spanning-tree mst 0 cost 21
FLEX24-10G(config-if)# end
FLEX24-10G# show spanning-tree interface GigabitEthernet 1/1
Mst    Port      Port Role      State      Pri  PathCost Edge  P2P        Uptime
-----  --------- -------------- ---------- ---  -------- ----  ---  -------------
CIST   Gi 1/1    DesignatedPort Forwarding 128        21 No    Yes  0d 00:14:15
FLEX24-10G# configure terminal
FLEX24-10G(config)# interface GigabitEthernet 1/1
FLEX24-10G(config-if)# spanning-tree mst 0 cost auto
FLEX24-10G(config-if)# end
FLEX24-10G# show spanning-tree interface GigabitEthernet 1/1
Mst    Port      Port Role      State      Pri  PathCost Edge  P2P        Uptime
-----  --------- -------------- ---------- ---  -------- ----  ---  -------------
CIST   Gi 1/1    DesignatedPort Forwarding 128    200000 No    Yes  0d 00:14:42
FLEX24-10G#
```

For example, a switch with a direct Gigabit connection to the root bridge will have a root path cost of 4 via STP and 20000 via RSTP.

Consider Figure 1 below:

SW1 will become the root bridge since it has a lower priority (4096 compared to the default 32768 on SW2). SW1 and SW2 are directly connected by a GigabitEthernet link and by an FastEthernet link. Since a loop is present in this topology one of the four interfaces must be in a blocking state. Since all interfaces on the root bridge must be designated ports, i.e. forwarding, one of the interfaces on SW2 must be blocking.

The GigabitEthernet link provides SW2 a path cost of 4 (20000 if using RSTP) to the root while the FastEthernet link provides SW2 a path cost of 19 (200000 if using RSTP). Since the GigabitEthernet link is preferred, the FastEthernet interface on SW2 will be put into a blocking state, eliminating the possibility of a switching loop from occurring.

In a multi-switch environment, the total path cost is calculated by the sum of all links between the switch in question and the root bridge.

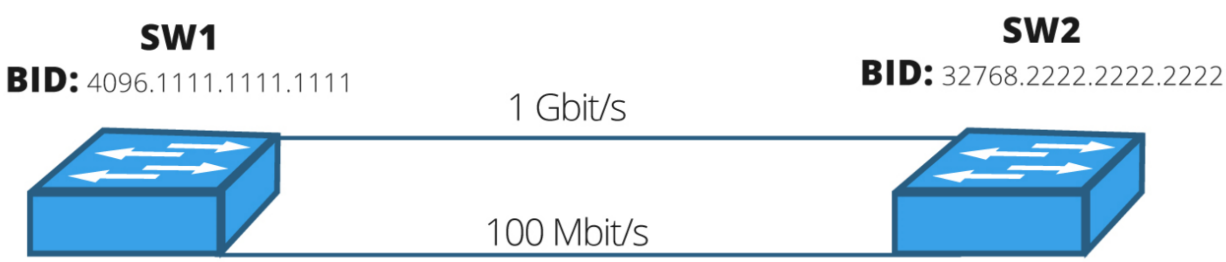


Figure 1: Redundant links with different speeds

Tie Breakers

Determining Root Ports – Switches not Directly Connected to the Root Bridge

When there are two lowest equal cost paths between a switch and the root bridge, a switch will choose the path through the neighbor with the lowest BID. Since the BID contains the switch's MAC address, the BID's are guaranteed to be unique so no further tie breaker will have to take place.

The interface connected to the switch with the lower BID will become the root port.

Determining Root Ports – Switches Directly Connected to the Root Bridge

Consider Figure 2 below. This topology is identical to the topology in Figure 1 except both links are Gigabit links. SW1 will operate as the root bridge. How will spanning tree decide which interface on SW2 to put into a Blocking state?

The following process is followed by spanning tree to select the best path to the root bridge:

1. Lowest root bridge ID

2. Lowest root path cost to the root bridge
3. Lowest sender bridge ID
4. Lowest sender port ID

In Figure 2 the first three criteria all result in a tie. Therefore, the root port on SW2 will be the interface with the lowest port ID. An interface's port ID is comprised of the interface's 4-bit priority value and its 12-bit interface identifier. By default, all switchports have a priority value of 128. The interface identifier is simply the interface number. For example: GigabitEthernet 1/11 would have a port ID of 128.11.

In Figure 2, G 1/1 will have a port ID of 128.1 while G 1/2 will have a port ID of 128.2. Since G 1/1 has the lower port ID, it will go into a forwarding state, with G 1/2 going into a blocking state.

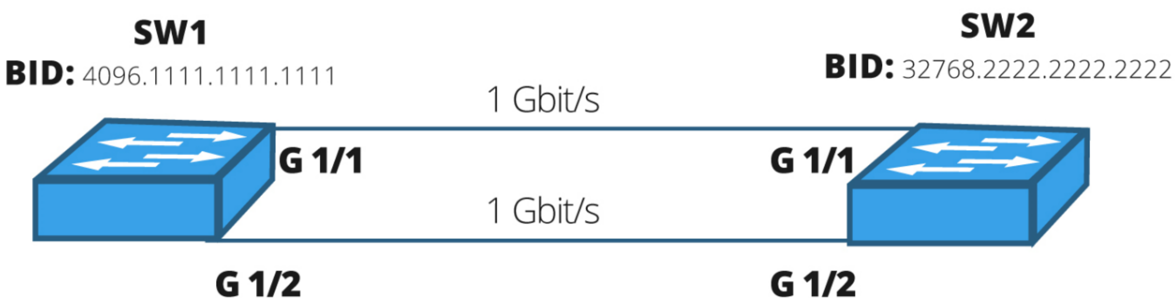


Figure 2: Redundant links with identical speeds

Modifying an Interface's Port-Priority

By default, all interfaces have a port-priority of 128. An interface's port priority can be changed within that interface's configuration mode as follows:

	Command	Explanation
Step 1	configure terminal	Enter Global Configuration mode.
Step 2	interface {*, GigabitEthernet <1/1-24>, 10GigabitEthernet<1/1-2>}	Enter Interface Configuration mode for the interface to configure.
Step 3	spanning-tree mst <0-7> port-priority <0-240>	Set the interface's port-priority. The port-priority must be a multiple of 16, i.e. 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, 240. **<0-7>** represents the spanning tree instance.
Step 4	end	**(Optional)** Exit Interface Configuration mode and return to Privileged EXEC mode.
Step 5	copy running-config startup-config	**(Optional)** Copy the contents of the running-config to the startup-config.

The below CLI snippet changes the port-priority of GigabitEthernet 1/1 from 128 to 48.

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# interface GigabitEthernet 1/1
FLEX24-10G(config-if)# spanning-tree mst 0 port-priority 48
FLEX24-10G(config-if)# end
FLEX24-10G# copy running-config startup-config
Building configuration...
% Saving 2255 bytes to flash:startup-config
FLEX24-10G# show spanning-tree interface GigabitEthernet 1/1
Mst    Port       Port Role      State      Pri  PathCost  Edge  P2P        Uptime
-----  ---------  -------------- ---------- ---  --------  ----  ---  -------------
CIST   Gi 1/1     DesignatedPort Forwarding  48    200000  No    Yes  0d 01:12:08
FLEX24-10G#
```

Spanning Tree Modes

The FLEX24-10G supports Spanning Tree Protocol (STP), Multiple Spanning Tree Protocol (MSTP), and Rapid Spanning Tree Protocol (RSTP).

Spanning Tree Protocol: First version of STP, has since been replaced by the RSTP and MSTP. All information described earlier in this chapter pertains specifically to STP.

Rapid Spanning Tree Protocol: While STP had the five ports states of Blocking, Listening, Learning, Forwarding, and Disabled, RSTP's number of ports states have been reduced to three.

The three RSTP port states are:

1. **Discarding:** The Discarding state replaces the Blocking state originally found in STP.
2. **Learning:** The Learning state absorbs the roles of the Listening and Learning states originally found in STP.
3. **Forwarding:** The Forwarding state is identical to the Forwarding state in STP and any other spanning tree mode.

With the reduction in number of port states, RSTP can converge much faster than traditional STP. While STP would typically require 30 to 50 seconds to respond to a topology change, RSTP can respond to a topology change in less than 10 seconds.

Multiple Spanning Tree Protocol: With MSTP, multiple VLANs can be assigned to a spanning tree instance. Multiple instances can be created, and each instance operates independently from the others. A physical cabling loop may not necessarily cause any issues with MSTP since MSTP works at the logical VLAN level. MSTP runs on top of RSTP, so users can expect the same rapid convergence time with MSTP.

MSTP reduces the number of spanning tree instances required to support many VLANs.

Configuration

Bridge Configuration

All non-root switches inherit the Max-Age and Forward-Delay timers from the root bridge.

	Command	Explanation
Step 1	configure terminal	Enter Global Configuration mode.
Step 2	spanning-tree mode {stp | rstp | mstp}	Enable Spanning Tree and set the desired STP mode.
Step 3	spanning-tree mst <0-7> priority <0-61440>	**(Optional)** Create a spanning tree instance on the switch and set the priority to a value other than 32768. The priority value must be divisible by 4096, i.e. 0, 4096, 8192, 2288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440. **<0-7>** represents the spanning tree instance. **Note:** By default, the bridge priority is set to 32768.
Step 4	spanning-tree mst forward-time <4-30>	**(Optional)** Set the forward-time. The forward-time is the amount of time a root or designated port takes to enter a Forwarding state (used in STP compatible mode). All other switches in the spanning tree domain will inherit this timer value. **Note:** This command only takes effect if the local switch is the root bridge.
Step 5	spanning-tree mst hello-time <1-10>	**(Optional)** Set the time interval when the switch should send BPDU's. Valid values are 1-10 seconds. By default, BPDU's are sent every 2 seconds. **Note:** This command only takes effect if the local switch is the root bridge.
Step 6	spanning-tree mst max-age <6-40>	**(Optional)** Set the maximum age, in seconds, of the information transmitted by the root bridge. Valid values are from 6 to 40 seconds. **Note:** MaxAge value must be less than or equal to 2 x (FwdDelay - 1). All other switches in the spanning tree domain will inherit this timer value.

		Note: This command only takes effect if the local switch is the root bridge.
Step 7	spanning-tree mst max-hops <6-40>	**(Optional)** Set how many hops a BPDU can take before it is discarded. Valid values are from 6 to 40 hops. **Note:** This command only takes effect if the local switch is the root bridge.
Step 8	end	**(Optional)** Return to Privileged EXEC mode.
Step 9	copy running-config startup-config	**(Optional)** Copy the contents of the running-config to the startup-config.

Interface Specific Configuration

	Command	Explanation
Step 1	configure terminal	Enter Global Configuration mode.
Step 2	interface {*, GigabitEthernet <1/1-24>, 10GigabitEthernet<1/1-2>}	Enter Interface Configuration mode for the interface to configure.
Step 3	[no] spanning-tree auto-edge	**(Optional)** Controls whether the switch should enable automatic edge detection on the interface. By default, automatic edge detection is enabled on all interfaces.
Step 4	spanning-tree bpdu-guard	**(Optional)** When enabled, the interface will disable itself upon receiving a BPDU. This should be enabled on all edge ports where only single hosts will be connected.
Step 5	spanning-tree edge	**(Optional)** When enabled, an *operEdge* flag is set when the port is initialized. Interfaces configured with the **spanning-tree edge** command will transition immediately into the Forwarding state. Since the interface is an edge port and should only have one endpoint connected, there should be no possibility of a switching loop existing on the interface.
Step 6	spanning-tree restricted-role	**(Optional)** When enabled on an interface, the interface will not be selected as a root port.

Step 7	spanning-tree restricted-tcn	**(Optional)** When enabled on an interface, the interface will not propagate topology change notifications to other switchports.
Step 8	spanning-tree link-type {auto | point-to-point | shared}	**(Optional)** Controls whether a port connects to a point-to-point LAN rather than to a shared medium. When set to **auto** the switch will automatically determine the interface's link-type.
Step 9	end	**(Optional)** Exit Interface Configuration mode and return to Privileged EXEC mode.
Step 10	copy running-config startup-config	**(Optional)** Copy the contents of the running-config to the startup-config.

MSTP Configuration

Up to seven different MSTP instances can be running on the switch at one time. Each individual VLAN can only be a member of one MSTP instance. Each MSTP instance is independent of any other and can have its own bridge priority.

Creating MSTP Instances

Any VLAN which is not mapped to a specific MSTP instance, is mapped to the Common and Internal Spanning Tree (CIST), or MSTP instance 0.

	Command	Explanation
Step 1	configure terminal	Enter Global Configuration mode.
Step 2	spanning-tree mst <0-7> vlan <vlan_list> Example: spanning-tree mst 1 vlan 50,60,70	Create MSTP instance with an index from 0 to 7. MSTP instance 0 already exists and contains all VLANs which are not mapped to any other instance. **<vlan_list>** must be a list of VLANs. Each entry in the list must be separated by a comma and a VLAN range can be specified with a dash separating the first entry from the last entry in the range. **Note:** A VLAN must be first created before it can be mapped to a MSTP instance.
Step 3	spanning-tree mst <0-7> priority <0-61440>	**(Optional)** Modify the priority value of the newly created MSTP instance if the local switch is to be the root bridge for the instance in question.

	Example: spanning-tree mst 1 priority 24576	The priority value must be divisible by 4096, i.e. 0, 4096, 8192, 2288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440. **<0-7>** represents the spanning tree instance. **<u>Note:</u>** By default, the bridge priority is set to 32768.
Step 4	end	**(Optional)** Return to Privileged EXEC mode.
Step 5	copy running-config startup-config	**(Optional)** Copy the contents of the running-config to the startup-config.

The below CLI snippet creates VLANs 50, 60, and 70 and maps them to MSTP instance 1.

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# vlan 50
FLEX24(config-vlan)# vlan 60
FLEX24(config-vlan)# vlan 70
FLEX24(config-vlan)# exit
FLEX24-10G(config)# spanning-tree mst 1 vlan 50,60,70
FLEX24-10G(config)# spanning-tree mst 1 priority 24576
FLEX24-10G(config)# end
FLEX24-10G# copy running-config startup-config
Building configuration...
% Saving 2640 bytes to flash:startup-config
FLEX24-10G#
```

Modifying MSTP Instances on Trunk Ports

A trunk link can be configured to carry traffic for one or more MSTP instances. Each instance which is present on the trunk can have its port priority and port cost configured separately from the other instances.

<u>Example:</u> Interface GigabitEthernet 1/1 is configured as a trunk port and there are currently three MSTP instances created on the switch as follows:

MSTP 1 – Contains VLAN 10. Assign a port cost of 10 and port priority of 176 to GigabitEthernet 1/1

MSTP 2 – Contains VLAN 20. Leave MSTP with its default port cost and port priority.

MSTP 3 – Contains VLAN 30. Assign a port cost of 3 and port priority of 80 to GigabitEthernet 1/1

	<u>Command</u>	**<u>Explanation</u>**
Step 1	configure terminal	Enter Global Configuration mode.
Step 2	interface GigabitEthernet 1/1	Enter Interface Configuration mode for GigabitEthernet 1/1.
Step 3	switchport mode trunk	Set the interface to a permanent trunking mode.

Step 4	spanning-tree mst 1 cost 10	Modifies the port cost from the default value of 4. Since the port cost is increasing, this link will appear to be worse and will not be as preferred when trying to find the best path to the root bridge. **Note:** A matching port cost should be configured on the remote interface.
Step 5	spanning-tree mst 1 port-priority 176	Changes the port priority from the default value of 128 to 176. The port-priority comes in effect in the event of a tiebreak when choosing root and designated ports. A port-priority of 176 will likely lose a tiebreak as an interfaces default port priority is 128.
Step 6	spanning-tree mst 3 cost 3	Modifies the port cost from the default value of 4. Since the port cost is decreasing, this link will appear to be better and will be more preferred when trying to find the best path to the root bridge. **Note:** A matching port cost should be configured on the remote interface.
Step 7	spanning-tree mst 3 port-priority 80	Changes the port priority from the default value of 128 to 80. The port-priority comes in effect in the event of a tiebreak when choosing root and designated ports. A port-priority of 80 will likely win a tiebreak as an interfaces default port priority is 128.
Step 8	end	**(Optional)** Exit Interface Configuration mode and return to Privileged EXEC mode.
Step 9	copy running-config startup-config	**(Optional)** Copy the contents of the running-config to the startup-config.

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# interface GigabitEthernet 1/1
FLEX24-10G(config-if)# switchport mode trunk
FLEX24-10G(config-if)# spanning-tree mst 1 cost 10
FLEX24-10G(config-if)# spanning-tree mst 1 port-priority 176
FLEX24-10G(config-if)# spanning-tree mst 3 cost 3
FLEX24-10G(config-if)# spanning-tree mst 3 port-priority 80
FLEX24-10G(config-if)# end
FLEX24-10G# copy run start
Building configuration...
% Saving 2706 bytes to flash:startup-config
FLEX24-10G# show spanning-tree mst configuration
MSTI1  10
MSTI2  20
```

```
MSTI3   30
MSTI4   No VLANs mapped
MSTI5   No VLANs mapped
MSTI6   No VLANs mapped
MSTI7   No VLANs mapped
FLEX24-10G#
```

Verification

To display the current spanning tree configuration, use one of the following privileged EXEC commands below:

show spanning-tree: Displays general STP information such as STP port status, bridge ID, and root bridge ID.

show spanning-tree active: Displays information regarding all active spanning tree interfaces.

show spanning-tree detailed [interface {*, GigabitEthernet <1/1-24>, 10GigabitEthernet<1/1-2>}]: Shows detailed information counters on all spanning tree interfaces. Output can be filtered to only include specific interfaces.

show spanning-tree interface {*, GigabitEthernet <1/1-24>, 10GigabitEthernet<1/1-2>}: Display various STP port information for a specific spanning tree interface.

show spanning-tree mst [configuration]: Displays all MSTP instances and all VLANs mapped to each instance.

show spanning-tree mst <0-7> [interface {*, GigabitEthernet <1/1-24>, 10GigabitEthernet<1/1-2>}]: Displays information pertaining to the specified MSTP instance on the specified interface.

show spanning-tree summary: Displays global spanning tree timers, and status of features such as BPDU Filtering, BPDU Guard, and Error Recovery.

Clearing Spanning Tree Information

Spanning tree protocols and statistics can be cleared from the switch's memory with the following Privileged EXEC mode commands:

clear spanning-tree detected-protocols [interface {*, GigabitEthernet <1/1-24>, 10GigabitEthernet<1/1-2>}]

clear spanning-tree statistics [interface {*, GigabitEthernet <1/1-24>, 10GigabitEthernet<1/1-2>}]

Chapter 15: UDLD

Introduction

Unidirectional Link Detection (UDLD) is one of the several loop prevention mechanisms contained on the FLEX24-10G.

UDLD is configured at the interface level and is used to detect unidirectional links between switches. For a successful UDLD configuration, both the local and remote switch must be UDLD enabled.

When both switches are UDLD enabled on their connected interfaces, each switch will send a UDLD frame to the remote switch every 7 seconds by default. These UDLD frames act as keepalives on the link. When one of the switches receives a UDLD frame on an UDLD enabled interface, it will echo that frame back to the remote switch.

UDLD frames contain the interface ID of the interface which produced the frame. When the remote switch receives a UDLD frame, the retransmitted frame will contain the interface ID of the interface (on the remote switch) which received the oricginal message.

Unidirectional links are detected by the absence of UDLD frames from the remote switch. It is important to note that a switch will never echo a UDLD frame from an interface which does not have UDLD enabled. One possible issue with this is that if only one switch on a link is UDLD enabled, it will send UDLD frames but will never receive echoes from the remote switch. To overcome this, the UDLD enabled interface will assume that the remote interface is not UDLD enabled until it receives a UDLD reply.

There are two UDLD modes: Normal and Aggressive.

Normal Mode

In normal mode, a UDLD enabled interface will send a UDLD frame to the remote switch every 7 seconds. When an interface stops receiving UDLD frames from the remote switch, the link will be considered unidirectional. Both interfaces will remain in an up state however a syslog message will be generated if a unidirectional link is detected.

Aggressive Mode

In aggressive mode, UDLD enabled interfaces will also send a UDLD frame every 7 seconds by default. Once an interface in UDLD-aggressive mode does not receive a UDLD echo from the remote switch, all subsequent UDLD frames are sent every second. The interface will be put into an error-disabled state after eight failed echoes.

Configuration

Enabling UDLD

UDLD must be enabled at the interface level. Additionally, to only enable UDLD on the FLEX24-10G's fiber interfaces, issue the **udld {aggressive | enable} command** from Global Configuration**.**

Note: UDLD must be enabled on both switches on the point-to-point link.

	Command	**Explanation**
Step 1	configure terminal	Enter Global Configuration mode.
Step 2	udld {aggressive | enable | message time-interval <7-90>}	**(Optional)** Enable UDLD in normal or aggressive mode on only the fiber interfaces. Optionally, the time period between UDLD probe messages can be configured with the **message time-interval** parameter. Valid time-interval values are from 7 to 90 seconds. 7 seconds is the default.
Step 3	interface {*, GigabitEthernet <1/1-24>, 10GigabitEthernet<1/1-2>}	Enter Interface Configuration mode for the interface(s) to configure UDLD.
Step 4	udld port {aggressive [message time-interval <7-90>] | message time-interval <7-90>}	Enable UDLD on a specific interface or interface(s). The time period between UDLD probe messages scan also be configured on a per-interface basis.
Step 5	end	**(Optional)** Exit interface configuration and return to Privileged EXEC mode.
Step 6	copy running-config startup-config	**(Optional)** Copy the contents of the running-config to the startup-config.

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# udld aggressive
% Only fiber ports are allowed, port_no: 1
-----------OUTPUT TRUNCATED-----------
-----------OUTPUT TRUNCATED-----------
% Only fiber ports are allowed, port_no: 24
% Only fiber ports are allowed, port_no: 25
FLEX24-10G(config)# udld message time-interval 15
% Only fiber ports are allowed, port_no: 1
-----------OUTPUT TRUNCATED-----------
-----------OUTPUT TRUNCATED-----------
% Only fiber ports are allowed, port_no: 24
% Only fiber ports are allowed, port_no: 25
FLEX24-10G(config)# interface GigabitEthernet 1/1
FLEX24-10G(config-if)# udld port aggressive message time-interval 10
FLEX24-10G(config-if)# end
FLEX24-10G# copy running-config startup-config
Building configuration...
```

```
% Saving 2081 bytes to flash:startup-config
FLEX24-10G# show udld interface GigabitEthernet 1/1

GigabitEthernet 1/1
----------------------------------------------------------------------
UDLD Mode                  : Aggressive
Admin State                : Enable
Message Time Interval(Sec): 10
Device ID(local)           : 00-24-63-04-2A-80
Device Name(local)         : FLEX24-10G
Bidirectional state        : Indeterminant

No neighbor cache information stored
---------------------
FLEX24-10G#
```

Verification

show udld [interface {*, GigabitEthernet <1/1-24>, 10GigabitEthernet<1/1-2>}]: Show UDLD information on per-interface basis. Output can be filtered to only include UDLD information for specific interfaces.

```
FLEX24-10G# show udld

GigabitEthernet 1/1
----------------------------------------------------------------------
UDLD Mode                  : Aggressive
Admin State                : Enable
Message Time Interval(Sec): 10
Device ID(local)           : 00-24-63-04-2A-80
Device Name(local)         : FLEX24-10G
Bidirectional state        : Indeterminant

No neighbor cache information stored
---------------------

GigabitEthernet 1/2
----------------------------------------------------------------------
UDLD Mode                  : Disable
Admin State                : Disable
Message Time Interval(Sec): 7
Device ID(local)           : 00-24-63-04-2A-80
Device Name(local)         : FLEX24-10G
Bidirectional state        : Indeterminant

No neighbor cache information stored
         ------------------------------OUTPUT TRUNCATED------------------------------
```

Chapter 16: Loop Protection

Introduction

Loop Protection works in conjunction with Spanning Tree to ensure that a loop free network is present. Loop Protection is enabled globally and at the interface level and monitors the presence of BPDUs on Loop Protection-enabled interfaces.

When an interface enabled with loop-protection stops receiving BPDU's from its designated port, the interface will not transition into the forwarding state. Typically, when an interface stops receiving BPDUs from its directly connected neighbor it will assume that there is no longer a switch on the other side of the link and will place the interface into a forwarding mode.

Loop Protection-enabled interfaces transition to a loop-inconsistent state when they no longer receive BPDUs. If the interface recovers and begins to receive BPDUs, the interface will transition into a blocking state.

Loop-protection should be enabled on all switch interfaces which have a possibility of becoming root or designated ports. When loop-protection is enabled on an interface, an action and transmission-mode can also be configured.

The action is configured to create a log or shutdown the interface when a loop is detected.

Configuration

Loop Protection must be enabled from Global Configuration and from Interface Configuration.

Enabling Loop Protection Globally

	Command	Explanation
Step 1	configure terminal	Enter Global Configuration mode.
Step 2	loop-protect	Enable Loop Protection.
Step 3	loop-protect shutdown-time <0-604800>	**(Optional)** Configure the Shutdown Time in seconds. The Shutdown Time is the amount of time in which an interface will be kept disabled in the event a loop is detected on that interface. Valid values are from 0 to 604800 seconds (7 days). The default value is 180 seconds.
Step 4	loop-protect transmit-time <1-10>	**(Optional)** Configure how often loop protection PDUs are sent on each loop protection-enabled interface. By default, loop protection PDUs are sent every 5 seconds with valid values being from 1 to 10 seconds.

Step 5	end	**(Optional)** Return to Privileged EXEC mode.
Step 6	copy running-config startup-config	**(Optional)** Copy the contents of the running-config to the startup-config.

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# loop-protect
FLEX24-10G(config)# loop-protect shutdown-time 300
FLEX24-10G(config)# loop-protect transmit-time 3
FLEX24-10G(config)# end
FLEX24-10G# copy running-config startup-config
Building configuration...
% Saving 2132 bytes to flash:startup-config
FLEX24-10G#
```

Enabling Loop Protection at the Interface Level

	Command	Explanation
Step 1	configure terminal	Enter Global Configuration mode.
Step 2	interface {*, GigabitEthernet <1/1-24>, 10GigabitEthernet<1/1-2>}	Enter Interface Configuration mode for the interface to configure with loop protection.
Step 3	loop-protect	Enable Loop Protection.
Step 4	loop-protect action {log | shutdown | log shutdown | shutdown log}	**(Optional)** Configure the action taken when a loop is detected on the interface. **log:** Generate a log message. **shutdown:** Shutdown the interface. **log shutdown** or **shutdown log:** Generate a log message and shutdown the interface.
Step 5	loop-protect tx-mode	**(Optional)** Configure whether the interface should actively generate loop detection PDUs or passively look for PDUs from neighbor switches. If **tx-mode** is present, the interface will actively generate PDUs.
Step 6	end	**(Optional)** Return to Privileged EXEC mode.
Step 7	copy running-config startup-config	**(Optional)** Copy the contents of the running-config to the startup-config.

Verification

Loop Protection configuration details can be displayed using the **show loop-protect** command from Privileged EXEC mode.

show loop-protect [interface {*, GigabitEthernet <1/1-24>, 10GigabitEthernet<1/1-2>}]: Displays both Global Loop Protection details as well as interface specific loop protection configuration details. Output can be filtered to only include loop protection details pertaining to a specific interface or interfaces.

```
FLEX24-10G# show loop-protect interface ?
    *                    All switches or All ports
    GigabitEthernet      1 Gigabit Ethernet Port
    10GigabitEthernet    10 Gigabit Ethernet Port
FLEX24-10G# show loop-protect

Loop Protection Configuration
======================================
Loop Protection   : Enable
Transmission Time : 3 sec
Shutdown Time     : 300 sec

GigabitEthernet 1/1
------------------------------
    Loop protect mode is enabled.
    Action is shutdown.
    Transmit mode is enabled.
    No loop.
    The number of loops is 0.
    Status is up.

GigabitEthernet 1/2
------------------------------
    Loop protect mode is enabled.
    Action is shutdown.
    Transmit mode is enabled.
    No loop.
    The number of loops is 0.
    Status is down.
     ----------------------------------OUTPUT TRUNCATED----------------------------------
```

Chapter 17: SNMP

Introduction

The Simple Network Management Protocol (SNMP) is an internet standard used to collect various information from network devices which is sent to be analyzed by an SNMP manager. An SNMP manager is a centralized software application which can be used to monitor all devices on a network running SNMP.

In an SNMP environment, all devices which the SNMP manager is polling are running an SNMP agent. The SNMP agent is software running on top of the device which reports information to the manager. Every client running an SNMP agent will also contain its own Management Information Base (MIB). The MIB is a database containing several variables which can be requested or changed by the SNMP manager. Example variables contained in the MIB are CPU Load, Temperature, Linkdowns, Port Status, etc.

Devices running an SNMP agent will send device information to the SNMP manager in the form of SNMP traps and informs.

SNMP traps are not explicitly requested by the manager. Traps are used by the SNMP agent to notify the manager of significant events occurring on the agent.

Informs were introduced in SNMPv2 and are used in manager-to-manager and agent-to-manager communications. With SNMPv1, Traps were used for manager-to-manager communications. Because SNMP communicates over UDP, delivery of these traps was not guaranteed. This was fixed with the introduction of Informs because Informs provide an acknowledgement to the sender upon successful delivery.

SNMP Versions

There are three versions of SNMP, with SNMPv3 being the latest. The ways in which SNMP has handled key features such as Authentication, Privacy, and Access Control have changed quite substantially over the versions. The FLEX24-10G can run all three versions of SNMP at once.

SNMPv1

In contrast to SNMPv2c and SNMPv3, SNMPv1 provides very poor security. SNMPv1 uses an identical cleartext community secret which much be configured on both the agent and the manager for messages to be exchanged.

SNMPv1 does not support encryption of any kind.

SNMPv2c

SNMPv2c is identical to SNMPv1 with the exception that version 2c includes 64-bit counters. Most network devices today will support SNMPv2c.

A major addition with SNMPv2c over SNMPv1 is the presence of Informs. Informs offer the same functionality as Traps, however, Informs require an acknowledgement to be sent by the receiver. If the sender does not receive an acknowledgement, it will resend the Inform.

SNMPv3

SNMPv3 offers enhanced security over SNMP versions 1 and 2c. SNMPv3 includes an Engine-ID which is used to uniquely identify the SNMP agent to the SNMP manager. The Engine-ID is a 10-64-character hexadecimal string which must be configured on both the agent and the manager.

SNMPv3 provides security in the forms of Authentication and Privacy.

Authentication is used by the SNMP manager to confirm the identity of the sender when Traps and Informs are sent. The identity of the sender is verified using the Engine-ID. The FLEX24-10G supports both MD5 and SHA authentication.

Privacy ensures that SNMP Traps and Informs are encrypted such that only the intended recipient can decrypt them. Traps and Informs are encrypted using the Engine-ID. Since the manager and the agent should be the only devices containing the Engine-ID, only they would be able to encrypt/decrypt Traps and Informs. The FLEX24-10G supports both AES and DES privacy encryption.

Authentication and Privacy can be configured in one of three ways:

1. **noAuthnoPriv**: No Authentication or Privacy
2. **authNoPriv**: Authentication without Privacy
3. **AuthPriv**: Authentication with Privacy

One major security addition which was introduced with SNMPv3 are SNMP users and groups.

SNMP users are configured on the switch and can be assigned one of the three security settings above. Once an SNMP user has been created, the user can then be mapped to an SNMPv3 group.

When the FLEX24-10G is running SNMPv3, the administrator must provide the SNMP manager with the username and password of any SNMPv3 users.

Feature	SNMPv1	SNMPv2c	SNMPv3
Traps	Supported	Supported	Supported
Informs	Not Supported	Supported	Supported
Bulk Retrieval	Not Supported	Supported	Supported
Access Control	SNMP Community String/MIB View	SNMP Community String/MIB View	SNMP User/Group Combination
Authentication/Privacy	Plaintext authentication using community strings	Plaintext authentication using community strings	Supports authentication and privacy

SNMPv3 User and Group Configuration

	Command	Explanation
Step 1	configure terminal	Enter Global Configuration mode.
Step 2	snmp-server	Enable SNMP. By default, SNMP is enabled by default so this command may not be necessary.
Step 3	snmp-server engine-id local <engine_id> **Example:** snmp-server engine-id local 1234567890	**(Optional)** An Engine-ID is only required when using SNMPv3. Configure a local Engine-ID on the switch. **<engine_id>** must be a 10-64 character hexadecimal string. The Engine-ID must be unique among all SNMP agents and the manager must be configured with a matching Engine-ID.
Step 4	snmp-server user <username> engine-id <engine_id> [md5 | sha] [encrypted] [<password>] priv [aes | des] [encrypted] [<password>] Example: snmp-server testuser engine-id 1234567890 sha password1 priv des password2	Create an SNMPv3 user and associate them with the switch's engine-id. A user can be configured to use no authentication/privacy, authentication, or authentication and privacy. Supported authentication algorithms are md5 and sha. Supported privacy/encryption algorithms are AES and DES.
Step 5	snmp-server security-to-group model [v1 | v2c | v3] name <username> group <group_name>	Map an SNMP user to a SNMP group. If **group_name** is not created, it will be created upon execution of this command. **[v1 | v2c | v3]** indicates the security model that the group will belong to.
Step 6	end	**(Optional)** Return to Privileged EXEC mode.
Step 7	copy running-config startup-config	**(Optional)** Overwrite the startup-config with the current entries of the running-config.

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# snmp-server
```

```
FLEX24-10G(config)# snmp-server engine-id local 1234567890
FLEX24-10G(config)# snmp-server John 1234567890 sha supersecurepassword priv des
evermoresecurepassword
FLEX24-10G(config)# snmp-server security-to-group model v3 name John group IT
FLEX24-10G(config)# end
FLEX24-10G# copy running-config startup-config
Building configuration...
% Saving 3466 bytes to flash:startup-config
FLEX24-10G#
```

SNMPv3 Access Configuration

SNMP access configuration allows security settings to be applied to SNMP groups. By default, the FLEX24-10G contains two groups, default_ro_group, and default_rw_group, two SNMPv1 users: public, and private, and two SNMPv2c users: public, and private.

The default_ro_group contains both public users while the default_rw_group contains both private users.

The below steps illustrate how to apply security settings to any SNMP group present on the FLEX24-10G.

	Command	**Explanation**
Step 1	configure terminal	Enter Global Configuration mode.
Step 2	snmp-server access <group_name> model {any | v1 | v2c | v3} level {auth | noauth | priv} [read | write] [<read_view_name>] [<write_view_name>]	Configure **<group_name>** to be either a v1, v2c, or (inclusive) v3 group. Authentication and Privacy settings can be configured with the **auth, noauth,** or **priv** parameters. **(Optional)** The **read** and **write** parameters allow for SNMP groups to be mapped to no view, the default_view, or a user created view.
Step 3	end	**(Optional)** Return to Privileged EXEC mode.
Step 4	copy running-config startup-config	**(Optional)** Overwrite the startup-config with the current entries of the running-config.

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# snmp-server access IT model any level auth
FLEX24-10G(config)# end
FLEX24-10G# copy running-config startup-config
Building configuration...
% Saving 3511 bytes to flash:startup-config
FLEX24-10G#
```

SNMPv3 View Configuration

An SNMP view is a family of view subtrees within the MIB hierarchy. A subtree is identified by the pairing of an OID to a bit string mask value. Every MIB view is defined by two sets of subtrees. These subtrees can be included or excluded from the overall MIB view.

The OID subtree specified identifies the root of the subtree to be added to the named view.

	Command	**Explanation**
Step 1	configure terminal	Enter Global Configuration mode.
Step 2	snmp-server view <view_name> <oid_subtree> {include | exclude}	Create a new SNMPv3 view. The **<oid_subtree>** value ranges from 1 to 128 entries in length. The **{include | exclude}** option specifies whether the view subtree should be included or excluded for the MIB view.
Step 3	end	**(Optional)** Return to Privileged EXEC mode.
Step 4	copy running-config startup-config	**(Optional)** Overwrite the startup-config with the current entries of the running-config.

SNMPv1/2c Community Configuration

Custom SNMP community secrets can be created and then applied to a single IP address within a range. A wildcard range of 0.0.0.0 and a wildcard mask of 0.0.0.0 will match all IP addresses.

Community secrets are used as a handshake between the SNMP agent and the SNMP manager. Devices which are not operating in SNMPv3 will not contain an Engine-ID so they resort to community secrets.

By default, the switch contains a public (read-only) community secret of “public” and a private (read-write) community secret of “private”. When an SNMP manager is provided with a read-only secret, the manager will only be able to read information from the FLEX24-10G. In contrast, when the read-write secret is provided, the manager is granted permission by the switch’s agent to modify device settings.

Configuring a Community Name and Secret

	Command	**Explanation**
Step 1	configure terminal	Enter Global Configuration mode.
Step 2	snmp-server community <community_name> { <community_secret> | encrypted <encrypted_community_secret> | ip-range <ipv4_address> <ipv4_netmask> { <community_secret> | encrypted <encrypted_community_secret>} | ipv6-range	Create an SNMP community name and secret. Additionally, configure a source IPv4/IPv6 address and prefix. **Note:** The IP address must be the network address of the network.

	<ipv6_subnet> {community_secret> | encrypted <encrypted_community_secret>}}	If **<community_name>** does not exist, it will be created upon execution of the command.
Step 3	end	**(Optional)** Return to Privileged EXEC mode.
Step 4	copy running-config startup-config	**(Optional)** Overwrite the startup-config with the current entries of the running-config.

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# snmp-server community testcommunity ip-range 192.168.100.1 255.255.255.255
testsecret
FLEX24-10G(config)# end
FLEX24-10G# copy running-config startup-config
Building configuration...
% Saving 3258 bytes to flash:startup-config
FLEX24-10G#
```

SNMP Trap Configuration

Destinations

Detailed information can be configured regarding how the switch will deliver SNMP traps. Information such as trap destination IP address, destination port, retry count, and timeout period can all be set on the switch. Traps can also be disabled entirely.

Trap destination configurations can be modified using the below configuration commands.

	Command	**Explanation**
Step 1	configure terminal	Enter Global Configuration mode.
Step 2	snmp-server host <config_name> **Note:** Prompt will change to: FLEX24-10G(config-snmps-host)#	Enter SNMP-Host Configuration mode.
Step 3	version {v1 | v2 | v3} engineID <engine_id> <security_name>	Set the SNMP trap version.
Step 4	host {<domain_name> | <ipv4_address> | <ipv6_address>} [<udp_trap_port>] [traps | informs]	Specify the IP address or hostname in which SNMP traps or informs will be sent to. **Note:** The **traps** and **informs** keywords cannot be used together.
Step 5	informs retries <0-255> timeout <0-2147>	**(Optional)** Set the inform retry count and timeout period. The retry value ranges from 0 to 255, inclusive.

		The timeout period ranges from 0 to 2147 seconds.
Step 6	shutdown	**(Optional)** Disable SNMP trap configuration.
Step 7	end	**(Optional)** Return to Privileged EXEC mode.
Step 8	copy running-config startup-config	**(Optional)** Overwrite the startup-config with the current entries of the running-config.

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# snmp-server host TrapServer
FLEX24-10G(config-snmps-host)# version v3 engineID 1234567890 public
FLEX24-10G(config-snmps-host)# host 192.168.100.1 162 traps
FLEX24-10G(config-snmps-host)# informs retries 10 timeout 300
FLEX24-10G(config-snmps-host)# shutdown
FLEX24-10G(config-snmps-host)# end
FLEX24-10G# copy running-config startup-config
Building configuration...
% Saving 3642 bytes to flash:startup-config
FLEX24-10G#
```

Sources

Additionally, SNMP Trap Sources can also be configured. Internal switch filters can be created such that if the switch produces a trap which matches the source found in a filter, the trap can either be sent to the manager or dropped by the switch.

For example, a trap source filter could be created matching only traps with a trap source of linkUp. This filter can then specify whether the switch should send the trap or not. If the switch is configured to send the trap, a subset OID can be specified for the entry. This subset OID will specifically depend on the trap source and should not begin with an asterisk.
For example, the ifIndex is the subset OID of linkUp and linkDown so the subset OID should be set appropriately.

A valid subset OID consists of one or more numbers, or asterisks, separated by periods. The first character of the subset OID cannot be an asterisk, and the maximum length of the subset OID cannot exceed 128 values.

	Command	Explanation
Step 1	configure terminal	Enter Global Configuration mode.

Step 2	snmp-server trap <trap_source> [id] <0-127> [index_filter] {include | exclude}	Create a trap source. Only the trap source and switch behavior must be specified. Valid entries for **<trap_source>** are 'alarmTrapStatus', 'authenticationFailure', 'bpdu', 'coldStart', 'entConfigChange', 'fallingAlarm', 'fan', 'ipTrapInterfacesLink', 'linkDown', 'linkUp', 'linkdown_timeout', 'lldpRemTablesChange', 'newRoot', 'psecTrapGlobalsMain', 'psecTrapInterfaces', 'risingAlarm', 'rx_timeout', 'topologyChange', and 'warmStart' **{include | exclude}** specifies whether the trap should be sent or dropped by the switch **(Optional)** The subset OID is an optional parameter and does not need to be specified in the snmp-server trap command.
Step 3	end	**(Optional)** Return to Privileged EXEC mode.
Step 4	copy running-config startup-config	**(Optional)** Overwrite the startup-config with the current entries of the running-config.

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# snmp-server trap alarmTrapStatus id 0
FLEX24-10G(config)# snmp-server trap coldstart ?
    <word255>     OID to use as index filter
    id            Use specific filter ID
    <cr>
FLEX24-10G(config)# snmp-server trap coldstart
FLEX24-10G(config)# snmp-server trap newRoot 1.2.3.4.*.6.7.8.9.10 exclude
FLEX24-10G(config)# end
FLEX24-10G# copy running-config startup-config
Building configuration...
% Saving 2165 bytes to flash:startup-config
FLEX24-10G#
```

Verification

General SNMP configuration information be displayed using the **show snmp** command.

Below are outputs from a factory defaulted switch showing the default SNMP configuration.

```
FLEX24-10G# show snmp

SNMP Configuration
SNMP Mode   : enabled
Engine ID   : 800019cb03002463042a80
```

```
SNMPv3 Communities Table:
Community/Security Name : public
Source IP               : 0.0.0.0/0
Community secret        : public

Community/Security Name : private
Source IP               : 0.0.0.0/0
Community secret        : private

SNMPv3 Users Table:

SNMPv3 Groups Table;
Security Model : v1
Security Name  : public
Group Name     : default_ro_group

Security Model : v1
Security Name  : private
Group Name     : default_rw_group

Security Model : v2c
Security Name  : public
Group Name     : default_ro_group

Security Model : v2c
Security Name  : private
Group Name     : default_rw_group


SNMPv3 Accesses Table:
Group Name       : default_ro_group
Security Model   : any
Security Level   : NoAuth, NoPriv
Read View Name   : default_view
Write View Name  : <no writeview specified>

Group Name       : default_rw_group
Security Model   : any
Security Level   : NoAuth, NoPriv
Read View Name   : default_view
Write View Name  : default_view


SNMPv3 Views Table:
View Name   : default_view
OID Subtree : .1
View Type   : included
```

```
FLEX24-10G#
```

More detailed SNMP information can be viewed by adding an optional parameter to the trailing end of the **show snmp** command.

```
FLEX24-10G# show snmp ?
    |                     Output modifiers
    access                access configuration
    community             Community
    host                  Set SNMP host's configurations
    mib                   MIB (Management Information Base)
    security-to-group     security-to-group configuration
    trap                  Set SNMP host's configurations
    user                  User
    view                  MIB view configuration
    <cr>

FLEX24-10G# show snmp
```

show snmp access [group_name]: By default, the switch contains two access groups. One read-only group (default_ro_group) and one read-write group (default_rw_group).

```
FLEX24-10G# show snmp access
Group Name        : default_ro_group
Security Model    : any
Security Level    : NoAuth, NoPriv
Read View Name    : default_view
Write View Name   : <no writeview specified>

Group Name        : default_rw_group
Security Model    : any
Security Level    : NoAuth, NoPriv
Read View Name    : default_view
Write View Name   : default_view

FLEX24-10G#
```

show snmp community [community_name]: Displays all SNMP communities, community secrets, and IP ranges which have access to the community.

```
FLEX24-10G# show snmp community
Community/Security Name : public
Source IP               : 0.0.0.0/0
Community secret        : public

Community/Security Name : private
Source IP               : 0.0.0.0/0
Community secret        : private
```

```
FLEX24-10G#
```

show snmp host [host_configuration]: If an SNMP host has been configured, its details will be displayed here. By default, no SNMP host is configured.

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# snmp-server host Testing
FLEX24(config-snmps-host)# host 192.168.1.2
FLEX24(config-snmps-host)# version v3 engineID 1234567890
FLEX24(config-snmps-host)# ^Z
FLEX24-10G# show snmp host
Trap Testing (ID:0) is disabled
Community        : public
Destination Host: 192.168.1.2
UDP Port         : 162
Version          : V3
Inform Mode      : disabled
Inform Timeout   : 3
Inform Retry     : 5
Engine ID        : 1234567890
Security Name    : None

FLEX24-10G#
```

show snmp mib context: Shows all the root OID's contained on the switch as well as the subtrees with their MIB's. Output is quite verbose.

```
FLEX24-10G# show snmp mib context
BRIDGE-MIB :
    - dot1dBase (.1.3.6.1.2.1.17.1)
    - dot1dTp (.1.3.6.1.2.1.17.4)
ENTITY-MIB :
    - entityMIBObjects (.1.3.6.1.2.1.47.1)
EtherLike-MIB :
    - transmission (.1.3.6.1.2.1.10)
IEEE8021-BRIDGE-MIB :
    - ieee8021BridgeBasePortTable (.1.3.111.2.802.1.1.2.1.1.4)
IEEE8021-MSTP-MIB :
    - ieee8021MstpMib (.1.3.111.2.802.1.1.6)
IEEE8021-PAE-MIB :
    - ieee8021paeMIB (.1.0.8802.1.1.1.1)
IEEE8021-Q-BRIDGE-MIB :
    - ieee8021QBridgeMib (.1.3.111.2.802.1.1.4)
IEEE8023-LAG-MIB :
    - lagMIBObjects (.1.2.840.10006.300.43.1)
IF-MIB :
    - ifMIB (.1.3.6.1.2.1.31)
IP-FORWARD-MIB :
```

```
- ipForward (.1.3.6.1.2.1.4.24)
  --------------------------------OUTPUT TRUNCATED--------------------------------
```

show snmp mib ifmib ifIndex [aggregation] [port] [vlan]: Shows the MIB database for all physical and logical interfaces on the switch. This includes all VLANs, aggregations, and physical interfaces.

```
FLEX24-10G# show snmp mib ifmib ifIndex
ifIndex     ifDescr                               Interface
----------  ------------------------------------  ---------
         1  VLAN    1                             vlan 1
   1000001  Switch  1 - Port  1                   GigabitEthernet 1/1
   1000002  Switch  1 - Port  2                   GigabitEthernet 1/2
   1000003  Switch  1 - Port  3                   GigabitEthernet 1/3
   1000004  Switch  1 - Port  4                   GigabitEthernet 1/4
   1000005  Switch  1 - Port  5                   GigabitEthernet 1/5
   1000006  Switch  1 - Port  6                   GigabitEthernet 1/6
   1000007  Switch  1 - Port  7                   GigabitEthernet 1/7
   1000008  Switch  1 - Port  8                   GigabitEthernet 1/8
   1000009  Switch  1 - Port  9                   GigabitEthernet 1/9
   1000010  Switch  1 - Port 10                   GigabitEthernet 1/10
   1000011  Switch  1 - Port 11                   GigabitEthernet 1/11
   1000012  Switch  1 - Port 12                   GigabitEthernet 1/12
   1000013  Switch  1 - Port 13                   GigabitEthernet 1/13
   1000014  Switch  1 - Port 14                   GigabitEthernet 1/14
   1000015  Switch  1 - Port 15                   GigabitEthernet 1/15
   1000016  Switch  1 - Port 16                   GigabitEthernet 1/16
   1000017  Switch  1 - Port 17                   GigabitEthernet 1/17
   1000018  Switch  1 - Port 18                   GigabitEthernet 1/18
   1000019  Switch  1 - Port 19                   GigabitEthernet 1/19
   1000020  Switch  1 - Port 20                   GigabitEthernet 1/20
   1000021  Switch  1 - Port 21                   GigabitEthernet 1/21
   1000022  Switch  1 - Port 22                   GigabitEthernet 1/22
   1000023  Switch  1 - Port 23                   GigabitEthernet 1/23
   1000024  Switch  1 - Port 24                   GigabitEthernet 1/24
   1000025  Switch  1 - Port 25                   GigabitEthernet 1/25
   1000026  Switch  1 - Port 26                   10GigabitEthernet 1/1
   1000027  Switch  1 - Port 27                   10GigabitEthernet 1/2
FLEX24-10G#
```

show snmp security-to-group [v1| v2c | v3] [security_username]: Shows all SNMP users contained within the switch, their SNMP version, and their respective group. By default, four SNMP users exist, a public and private user for both SNMPv1 and SNMPv2c.

```
FLEX24-10G# show snmp security-to-group
Security Model : v1
Security Name  : public
Group Name     : default_ro_group

Security Model : v1
```

```
Security Name  : private
Group Name     : default_rw_group

Security Model : v2c
Security Name  : public
Group Name     : default_ro_group

Security Model : v2c
Security Name  : private
Group Name     : default_rw_group

FLEX24-10G#
```

show snmp trap [trap_source]: By default, no SNMP trap sources are configured.

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# snmp-server trap ?
    <cword>    Valid words are 'alarmTrapStatus' 'authenticationFailure' 'bpdu'
               'coldStart' 'entConfigChange' 'fallingAlarm' 'fan'
               'ipTrapInterfacesLink' 'linkDown' 'linkUp' 'linkdown_timeout'
               'lldpRemTablesChange' 'newRoot' 'psecTrapGlobalsMain'
               'psecTrapInterfaces' 'risingAlarm' 'rx_timeout' 'topologyChange'
               'warmStart'
FLEX24-10G(config)# snmp-server trap fan 1.2.3.4.5 exclude
FLEX24-10G(config)# snmp-server trap bpdu 6.7.8.9.10 exclude
FLEX24-10G(config)# snmp-server trap linkDown 1.2.3.4.5.6.7.8.9.10 include
FLEX24-10G(config)# ^Z
```

FLEX24-10G# show snmp trap

```
Trap fan (ID:0) enabled with filters
 .14417920.2.3.4 excluded (ID:0)

Trap bpdu (ID:1) enabled with filters
 .14417920.7.8.9 excluded (ID:0)

Trap linkDown (ID:2) enabled with filters
 .14417920.2.3.4.5.6.7.8.9 included (ID:0)

FLEX24-10G#
```

show snmp user [username] [engine-id]: Show all non-default users. By default, this command will return nothing as there are no custom users created.

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# $user engine-id 1234567890 sha password1 priv des password2
FLEX24-10G(config)# ^Z
```

FLEX24-10G# show snmp user

```
User/Security Name      : testuser
Engine ID               : 1234567890
Security Level          : Auth, Priv
Authentication Protocol : SHA
Privacy Protocol        : DES

FLEX24-10G#
```

show snmp view [mib_view_name]: Shows the default MIB view and any custom MIB views. By convention, the only created view is *default_view* whose root is the parent of the tree (.1)

```
FLEX24-10G# show snmp view
View Name   : default_view
OID Subtree : .1
View Type   : included

FLEX24-10G#
```

Chapter 18: Access Control Lists (ACLs)

Introduction

Access Control Lists exist as a way for the switch to filter ingress traffic on a switch interface. ACLs are configured on a per-interface basis and will examine the contents of the packet header belonging to ingress traffic. If the contents in the header match the contents in the ACL, the switch will perform an action on the packet (i.e. either allow or drop the packet).

ACLs support a vast amount of customization, much more than will typically be required. Access Control Lists are made up of Access Control Entries (ACEs). Each entry in an ACL contains its own filter which is checked against the contents of ingress traffic to see if a match exists. Once a match has been made all access control entries below the entry which made the match are ignored.

The last entry of an ACL will always be an implicit allow. This implicit allow is not seen in the running-config and is not configured by the administrator. If ingress traffic does not match any of the ACEs in the ACL, the implicit allow will kick in and allow the traffic to be processed by the switch.

The FLEX24-10G contains a single global ACL. Up to 512 ACEs can be configured.

Configuration

All ACEs are configured from Global Configuration.

To create an ACE, begin the command with **access-list ace [update] <1-512>.** The optional **[update]** keyword is used when the ACE already exists, but needs to be updated.

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# access-list ace ?
    <1-512>     ACE ID
    update      Update an existing ACE
FLEX24-10G(config)# access-list ace 1 ?
    action          Access list action
    dmac-type       The type of destination MAC address
    frame-type      Frame type
    ingress         Ingress
    logging         Logging frame information. Note: The logging feature only
                    works when the packet length is less than 1518 (without
                    VLAN tags) and the System Log memory size and logging rate
                    is limited.
    mirror          Mirror frame to destination mirror port
    next            insert the current ACE before the next ACE ID
    policy          Policy
    rate-limiter    Rate limiter
    redirect        Redirect frame to specific port
    shutdown        Shutdown incoming port. The shutdown feature only works
                    when the packet length is less than 1518 (without VLAN
                    tags).
    tag             Tag
    tag-priority    Tag priority
    vid             VID field
    <cr>
```

```
FLEX24-10G(config)# access-list ace 1
```

Access List Entry Parameters Explained

Action

The action parameter specifies the action to take when a frame matches an access control entry.

Available actions are:

- **Permit:** Frames which match the ACE are granted permission and are processed by the switch.
- **Deny:** Frames which match the ACE are dropped by the switch. Frames which are dropped can optionally be redirected to another interface. See redirect.
- **Filter:** Frames which match the ACE are filtered to another interface on the switch.

Parameter Syntax

The below snippet is used to demonstrate the syntax of the **action** parameter.

access-list ace 1 **action {permit | deny | filter interface {*, GigabitEthernet <1/1-24>, 10GigabitEthernet<1/1-2>}}**

```
FLEX24-10G(config)# access-list ace 1 action ?
    deny      Deny
    filter    Filter
    permit    Permit
FLEX24-10G(config)# access-list ace 1 action filter ?
    interface    Select an interface to configure
FLEX24-10G(config)# access-list ace 1 action filter interface GigabitEthernet 1/1 ?
    *                    All switches or All ports
    GigabitEthernet      1 Gigabit Ethernet Port
    10GigabitEthernet    10 Gigabit Ethernet Port
    dmac-type            The type of destination MAC address
    frame-type           Frame type
    ingress              Ingress
    logging              Logging frame information. Note: The logging feature
                         only works when the packet length is less than 1518
                         (without VLAN tags) and the System Log memory size and
                         logging rate is limited.
    mirror               Mirror frame to destination mirror port
    next                 insert the current ACE before the next ACE ID
    policy               Policy
    rate-limiter         Rate limiter
    redirect             Redirect frame to specific port
    shutdown             Shutdown incoming port. The shutdown feature only
                         works when the packet length is less than 1518
                         (without VLAN tags).
    tag                  Tag
    tag-priority         Tag priority
    vid                  VID field
    <cr>
FLEX24-10G(config)# access-list ace 1 action filter interface GigabitEthernet 1/1
```

Source MAC Address Filter

When the frame-type is configured as either EtherType or ARP, a filter can be applied to the Source MAC address of ingress traffic. The Source MAC address filter is applied to an ACE to check ingress traffic for a specific MAC address.

Parameter Syntax

The following snippet is used to demonstrate the syntax of the **smac** parameter.

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# access-list ace 1 frame-type arp ?
    action          Access list action
    arp-flag        ARP flag
    arp-opcode      ARP/RARP opcode field
    dip             Destination IP address field
    dmac-type       The type of destination MAC address
    ingress         Ingress
    logging         Logging frame information. Note: The logging feature only
                    works when the packet length is less than 1518 (without
                    VLAN tags) and the System Log memory size and logging rate
                    is limited.
    mirror          Mirror frame to destination mirror port
    next            insert the current ACE before the next ACE ID
    policy          Policy
    rate-limiter    Rate limiter
    redirect        Redirect frame to specific port
    shutdown        Shutdown incoming port. The shutdown feature only works
                    when the packet length is less than 1518 (without VLAN
                    tags).
    sip             Source IP address field
    smac            Source MAC address field
    tag             Tag
    tag-priority    Tag priority
FLEX24-10G(config)# access-list ace 1 frame-type arp smac ?
    <mac_addr>    The value of source MAC address field
    any           Don't-care the value of source MAC address field
FLEX24-10G(config)# access-list ace 1 frame-type arp smac 00:0a:95:9d:68:16
FLEX24-10G(config)#
```

Destination MAC Address Type

The destination MAC address type can be configured to examine ingress packets based on their MAC address type.

Available MAC address types are:

- **Any:** No destination MAC filter is applied.

- **Broadcast:** ACE will only match ingress traffic containing a broadcast destination MAC address.
- **Multicast:** ACE will only match ingress traffic containing a multicast destination MAC address.
- **Unicast:** ACE will only match ingress traffic containing a unicast destination MAC address.
- **Specific:** ACE will only match ingress traffic containing a specific destination MAC address.

Note: For the destination MAC address type to be modified, the frame-type must be changed to ARP, an Ethertype, or any IPv4/IPv6 frame type. When the frame-type is set to **etype**, a specific MAC address can be set using the **dmac {<mac_addr> | any}** parameter.

Parameter Syntax

The following snippet is used to demonstrate the syntax of the **dmac-type** parameter.

access-list ace 1 **dmac-type {any | broadcast | multicast | unicast}**

```
FLEX24-10G(config)# access-list ace 1 dmac-type ?
    any           Don't-care the type of destination MAC address
    broadcast     Broadcast destination MAC address
    multicast     Multicast destination MAC address
    unicast       Unicast destination MAC address
FLEX24-10G(config)# access-list ace 1 dmac-type
```

When the frame-type is set to **etype**, a specific MAC address can be set as follows:

```
FLEX24-10G(config)# access-list ace 1 frame-type etype dmac ?
    <mac_addr>     The value of destination MAC address field
    any            Don't-care the value of destination MAC address field
FLEX24-10G(config)# access-list ace 1 frame-type etype dmac 00:0a:95:9d:68:16 ?
    action           Access list action
    dmac-type        The type of destination MAC address
    etype-value      EtherType value
    ingress          Ingress
    logging          Logging frame information. Note: The logging feature only
  -------------------------------------OUTPUT TRUNCATED------------------------------------
```

Frame Type

The frame type can be configured to examine ingress packets based on their frame type.

Available frame types are:

- **Any:** ACE will match ingress traffic regardless of the frame-type.
- **ARP:** ACE will match only ingress ARP traffic.
- **Etype:** ACE will match only ingress traffic with a specific EtherType value.
- **IPv4:** ACE will match only IPv4 ingress traffic.
- **IPv4-ICMP:** ACE will match only IPv4 ICMP ingress traffic.
- **IPv4-TCP:** ACE will match only IPv4 TCP ingress traffic.
- **IPv4-UDP:** ACE will match only IPv4 UDP ingress traffic.
- **IPv6:** ACE will match only IPv6 ingress traffic.
- **IPv6-ICMP:** ACE will match only IPv6 ICMP ingress traffic.

- **IPv6-TCP:** ACE will match only IPv6 TCP ingress traffic.
- **IPv6-UDP:** ACE will match only IPv6 UDP ingress traffic.

Note: When the frame-type is set to **etype**, a specific EtherType can be set using the **etype-value {<ethertype> | any}** parameter.

ARP ACL Parameters

When the frame-type has been set to detect ARP packets, additional ARP parameters can be set in the ACE. The following ARP properties can be configured within an ACE:

- **ARP/RARP Status:** Match the ARP frame based on the status of the ARP/RARP opcode flag. Configured with the **arp {arp-ether {<0-1> | any} | arp-ip {<0-1> | any} | arp-len {<0-1> | any} | arp-opcode {any | arp | other | rarp}}** parameter.
- **Request/Reply:** Match the ARP frame based on whether it is an ARP/RARP request or reply. Configured with the **arp-request {<0-1> | any}** parameter.
- **Sender IP Filter:** The sender IP filter can be set to a specific host or an entire network. If set to a host, the host's IP address will need to be specified. If set to a network, an IP address and network mask must be specified. When set to **any,** no sender IP filter is configured. Configured with the **arp-smac {<0-1> | any}** parameter.
- **Target IP Filter:** The target IP filter can be set to a specific host or an entire network. If set to a host, the host's IP address will need to be specified. If set to a network, an IP address and network mask must be specified. When set to **any,** no target IP filter is configured.
- **ARP Sender MAC Match:** The ARP Sender MAC Match is either set to **0**, **1**, or **any**. This parameter compares the ARP frame's sender hardware address to the source MAC address. If this parameter is set to 0, a match occurs when the two addresses are not equal. When set to 1, a match occurs when the addresses are equal. A keyword of **any** and the ACE does not care whether the addresses match.
- **RARP Target MAC Match:** Like the ARP sender MAC match except here the ARP frame's target hardware address is being compared to the target MAC address.
- **IP/Ethernet Length:** The IP/Ethernet Length parameter examines the ARP/RARP frame's hardware address length and protocol address length and compares them to 0x06 (Ethernet) and 0x04 (IPv4) respectively. If this parameter is set to 0, a match occurs when the two values are not equal. When set to 1, a match occurs when the values are equal. A keyword of **any** and the ACE does not care whether the values match.
- **Ethernet:** Examines the ARP/RARP frame's hardware address space settings. Valid values for this parameter are **0**, **1**, and **any**. A value of 0 matches all ARP/RARP frames whose HLD is not equal to 1 (Ethernet). A value of 1 matches all ARP/RARP frames whose HLD is equal to 1 (Ethernet). A keyword of **any** and the ACE does not care about the value of the HLD.
- **IP:** Examines the ARP/RARP frame's hardware address space settings. Valid values for this parameter are **0**, **1**, and **any**. A value of 0 matches all ARP/RARP frames whose PRO is not equal to 0x800 (IP). A value of 1 matches all ARP/RARP frames whose PRO is equal to 0x800 (IP). A keyword of **any** and the ACE does not care about the value of the PRO.

Sample ACE with all ARP Parameters

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# access-list ace 5 frame-type arp sip 192.168.100.50/32 dip
192.168.100.30/32 arp-flag arp-smac 1 arp-tmac 1 arp-len 1 arp-ip 1 arp-ether 0 arp-request 1
arp-opcode other
FLEX24-10G(config)# end
FLEX24-10G#
```

From the above snippet, ACE's can become very long quite quickly. When creating ACE's, it is best to be comfortable using the switch's context sensitive help.

IPv4 ACL Parameters

When the frame-type has been set to **ipv4, ipv4-icmp, ipv4-tcp,** or **ipv4-udp,** several additional parameters can be set. The parameter options available for each IPv4 protocol listed above differ for each type.

IPv4 Frame Types

IPv4

When a frame-type of **ipv4** has been configured the following additional ACE parameters can be set:

- **IP Protocol Filter:** The IP Protocol Filter specifies a protocol number to match within ingress traffic. Valid values are 0 through 255 excluding 1, 6, and 17. 1, 6, and 17 are excluded since they correspond to the IP protocols of ICMP, TCP, and UDP respectively. To filter ICMP, TCP, or UDP IPv4 packets, set the frame-type to **ipv4-icmp, ipv4-tcp,** or **ipv4-udp** respectively. An IP protocol filter of **any** does not discriminate ingress traffic based on IP protocol.
- **IP TTL:** Filter ingress traffic based on the value of the IPv4 TTL field. An **ip-ttl** value of 0 will match all ingress traffic with a TTL value equal to 0. An **ip-ttl** value of 1 will match all ingress traffic with a TTL value greater than 0. An **ip-ttl** value of **any** does not care about the TTL value of ingress traffic.
- **IP Fragment:** The IP Fragment parameter will examine the Fragment Offset field of ingress traffic. Valid values for the **ip-fragment** are **0, 1**, and **any**. An **ip-fragment** value of 0 will match ingress traffic with a Fragment Offset equal to 0. An **ip-fragment** value of 1 will match ingress traffic with a Fragment Offset greater than 0. An **ip-fragment** value of **any** does not care about the Fragment Offset value of ingress traffic.
- **IP Option:** The IP Option parameter examines the Flags field of ingress traffic. Valid values for the **ip-options** are **0**, **1,** and **any**. An **ip-options** value of 0 will not match traffic with Flags set while an **ip-options** value of 1 will only match traffic with Flags set. An **ip-options** value of **any** does not care whether ingress traffic contains Flags.
- **Sender and Target IP Filter:** Identical to the Source and Target IP filter for a frame-type of ARP.

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# access-list ace 1 frame-type ipv4 ip-protocol 23 ip-flag ip-ttl 0 ip-
fragment 1 ip-options 0
FLEX24-10G(config)#
```

IPv4-ICMP

When a frame-type of **ipv4-icmp** has been configured, all the parameters available for a frame-type of **ipv4** are available plus the following:

- **ICMP Type Filter:** An ICMP Type Filter will examine the contents of the Type field within ICMP packets. Valid values for the **icmp-type** parameter are **0 through 255**, or **any**. A value of **any** does not care about the value of Type Field.
- **ICMP Code Filter:** An ICMP Code Filter will examine the contents of the Code field within ICMP packets. Valid values for the **icmp-code** parameter are **0 through 255**, or **any**. A value of **any** does not care about the value of Code Field.

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# access-list ace 1 frame-type ipv4-icmp icmp-code 100 icmp-type 100
FLEX24-10G(config)#
```

IPv4-UDP

When a frame-type of **ipv4-udp** has been configured, all the parameters available for a frame-type of **ipv4** are available plus the following:

- **Source Port Filter:** A Source Port Filter will examine the source port of all ingress segments. If the source port of the traffic is within the configured range of the ACE, a match has been made. Valid values for the **sport** parameter are **0 through 65535**, or **any**.
- **Destination Port Filter:** A Destination Port Filter will examine the destination port of all ingress segments. If the destination port of the traffic is within the configured range of the ACE, a match has been made. Valid values for the **dport** parameter are **0 through 65535**, or **any**.

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# access-list ace 1 frame-type ipv4-udp sport 118 dport ?
    <0-65535>    The value of UDP destination port field
    any          Don't-care the value of UDP destination port field
FLEX24-10G(config)# access-list ace 1 frame-type ipv4-udp sport 118 dport 15
```

IPv4-TCP

When a frame-type of **ipv4-tcp** has been configured, all the parameters available for a frame-type of **ipv4** and **ipv4-udp** are available plus the following:

- **TCP FIN:** The FIN bit denotes whether the sender has finished sending data. Valid values are **0**, **1**, or **any**. A value of 0 will match all ingress packets where the FIN field is not set. A value of 1 will match all ingress packets where the FIN field is set. A value of any will match ingress packets regardless of the status of the FIN field.
- **TCP SYN:** The SYN bit is used for sequence number synchronization. Valid values are **0**, **1**, or **any**. A value of 0 will match all ingress packets where the SYN field is not set. A value of 1 will match all ingress packets where the SYN field is set. A value of any will match ingress packets regardless of the status of the SYN field.

- **TCP RST:** The RST bit is used to terminate the connection when the sender believes there is something wrong with the connection. Valid values are **0**, **1**, or **any**. A value of 0 will match all ingress packets where the RST field is not set. A value of 1 will match all ingress packets where the RST field is set. A value of any will match ingress packets regardless of the status of the RST field.
- **TCP PSH:** The PSH bit indicates whether the data in the PDU should be immediately sent to the application layer. Valid values are **0**, **1**, or **any**. A value of 0 will match all ingress packets where the PSH field is not set. A value of 1 will match all ingress packets where the PSH field is set. A value of any will match ingress packets regardless of the status of the PSH field.
- **TCP ACK:** The ACK bit is used to acknowledge packets which have been successfully received by a host. Valid values are **0**, **1**, or **any**. A value of 0 will match all ingress packets where the ACK field is not set. A value of 1 will match all ingress packets where the ACK field is set. A value of any will match ingress packets regardless of the status of the ACK field.
- **TCP URG:** The URG bit indicates that the packet contains urgent data. Valid values are **0**, **1**, or **any**. A value of 0 will match all ingress packets where the URG field is not set. A value of 1 will match all ingress packets where the URG field is set. A value of any will match ingress packets regardless of the status of the URG field.

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# access-list ace 1 frame-type ipv4-tcp tcp-flag ?
    action          Access list action
    dip             Destination IP address field
    dmac-type       The type of destination MAC address
    dport           TCP destination port field
    ingress         Ingress
    ip-flag         IP flag
    logging         Logging frame information. Note: The logging feature only
                    works when the packet length is less than 1518 (without
                    VLAN tags) and the System Log memory size and logging rate
                    is limited.
    mirror          Mirror frame to destination mirror port
    next            insert the current ACE before the next ACE ID
    policy          Policy
    rate-limiter    Rate limiter
    redirect        Redirect frame to specific port
    shutdown        Shutdown incoming port. The shutdown feature only works
                    when the packet length is less than 1518 (without VLAN
                    tags).
    sip             Source IP address field
    sport           TCP source port field
    tag             Tag
    tag-priority    Tag priority
    tcp-ack         TCP ACK field
    tcp-fin         TCP FIN field
    tcp-psh         TCP PSH field
    tcp-rst         TCP RST field
    tcp-syn         TCP SYN field
    tcp-urg         TCP URG field
    vid             VID field
    <cr>
FLEX24-10G(config)# access-list ace 1 frame-type ipv4-tcp tcp-flag tcp-fin 0 tcp-syn 1 tcp-rst
1 tcp-psh 0 tcp-ack 1 tcp-urg 1
```

IPv6 ACL Parameters

ACEs which filter ingress IPv6 traffic are configured in much the same way as ACEs which filter IPv4 traffic. Just as an ACE can filter TCP, UDP, and ICMP IPv4 traffic, TCP, UDP, and ICMP IPv6 traffic can also be filtered.

The IPv6 frame-type is configured with the **frame-type {ipv6 | ipv6-icmp | ipv6-tcp | ipv6-udp}** parameter.

IPv6 Frame Types

IPv6

When a frame-type of **ipv6** has been configured, the following additional ACE parameters can be set:

- **Source IP Filter:** The source IP filter works in the same way as IPv4 with the exception that an IPv6 address must be specified. To configure an IPv6 source IP filter, a 32-bit IP address and bitmask must be provided.
- **Hop Limit:** The IPv6 hop-limit replaces the IPv4 TTL value. Valid values for the hop-limit parameter are **0**, **1**, or **any**. A hop-limit of 0 will match ingress traffic with a hop-limit of 0. A hop-limit of 1 will match ingress traffic with a hop-limit greater than 0. A hop-limit of any does not care about the hop-limit of ingress traffic.

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# access-list ace 1 frame-type ipv6 sip 2001::3 sip-bitmask 0xFFFFFFFE hop-
limit 1
```

IPv6-ICMP

When a frame-type of **ipv6-icmp** has been configured all the parameters available for a frame-type of **ipv6** are available plus the following:

- **ICMP Type Filter:** An ICMP Type Filter will examine the contents of the Type field within ICMP packets. Valid values for the **icmp-type** parameter are **0 through 255**, or **any**. A value of any does not care about the value of the Type Field.
- **ICMP Code Filter:** An ICMP Code Filter will examine the contents of the Code field within ICMP packets. Valid values for the **icmp-code** parameter are **0 through 255**, or **any**. A value of any does not care about the value of the Code Field.

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# access-list ace 2 frame-type ipv6-icmp sip 2001::3 sip-bitmask 0xFFFFFFFE
icmp-type 100 icmp-code 100 hop-limit 1
```

IPv6-UDP

When a frame-type of **ipv6-udp** has been configured, all the parameters available for a frame-type of **ipv6** are available plus the following:

- **Source Port Filter:** A Source Port Filter will examine the source port of all ingress segments. If the source port of the traffic is within the configured range of the ACE, a match has been made. Valid values for the **sport** parameter are **0 through 65535**, or **any**.
- **Destination Port Filter:** A Destination Port Filter will examine the destination port of all ingress segments. If the destination port of the traffic is within the configured range of the ACE, a match has been made. Valid values for the **dport** parameter are **0 through 65535**, or **any**.

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# access-list ace 2 frame-type ipv6-udp sip 2001::3 sip-bitmask 0xFFFFFFFE
sport 0 to 1024 dport 512 to 1024 hop-limit 1
```

IPv6-TCP

When a frame-type of **ipv6-tcp** has been configured all the parameters available for a frame-type of **ipv6** and **ipv6-udp** are available plus the following:

- **TCP FIN**
- **TCP SYN**
- **TCP RST**
- **TCP PSH**
- **TCP ACK**
- **TCP URG**
- **Hop Limit**

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# access-list ace 2 frame-type ipv6-tcp sip 2001::3 sip-bitmask 0xFFFFFFFE
sport 22 hop-limit 1 tcp-flag tcp-fin 1 tcp-syn 1 tcp-rst 1 tcp-psh 1 tcp-ack 1 tcp-urg 1
```

Ethernet Type ACL Parameters

When the frame-type has been set to **etype**, a specific Ethertype can be set such that only ingress traffic with that EtherType will match the ACE.

For example, LLDP frames have an EtherType of 0x88cc. The following ACE will match ingress LLDP frames:

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# access-list ace 1 frame-type etype ?
    action          Access list action
    dmac            Destination MAC address field
    dmac-type       The type of destination MAC address
    etype-value     EtherType value
    ingress         Ingress
    logging         Logging frame information. Note: The logging feature only
                    works when the packet length is less than 1518 (without
                    VLAN tags) and the System Log memory size and logging rate
                    is limited.
    mirror          Mirror frame to destination mirror port
    next            insert the current ACE before the next ACE ID
    policy          Policy
    rate-limiter    Rate limiter
```

```
    redirect        Redirect frame to specific port
    shutdown        Shutdown incoming port. The shutdown feature only works
                    when the packet length is less than 1518 (without VLAN
                    tags).
    smac            Source MAC address field
    tag             Tag
    tag-priority    Tag priority
    vid             VID field
    <cr>
FLEX24-10G(config)# access-list ace 1 frame-type etype etype-value 0x88cc
FLEX24-10G(config)#
```

Whenever ingress LLDP traffic enters an interface configured with the above ACE, a match will be made.

The syntax for configuring an EtherType ACE is **access-list ace <ace_id> frame-type etype etype-value {any | <0x600 – 0xFFFF>}.**

Parameter Syntax

The following snippet is used to demonstrate the syntax of the **frame-type** parameter.

access-list ace 1 **frame-type {any | arp | etype | ipv4 | ipv4-icmp | ipv4-tcp | ipv4-udp | ipv6 | ipv6-icmp | ipv6-tcp | ipv6-udp}**

```
FLEX24-10G(config)# access-list ace 1 frame-type ?
    any          Don't-care the frame type
    arp          Frame type of ARP
    etype        Frame type of EtherType
    ipv4         Frame type of IPv4
    ipv4-icmp    Frame type of IPv4 ICMP
    ipv4-tcp     Frame type of IPv4 TCP
    ipv4-udp     Frame type of IPv4 TCP
    ipv6         Frame type of IPv6
    ipv6-icmp    Frame type of IPv6 ICMP
    ipv6-tcp     Frame type of IPv6 TCP
    ipv6-udp     Frame type of IPv6 UDP
FLEX24-10G(config)# access-list ace 1 frame-type
```

Ingress

The Ingress parameter is used to specify which ingress interface the ACE applies to. An ACE can apply to all interfaces or only a single interface. If **ingress** is not configured, the ACE will apply to all interfaces on the FLEX24-10G.

Parameter Syntax

access-list ace 1 **ingress {any | interface {*, GigabitEthernet <1/1-24>, 10GigabitEthernet<1/1-2>}}**

```
FLEX24-10G(config)# access-list ace 1 ingress ?
    any          Don't-care the ingress interface
    interface    Select an interface to configure
FLEX24-10G(config)# access-list ace 1 ingress interface GigabitEthernet 1/1 ?
```

```
    *                    All switches or All ports
    GigabitEthernet      1 Gigabit Ethernet Port
    10GigabitEthernet    10 Gigabit Ethernet Port
    action               Access list action
    dmac-type            The type of destination MAC address
    ------------------------------------OUTPUT TRUNCATED------------------------------------
```

Logging

When the **logging** parameter is issued, the frame will be logged only if the frame has a length of less than 1518 bytes, and the System Log memory size and logging rate is limited.

Parameter Syntax

To enable logging, add the **logging** keyword to the **access-list ace <1-512>** command as follows:

```
FLEX24-10G(config)# access-list ace 1 ?
    action          Access list action
    dmac-type       The type of destination MAC address
    frame-type      Frame type
    ingress         Ingress
    logging         Logging frame information. Note: The logging feature only
                    works when the packet length is less than 1518 (without
                    VLAN tags) and the System Log memory size and logging rate
                    is limited.
    mirror          Mirror frame to destination mirror port
    next            insert the current ACE before the next ACE ID
    policy          Policy
    rate-limiter    Rate limiter
    redirect        Redirect frame to specific port
    shutdown        Shutdown incoming port. The shutdown feature only works
                    when the packet length is less than 1518 (without VLAN
                    tags).
    tag             Tag
    tag-priority    Tag priority
    vid             VID field
    <cr>
FLEX24-10G(config)# access-list ace 1 logging
```

Mirroring

When packets match an ACE with mirroring enabled, the packets are duplicated and sent to a mirror destination. Rate-limiters do not affect frames on mirrored ports. By default, port mirroring is disabled.

Parameter Syntax

To enable mirroring, add the **mirror** keyword to the **access-list ace <1-512>** command as follows:

```
FLEX24-10G(config)# access-list ace 1 ?
```

```
    action          Access list action
    dmac-type       The type of destination MAC address
    frame-type      Frame type
    ingress         Ingress
    logging         Logging frame information. Note: The logging feature only
                    works when the packet length is less than 1518 (without
                    VLAN tags) and the System Log memory size and logging rate
                    is limited.
    mirror          Mirror frame to destination mirror port
    next            insert the current ACE before the next ACE ID
    policy          Policy
    rate-limiter    Rate limiter
    redirect        Redirect frame to specific port
    shutdown        Shutdown incoming port. The shutdown feature only works
                    when the packet length is less than 1518 (without VLAN
                    tags).
    tag             Tag
    tag-priority    Tag priority
    vid             VID field
    <cr>
FLEX24-10G(config)# access-list ace 1 mirror
```

Next

The **next** parament allows the administrator to configure the order of the ACEs. By default, when a new ACE is created without the next command, it will be added to the bottom of the list. The **next** parameter specifies the ACE ID of the ACE to follow the current ACE.

This parameter is especially useful because entries in all ACL are read from top to bottom until a match is found. Once a match is found, no further ACE's are read in the list.

Since the entries in an ACL are read from top to bottom, their order in which they appear in the list is important.

Parameter Syntax

To position an ACE entry before an already existing ACE, the **next <1-512>** parameter must be included in the ACE. **<1-512>** represents the ACE ID of the ACE to appear after the current ACE.

The below snippet with create three ACEs, and position the third ACE in between ACE 1 and ACE 2:

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# access-list ace 1 mirror
FLEX24-10G(config)# access-list ace 2 logging
FLEX24-10G(config)# access-list ace 3 frame-type ipv4 next 2
FLEX24-10G(config)# do show access-list
ID   Type      Policy   Frame   Action Rate L.  Mirror   Counter
--   --------- -------- -----   ------- ------- -------- -------
1    GLOBAL    Any      Any     Permit Disabled Enabled       62
3    GLOBAL    Any      IPv4    Permit Disabled Disabled       0
2    GLOBAL    Any      Any     Permit Disabled Disabled       0
  -------------------------------------OUTPUT TRUNCATED-------------------------------------
```

If the next parameter had not been included, the order in which the ACE's appear in the **show access-list** output would match the order in which they were configured. Since the **next 2** parameter is included with ACE 3, ACE 3 should precede ACE 2 in **show access-list** output. This is reflected above.

Policy

The policy value is a value from 0 to 127 inclusive. If a specific policy value has been set, a policy bitmask can also be set. The policy bitmask is a value from 0x0 to 0x7f.

Parameter Syntax

access-list ace 1 **policy <0-127> policy-bitmask <0-127>**

Note: The **policy-bitmask** cannot be set until the **policy** parameter has been set. The policy-bitmask can be entered in decimal or hexadecimal.

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# access-list ace 1 ?
    action          Access list action
    dmac-type       The type of destination MAC address
    frame-type      Frame type
    ingress         Ingress
    logging         Logging frame information. Note: The logging feature only
                    works when the packet length is less than 1518 (without
                    VLAN tags) and the System Log memory size and logging rate
                    is limited.
    mirror          Mirror frame to destination mirror port
    next            insert the current ACE before the next ACE ID
    policy          Policy
    rate-limiter    Rate limiter
    redirect        Redirect frame to specific port
    shutdown        Shutdown incoming port. The shutdown feature only works
                    when the packet length is less than 1518 (without VLAN
                    tags).
    tag             Tag
    tag-priority    Tag priority
    vid             VID field
    <cr>
FLEX24-10G(config)# access-list ace 1 policy 1 ?
    action            Access list action
    dmac-type         The type of destination MAC address
    frame-type        Frame type
    ingress           Ingress
    logging           Logging frame information. Note: The logging feature only
                      works when the packet length is less than 1518 (without
                      VLAN tags) and the System Log memory size and logging
                      rate is limited.
    mirror            Mirror frame to destination mirror port
    next              insert the current ACE before the next ACE ID
    policy-bitmask    The bitmask for policy ID
    rate-limiter      Rate limiter
    redirect          Redirect frame to specific port
    shutdown          Shutdown incoming port. The shutdown feature only works
                      when the packet length is less than 1518 (without VLAN
```

```
                    tags).
    tag             Tag
    tag-priority    Tag priority
    vid             VID field
    <cr>
FLEX24-10G(config)# access-list ace 1 policy 1 policy-bitmask 1
FLEX24-10G(config)#
```

Rate-Limiter

Rate-limiters are used to limit the total amount of ingress of egress traffic on an interface. On the FLEX24-10G, rate limiters are configured in profiles and then bound to an interface or an ACE. By default, 16 profiles exist with a rate-limit of 10 packets per second (pps).

Configuration

A rate-limiter profile is configured from Global Configuration as follows:

	Command	Explanation
Step 1	configure terminal	Enter Global Configuration mode.
Step 2	access-list rate-limiter {10pps <0-500000> | 25kbps <0-400000> | <1-16> {10pps | 25kbps} {<0-500000> | <0-400000>}}	Create a rate-limiter with an associated rate. If **<1-16>** is not provided, the metric and speed specified will be applied to all rate-limiters. If **<1-16>** is provided, the metric and speed specified will only be applied to the specified rate-limiter. **pps:** packets per second **kbps:** Kilobits per second By default, all 16 rate-limiters are configured with a rate of 10 pps. **Note:** The rate if specified, in pps or kbps, must be in increments of 10 or 25 respectively.
Step 3	end	**(Optional)** Return to Privileged EXEC mode.

Step 4	copy running-config startup-config	**(Optional)** Copy the contents of the running-config to the startup-config.

Modifying all Rate-Limiters – Rate-Limiter ID should be Exempt

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# access-list rate-limiter 25kbps 300000
FLEX24-10G(config)# do show access-list rate-limiter
Switch access-list rate limiter ID 1 is 7500000 kbps
Switch access-list rate limiter ID 2 is 7500000 kbps
Switch access-list rate limiter ID 3 is 7500000 kbps
Switch access-list rate limiter ID 4 is 7500000 kbps
Switch access-list rate limiter ID 5 is 7500000 kbps
Switch access-list rate limiter ID 6 is 7500000 kbps
Switch access-list rate limiter ID 7 is 7500000 kbps
Switch access-list rate limiter ID 8 is 7500000 kbps
Switch access-list rate limiter ID 9 is 7500000 kbps
Switch access-list rate limiter ID 10 is 7500000 kbps
Switch access-list rate limiter ID 11 is 7500000 kbps
Switch access-list rate limiter ID 12 is 7500000 kbps
Switch access-list rate limiter ID 13 is 7500000 kbps
Switch access-list rate limiter ID 14 is 7500000 kbps
Switch access-list rate limiter ID 15 is 7500000 kbps
Switch access-list rate limiter ID 16 is 7500000 kbps
FLEX24-10G(config)#
```

Modifying a Single Rate-Limiter – Must Include Rate-Limiter ID

```
FLEX24-10G(config)# access-list rate-limiter 1 10pps 500000
FLEX24-10G(config)# do show access-list rate-limiter
Switch access-list rate limiter ID 1 is 5000000 pps
Switch access-list rate limiter ID 2 is 7500000 kbps
Switch access-list rate limiter ID 3 is 7500000 kbps
Switch access-list rate limiter ID 4 is 7500000 kbps
Switch access-list rate limiter ID 5 is 7500000 kbps
Switch access-list rate limiter ID 6 is 7500000 kbps
Switch access-list rate limiter ID 7 is 7500000 kbps
Switch access-list rate limiter ID 8 is 7500000 kbps
Switch access-list rate limiter ID 9 is 7500000 kbps
Switch access-list rate limiter ID 10 is 7500000 kbps
Switch access-list rate limiter ID 11 is 7500000 kbps
Switch access-list rate limiter ID 12 is 7500000 kbps
Switch access-list rate limiter ID 13 is 7500000 kbps
Switch access-list rate limiter ID 14 is 7500000 kbps
Switch access-list rate limiter ID 15 is 7500000 kbps
Switch access-list rate limiter ID 16 is 7500000 kbps
FLEX24-10G(config)#
```

Default Rate-Limiter Configuration

From a default state, all rate-limiters are configured with a rate of 10 packets per second (pps).

```
FLEX24-10G# configure terminal
FLEX24-10G# show access-list rate-limiter
Switch access-list rate limiter ID 1 is 10 pps
Switch access-list rate limiter ID 2 is 10 pps
Switch access-list rate limiter ID 3 is 10 pps
Switch access-list rate limiter ID 4 is 10 pps
Switch access-list rate limiter ID 5 is 10 pps
Switch access-list rate limiter ID 6 is 10 pps
Switch access-list rate limiter ID 7 is 10 pps
Switch access-list rate limiter ID 8 is 10 pps
Switch access-list rate limiter ID 9 is 10 pps
Switch access-list rate limiter ID 10 is 10 pps
Switch access-list rate limiter ID 11 is 10 pps
Switch access-list rate limiter ID 12 is 10 pps
Switch access-list rate limiter ID 13 is 10 pps
Switch access-list rate limiter ID 14 is 10 pps
Switch access-list rate limiter ID 15 is 10 pps
Switch access-list rate limiter ID 16 is 10 pps
FLEX24-10G#
```

Redirect

When the ACE's **action** is set to **deny**, the optional **redirect** parameter is made available. Redirect allows dropped frames to be redirected to another interface on the FLEX24-10G. If a rate limiter has been configured, it will affect these interfaces.

Parameter Syntax

access-list ace <1-512> action deny **redirect interface {*, GigabitEthernet <1/1-24>, 10GigabitEthernet<1/1-2>}**

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# access-list ace 1 action deny ?
    dmac-type       The type of destination MAC address
    frame-type      Frame type
    ingress         Ingress
    logging         Logging frame information. Note: The logging feature only
                    works when the packet length is less than 1518 (without
                    VLAN tags) and the System Log memory size and logging rate
                    is limited.
    mirror          Mirror frame to destination mirror port
    next            insert the current ACE before the next ACE ID
    policy          Policy
    rate-limiter    Rate limiter
    redirect        Redirect frame to specific port
    shutdown        Shutdown incoming port. The shutdown feature only works
                    when the packet length is less than 1518 (without VLAN
                    tags).
    tag             Tag
    tag-priority    Tag priority
    vid             VID field
    <cr>
FLEX24-10G(config)# access-list ace 1 action deny redirect ?
    disable      Disable
```

```
    interface    Select an interface to configure
FLEX24-10G(config)# access-list ace 1 action deny redirect interface GigabitEthernet 1/1
FLEX24-10G(config)#
```

Note: If no ingress interface has been configured, traffic from all interfaces will be redirected to the interface configured in the **redirect** parameter. All the redirected traffic will be substantially rate limited due to traffic from all interfaces being funneled into a single interface.

Shutdown

When ingress traffic enters a switchport and matches an ACE with the **shutdown** parameter, the traffic will cause the port to shut itself down. By default, this feature is disabled.

Parameter Syntax

Note: The shutdown feature only functions when the incoming packet is less than 1518 bytes in length (excluding VLAN tags).

access-list ace <1-512> **shutdown**

```
FLEX24-10G(config)# access-list ace 1 shutdown
```

Tag, Tag-Priority, and VID

The **tag** parameter configures the ACE to match ingress packets based on the presence of an 802.1Q tag.

The available tag options are as follows:

- **Any:** Packets with and without an 802.1Q tag are allowed. This is the default.
- **Tagged:** Only ingress traffic present with an 802.1Q have a possibility of matching the ACE.
- **Untagged:** Only ingress traffic lacking an 802.1Q have a possibility of matching the ACE.

If the **vid** parameter has been configured, the ACE can filter ingress traffic based on the packets VLAN membership. Untagged packets are assumed to have a VLAN membership of the native VLAN.

Parameter Syntax

The **tag**, **vid**, and **tag-priority** can all be enabled together within a single ACE.

access-list ace <1-512> **tag {any | tagged | untagged} vid {any | <1-4095>} tag-priority {any | <0-7> | 0-1 | 0-3 | 2-3 | 4-5 | 4-7 | 6-7}**

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# access-list ace 1 tag ?
    any         Don't-care tagged or untagged
    tagged      Tagged
    untagged    Untagged
FLEX24-10G(config)# access-list ace 1 tag tagged vid 10 tag-priority ?
    0-1      The range of tag priority
    0-3      The range of tag priority
    2-3      The range of tag priority
```

```
    4-5      The range of tag priority
    4-7      The range of tag priority
    6-7      The range of tag priority
    <0-7>    The value of tag priority
    any      Don't-care the value of tag priority field
FLEX24-10G(config)# access-list ace 1 tag tagged vid 10 tag-priority any
FLEX24-10G(config)#
```

Enabling an ACE on an Interface

Once an ACE has been configured from Global Configuration mode, it exists in the running-config but has not yet been enabled on any interfaces. A single ACE can be present on multiple interfaces.

To enable an ACE on an interface or interface(s) follow the below configuration:

	Command	**Explanation**
Step 1	configure terminal	Enter Global Configuration mode.
Step 2	interface {*, GigabitEthernet <1/1-24>, 10GigabitEthernet<1/1-2>}	Enter Interface Configuration mode for the interface(s) to configure.
Step 3	access-list policy <policy_id>	Enable ACE with an ID of **<policy_id>** on the specified interface. To view all ACEs on the switch and their IDs issue **show access-list** from Privileged EXEC mode.
Step 4	access-list action {deny | permit}	**(Optional)** Specify the action the interface takes when ingress traffic matches an ACE on that interface. **Deny** will drop the traffic. **Permit** will allow the traffic to be processed by the switch engine. By default, the traffic is permitted.
Step 5	access-list logging	**(Optional)** Configures whether the switch should log ingress traffic on the interface. When the **logging** is enabled, the frame will be logged only if the frame has a length of less than 1518 bytes, and the System Log memory size and logging rate is limited.
Step 6	access-list mirror	**(Optional)** Configure the mirroring operation on the specified interface. When **access-list mirror** is issued, ingress traffic is mirrored.
Step 7	[no] access-list port-state	**(Optional)** This command is enabled by default, hence when it is not in the running-config.

		When enabled: To reopen ports by changing the volatile port configuration of the ACL user module. **When disabled:** To close ports by changing the volatile port configuration of the ACL user module.
Step 8	access-list rate-limiter <1-16>	**(Optional)** Specify which rate-limiter profile to enable on the interface(s). Up to 16 rate-limiters can be configured. Rate limiters are configured from Global Configuration with the **access-list rate-limiter** command. See here for Rate-limiter configuration.
Step 9	access-list redirect interface {*, GigabitEthernet <1/1-24>, 10GigabitEthernet<1/1-2>}	**(Optional)** Redirect ingress traffic to another interface on the switch.
Step 10	access-list shutdown	**(Optional)** Shutdown the interface the moment ingress traffic is received.
Step 11	end	**(Optional)** Exit Interface Configuration mode and return to Privileged EXEC mode.
Step 12	copy running-config startup-config	**(Optional)** Copy the contents of the running-config to the startup-config.

Verification

show access-list [interface {*, GigabitEthernet <1/1-24>, 10GigabitEthernet<1/1-2>}] [ace statistics] [rate-limiter <1-16>]: Displays all configured ACEs as well as interface ACE information on a per-interface basis. Output can be filtered to only show ACE information for a specific interface.

```
FLEX24-10G# show access-list
ID   Type      Policy   Frame   Action Rate L.  Mirror   Counter
--   --------- -------- -----   ------- ------- -------- -------
1    GLOBAL    Any      IPv4    Permit Disabled Disabled     152
4    GLOBAL    Any      ICMP    Permit Disabled Disabled       0
2    GLOBAL    Any      UDP     Permit Disabled Disabled       0
3    GLOBAL    Any      IPv6    Permit Disabled Disabled       0

Switch access-list ace number: 4

Switch access-list rate limiter ID 1 is 10 pps
Switch access-list rate limiter ID 2 is 10 pps
Switch access-list rate limiter ID 3 is 10 pps
Switch access-list rate limiter ID 4 is 10 pps
Switch access-list rate limiter ID 5 is 10 pps
Switch access-list rate limiter ID 6 is 10 pps
Switch access-list rate limiter ID 7 is 10 pps
Switch access-list rate limiter ID 8 is 10 pps
Switch access-list rate limiter ID 9 is 10 pps
Switch access-list rate limiter ID 10 is 10 pps
Switch access-list rate limiter ID 11 is 10 pps
Switch access-list rate limiter ID 12 is 10 pps
Switch access-list rate limiter ID 13 is 10 pps
```

```
Switch access-list rate limiter ID 14 is 10 pps
Switch access-list rate limiter ID 15 is 10 pps
Switch access-list rate limiter ID 16 is 10 pps

GigabitEthernet 1/1 :
---------------------
  action is permit
  policy ID is 0
  rate limiter ID is disabled
  redirect is disabled
  mirror is disabled
  logging is disabled
  shutdown is disabled
  port-state is enabled
  counter is 0

GigabitEthernet 1/2 :
---------------------
  action is permit
  policy ID is 0
  rate limiter ID is disabled
  redirect is disabled
  mirror is disabled
  logging is disabled
-------------------------------------OUTPUT TRUNCATED-------------------------------------
```

show access-list rate-limiter [ace statistics] [interface {*, GigabitEthernet <1/1-24>, 10GigabitEthernet<1/1-2>}]: Displays all rate-limiter information. Output can be filtered to only show rate-filter information for a specific ACE of interface.

```
FLEX24-10G# reload defaults
% Reloading defaults. Please stand by.
FLEX24-10G# show access-list rate-limiter
Switch access-list rate limiter ID 1 is 10 pps
Switch access-list rate limiter ID 2 is 10 pps
Switch access-list rate limiter ID 3 is 10 pps
Switch access-list rate limiter ID 4 is 10 pps
Switch access-list rate limiter ID 5 is 10 pps
Switch access-list rate limiter ID 6 is 10 pps
Switch access-list rate limiter ID 7 is 10 pps
Switch access-list rate limiter ID 8 is 10 pps
Switch access-list rate limiter ID 9 is 10 pps
Switch access-list rate limiter ID 10 is 10 pps
Switch access-list rate limiter ID 11 is 10 pps
Switch access-list rate limiter ID 12 is 10 pps
Switch access-list rate limiter ID 13 is 10 pps
Switch access-list rate limiter ID 14 is 10 pps
Switch access-list rate limiter ID 15 is 10 pps
Switch access-list rate limiter ID 16 is 10 pps
FLEX24-10G#
```

show access-list ace statistics [interface {*, GigabitEthernet <1/1-24>, 10GigabitEthernet<1/1-2>}] [rate-limiter <1-16>]: Displays all ACEs on the switch. Output can be further filtered to only include ACE statistics from a particular interface.

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# access-list ace 1 frame-type ipv4
FLEX24-10G(config)# access-list ace 4 frame-type ipv4-icmp
FLEX24-10G(config)# access-list ace 2 frame-type ipv4-udp
FLEX24-10G(config)# access-list ace 3 frame-type ipv6
FLEX24-10G(config)# end
FLEX24-10G# show access-list ace statistics
ID   Type      Policy   Frame   Action Rate L.  Mirror   Counter
--   --------- -------- -----   ------- ------- -------- -------
1    GLOBAL    Any      IPv4    Permit Disabled Disabled      41
4    GLOBAL    Any      ICMP    Permit Disabled Disabled       0
2    GLOBAL    Any      UDP     Permit Disabled Disabled       0
3    GLOBAL    Any      IPv6    Permit Disabled Disabled       0

Switch access-list ace number: 4
FLEX24-10G#
```

show access-list ace-status: Displays the status of all ACEs. Output can be filtered heavily using the additional parameters below.

```
FLEX24-10G# show access-list ace-status ?
    |                     Output modifiers
    arp-inspection        The ACEs that are configured by ARP Inspection module
    conflicts             The ACEs that did not get applied to the hardware due
                          to hardware limitations
    dhcp                  The ACEs that are configured by DHCP module
    dhcp6-snooping        The ACEs that are configured by DHCPv6 Snooping module
    ip                    The ACEs that are configured by IP module
    ip-source-guard       The ACEs that are configured by IP Source Guard module
    ipmc                  The ACEs that are configured by IPMC module
    ipv6-source-guard     The ACEs that are configured by IPv6 Source Guard
                          module
    loop-protect          The ACEs that are configured by Loop Protect module
    static                The ACEs that are configured by users manually
    upnp                  The ACEs that are configured by UPnP module
    <cr>
FLEX24-10G# show access-list ace-status
User
----
S   : static
IPSG: ipSourceGuard
IP6SG: ipv6SourceGuard
IP: IP
IPMC: ipmc
ARPI: arpInspection
UPnP: upnp
DHCP: dhcp
D6SN: dhcp6Snooping
LOOP: loopProtect

User ID   Frame   Action Rate L.  Mirror   CPU    Counter Conflict
---- --   ------  ------ -------- -------- ------ ------- -------
IP   1    IPv4    Permit Disabled Disabled Yes          0 No
S    1    IPv4    Permit Disabled Disabled No         465 No
S    4    ICMP    Permit Disabled Disabled No           0 No
S    2    UDP     Permit Disabled Disabled No           0 No
```

```
S    3    IPv6    Permit Disabled Disabled No          5 No
Switch 1 access-list ace number: 5
FLEX24-10G#
```

Chapter 19: Private VLANs and Port Isolation

Introduction

VLANs are used primarily to segment a large network into smaller subnetworks often grouping similar types of traffic together. One major advantage with VLANs are their ability to partition a single broadcast domain into several smaller broadcast domains. Private VLANs take this partitioning of broadcast domains one step further.

Private VLANs (PVLANs) divide VLANs into “sub-VLANs”. Members of private VLANs must still follow the same rules to communicate with members of other private VLANs. Just as a Layer-3 device is required for inter-VLAN routing, a Layer-3 device is also required for inter-private-VLAN routing. Of course, since the FLEX24-10G is a Layer-3 switch, no additional hardware is required for inter-private-VLAN routing.

Port isolation prevents interfaces from communicating with any other interfaces regardless of their VLAN or PVLAN membership.

By default, all interfaces on the FLEX24-10G are a member of VLAN 1 and PVLAN 1.

Configuration

Private VLAN Membership and Isolated Ports

An interface can be a member of a single private VLAN or multiple private VLANs at one time.

	Command	Explanation
Step 1	configure terminal	Enter Global Configuration mode.
Step 2	interface {*, GigabitEthernet <1/1-24>, 10GigabitEthernet<1/1-2>}	Enter Interface Configuration mode for the interface(s) to configure.
Step 3	pvlan <vlan_list>	Add the interface to the PVLANs in **<vlan_list>.** By default, all interfaces are members of PVLAN 1. To remove PVLAN 1 from an interface’s PVLAN membership, **no pvlan <vlan_list>** must be configured at the interface level.
Step 4	pvlan isolation	Enable port isolation on the interface.
Step 5	end	**(Optional)** Exit Interface Configuration mode and return to Privileged EXEC mode.
Step 6	copy running-config startup-config	**(Optional)** Copy the contents of the running-config to the startup-config.

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# interface GigabitEthernet 1/1
FLEX24-10G(config-if)# pvlan 10
FLEX24-10G(config-if)# pvlan isolation
FLEX24-10G(config-if)# end
FLEX24-10G# copy running-config startup-config
Building configuration...
% Saving 2312 bytes to flash:startup-config
FLEX24-10G#
```

Verification

PVLAN configuration information can be displayed with the following show commands:

show pvlan [<pvlan_id>]: Displays all PVLANs and interfaces which are a member of those PVLANs. Output can be filtered to only show specific PVLANs by applying the **<pvlan_id>** filter.

```
FLEX24-10G# show pvlan
PVLAN ID  Ports
--------  ---------------------------------------------------------------------------
1         GigabitEthernet 1/1, GigabitEthernet 1/2, GigabitEthernet 1/3,
          GigabitEthernet 1/4, GigabitEthernet 1/5, GigabitEthernet 1/6,
          GigabitEthernet 1/7, GigabitEthernet 1/8, GigabitEthernet 1/9,
          GigabitEthernet 1/10, GigabitEthernet 1/11, GigabitEthernet 1/12,
          GigabitEthernet 1/13, GigabitEthernet 1/14, GigabitEthernet 1/15,
          GigabitEthernet 1/16, GigabitEthernet 1/17, GigabitEthernet 1/18,
          GigabitEthernet 1/19, GigabitEthernet 1/20, GigabitEthernet 1/21,
          GigabitEthernet 1/22, GigabitEthernet 1/23, GigabitEthernet 1/24,
          GigabitEthernet 1/25, 10GigabitEthernet 1/1, 10GigabitEthernet 1/2
10        GigabitEthernet 1/1
FLEX24-10G#
```

show pvlan isolation [interface {*, GigabitEthernet <1/1-24>, 10GigabitEthernet<1/1-2>}]: Displays the port isolation status of all interfaces. Output can be filtered to only show the port isolation status of specific interfaces.

```
FLEX24-10G# show pvlan isolation
Port                              Isolation
--------------------------------  ---------
GigabitEthernet 1/1               Enabled
GigabitEthernet 1/2               Disabled
GigabitEthernet 1/3               Disabled
GigabitEthernet 1/4               Disabled
GigabitEthernet 1/5               Disabled
GigabitEthernet 1/6               Disabled
GigabitEthernet 1/7               Disabled
GigabitEthernet 1/8               Disabled
GigabitEthernet 1/9               Disabled
GigabitEthernet 1/10              Disabled
GigabitEthernet 1/11              Disabled
GigabitEthernet 1/12              Disabled
  -------------------------------------OUTPUT TRUNCATED -------------------------------------
```

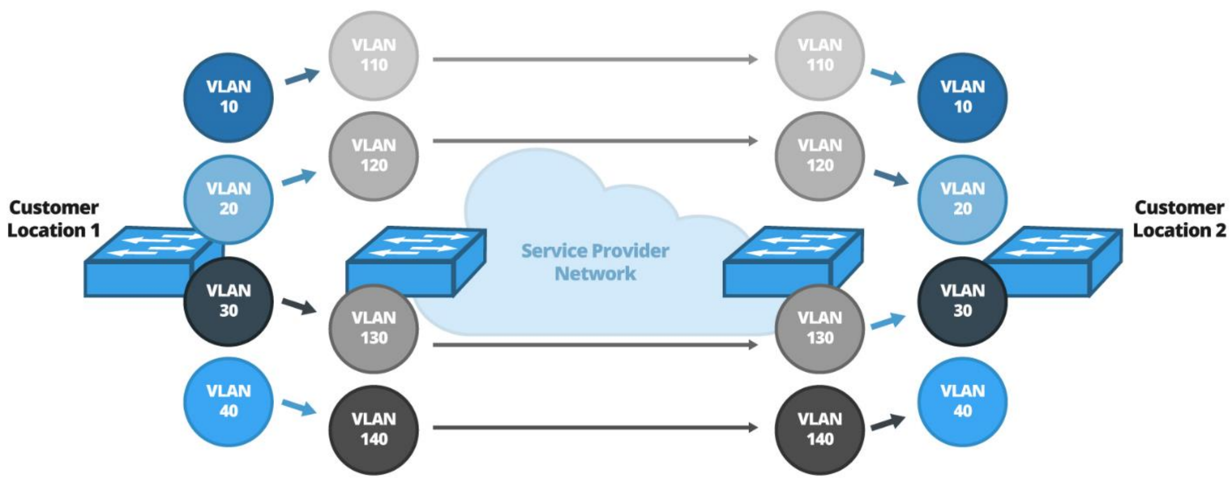
Chapter 20: VLAN Translation

Introduction

VLAN translation allows VLANs to be mapped to other VLANs when crossing a switch boundary. It is quite common of service providers to use their own set of VLANs within their network which are different than the VLANs used at a customer site.

For example, VLAN 10 at a customer site may be used as a voice VLAN while a service provider's voice VLAN may be completely different. For this reason, a mapping must exist which will overwrite (translate) the VLAN membership of the frame when the frame reaches the switch boundary. The translated VLAN will be in effect for the duration that the frame is a member of the service provider's network.

When the frame enters the destination network the VLAN will have to be translated once again at the network boundary. In the case where the frame is travelling from one site to another, with both sites being members of the same organization, the source and destination VLANs should match. When the frame enters the service provider's network VLAN X is translated to VLAN Y. When the frames exit the service provider's network VLAN Y is translated back to VLAN X.



Configuration

By default, no VLAN translation mappings exist. Each interface is the sole member of a Group ID matching the *interface-id.* For example, G 1/1 is the only member of Group ID 1, G 1/2 is the only member of Group ID 2, so on and so forth. The number of possible groups is equal to the number is interfaces present on the switch. In the case of the FLEX24-10G, this equates to 27 possible groups.

Mappings are created by creating entries in the VLAN Translation Mapping Table. By default, there are no entries in the table. VLAN Translation Mapping Table entries map Group ID's to a VLAN ID, and translated VLAN ID.

Mapping an Interface to a Group

Interfaces are mapped to groups from Interface Configuration mode for the specific interface.

	Command	Explanation
Step 1	configure terminal	Enter Global Configuration mode.
Step 2	interface {*, Gigabit Ethernet <1/1-24>, 10GigabitEthernet<1/1-2>}	Enter Interface Configuration mode for the Interface(s) in which to assign a Group ID to. By default, interface GigabitEthernet 1/x will be a member of Group ID x.
Step 3	switchport vlan mapping <1-27>	Map the interface to a specific Group ID. The FLEX24-10G supports 27 different groups.
Step 4	end	**(Optional)** Exit Interface Configuration mode and return to Privileged EXEC mode.
Step 5	copy running-config startup-config	**(Optional)** Copy the contents of the running-config to the startup-config.

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# interface GigabitEthernet 1/1
FLEX24-10G(config-if)# switchport vlan mapping 10
FLEX24-10G(config-if)# end
FLEX24-10G# copy running-config startup-config
Building configuration...
% Saving 2683 bytes to flash:startup-config
FLEX24-10G#
```

Multiple interfaces can be mapped to the same group by specifying an interface range when entering Interface Configuration mode.

Creating Entries in the VLAN Translation Mapping Table

VLAN Translation Mapping Table Entries are created by Global Configuration as follows:

	Command	Explanation
Step 1	configure terminal	Enter Global Configuration mode.
Step 2	switchport vlan mapping <1-27> {<vlan_list> <translated_vid>| both <vlan_id> <translated_vid>| egress <vlan_id> <translated_vid> | ingress <vlan_id> <translated_vid>}	Create an entry in the VLAN Translation Mapping Table. Each entry must contain a group ID, direction, source VLAN, and translated VLAN. When a **<vlan_list>** is provided the directional is automatically set to both (egress and ingress).

		Egress will only examine egress traffic while **Ingress** will only examine ingress traffic. **Both** examines both egress and ingress traffic.
Step 3	end	**(Optional)** Return to Privileged EXEC mode.
Step 4	copy running-config startup-config	**(Optional)** Copy the contents of the running-config to the startup-config.

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# switchport vlan mapping 10 ingress 10 110
FLEX24-10G(config)# switchport vlan mapping 10 egress 110 10
FLEX24-10G(config)# end
FLEX24-10G# copy running-config startup-config
Building configuration...
% Saving 2766 bytes to flash:startup-config
FLEX24-10G#
```

When egress, and/or ingress traffic is found on an interface matching a VLAN Translation Mapping Table entry, the traffic's VLAN membership is checked against the entry. If the VLAN membership matches the VID in the entry, the traffic's VLAN membership will be overridden with the translated VLAN in the entry.

Verification

There are no **show** commands related to VLAN Translation. Entries contained within the VLAN Translation Mapping Table can be viewed directly from the running-config/startup-config. Interface-to-Group Mappings can also be viewed from the running-config/startup-config under the specific interfaces.

```
FLEX24-10G# show running-config | begin switchport vlan mapping
switchport vlan mapping 2 both 10 110
switchport vlan mapping 10 ingress 10 110
switchport vlan mapping 10 egress 110 10
!
interface GigabitEthernet 1/1
 switchport vlan mapping 10
!
interface GigabitEthernet 1/2
!
         ------------------------------OUTPUT TRUNCATED------------------------------
```

Chapter 21: Voice VLANs

Introduction

Voice VLANs provide a means for voice traffic and data traffic to travel along the same network cable while being members of separate VLANs. An access port is typically only capable of supporting traffic belonging to a single VLAN. Voice VLANs are the exception to this rule, allowing an access VLAN and voice VLAN to belong to a single interface while keeping the VLANs separate.

A Voice VLAN can be applied to an interface when a compatible VoIP device is detected. If the endpoint's MAC address contains a OUI which matches a FLEX24-10G OUI entry, the Voice VLAN will be applied on the interface. Additionally, an interface can be applied a voice VLAN if LLDP advertisements are detected from a VoIP device.

Configuration

Before a voice VLAN can be enabled on individual interfaces, the voice VLAN service must be enabled globally from Global Configuration.

This is done as follows:

	Command	**Explanation**
Step 1	configure terminal	Enter Global Configuration mode.
Step 2	voice vlan	Enable the voice VLAN feature globally.
Step 3	voice vlan aging-time <10-10000000>	**(Optional)** Specify the Voice VLAN secure aging time, in seconds. The aging time is used when the interface voice VLAN mode is set to **auto**, or when security is enabled. More on the interface voice VLAN mode and security state here. By default, the aging time is set to 86400 seconds.
Step 4	voice vlan class <0-7>	**(Optional)** Set the CoS value which voice traffic on the Voice VLAN will possess. By default, traffic on the Voice VLAN has CoS priority level 7.
Step 5	voice vlan vid <vlan_id>	**(Optional)** Specify the voice VLAN ID. The voice VLAN must be unique and cannot equal any other Port VLAN ID, Management VLAN ID, or MVR VLAN ID.

		By default, VLAN 1000 is reserved as the Voice VLAN.
Step 6	voice vlan oui <oui> [description]	**(Optional)** Create an OUI entry. The OUI represents the first 24-bits of a devices MAC address. When a VoIP device is connected to the switch with an OUI which matches an OUI entry, that device will be dynamically assigned to the voice VLAN. By default, four OUI entries exist on the switch, one entry for Cisco IP phones, Polycom IP phones, Mitel IP phones, and Avaya IP phones. Up to 16 OUI entries can exist on the switch.
Step 7	end	**(Optional)** Return to Privileged EXEC mode.
Step 8	copy running-config startup-config	**(Optional)** Copy the contents of the running-config to the startup-config.

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# voice vlan
FLEX24-10G(config)# voice vlan aging-time 555555
FLEX24-10G(config)# voice vlan class 6
FLEX24-10G(config)# voice vlan vid 500
FLEX24-10G(config)# voice vlan oui 22-22-22 description Demo OUI
FLEX24-10G(config)# end
FLEX24-10G# copy running-config startup-config
Building configuration...
% Saving 2466 bytes to flash:startup-config
FLEX24-10G#
```

Configuring a Voice VLAN at the Interface Level

Once the Voice VLAN has been enabled globally, it can be enabled at the interface level as follows:

	Command	**Explanation**
Step 1	configure terminal	Enter Global Configuration mode.
Step 2	interface {*, GigabitEthernet <1/1-24>, 10GigabitEthernet<1/1-2>}	Enter Interface Configuration mode for the interface(s) to enable the voice VLAN on.
Step 3	switchport voice vlan mode {auto | disable | force}	Specify the interfaces voice VLAN mode. **Auto:** The switch will auto detect whether a VoIP phone has been connected to the interface and will configure the interfaces VLAN membership accordingly.

		Disable: The Voice VLAN is disabled on the interface. **Force:** The interface and endpoint will force join the Voice VLAN.
Step 4	switchport voice vlan discovery-protocol {both | lldp | oui}	**(Optional)** Change the method in which the switch detects a directly connected VoIP device. The switch can detect a VoIP device via the devices OUI, through the exchange of LLDP packets, or by the devices OUI and LLDP information. By default, the switch will only detect a VoIP device via the devices OUI.
Step 5	switchport voice vlan security	**(Optional)** Enable Voice VLAN port-security. When enabled, all traffic from non-telephonic devices in the Voice VLAN is not forwarded for 10 seconds. By default, voice VLAN port-security is not enabled.
Step 6	end	**(Optional)** Return to Privileged EXEC mode.
Step 7	copy running-config startup-config	**(Optional)** Copy the contents of the running-config to the startup-config.

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# interface GigabitEthernet 1/1
FLEX24-10G(config-if)# switchport voice vlan mode force
FLEX24-10G(config-if)# switchport voice vlan discovery-protocol both
FLEX24-10G(config-if)# switchport voice vlan security
FLEX24-10G(config-if)# end
FLEX24-10G# copy running-config startup-config
Building configuration...
% Saving 2547 bytes to flash:startup-config
FLEX24-10G#
```

Verification

show voice vlan [interface {*, GigabitEthernet <1/1-24>, 10GigabitEthernet<1/1-2>}]: Displays voice VLAN configuration parameters for all switchports. Output can be filtered to only include Voice VLAN information for specific switchports with the optional **interface** parameter.

```
FLEX24-10G# show voice vlan
Switch voice vlan is disabled
Switch voice vlan ID is 1000
Switch voice vlan aging-time is 86400 seconds
Switch voice vlan traffic class is 7
```

```
Telephony OUI  Description
-------------  -----------
00-03-6B       Cisco phones
00-E0-75       Polycom phones
08-00-0F       Mitel phones
22-22-22
C8-1F-EA       Avaya phones

Voice VLAN switchport is configured on following:

GigabitEthernet 1/1 :
---------------------
GigabitEthernet 1/1 switchport voice vlan mode is disabled
GigabitEthernet 1/1 switchport voice security is enabled
GigabitEthernet 1/1 switchport voice discovery protocol is oui

GigabitEthernet 1/2 :
---------------------
GigabitEthernet 1/2 switchport voice vlan mode is disabled
GigabitEthernet 1/2 switchport voice security is disabled
GigabitEthernet 1/2 switchport voice discovery protocol is oui

GigabitEthernet 1/3 :
---------------------
GigabitEthernet 1/3 switchport voice vlan mode is disabled
GigabitEthernet 1/3 switchport voice security is disabled
GigabitEthernet 1/3 switchport voice discovery protocol is oui
         ------------------------------OUTPUT TRUNCATED------------------------------
```

show voice vlan oui [<oui>]: Display all OUI entries. Output can be filtered to only single OUI entries.

```
FLEX24-10G# show voice vlan oui
Telephony OUI  Description
-------------  -----------
00-03-6B       Cisco phones
00-E0-75       Polycom phones
08-00-0F       Mitel phones
22-22-22
C8-1F-EA       Avaya phones
FLEX24-10G#
```

Chapter 22: Access Management

Introduction

By default, VLAN 1001 is the management VLAN and is bound an IP address of 192.168.1.1 and subnet mask of 255.255.255.0. With the default configuration, any host with an IP address on the 192.168.1.1/24 subnet will be able to access the switch via the WEB GUI, SNMP, and TETLNET/SSH.

Access Management allows the administrator to create access management entries which grant additional IP address range access to the switch's management.

When access management is enabled on the switch, VLAN 1001 is no longer a management VLAN. To re-enable VLAN 1001 as a management VLAN, an access management entry will have to be explicitly created for VLAN 1001.

It is worth noting that from a default state, the FLEX24-10G can be managed from any VLAN configured on the switch, not just VLAN 1001. VLAN 1001 is referred to as the "management VLAN" because switch management is the sole purpose of this VLAN.

When access management is enabled, the switch will not be able to be accessed remotely until access management entries are configured for specific VLANs.

Configuration

Enabling Access Management

Regardless of how many access management entries exist on the switch, if the feature is not globally enabled, none of the entries will take effect.

	Command	**Explanation**
Step 1	configure terminal	Enter Global Configuration mode.
Step 2	access management	Enable access management globally. If this command has not been issued, none of the access management entries will be operational. **Note:** Once access management is enabled, VLAN 1001 will no longer be the management VLAN until an entry for VLAN 1001's subnet is explicitly created.
Step 3	end	**(Optional)** Return to Privileged EXEC mode.
Step 4	copy running-config startup-config	**(Optional)** Copy the contents of the running-config to the startup-config.

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# access management
```

```
FLEX24-10G(config)# end
FLEX24-10G# copy running-config startup-config
Building configuration...
% Saving 1958 bytes to flash:startup-config
FLEX24-10G#
```

Creating Access Management Entries

By default, no access management entries exist on the switch. Up to 16 access management entries can exist at one time. Each access management entry contains a VLAN ID, IP address range to allow, and which methods via which to allow the host to access the switch's management (i.e SNMP, WEB GUI, TELNET/SSH).

Creating access management entries can be done as follows:

	Command	Explanation
Step 1	configure terminal	Enter Global Configuration mode.
Step 2	[no] access management <1-16> <vlan_id> {<start_ipv4addr> | <start_ipv6addr>} [to {<end_ipv4addr> | <end_ipv6addr>}] {all | [snmp | telnet | web]} **Example:** access management 1 1 192.168.1.1 to 192.168.1.255 all	Create an access management entry. **<1-16>** represents the access management entry number. Up to 16 entries can exist on the switch. **<vlan_id>** represents the VLAN ID for the entry. **{all | [snmp | telnet | web]}** specifies which method via which to allow hosts to access the switch's management. **all:** Enable management across SNMP, TELNET/SSH, and the web GUI. **snmp:** Enable management via SNMP only. **telnet:** Enable management via TELNET/SSH sessions only. **web:** Enable management via web GUI instances only. Use a leading "no" to delete an access management entry.
Step 3	end	**(Optional)** Return to Privileged EXEC mode.
Step 4	copy running-config startup-config	**(Optional)** Copy the contents of the running-config to the startup-config.

The below CLI snippet re-enables switch management on VLAN 1001:

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# access management 1 1001 192.168.1.1 to 192.168.1.255 all
FLEX24-10G(config)# end
FLEX24-10G# copy running-config startup-config
Building configuration...
% Saving 2013 bytes to flash:startup-config
FLEX24-10G#
```

Access management entries for non-default VLANs can exist even if the VLAN has not been created on the switch.

For example, the below CLI snippet is a valid configuration even though VLAN 50 has not been created. Of course, this entry will have no effect until the VLAN is created and at least one interface is configured with the **switchport access vlan 50** command.

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# access management 2 50 192.168.0.1 to 192.168.0.255 all
FLEX24-10G(config)# end
FLEX24-10G# copy running-config startup-config
Building configuration...
% Saving 2069 bytes to flash:startup-config
FLEX24-10G#
```

Verification

show access management [<1-16>]: Displays all access management entries on the switch. Output can be filtered to only display a single entry at a time.

```
FLEX24-10G# show access management
Switch access management mode is enabled

W: WEB/HTTPS
S: SNMP
T: TELNET/SSH

Idx VID  Start IP Address                End IP Address                 W S T
--- ---  ------------------------------- ------------------------------ - - -
1   1001 192.168.1.1                     192.168.1.255                  Y Y Y
2   50   192.168.0.1                     192.168.0.255                  Y Y Y
FLEX24-10G#
```

show access management statistics: Displays cumulative access management packets statistics for all access methods.

```
FLEX24-10G# show access management statistics

Access Management Statistics:
-----------------------------
HTTP     Receive:       1433    Allow:        715    Discard:        718
HTTPS    Receive:          0    Allow:          0    Discard:          0
SNMP     Receive:          0    Allow:          0    Discard:          0
```

```
TELNET    Receive:          0    Allow:          0    Discard:          0
SSH       Receive:          0    Allow:          0    Discard:          0
FLEX24-10G#
```

Chapter 23: DHCP

Introduction

The Dynamic Host Configuration Protocol (DHCP) provides a means for network devices to dynamically be assigned IP address from a DHCP server. DHCP greatly reduces the administrative workload required when managing IP addresses on multiple hosts.

IP addresses are selected from an administrator configured pool on the DHCP server and then leased to network devices. Additional parameters such as default gateway, and DNS server can also be provided to hosts. By default, a DHCP server will lease an IP address to a host for 24 hours and then attempt to renew the lease after 12 hours.

The DHCP server keeps track of all active leases and will not lease IP addresses which have already been leased.

The FLEX24-10G can act as its own standalone DHCP server, leasing IP addresses to hosts, or as a relay, relaying DHCP packets between hosts and a separate DHCP server.

DHCP operates using a 4-message exchange known as Discover, Offer, Request, Acknowledgement. The process begins with the client broadcasting DHCPDISCOVER messages. These Discover messages contain a parameter called the "Parameter Request List". The Parameter Request List contains all the parameters which the client would like to receive from the DHCP server. Only parameters included in the Parameter Request List will be answered by the DHCP server.

For example, parameters included in Discover messages originating from a Windows 10 workstation are the following:

- Subnet Mask (DHCP Option 1)
- Router/Default Gateway (DHCP Option 3)
- Domain Name Server (DHCP Option 6)
- Domain Name (DHCP Option 15)
- Perform Router Discover (DHCP Option 31)
- Static Route (DHCP Option 33)
- Vendor-Specific Information (DHCP Option 43)
- NetBIOS over TCP/IP Name Server (DHCP Option 44)
- NetBIOS over TCP/IP Node Type (DHCP Option 46)
- NetBIOS over TCP/IP Scope (DHCP Option 47)
- Domain Search (DHCP Option 119)
- Classless Static Route (DHCP Option 121)
- Private/Classless Static Route (Microsoft) (DHCP Option 249)
- Private/Proxy Autodiscovery (DHCP Option 252)

DHCP servers will receive the Discover messages and reply with DHCPOFFER messages. These Offers offer a DHCP lease to the client and will attempt to satisfy as many parameters in the Parameter

Request List as possible. If the DHCP server is not configured with one or more of the parameters in the clients Parameter Request List, the offer message will also not contain these parameters.

Next, the DHCP client will broadcast a DHCPREQUEST message requesting the IP address contained in the DHCPOFFER. The client can receive DHCPOFFER messages from multiple servers but will only accept one offer. Since DHCPREQUEST messages are sent as broadcast traffic, all DHCP servers will receive them. Thankfully the DHCPREQUEST message contains a DHCP Server Identifier which is the IP address of the DHCP server whose offer the client would like to accept. When a DHCP server receives a DHCPREQUEST message with a DHCP Server Identifier different than its own IP address, the server will withdraw any offers it made to the client and return the offered IP addresses to the DHCP pool.

When the correct DHCP server receives a DHCPREQUEST message from the client, the server will respond with a DHCPACK. The DHCPACK is an acknowledgement which provides the client with the lease duration and any other configuration information which the client may request. At this point the DHCP process is complete.

Configuration

Excluded Addresses

Excluded addresses are IP addresses which the DHCP server will not assign to hosts. In a network there are often critical servers which have been assigned a static IP address. If the DHCP server does not know about these statically configured IP addresses, there is a possibility of the server trying to assign the same address to another host. This would create a duplicate IP address in the network.

An excluded address should be created for every device in the network configured with a static IP address or whose IP we would not like to be reassigned elsewhere.

IP addresses can be excluded as part of a range or individually.

	Command	**Explanation**
Step 1	configure terminal	Enter Global Configuration mode.
Step 2	ip dhcp excluded-address <ipv4_addr> [end_ipv4_addr]	Prevent the FLEX24-10G's DHCP server from assigning **<ipv4_addr>** to hosts. If the optional second IP address is specified, all IP addresses within the **<ipv4_addr>** – **<end_ipv4_addr>** range will be excluded.
Step 3	end	**(Optional)** Return to Privileged EXEC mode.
Step 4	copy running-config startup-config	**(Optional)** Copy the contents of the running-config to the startup-config.

Example: 192.168.100.1 is the default gateway for all hosts on the 192.168.100.0/24 subnet. To below CLI snippet will exclude 192.168.100.1 from being assigned to hosts.

```
FLEX24-10G# configure terminal
```

```
FLEX24-10G(config)# ip dhcp excluded-address 192.168.100.1
FLEX24-10G(config)# end
FLEX24-10G# copy running-config startup-config
Building configuration...
% Saving 2839 bytes to flash:startup-config
FLEX24-10G#
```

Example: The IP address range 192.168.100.20 – 192.168.100.25 have been statically assigned to mission critical servers. It would be undesirable for the IP addresses of these servers to change or be reassigned to other hosts. The below CLI snippet creates an excluded address for the six addresses in the range.

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# ip dhcp excluded-address 192.168.100.20 192.168.100.25
FLEX24-10G(config)# end
FLEX24-10G# copy running-config startup-config
Building configuration...
% Saving 2894 bytes to flash:startup-config
FLEX24-10G#
```

Creating a DHCP Pool

A DHCP Pool specifies the address space in which the DHCP server can assign IP addresses from.

	Command	**Explanation**
Step 1	configure terminal	Enter Global Configuration mode.
Step 2	ip dhcp pool <pool_name>	Create a DHCP Pool and assign a name to the pool.
Step 3	network <ipv4_ucast> <ipv4_netmask> **or** host <ipv4_ucast> <ipv4_netmask>	Specify the subnet or individual IP address in which the pool can assign IP addresses from. When using the **network** parameter, the pool will select IP addresses from the entire subnet to assign to DHCP clients. If the **host** parameter is used, only a single DHCP client will be assigned **<ipv4_ucast>** and **<ipv4_netmask>.** **Note:** When using the **host** parameter, the **client-identifier** must be specified for the single DHCP client to receive DHCP information. See **Step 10** for setting the **client-identifier.**
Step 4	default-router <ipv4_ucast> [ipv4_ucast] [ipv4_ucast] [ipv4_ucast]	Specify the IP address of the default gateway. Up to four default gateways can be configured. The DHCP server will provide hosts

		with however many default gateways have been configured.
Step 5	dns-server <ipv4_ucast> [ipv4_ucast] [ipv4_ucast] [ipv4_ucast]	Specify the IP address of the DNS server to advertise in DHCP advertisements. Up to four DNS servers can be advertised to hosts.
Step 6	broadcast <ipv4_ucast>	**(Optional)** Specify the broadcast address for the subnet in which the hosts are members of.
Step 7	ntp-server <ipv4_ucast> [ipv4_ucast] [ipv4_ucast] [ipv4_ucast]	**(Optional)** Specify the IP of the NTP servers to advertise in DHCP advertisements. Up to four NTP servers can be configured. **Note:** NTP server information will only be advertised to the host if the host requests NTP information in the Discover Message.
Step 8	domain-name <domain_name>	**(Optional)** Specify the domain name that hosts should use when resolving hostnames via DNS. The domain name can be up to 128 characters in length.
Step 9	lease {infinite | <days> <hours> <minutes>}	**(Optional)** Specify how long addresses are leased to hosts for. By default, IP addresses are leased to hosts for 24 hours. If set to **infinite,** leases never expire. The DHCP client will attempt to renew its lease as soon as 50% of the period has expired.
Step 10	client-identifier {fqdn <fqdn> | mac-address <mac_address> | name <name>}	This command is required when the pool type is set to **host.** DHCP Discover messages broadcasted from potential DHCP clients containing a matching client identifier will be assigned the IP address specified in the **host <ipv4_ucast> <ipv4_netmask>** command.
Step 11	hardware-address <mac_ucast>	**(Optional)** Specify the client's hardware address to be used when the pool type is set to host.
Step 12	reserved-only	**(Optional)** Restrict the assignable IP addresses to those contained within the Reserved Addresses Table.

		Entries of the Reserved Address Table are configured using the **address <ipv4_ucast> interface {GigabitEthernet <1/1-24>, 10GigabitEthernet<1/1-2>}**
Step 13	address <ipv4_ucast> interface {GigabitEthernet <1/1-24>, 10GigabitEthernet<1/1-2>}	**(Optional)** Create an entry in the Reserved IP Addresses Table. If **reserved-only** is set, only IP addresses contained in the Reserved IP table will be assigned to DHCP clients.
Step 14	netbios-node-type {b-node | h-node | m-node | p-node}	**(Optional)** Configure the NetBIOS Node Type. The NetBIOS Node Type determines the method in which a DHCP client will resolve a NetBIOS name into an IP address. **<u>B-node:</u>** Uses broadcast traffic for name resolution. Traffic is limited to the local network since routers will not forward broadcast traffic. **<u>P-node:</u>** Uses an NBNS (NetBIOS name server) such as WINS to resolve NetBIOS names. P-node will directly query the name server, allowing computers to query the NBNS across a network boundary. All computers configured with p-node must also be configured with the NBNS's IP address. **<u>M-node (Mixed):</u>** M-node attempts to resolve the NetBIOS name into an IP address via B-node. If the NetBIOS name cannot be resolved, the computer will attempt to use P-node to resolve the NetBIOS name into an IP address. **<u>H-node (Hybrid):</u>** H-node is like M-node except the order is reversed. Initially P-node will be used by default. If P-node fails, the computer will attempt to use B-node to resolve the NetBIOS name.
Step 15	netbios-scope <scope>	**(Optional)** Configure the NetBIOS Scope ID. The NetBIOS Scope ID is a string appended to the NetBIOS name. The Scope ID provides a means to isolate multiple computers which only need to communicate with each other.

		Computers configured with the same Scope ID all belong to the same scope. The scope ID is limited to 128 characters.
Step 16	nis-domain-name <domain_name>	**(Optional)** Specify the name of the client's NIS domain.
Step 17	nis-server <ipv4_ucast> [ipv4_ucast] [ipv4_ucast] [ipv4_ucast]	**(Optional)** Specify the IP address of NIS servers which are available to DHCP clients. Up to four NIS servers can be advertised within DHCP offer messages (if requested by the client).
Step 18	vendor class-identifier <class_id> specific-info <hex-value>	**(Optional)** DHCP Discover messages contain a class-identifier identifying the type of endpoint. A class-identifier and specific-info can be configured within the DHCP Pool such that when a device makes a request with a matching class-identifier, specific configuration details can be sent to the client. **Example Class Identifiers:** "MSFT 5.0" for Windows 2000 clients are newer. "alcatel.noe.0" for Alcatel IP touch phones. "MSFT 98" for Windows 98 and Me clients. Up to 4 different vendor class-identifiers and specific-information combinations can be configured.
Step 19	end	**(Optional)** Return to Privileged EXEC mode.
Step 20	copy running-config startup-config	**(Optional)** Copy the contents of the running-config to the startup-config.

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# ip dhcp pool TESTPOOL
FLEX24-10G(config-dhcp-pool)# network 192.168.100.0 255.255.255.0
FLEX24-10G(config-dhcp-pool)# default-router 192.168.100.1 192.168.100.254 192.168.100.253
192.168.100.252
FLEX24-10G(config-dhcp-pool)# dns-server 8.8.8.8 199.85.126.10 208.67.222.222 84.200.69.80
FLEX24-10G(config-dhcp-pool)# broadcast 192.168.100.255
FLEX24-10G(config-dhcp-pool)# ntp-server 149.56.27.12 50.101.251.61 35.183.8.3 162.159.200.1
FLEX24-10G(config-dhcp-pool)# domain-name testdomain.com
FLEX24-10G(config-dhcp-pool)# netbios-node-type h-node
FLEX24-10G(config-dhcp-pool)# nis-domain-name anothertestdomain.com
FLEX24-10G(config-dhcp-pool)# nis-server 192.168.100.100 192.168.100.101 192.168.100.102
192.168.100.103
FLEX24-10G(config-dhcp-pool)# lease 0 12 0
```

```
FLEX24-10G(config-dhcp-pool)# vendor class-identifier "MSFT 5.0" specific-info 0x00
```

Enabling the DHCP Server

Once the DHCP pool has been properly configured, the server is not yet operational. The server must be enabled both globally and on the VLAN in which the clients are located.

	Command	Explanation
Step 1	configure terminal	Enter Global Configuration mode.
Step 2	ip dhcp server	Enable the DHCP Server globally.
Step 3	interface vlan <vlan_id>	Enter VLAN Interface Configuration mode for the VLAN to enable to DHCP server on.
Step 4	ip dhcp server	Enable the DHCP server on the specific VLAN.
Step 5	ip address <ipv4_addr> <subnet_mask>	Assign an IP address to the virtual VLAN interface. The IP address should be within the address range of the DHCP pool but also be explicitly excluded from assignment.
Step 5	end	**(Optional)** Return to Privileged EXEC mode.
Step 6	copy running-config startup-config	**(Optional)** Copy the contents of the running-config to the startup-config.

```
Username: admin
Password:
FLEX24-10G# configure terminal
FLEX24-10G(config)# ip dhcp server
FLEX24-10G(config)# interface vlan 1
FLEX24-10G(config-if-vlan)# ip dhcp server
FLEX24-10G(config-if-vlan)# end
FLEX24-10G# copy running-config startup-config
Building configuration...
% Saving 3037 bytes to flash:startup-config
FLEX24-10G#
```

At this point the DHCP server will be operational and will be leasing IP addresses to all clients (on the VLAN configured with the **ip dhcp server** command) configured to receive their IP address via DHCP. To bind a DHCP Pool to an VLAN, the VLAN interface must have an IP address within the address range for the DHCP Pool.

For example: Configure the FLEX24-10G with a DHCP server on the 192.168.100.0/24 network. The 192.168.100.0/24 address range will be in VLAN 100.

This would be performed as follows:

1. Create a DHCP pool with a network statement of **network 192.168.100.0 255.255.255.0**, and a broadcast statement of **broadcast 192.168.100.255.** Configure any other required DHCP values.
2. Create VLAN 100 and interface VLAN 100. Assign an IP address from the 192.168.100.0/24 subnet to the VLAN 100 interface.

3. Enable the DHCP server from global configuration mode and on the VLAN 100 interface. This is done using the **ip dhcp server** command.
4. Assign all applicable edge ports to VLAN 100. This is done with the **switchport mode access** and **switchport access vlan 100** commands from interface configuration mode.

DHCP Snooping and Relay

DHCP snooping is a security feature which is designed to drop DHCP traffic deemed to be unacceptable. DHCP traffic could be considered unacceptable for a variety of reasons. When DHCP snooping is enabled, only traffic from trusted DHCP servers will be permitted. A DHCP server is said to be trusted if its directly connected FLEX24-10G interface is in a trusted state. DHCP messages are permitted to flow through trusted interfaces but will be dropped if found on an untrusted interface.

Additionally, DHCP messages with a source MAC address and client MAC address which do not match will be dropped by DHCP snooping enabled switches.

Finally, if a DHCP release or decline message is found on an interface other than the interface in which the original DISCOVER -> OFFER -> REQUEST -> ACK exchange occurred, these frames are dropped. This feature prevents a rogue party from terminating a lease or declining an offer on behalf of a trusted DHCP server.

DHCP Relay is used when the DHCP client and server do not reside on the same subnet. Without DHCP relay, when the client and server reside on different subnets, the DHCPDISCOVER and DHCPOFFER messages would never reach the server since routers do not forward broadcast traffic. With DHCP relay, the relay agent acts as the middleman between the clients and the DHCP server, forwarding DHCP messages between the two.

Note: A DHCP server cannot be running on the FLEX24-10G for DHCP relay to be enabled.

DHCP for IPv4 (DHCPv4) Snooping

Enabling DHCPv4 Snooping

DHCP Snooping is enabled from Global Configuration mode with the **ip dhcp snooping** command.

	Command	Explanation
Step 1	configure terminal	Enter Global Configuration mode.
Step 2	ip dhcp snooping	Enable DHCPv4 snooping.
Step 3	end	**(Optional)** Return to Privileged EXEC mode.
Step 4	copy running-config startup-config	**(Optional)** Copy the contents of the running-config to the startup-config.

```
Username: admin
Password:
FLEX24-10G# configure terminal
FLEX24-10G(config)# ip dhcp snooping
FLEX24-10G(config)# end
FLEX24-10G# copy startup-config running-config
FLEX24-10G#
```

Configuring Trusted and Untrusted Interfaces

Trusted and Untrusted interfaces act as gateways for DHCP traffic. DHCP traffic is allowed on trusted interfaces and dropped on untrusted interfaces. For DHCPv4 snooping, all interfaces are configured as trusted by default.

Setting an Interfaces Trust State

	Command	Explanation
Step 1	configure terminal	Enter Global Configuration mode.
Step 2	interface {*, Gigabit Ethernet <1/1-24>, 10GigabitEthernet<1/1-2>}	Enter Interface Configuration mode the interface(s) for which to change the trust state.
Step 3	[no] ip dhcp snooping trust	Modify the interface's trust state. By default, when DHCPv4 snooping is enabled, all interfaces are configured as Untrusted. To configure an interface to be untrusted the **no** form must be appended.
Step 4	end	**(Optional)** Return to Privileged EXEC mode.
Step 5	copy running-config startup-config	**(Optional)** Copy the contents of the running-config to the startup-config.

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# interface GigabitEthernet 1/1
FLEX24-10G(config-if)# no ip dhcp snooping trust
FLEX24-10G(config-if)# end
FLEX24-10G# copy running-config startup-config
Building configuration...
% Saving 4257 bytes to flash:startup-config
FLEX24-10G#
```

DHCPv4 Relay

Configuring DHCPv4 Relay

DHCPv4 Relay is enabled from Global Configuration mode with the **ip dhcp relay** command.

	Command	Explanation
Step 1	configure terminal	Enter Global Configuration mode.
Step 2	ip dhcp relay	Enable DHCPv4 relay.
Step 3	end	**(Optional)** Return to Privileged EXEC mode.
Step 4	copy running-config startup-config	**(Optional)** Copy the contents of the running-config to the startup-config.

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# ip dhcp relay
FLEX24-10G(config)# end
FLEX24-10G# copy running-config startup-config
Building configuration...
% Saving 1987 bytes to flash:startup-config
FLEX24-10G#
```

Figure 1 below illustrates a network topology where the hosts reside on the 192.168.100.0/24 network while the DHCP server resides on the 192.168.99.0/24 network. Since the hosts and the DHCP server are on different subnets, the FLEX24-10G will need to act as a relay agent.

The below commands would reflect the commands which would need to be executed on the FLEX24-10G in Figure 1 for a correct DHCPv4 relay configuration.

	Command	Explanation
Step 1	configure terminal	Enter Global Configuration mode.
Step 2	ip helper-address 192.168.99.2	Configure an IP helper-address. An IP help-address should map to the IP address of the DHCP server. When the FLEX24-10G receives DHCP traffic from the 192.168.100.0/24 network, the destination IP address of the DHCP traffic will be modified to the IP address specified in the **ip helper-address** command. This ensures that the traffic will be properly delivered to the DHCP server. In the case of Figure 1's topology, the destination address will be changed to 192.168.99.2.
Step 3	ip dhcp relay information option	**(Optional)** Enable DHCP relay information mode. When DHCP relay information mode is enabled, the relay agent will insert specific information into DHCP frames destined for the server and will remove that same information from frames destined for the client. **Note:** DHCPv4 relay must be enabled for this feature to take effect.
Step 4	ip dhcp relay information policy {drop | keep | replace}	**(Optional)** The Relay Information Policy controls the agent's behavior when receiving DHCP traffic with relay agent information. **Drop:** Drop the relay agent information when a frame containing relay agent information is received. **Keep:** Keep the relay agent information when a frame containing relay agent information is received.

		Replace: Replace the original relay information when a DHCP message that already contains it is received.
Step 5	end	**(Optional)** Return to Privileged EXEC mode.
Step 6	copy running-config startup-config	**(Optional)** Copy the contents of the running-config to the startup-config.

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# ip helper-address 192.168.99.2
FLEX24-10G(config)# ip dhcp relay information option
FLEX24-10G(config)# ip dhcp relay information policy keep
FLEX24-10G(config)# end
FLEX24-10G# copy running-config startup-config
Building configuration...
% Saving 2020 bytes to flash:startup-config
FLEX24-10G#
```

Note: The directly connected interface to the DHCP server must be configured as a trusted interface. For the FLEX24-10G in Figure 1, this interface would be GigabitEthernet 1/2. By default, all IPv4 interfaces are trusted.

	Command	**Explanation**
Step 1	configure terminal	Enter Global Configuration mode.
Step 2	interface GigabitEthernet 1/2	Enter Interface Configuration mode for GigabitEthernet 1/2.
Step 3	ip dhcp snooping trust	Configure GigabitEthernet 1/2 as a trusted interface.
Step 4	end	**(Optional)** Return to Privileged EXEC mode.
Step 5	copy running-config startup-config	**(Optional)** Copy the contents of the running-config to the startup-config.

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# interface GigabitEthernet 1/2
FLEX24-10G(config-if)# ip dhcp snooping trust
FLEX24-10G(config-if)# end
FLEX24-10G# copy running-config startup-config
Building configuration...
% Saving 2020 bytes to flash:startup-config
FLEX24-10G#
```

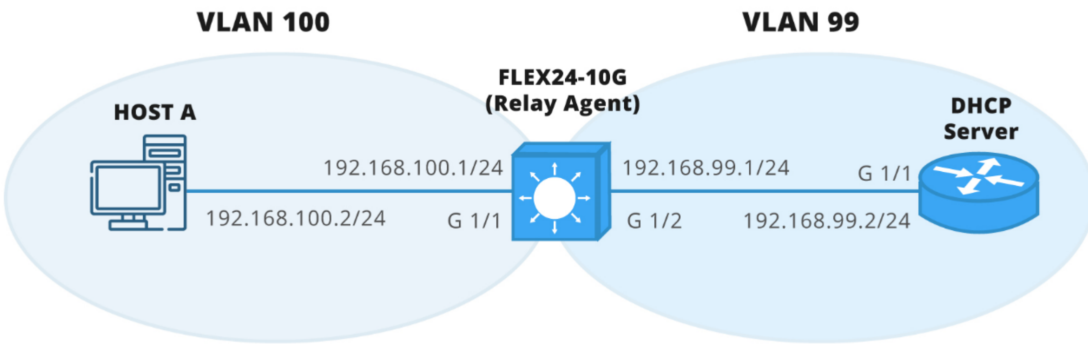


Figure 1: DHCPv4 Relay

DHCP for IPv6 (DHCPv6) Snooping

Enabling DHCPv6 Snooping

DHCP Snooping is enabled from Global Configuration mode with the **ip dhcp snooping** command.

	Command	Explanation
Step 1	configure terminal	Enter Global Configuration mode.
Step 2	ipv6 dhcp snooping	Enable DHCPv6 snooping.
Step 3	end	**(Optional)** Return to Privileged EXEC mode.
Step 4	copy running-config startup-config	**(Optional)** Copy the contents of the running-config to the startup-config.

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# DHCPv6 snooping
FLEX24-10G(config)# end
FLEX24-10G# copy running-config startup-config
Building configuration...
% Saving 4257 bytes to flash:startup-config
FLEX24-10G#
```

Configuring Trusted and Untrusted Interfaces

Trusted and Untrusted interfaces function in the same way with IPv6 as with IPv4.

Setting an Interfaces Trust State

	Command	Explanation
Step 1	configure terminal	Enter Global Configuration mode.
Step 2	interface {*, Gigabit Ethernet <1/1-24>, 10GigabitEthernet<1/1-2>}	Enter Interface Configuration mode the interface(s) for which to change the trust state.
Step 3	ipv6 dhcp snooping trust	Modify the interface's trust state.

		By default, when DHCPv6 snooping is enabled, all interfaces are configured as untrusted.
Step 4	end	**(Optional)** Return to Privileged EXEC mode.
Step 5	copy running-config startup-config	**(Optional)** Copy the contents of the running-config to the startup-config.

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# interface GigabitEthernet 1/1
FLEX24-10G(config-if)# DHCPv6 snooping trust
FLEX24-10G(config-if)# end
FLEX24-10G# copy running-config startup-config
Building configuration...
% Saving 4257 bytes to flash:startup-config
FLEX24-10G#
```

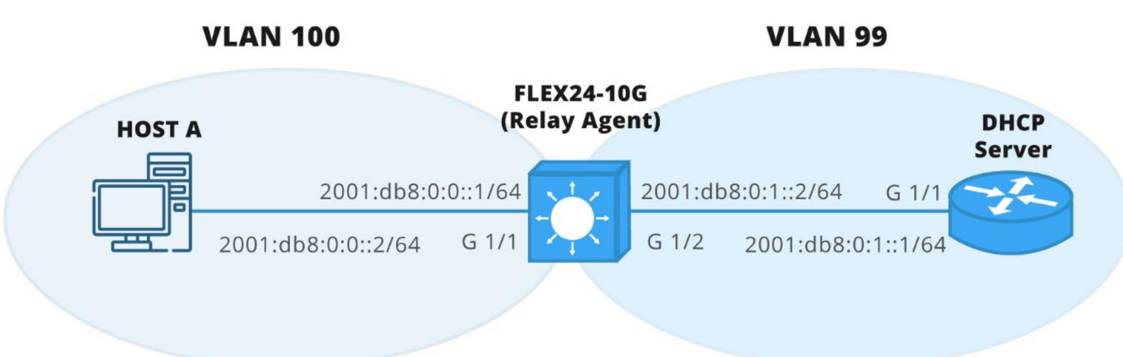
DHCPv6 Relay

DHCPv6 relay works functionally the same as DHCPv4 however both are configured in different ways.

Configuring DHCPv6 Relay

DHCPv6 relay is configured at the VLAN interface level of the VLAN which the clients are located. Given the below topology, HOST A is in VLAN 100 while the DHCP server is located in VLAN 99.

DHCPv6 relay configuration takes places at the VLAN interface level for VLAN 100.



The below commands reflect the configuration which would need to take place on the FLEX24-10G in the above topology.

	Command	Explanation
Step 1	configure terminal	Enter Global Configuration mode.

Step 2	interface vlan 100	Enter VLAN Interface Configuration mode for VLAN 100.
Step 3	ipv6 dhcp relay destination 2001:db8:0:1::1 interface vlan 99	Relay DHCP traffic from VLAN 100 to the destination address of 2001:db8:0:1::1 which is a member of VLAN 99. Optionally, **destination 2001:db8:0:1::1** can be omitted and the relay agent will broadcast DHCP traffic on VLAN 99 rather than unicasting DHCP traffic.
Step 4	end	**(Optional)** Return to Privileged EXEC mode.
Step 5	copy running-config startup-config	**(Optional)** Copy the contents of the running-config to the startup-config.

Verification

DHCPv4 Verification Commands

show ip dhcp detailed statistics {client … | combined … | normal-forward … | relay … | server … | snooping …}: Displays detailed statistics regarding various aspects of the DHCPv4 configuration. Best to use the context-sensitive help system to explore all combinations of command parameters.

```
FLEX24-10G# show ip dhcp detailed statistics client
GigabitEthernet 1/1 Statistics:
-------------------------------
Rx Discover:                     0   Tx Discover:                     0
Rx Offer:                        0   Tx Offer:                        0
Rx Request:                      0   Tx Request:                      0
Rx Decline:                      0   Tx Decline:                      0
Rx ACK:                          0   Tx ACK:                          0
Rx NAK:                          0   Tx NAK:                          0
Rx Release:                      0   Tx Release:                      0
Rx Inform:                       0   Tx Inform:                       0
Rx Lease Query:                  0   Tx Lease Query:                  0
Rx Lease Unassigned:             0   Tx Lease Unassigned:             0
Rx Lease Unknown:                0   Tx Lease Unknown:                0
Rx Lease Active:                 0   Tx Lease Active:                 0
Rx Discarded checksum error:     0

GigabitEthernet 1/2 Statistics:
-------------------------------
Rx Discover:                     0   Tx Discover:                     0
Rx Offer:                        0   Tx Offer:                        0
Rx Request:                      0   Tx Request:                      0
Rx Decline:                      0   Tx Decline:                      0
Rx ACK:                          0   Tx ACK:                          0
Rx NAK:                          0   Tx NAK:                          0
```

```
Rx Release:                     0   Tx Release:                     0
Rx Inform:                      0   Tx Inform:                      0
Rx Lease Query:                 0   Tx Lease Query:                 0
Rx Lease Unassigned:            0   Tx Lease Unassigned:            0
Rx Lease Unknown:               0   Tx Lease Unknown:               0
Rx Lease Active:                0   Tx Lease Active:                0
Rx Discarded checksum error:    0

GigabitEthernet 1/3 Statistics:
         ------------------------------OUTPUT TRUNCATED------------------------------
```

show ip dhcp excluded-address: Displays all IP addresses which have been excluded from being leased to clients.

```
FLEX24-10G# show ip dhcp excluded-address

     Low Address      High Address
     ---------------  ---------------
01   192.168.100.10   192.168.100.15
02   192.168.100.20   192.168.100.20
03   192.168.100.21   192.168.100.21
04   192.168.100.22   192.168.100.22
05   192.168.100.23   192.168.100.23
06   192.168.100.24   192.168.100.24

FLEX24-10G#
```

show ip dhcp pool [<pool_name>]: Displays all the configured DHCPv4 pools. Output can be filtered to only include details for a specific DHCP pool.

```
FLEX24-10G# show ip dhcp pool TESTPOOL

Pool Name: TESTPOOL
----------------------------------------------
  Type is network
  IP is 192.168.100.0
  Subnet mask is 255.255.255.0
  Subnet broadcast address is 192.168.100.255
  Lease time is 12 hours 0 minutes
  Default routers are 192.168.100.1 192.168.100.254 192.168.100.253 192.168.100.252
  Domain name is testdomain.com
  DNS servers are 8.8.8.8 199.85.126.10 208.67.222.222 84.200.69.80
  NTP servers are 149.56.27.12 50.101.251.61 35.183.8.3 162.159.200.1
  Netbios name server is -
  Netbios node type is H node
  Netbios scope identifier is -
  NIS domain name is anothertestdomain.com
  NIS servers are 192.168.100.100 192.168.100.101 192.168.100.102 192.168.100.103
  Vendor class identifier is "MSFT 5.0" with
```

```
       specific information is
  Client identifier is -
  Hardware address is -
  Client name is -
  Is not restricted to reserved addresses:
    No reserved addresses are configured
FLEX24-10G#
```

show ip dhcp relay [statistics]: Displays relay agent configuration.

```
FLEX24-10G# show ip dhcp relay
Switch DHCP relay mode is enabled
Switch DHCP relay server address is 192.168.99.2
Switch DHCP relay information option is enabled
Switch DHCP relay information policy is drop
FLEX24-10G#
```

show ip dhcp server [binding [<ipv4_ucast> | state {allocated | committed | expired} | type {automatic | expired | manual}] | declined-ip <ipv4_addr> | statistics]: Displays DHCPv4 server configuration information.

```
FLEX24-10G# show ip dhcp server

DHCP server is globally enabled.
  Enabled VLANs are 1.

FLEX24-10G#
```

show ip dhcp server binding [<ipv4_ucast> | state {allocated | committed | expired} | type {automatic | expired | manual}]: Displays DHCP server address lease information.

show ip dhcp snooping [interface <interface-id> | table]: Displays DHCPv4 snooping configuration information.

```
FLEX24-10G# show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following
GigabitEthernet 1/1 trusted
GigabitEthernet 1/2 trusted
GigabitEthernet 1/3 trusted
GigabitEthernet 1/4 trusted
GigabitEthernet 1/5 trusted
GigabitEthernet 1/6 trusted
GigabitEthernet 1/7 trusted
GigabitEthernet 1/8 trusted
GigabitEthernet 1/9 trusted
GigabitEthernet 1/10 trusted
GigabitEthernet 1/11 trusted
```

```
GigabitEthernet 1/12 trusted
GigabitEthernet 1/13 trusted
GigabitEthernet 1/14 trusted
GigabitEthernet 1/15 trusted
GigabitEthernet 1/16 trusted
GigabitEthernet 1/17 trusted
GigabitEthernet 1/18 trusted
GigabitEthernet 1/19 trusted
GigabitEthernet 1/20 trusted
GigabitEthernet 1/21 trusted
GigabitEthernet 1/22 trusted
GigabitEthernet 1/23 trusted
GigabitEthernet 1/24 trusted
GigabitEthernet 1/25 trusted
10GigabitEthernet 1/1 trusted
10GigabitEthernet 1/2 trusted
FLEX24-10G#
```

DHCPv6 Verification Commands

show ipv6 dhcp relay [statistics] [interface vlan <vlan_id>]: Displays DHCPv6 relay agent configuration.

```
FLEX24-10G# show ipv6 dhcp relay
Relaying interface vlan 6 to fd00:0:0:1::2 on interface vlan 2
FLEX24-10G#
```

show ipv6 dhcp snooping [interface <interface-id> | statistics [zero-suppress] [interface <interface-id>] | table [all]]: Displays DHCPv6 snooping configuration information.

```
FLEX24-10G# show ipv6 dhcp snooping
Switch DHCPv6 Configuration:
- DHCPv6 snooping is Enabled
- IPv6 packets with unknown ext. headers will be allowed

DHCPv6 snooping per-port configuration:
 Port Name                     Trust Mode
 --------------------------------------------------
 GigabitEthernet 1/1           Trusted
 GigabitEthernet 1/2           Trusted
 GigabitEthernet 1/3           Trusted
 GigabitEthernet 1/4           Trusted
 GigabitEthernet 1/5           Trusted
 GigabitEthernet 1/6           Untrusted
 GigabitEthernet 1/7           Untrusted
 GigabitEthernet 1/8           Untrusted
 GigabitEthernet 1/9           Untrusted
 GigabitEthernet 1/10          Untrusted
 GigabitEthernet 1/11          Untrusted
 GigabitEthernet 1/12          Untrusted
```

```
 GigabitEthernet 1/13         Untrusted
 GigabitEthernet 1/14         Untrusted
 GigabitEthernet 1/15         Untrusted
 GigabitEthernet 1/16         Untrusted
 GigabitEthernet 1/17         Untrusted
 GigabitEthernet 1/18         Untrusted
 GigabitEthernet 1/19         Untrusted
 GigabitEthernet 1/20         Untrusted
 GigabitEthernet 1/21         Untrusted
 GigabitEthernet 1/22         Untrusted
 GigabitEthernet 1/23         Untrusted
 GigabitEthernet 1/24         Untrusted
 GigabitEthernet 1/25         Untrusted
 10GigabitEthernet 1/1        Untrusted
 10GigabitEthernet 1/2        Untrusted
FLEX24-10G#
```

show ipv6 dhcp-client [interface vlan <vlan_id>]: Displays IPv6 client information. Output can be filtered to only include client information for a specific VLAN.

Chapter 24: IGMP Snooping

Introduction

With traditional unicast and broadcast traffic, data can successfully be sent to where it needs to go but often at the expense of network resources; in the cast of broadcasts, some devices may receive traffic not intended for them. Multicast solves this issue by sending network traffic to only the devices which require it.

Multicast allows network devices to subscribe to a multicast group. A multicast group is denoted by an IPv4 address within the range of 224.0.0.0 to 239.255.255.255 or an IPv6 address with the prefix ff00::/8. Once a device has subscribed to a group, it will receive all traffic with a destination IP address which matches the group.

IGMP is the Internet Group Management Protocol. IGMP snooping allows a switch to eavesdrop on the IGMP conversation between hosts and routers. Without IGMP snooping a switch would not be able to determine which multicast groups are needed on which switch interfaces. The absence of IGMP snooping on a switch would create a network where the switch broadcasts all multicast traffic it receives from the router.

IGMP Versions

There are three versions of IGMP, IGMPv1, IGMPv2, and IGMPv3. All three versions are backwards compatible with any previous versions.

IGMPv1

IGMPv1 was the first version of IGMP defined in RFC 1112. IGMPv1 has two different kinds of messages, Membership Query and Membership Reply messages.

Multicast query messages originate from the multicast routers and always had a destination address of 224.0.0.1. Membership Queries are sent out from the router every 60 seconds and are used to determine which multicast groups are still in use. In IGMPv1, group members had no way of informing the multicast router that they have left a group. Because of this, there could be up to a minute delay before the router realizes that a host has left a group.

Membership Reply messages are sourced by the hosts and are sent to multicast routers. Membership Reply messages allow a host to announce its willingness to join a multicast group.

IGMPv2

IGMPv2 offers several improvements over IGMPv1. Membership Queries are not restricted to a destination address of 224.0.0.1, their destination address can be that of a specific multicast group.

There are two types of Membership Queries with IGMPv2, General Queries and Group-Specific Queries.

General Queries are sent from the multicast router to hosts to determine the multicast groups they are subscribed to. Group-Specific Queries are used to determine whether a host is subscribed to a particular group.

Leave messages were introduced in IGMPv2. Unlike in IGMPv1 where a host had no way of informing the router that it was leaving a group, with IGMPv2 a host can send a Leave message to the router. Leave messages allow multicast routers to stop multicast streams much faster than in IGMPv1.

If multiple multicast routers reside on a network, IGMPv1 would expect all the multicast routers to send query group members. IGMPv2 only allows for one router to be the multicast querier. The router with the lowest IP address on a segment would be chosen to be the multicast querier. Only the router with the lowest IP address can send queries; all other multicast routers can reply to queries.

IGMPv3

IGMPv3 includes all the benefits of IGMPv2 with the addition of source-specific multicast. Multicast groups member configured with IGMPv1 and IGMPv2 receive all multicasts destined for the group they are subscribed to, regardless of the traffic's source address.

Source-specific multicast allows a multicast group subscriber to specify a specific sender to receive traffic from. This feature saves network bandwidth in circumstances when certain group members only require traffic from a particular sender.

Basic IGMP Snooping Configuration

By default, IGMP snooping is enabled on all switch interfaces. To disable IGMP snooping, follow the following procedure:

	Command	Explanation
Step 1	configure terminal	Enter Global Configuration mode.
Step 2	no ip igmp snooping	Disables IGMP snooping.
Step 3	end	**(Optional)** Exit Interface Configuration mode and return to Privileged EXEC mode.
Step 4	copy running-config startup-config	**(Optional)** Copy the contents of the running-config to the startup-config.

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# no ip igmp snooping
FLEX24-10G(config)# end
FLEX24-10G# copy running-config startup-config
Building configuration...
% Saving 3650 bytes to flash:startup-config
FLEX24-10G#
```

When a host no longer wants to receive traffic destined for a multicast group, it can issue a leave message which is forwarded to the router by the switch. Additionally, a host will send a join message to the router if the host would like to join a multicast group.

The switch can be configured such that it will not forward unnecessary join or leave messages to the router. The below commands demonstrate such a configuration:

	Command	Explanation
Step 1	configure terminal	Enter Global Configuration mode.
Step 2	ip igmp host-proxy [leave-proxy]	Enables IGMP Proxy. IGMP Proxy disables the forwarding of unnecessary join and leave messages to the router. The **leave-proxy** keyword disables the forwarding of leave messages only.
Step 3	end	**(Optional)** Exit Interface Configuration mode and return to Privileged EXEC mode.
Step 4	copy running-config startup-config	**(Optional)** Copy the contents of the running-config to the startup-config.

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# ip igmp host-proxy leave-proxy
FLEX24-10G(config)# end
FLEX24-10G# copy running-config startup-config
Building configuration...
% Saving 3681 bytes to flash:startup-config
FLEX24-10G#
```

Source Specific Multicast

A Source-Specific Multicast (SSM) range allows IGMPv3 hosts and routers to run the same SSM model for all multicast groups in the specified range.

Specifying an SSM Range

	Command	Explanation
Step 1	configure terminal	Enter Global Configuration mode.
Step 2	ip igmp ssm-range <ipv4_mcast> <prefix_length>	Specify a Source Specific Multicast Range. **<ipv4_mcast>** must be a valid multicast address. **<prefix_length>** must be a value from 4 to 32. The **<prefix_length>** identifies the number of network bits in the multicast address. Together the **<ipv4_mcast>** and the **<prefix_length>** identify the range of multicast addresses.
Step 3	end	**(Optional)** Return to Privileged EXEC mode.

Step 4	copy running-config startup-config	**(Optional)** Copy the contents of the running-config to the startup-config.

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# ip igmp ssm 224.0.0.0 8
FLEX24-10G(config)#end
FLEX24-10G# copy running-config startup-config
```

Throttling, Routed Ports, and Fast Leave

By enabling throttling on a switchport, the administrator can limit the amount of multicast groups which an interface can belong to. By default, there is no limit to the amount of multicast groups a switchport can belong to.

Routed ports are switch interfaces which lead to a Layer-3 multicast device or IGMP querier. If the link from the switch to the router is an aggregation, the entire aggregation will act as a routed port.

When a single IGMPv2 host is connected to a switchport, it is highly recommended to configure that interface with Fast Leave. A port configured with Fast Leave will remove the system group record and stop forwarding data upon receiving the IGMPv2 leave message. The interface will also not send any last member query messages.

	Command	**Explanation**
Step 1	configure terminal	Enter Global Configuration mode.
Step 2	interface {*, GigabitEthernet <1/1-24>, 10GigabitEthernet<1/1-2>}	Enter Interface Configuration mode for the interface(s) to configure.
Step 3	ip igmp snooping max-groups <1-10>	**(Optional)** Configure a limit to the amount of multicast groups an interface can belong to. The maximum value must be within the range of 1 to 10 inclusive. By default, there is no limit.
Step 4	ip igmp snooping mrouter	**(Optional)** Configure the interface as a router port.
Step 5	ip igmp snooping immediate-leave	**(Optional)** Configure the interface with Fast Leave.
Step 6	ip igmp snooping filter <profile_name>	Configure the interface with an IPMC profile named **<profile_name>.** Details on configuring an IPMC profile below.
Step 7	end	**(Optional)** Exit Interface Configuration mode and return to Privileged EXEC mode.
Step 8	copy running-config startup-config	**(Optional)** Copy the contents of the running-config to the startup-config.

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# interface GigabitEthernet 1/1
FLEX24-10G(config-if)# ip igmp snooping max-groups 8
FLEX24-10G(config-if)# ip igmp snooping immediate-leave
FLEX24-10G(config-if)# ip igmp snooping filter testing
```

```
FLEX24-10G(config-if)# end
FLEX24-10G# copy running-config startup-config
```

Creating an IPMC Profile

IPMC profiles are used to configure access control on multicast streams. The FLEX24-10G supports 64 profiles with each profile supporting 128 rules.

Each rule in an IPMC profile contains an index number, which identifies its order in the profile, an entry name, address range, permit/deny action, and a logging action.

	Command	**Explanation**
Step 1	configure terminal	Enter Global Configuration mode.
Step 2	[no] ipmc profile	Enable/Disable the Global IPMC Profile.
Step 3	ipmc range <entry_name> {<start_ipv4_mcast> | <start_ipv6_mcast>} [<end_ipv4_mcast> | <end_ipv6_mcast>] **Example**: ipmc range testingrange 224.0.0.1 224.255.255.255	Configure a multicast address range. A range can include a single address or a starting address and an ending address.
Step 4	ipmc profile <profile_name>	Create an IPMC profile. **<profile_name>** cannot exceed 16 characters.
Step 5	description <description>	**(Optional)** Give the IPMC profile a description. **<description>** cannot exceed 64 characters.
Step 6	range <range_entry> {deny | permit} [log] [next <range_entry>] **Example**: range testingrange deny log	Maps the range created in Step 3 to the IPMC profile created in Step 4. **{permit | deny}** describes the switch's action when receiving a Join/Report frame originating from a multicast group with the address range. The **[log]** parameter indicates the logging preference when receiving a Join/Report frame originating from a multicast group within the address range. If **[log]** is set, the corresponding information of the group address

		that matches the range specified in the rule, will be logged. The **next <range_entry>** parameter allows the administrator to specify which range entry should follow the current one. This allows the range entries to be placed in a specific order. If **next <range_entry>** is not specified, the entry will be placed at the bottom of the rule list. Additional ranges can be mapped to the IPMC profile by repeating Step 3 and Step 6.
Step 7	end	**(Optional)** Return to Privileged EXEC mode.
Step 8	copy running-config startup-config	**(Optional)** Copy the contents of the running-config to the startup-config.

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# ipmc profile
FLEX24-10G(config)# ipmc range testingrange 224.0.0.1 224.255.255.255
FLEX24-10G(config)# ipmc profile testing
FLEX24-10G(config-ipmc-profile)# description Testing Profile
FLEX24-10G(config-ipmc-profile)# range testingrange deny log
% Notice that this profile performs deny action for all groups since there is no any permit
entry is included in the profile name 'testing'.
FLEX24-10G(config-ipmc-profile)# end
FLEX24-10G#
```

IGMP Snooping VLAN Configuration

Every VLAN on the FLEX24-10G will also have its own entry in the IGMP Snooping VLAN Table. The IGMP Snooping VLAN Table allows for a per-VLAN IGMP snooping configuration. Although the FLEX24-10G supports up to 4096 VLANs, only 128 VLANs can be configured with IGMP snooping.

	Command	Explanation
Step 1	configure terminal	Enter Global Configuration mode.
Step 2	interface <vlan_id>	Enter VLAN Interface Configuration mode for the VLAN interface to configure.
Step 3	ip igmp snooping	Enables per-VLAN IGMP snooping.
Step 4	ip igmp snooping querier election	**(Optional)** Enable the switch to enter the IGMP Querier election in the VLAN.

		When this command is not issued, the switch will not act as an IGMP Querier.
Step 5	ip igmp snooping querier address <ipv4_address>	**(Optional)** Set the IP address which the switch should use in the IP header for the IGMP Querier election. The candidate with the lowest IP address will win the election and will serve as the IGMP querier for their VLAN. **Note:** If no querier address is set, the switch will use the IP address of the VLAN's SVI. If no SVI IP address is set, the switch will use the first available management address. Finally, if there are no available management addresses the switch will assign 192.0.2.1.
Step 6	ip igmp snooping compatibility {auto | v1 | v2 | v3}	**(Optional)** Set the VLAN interface IGMP compatibility level. By default, the compatibility is set to **auto.** A setting of auto will allow the VLAN to be compatible will all three versions of IGMP. Including the **v1, v2,** or **v3** parameter will force the VLAN to operate in either IGMPv1, IGMPv2, or IGMPv3 mode, respectively.
Step 7	ip igmp snooping priority <0-7>	**(Optional)** Set the IGMP snooping CoS priority level. This setting indicates the priority level of IGMP control frames generated by the switch. By default, the priority level is set to 0 (best effort). Valid priority levels are from 0 (lowest priority) to 7 (highest priority).
Step 8	ip igmp snooping robustness-variable <1-255>	**(Optional)** The IGMP Robustness Variable allows the administrator to allow for expected packet loss on a VLAN. The Robustness Variable is also used to determine the following IGMP message intervals: • Group Member Interval • Other querier present interval • Last-member query count The default robustness-variable value is 2, with valid values ranging from 1 to 255 inclusive.
Step 9	ip igmp snooping query-interval <1-31744>	**(Optional)** Set how often the IGMP querier will send out General Queries.

		The default query-interval is 125 seconds, with valid values ranging from 1 to 31744 inclusive.
Step 10	ip igmp snooping query-max-response-time <0-31774>	**(Optional)** Set the maximum amount of time in which stations must respond to IGMP queries once they have been received. The Maximum Response Interval is advertised within IGMP General Queries. **<0-31774>** specifies a value in tenths of a second. By default, the max-response-time is set to 100 (10 seconds).
Step 11	ip igmp snooping last-member-query-interval <0-31744>	**(Optional)** Set the interval in which the IGMP querier sends group-specific query messages. **<0-31774>** specifies a value in tenths of a second. By default, the last-member-query-interval is set to 10 (1 second).
Step 12	ip igmp snooping unsolicited-report-interval <0-31744>	**(Optional)** Set the time interval of how soon a host should send a second membership report to a multicast group when it first joins. The unsolicited report interval is beneficial when the first membership report sent by the host is lost or damaged. When the unsolicited-report-interval is set the host will automatically send a second membership report **<0-31744>** seconds after the first. By default, the unsolicited-report-interval is 1 second.
Step 13	end	**(Optional)** Return to Privileged EXEC mode.
Step 14	copy running-config startup-config	**(Optional)** Copy the contents of the running-config to the startup-config.

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# interface vlan 1
FLEX24-10G(config-if-vlan)# ip igmp snooping
FLEX24-10G(config-if-vlan)# ip igmp snooping querier election
FLEX24-10G(config-if-vlan)# ip igmp snooping querier address 192.168.0.1
FLEX24-10G(config-if-vlan)# ip igmp snooping compatibility v3
FLEX24-10G(config-if-vlan)# ip igmp snooping priority 0
FLEX24-10G(config-if-vlan)# ip igmp snooping robustness-variable 50
FLEX24-10G(config-if-vlan)# ip igmp snooping query-interval 120
FLEX24-10G(config-if-vlan)# ip igmp snooping query-max-response-time 50
FLEX24-10G(config-if-vlan)# ip igmp snooping last-member-query-interval 20
FLEX24-10G(config-if-vlan)# ip igmp snooping unsolicited-report-interval 2
FLEX24-10G(config-if-vlan)# end
FLEX24-10G# copy running-config startup-config
Building configuration...
% Saving 4314 bytes to flash:startup-config
```

```
FLEX24-10G#
```

Verification

show ip igmp snooping [detail]: Displays general switch wide IGMP information.

show ip igmp snooping [detail] <vlan_list>: Displays IGMP snooping information pertaining to all VLANs in <vlan_list>.

show ip igmp snooping [detail] group-database: Displays the IGMP multicast groups known to the switch.

show ip igmp snooping [detail] group-database interface {*, GigabitEthernet <1/1-24>, 10GigabitEthernet<1/1-2>} [sfm-information]: Displays the IGMP multicast groups present on a particular interface.

show ip igmp snooping [detail] group-database vlan <vlan_id>: Displays the IGMP multicast groups present on a particular VLAN.

show ip igmp snooping mrouter [detail]: Displays information pertaining to interfaces configured as router ports on the switch.

Chapter 25: Multicast VLAN Registration

Introduction

In a typical layer-2 network, multicast streams are not distributed to interfaces belonging to other VLANs. If multiple hosts in multiple VLANs request multicast identical multicast streams, a separate stream is created for each host.

This creation of identical streams for multiple hosts can cause network congestion depending on the number of required streams. In the case of IPTV multicast streams, which consume large amounts of bandwidth, network bandwidth allocation becomes a real concern.

Multicast VLAN Registration (MVR) solves this problem by creating a multicast VLAN. This multicast VLAN becomes the sole VLAN for IPTV multicast traffic. MVR enabled switches will designate its interfaces as either as an Inactive interface, a Source interface, or a Receiver interface.

Inactive interfaces do not participate in MVR operations.

Source interfaces can send and receive multicast data. Multicast subscribers (ex. end hosts) cannot be directly connected to source ports.

Receiver interfaces only receive multicast data. These interfaces only receive data once they have become members of a multicast group.

By default, all interfaces are configured as Inactive.

Configuration

Enabling MVR

By default, MVR is not enabled on the FLEX24-10G. MVR is enabled from Global Configuration as follows:

	Command	Explanation
Step 1	configure terminal	Enter Global Configuration mode.
Step 2	mvr	Enable MVR globally.
Step 3	end	**(Optional)** Return to Privileged EXEC mode.
Step 4	copy running-config startup-config	**(Optional)** Copy the contents of the running-config to the startup-config.

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# mvr
FLEX24-10G(config)# end
FLEX24-10G#
```

Creating a Multicast VLAN

A maximum of four Multicast VLANs can be created. Multicast VLANs are configured from Global Configuration as follows:

	Command	Explanation
Step 1	configure terminal	Enter Global Configuration mode.
Step 2	mvr vlan <vlan_id> [name <mvr_name>]	Create an MVR VLAN. The VLAN can also be named with the optional **name** parameter.
Step 3	mvr name <mvr_name> channel <profile_name>	**(Optional)** Specify an IPMC profile to act as the filter condition for the specified MVR VLAN.
Step 4	mvr name <mvr_name> election	**(Optional)** Allow the switch to join the IGMP Querier Election in the MVR VLAN. By default, the switch acts as a Non-Querier.
Step 5	mvr name <mvr_name> frame {tagged | priority <0-7>}	**(Optional)** Specify whether the traversed IGMP/MLD control frames are to be sent as tagged or untagged. By default, the frames are sent as tagged.
Step 6	mvr name <mvr_name> igmp-address <ipv4_address>	**(Optional)** Specify the IP address to be used when the switch acts as an IGMP Querier. This address is used in the IP header of IGMP control frames.
Step 7	mvr name <mvr_name> last-member-query-interval <0-31744>	**(Optional)** This setting applies when the switch is acting as a Querier. The last-member-query-interval defines the maximum time to wait for IGMP/MLD report memberships on a receiver interface before removing the interface from the multicast group. The time length is specified in tenths of a second. By default, the time is set to 5 tenths, or 0.5 seconds.
Step 8	mvr name <mvr_name> mode {dynamic | compatible}	**(Optional)** Specify the MVR operating mode. **Dynamic:** MVR allows dynamic MVR membership reports on source ports. **Compatible:** MVR memberships are forbidden on source ports.

		By default, the MVR operating mode is Dynamic.
Step 9	end	**(Optional)** Return to Privileged EXEC mode.
Step 10	copy running-config startup-config	**(Optional)** Copy the contents of the running-config to the startup-config.

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# mvr vlan 100 name Testing
FLEX24-10G(config)# mvr name Testing channel test
FLEX24-10G(config)# mvr name Testing election
FLEX24-10G(config)# mvr name Testing frame priority 0
FLEX24-10G(config)# mvr name Testing igmp-address 192.168.1.1
FLEX24-10G(config)# mvr name Testing last-member-query-interval 20
FLEX24-10G(config)# mvr name Testing mode compatible
FLEX24-10G(config)# end
FLEX24-10G# copy running-config startup-config
Building configuration...
% Saving 3283 bytes to flash:startup-config
FLEX24-10G#
```

Changing an Interfaces MVR State

By default, all interfaces are designated as Inactive. An interface's MVR state can be changed from Interface Configuration mode.

	Command	Explanation
Step 1	configure terminal	Enter Global Configuration mode.
Step 2	interface {*, GigabitEthernet <1/1-24>, 10GigabitEthernet<1/1-2>}	Enter Interface Configuration mode the interface(s) whose MVR state needs changing.
Step 3	mvr {name <mvr_name> | vlan <vlan_id>} type {source | receiver}	Set the interface(s) MVR state. **Source:** Source ports send and receive multicast data. **Receiver:** Receiver ports only receive multicast data.
Step 4	end	**(Optional)** Return to Privileged EXEC mode.
Step 5	copy running-config startup-config	**(Optional)** Copy the contents of the running-config to the startup-config.

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# interface GigabitEthernet 1/1
FLEX24-10G(config-if)# mvr name Testing type receiver
FLEX24-10G(config-if)# end
FLEX24-10G# copy running-config startup-config
Building configuration...
% Saving 2267 bytes to flash:startup-config
FLEX24-10G#
```

Note: Source interfaces should not overlap with any interfaces which are members of the management VLAN.

Immediate Leave

When Immediate Leave has been enabled on an interface, the interface will stop forwarding data upon receiving an IGMPv2/MLDv1 leave message. The interface will also not send any last member query messages when Immediate Leave has been enabled.

Enabling Immediate Leave

	Command	Explanation
Step 1	configure terminal	Enter Global Configuration mode.
Step 2	interface {*, GigabitEthernet <1/1-24>, 10GigabitEthernet<1/1-2>}	Enter Interface Configuration mode the interface in which to enable Immediate Leave on.
Step 3	mvr immediate-leave	Enable Immediate Leave.
Step 4	end	**(Optional)** Return to Privileged EXEC mode.
Step 5	copy running-config startup-config	**(Optional)** Copy the contents of the running-config to the startup-config.

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# interface GigabitEthernet 1/1
FLEX24-10G(config-if)# mvr immediate-leave
FLEX24-10G(config-if)# end
FLEX24-10G# copy running-config startup-config
Building configuration...
% Saving 3304 bytes to flash:startup-config
FLEX24-10G#
```

Verification

show mvr [detail]: Displays Global MVR Information, and all MVR VLANs. The optional **detail** parameter provides detailed information/statistics regarding the MVR group database.

```
FLEX24-10G# show mvr

MVR is now enabled to start group registration.

Switch-1 MVR-IGMP Interface Status

IGMP MVR VLAN 100 (Name is Testing) interface is enabled.
Querier status is ACTIVE
RX IGMP Query:0 V1Join:0 V2Join:0 V3Join:0 V2Leave:0
TX IGMP Query:0 / (Source) Specific Query:0
Interface Channel Profile: test

Switch-1 MVR-MLD Interface Status
```

```
MLD MVR VLAN 100 (Name is Testing) interface is enabled.
Querier status is ACTIVE
RX MLD Query:0 V1Report:0 V2Report:0 V1Done:0
TX MLD Query:0 / (Source) Specific Query:0
Interface Channel Profile: test
FLEX24-10G#
```

show mvr [vlan <vlan_id> | name <mvr_vlan>] [detail]: When including the **detail** keyword, displays detailed information pertaining to MVR VLAN **<vlan_id>** or MVR VLAN named **<mvr_vlan>**.

```
FLEX24-10G# show mvr vlan 100 detail

MVR is now enabled to start group registration.

Switch-1 MVR-IGMP Interface Status

IGMP MVR VLAN 100 (Name is Testing) interface is enabled.
Querier status is ACTIVE ( Join Querier-Election )
Querier Up time: 1069 seconds; Query Interval: 87 seconds
IGMP address is set to 192.168.1.1
Control frames will be sent as Tagged
PRI:0 / RV:2 / QI:125 / QRI:100 / LMQI:20 / URI:1
RX IGMP Query:0 V1Join:0 V2Join:0 V3Join:0 V2Leave:0
TX IGMP Query:8 / (Source) Specific Query:0
IGMP RX Errors:16; Group Registration Count:0
Port Role Setting:
Receiver Port: Gi 1/1
Inactive Port: Gi 1/2,Gi 1/3,Gi 1/4,Gi 1/5,Gi 1/6,Gi 1/7,Gi 1/8,Gi 1/9,Gi 1/10,Gi 1/11,Gi
1/12,Gi 1/13,Gi 1/14,Gi 1/15,Gi 1/16,Gi 1/17,Gi 1/18,Gi 1/19,Gi 1/20,Gi 1/21,Gi 1/22,Gi
1/23,Gi 1/24,Gi 1/25,10G 1/1,10G 1/2
Interface Channel Profile: test (In VER-INI Mode)
Description: test

Switch-1 MVR-MLD Interface Status

MLD MVR VLAN 100 (Name is Testing) interface is enabled.
Querier status is ACTIVE ( Join Querier-Election )
Querier Up time: 1069 seconds; Query Interval: 87 seconds
MLD address will use Link-Local address of this interface.
Control frames will be sent as Tagged
PRI:0 / RV:2 / QI:125 / QRI:100 / LMQI:20 / URI:1
RX MLD Query:0 V1Report:0 V2Report:0 V1Done:0
TX MLD Query:8 / (Source) Specific Query:0
MLD RX Errors:0; Group Registration Count:0
Port Role Setting:
Receiver Port: Gi 1/1
```

```
Inactive Port: Gi 1/2,Gi 1/3,Gi 1/4,Gi 1/5,Gi 1/6,Gi 1/7,Gi 1/8,Gi 1/9,Gi 1/10,Gi 1/11,Gi
1/12,Gi 1/13,Gi 1/14,Gi 1/15,Gi 1/16,Gi 1/17,Gi 1/18,Gi 1/19,Gi 1/20,Gi 1/21,Gi 1/22,Gi
1/23,Gi 1/24,Gi 1/25,10G 1/1,10G 1/2
Interface Channel Profile: test (In VER-INI Mode)
Description: test
FLEX24-10G#
```

show mvr name <mvr_name> group-database [interface {*, GigabitEthernet <1/1-24>, 10GigabitEthernet<1/1-2>} [sfm-information]]: Displays group-database information for MVR VLAN with name **<mvr_vlan>.**

```
FLEX24-10G# show mvr name Testing group-database interface GigabitEthernet 1/1 sfm-information

MVR is now enabled to start group registration.

MVR Group Database

Switch-1 MVR Group Count: 0
FLEX24-10G#
```

Chapter 26: ARP Inspection

Introduction

ARP (Address Resolution Protocol) is an essential part of any layer-2 network. ARP allows switches to resolve a host's MAC address to its IP address. Since switches communicate at layer-2, a host's MAC address must be known by the switch for the switch and the host to form a connection.

Take for instance the topology in Figure 1. If HOST A tries to send data to HOST B and HOST A does not have an entry in its ARP table for HOST B, an ARP request will be generated. The ARP request is sent as broadcast traffic to the switch and then flooded out all interfaces except the one it was received on. The ARP Request is a packet saying, "If your IP address is 192.168.100.20, what is your MAC address?". When HOST B receives the request, an ARP Reply is generated as unicast traffic and sent to HOST A. The reply contains HOST B's MAC address so HOST A can add an entry for HOST B in its ARP table. During this process, the switch is also dynamically updating its own ARP cache with entries for HOST A and HOST B.

The ARP table is a list of IP address to MAC address mappings.

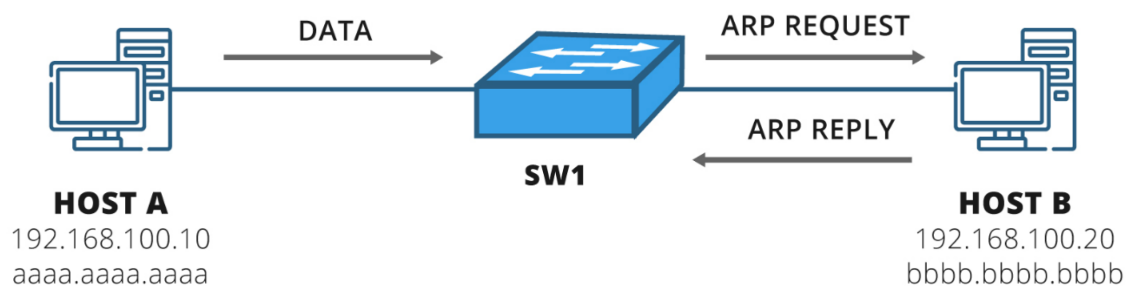


Figure 1: ARP Conversation Between two Hosts

Now consider Figure 2 with a third host introduced into the topology. HOST C can poison the switch's ARP entries for HOST A and HOST B by generating fake ARP responses. Because ARP traffic is gratuitous, a host can generate an ARP Reply even when it has not first received an ARP Request. These fake ARP responses contain the MAC Address of HOST C and the IP address of either HOST A or HOST B. When the switch receives the ARP Reply, it will update its ARP table with an entry containing HOST C's MAC and either HOST A or HOST B's IP address. Now when the switch needs to make a forwarding decision to the host with the poisoned ARP entry, the traffic will be forwarded to HOST C.

HOST C also knows the true MAC addresses of HOST A and HOST B so the traffic can still be redirected to the correct destination. HOST A or HOST B will not be aware of HOST C's presence because they are still receiving traffic destined for them.

This is known as a *man-in-the-middle* attack. In essence, HOST C snoops on traffic being sent between HOST A and B before redirecting the traffic to the intended recipient.

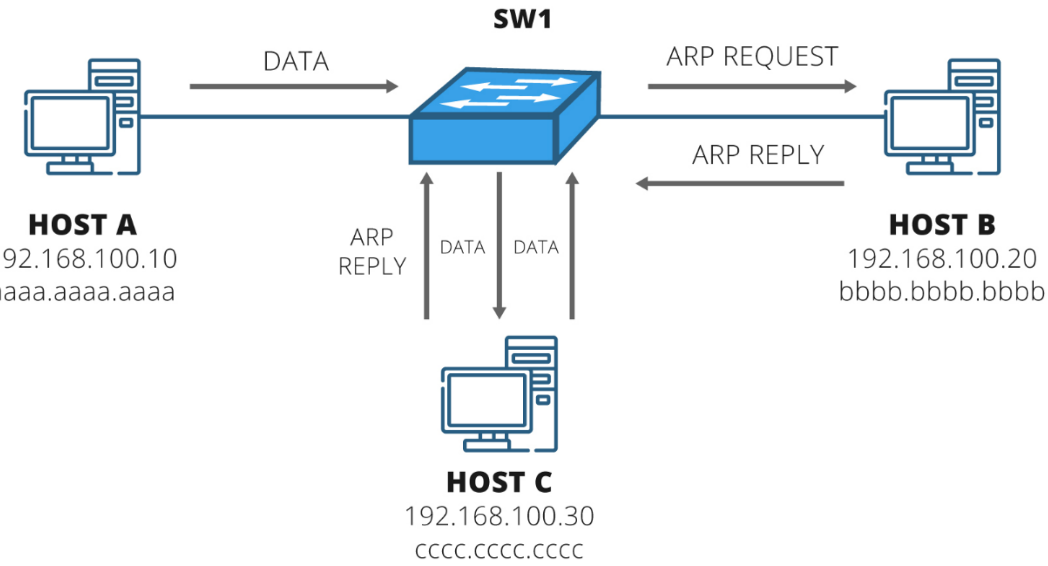


Figure 3: HOST C performing Man-in-the-Middle Attack

ARP Inspection inspects ARP packets and examines their IP-to-MAC address pairings. ARP packets with invalid IP-to-MAC Address pairings are discarded by the switch. When an ARP packet is inspected the IP-to-MAC Address pairing is compared against the entries in the DHCP Snooping Binding Database.

The DHCP Snooping Database is enabled only if DHCP Snooping is also enabled on the switch's VLANs. DHCP Snooping uses trusted interfaces to determine which interfaces to allow DHCP traffic on. ARP traffic received on trusted interfaces will be processed without any checks while ARP traffic received on untrusted interfaces will be forwarded only after they pass an inspection.

Configuration

Enabling ARP Inspection – Interface Configuration

To enable ARP Inspection, it must be enabled globally from Global Configuration as well as on the participating interface(s).

	Command	Explanation
Step 1	configure terminal	Enter Global Configuration mode.
Step 2	ip arp inspection	Enable ARP Inspection globally.
	ip arp inspection translate [interface *interface-id* <vlan_id> <mac_ucast> <ipv4_ucast>]	**(Optional)** Translate dynamically learnt ARP entries to static entries. All dynamic entries can be translated at once or one at a time.

Step 3	interface {*, GigabitEthernet <1/1-24>, 10GigabitEthernet<1/1-2>}	Enter Interface Configuration mode for the interface(s) to configure with ARP Inspection.
Step 4	[no] ip arp inspection trust	Enable ARP Inspection on the interface. If an interface is set as trusted, ARP Inspection will not be performed. By default, all interfaces are configured with the **ip arp inspection trust** command, hence why it is not in the running-config. The **no** form makes the interface untrusted and enables ARP Inspection.
Step 5	ip arp inspection check-vlan	**(Optional)** Checks the VLAN configuration of ARP packets. By default, the **check-vlan** setting is disabled on all interfaces. When disabled, the log type refers to the port setting. When enabled, the log type refers to the VLAN setting.
Step 6	ip arp inspection logging {all | deny | permit}	**(Optional)** Configure ARP Inspection logging on the interface. **All:** Log both denied and permitted ARP packets. **Deny:** Log only denied ARP packets. **Permit:** Log only permitted ARP packets. **Note:** If the check-vlan setting is disabled, the log type refers to the port setting.
Step 7	end	**(Optional)** Exit Interface Configuration mode and return to Privileged EXEC mode.
Step 8	copy running-config startup-config	**(Optional)** Copy the contents of the running-config to the startup-config.

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# ip arp inspection
FLEX24-10G(config)# ip arp inspection translate
FLEX24-10G(config)# interface GigabitEthernet 1/1
FLEX24-10G(config-if)# no ip arp inspection trust
FLEX24-10G(config-if)# ip arp inspection check-vlan
FLEX24-10G(config-if)# ip arp inspection logging all
FLEX24-10G(config-if)# end
FLEX24-10G# copy running-config startup-config
Building configuration...
% Saving 2049 bytes to flash:startup-config
FLEX24-10G#
```

Enabling ARP Inspection – VLAN Configuration

ARP Inspection can also be enabled on a per-VLAN basis. When ARP Inspection is enabled on a VLAN, all interfaces which are members of that VLAN will have ARP Inspection enabled. The logging behavior can also be configured.

	Command	Explanation
Step 1	configure terminal	Enter Global Configuration mode.
Step 2	ip arp inspection vlan <vlan_list> [logging {all | deny | permit}]	Enable ARP Inspection on all VLANs in **<vlan_list>.** The **logging** parameter configures the ARP frame logging behavior on all VLANs in **<vlan_list>.** See here for the different logging behaviors.
Step 3	end	**(Optional)** Return to Privileged EXEC mode.
Step 4	copy running-config startup-config	**(Optional)** Copy the contents of the running-config to the startup-config.

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# ip arp inspection vlan 1-5 logging all
FLEX24-10G(config)# end
FLEX24-10G# copy running-config startup-config
Building configuration...
% Saving 2234 bytes to flash:startup-config
FLEX24-10G#
```

Static ARP Inspection Table

Static ARP entries are entries manually configured by the administrator which never age out of the ARP table. Static ARP entries are generally configured for important devices with static IP addresses (printers, servers, etc.)

Creating a Static ARP Entry

	Command	Explanation
Step 1	configure terminal	Enter Global Configuration mode.
Step 2	ip arp inspection entry interface {GigabitEthernet <1/1-24>, 10GigabitEthernet<1/1-2>} <vlan_id> <mac_ucast> <ipv4_ucast>	Create a static ARP entry in the switch's ARP table. The static ARP entry requires the IP address, MAC address, and VLAN membership of the host which the static entry belongs to.
Step 3	end	**(Optional)** Return to Privileged EXEC mode.
Step 4	copy running-config startup-config	**(Optional)** Copy the contents of the running-config to the startup-config.

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# ip arp inspection entry interface GigabitEthernet 1/1 1 00-E0-4C-30-0D-65
192.168.100.2
FLEX24-10G(config)# end
```

```
LEX24-10G# copy running-config startup-config
Building configuration...
% Saving 2322 bytes to flash:startup-config
FLEX24-10G#
```

Dynamic ARP Inspection Table

The Dynamic ARP Inspection Table does not require any administration from the administrator. Each entry in the Dynamic ARP Inspection Table contains an interface-id, VLAN ID, MAC address, and IP address. The Dynamic ARP Inspection table lists entries for each host which has been learnt dynamically via ARP.

The Dynamic ARP Inspection Table can be displayed using the **show ip arp** command.

Verification

There are two show commands relating to ARP Inspection on the FLEX24-10G.

show ip arp: Displays ARP mappings. Each ARP mappings contains the host's IP address, MAC address, and VLAN membership.

```
FLEX24-10G# show ip arp
192.168.100.2 via VLAN1:00-e0-4c-30-0d-65
FLEX24-10G#
```

show ip arp inspection [entry [interface *interface-id*] [static] [dhcp-snooping] | interface *interface-id* | vlan <vlan_list>]: Displays the ARP Inspection status off all interfaces on the switch. Output can be filtered to only include a specific entry, interface, VLAN, or DHCP-snooping configuration.

```
FLEX24-10G# show ip arp inspection
ARP Inspection Mode : enabled

Port                       Port Mode    Check VLAN   Log Type
----                       ---------    ----------   --------
GigabitEthernet 1/1        enabled      enabled      ALL
GigabitEthernet 1/2        disabled     disabled     NONE
GigabitEthernet 1/3        disabled     disabled     NONE
GigabitEthernet 1/4        disabled     disabled     NONE
GigabitEthernet 1/5        disabled     disabled     NONE
GigabitEthernet 1/6        disabled     disabled     NONE
GigabitEthernet 1/7        disabled     disabled     NONE
GigabitEthernet 1/8        disabled     disabled     NONE
GigabitEthernet 1/9        disabled     disabled     NONE
GigabitEthernet 1/10       disabled     disabled     NONE
GigabitEthernet 1/11       disabled     disabled     NONE
        ------------------------------OUTPUT TRUNCATED-------------------------------
```

Chapter 27: DDMI

Introduction

DDMI is the Digital Diagnostic Monitoring Interface. DDMI is used to monitor the health of the FLEX24-10G's fiber optic ports.

By default, DDMI is enabled. When disabled, the **show interface 10GigabitEthernet {1/1 | 1/2} transceiver** will produce an error message.

While DDMI is enabled, the following information can be viewed regarding the 10 Gigabit interfaces and SFP modules:

Transceiver Information

The following transceiver properties are collected when DDMI is enabled:

- Vendor
- Part Number
- Serial Number
- Revision
- Date Code
- Transceiver

DDMI Information

Information specific to DDMI is as follows:

- Temperature (°C)
- Voltage (V)
- Tx Bias (mA)
- Tx Power (mW)
- Rx Power (mW)

Configuration

DDMI configuration on the FLEX24-10G is very straightforward. The only configuration required is to enable/disable DDMI from Global Configuration. This is done as follows:

	Command	Explanation
Step 1	configure terminal	Enter Global Configuration mode.
Step 2	[no] ddmi	Enable/disable DDMI. By default, DDMI is enabled on the FLEX24-10G.
Step 3	end	**(Optional)** Return to Privileged EXEC mode.

Step 4	copy running-config startup-config	**(Optional)** Copy the contents of the running-config to the startup-config.

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# ddmi
FLEX24-10G(config)# end
FLEX24-10G# copy running-config startup-config
Building configuration...
% Saving 2188 bytes to flash:startup-config
FLEX24-10G#
```

Verification

show ddmi: Displays the current state of DDMI.

```
FLEX24-10G# show ddmi
Current mode: Enabled
FLEX24-10G#
```

show interface 10GigabitEthernet {1/1 | 1/2} transceiver: Displays interface transceiver information. If DDMI is not enabled, the command will return: `% DDMI is disabled.`

```
FLEX24-10G# show interface 10GigabitEthernet 1/1 transceiver
% DDMI is disabled.
FLEX24-10G# configure terminal
FLEX24-10G(config)# ddmi
FLEX24-10G(config)# end
FLEX24-10G# show interface 10GigabitEthernet 1/1 transceiver

10GigabitEthernet 1/1
------------------------------
Transceiver Information
==========================================================================
Vendor              : OEM
Part Number         : NV-SFP-10G-SR
Serial Number       : HL085C90610023
Revision            : V02
Date Code           : 2019-06-03
Transceiver         : DDMI: Unknown error code

DDMI Information
++ : high alarm, +  : high warning, -  : low warning, -- : low alarm.
Tx: transmit, Rx: receive, mA: milliamperes, mW: milliwatts.
==========================================================================
              current   High Alarm   High Warn     Low Warn      Low Alarm
                         Threshold   Threshold    Threshold      Threshold
-------------  --------  ----------  ----------  ----------    --------
Temperature(C) 34.836      100.000      95.000       -35.000      -40.000
Voltage(V)     3.2652      3.6000       3.5000       2.9000       2.8000
```

```
Tx Bias(mA)    7.410       15.000       13.000       2.000        1.000
Tx Power(mW)   0.6204      1.2589       1.0000       0.1995       0.1585
Rx Power(mW)   0.4739      1.9953       1.0000       0.0501       0.0251

FLEX24-10G#
```

Chapter 28: IP, MAC, and Protocol Based Subnets

Introduction

IP, MAC, and Protocol Based VLANs allow for dynamic VLAN assignment based on ingress packet characteristics.

For example, a MAC based VLAN allows any individual to physically connect to a network from any ethernet interface and that individual will be assigned to a specific VLAN. When the interface detects ingress traffic, it will examine the entries of the MAC to VLAN table for the specific interface. If an entry is found for the source MAC address of the ingress traffic, such traffic will be assigned to the VLAN in the entry.

Similar configurations can be carried out where instead of examining the source MAC of ingress traffic, either the IP address or frame protocol are examined. If the IP address or protocol match an entry in the switch's IP to VLAN or Protocol to VLAN table respectively, the traffic will be assigned to the VLAN specified in the entry.

By allowing a host's VLAN membership to be dynamically assigned by the switch, this greatly decreases the amount of manual configuration required by the network administrator as a host can use a static IP (assuming the IP address is not in use on the network) or MAC address and always be assigned to the correct VLAN.

Configuration

MAC-Based VLANs

Each entry in the MAC to VLAN table contains a MAC address, VLAN ID, and interface ID. The interface ID tells the switch which interface to examine the ingress traffic of. If ingress traffic appears on this interface with a source MAC address matching the MAC address in the entry, a Dot1Q tag will be appended to the frame. The Dot1Q tag contains the VLAN ID from the MAC to VLAN table entry.

MAC to VLAN table entries are created at the interface level as follows:

	Command	**Explanation**
Step 1	configure terminal	Enter Global Configuration mode.
Step 2	interface {*, GigabitEthernet <1/1-24>, 10GigabitEthernet<1/1-2>}	Enter Interface Configuration mode for the interface(s) to apply the MAC to VLAN entry to.
Step 3	switchport vlan mac <mac_ucast> vlan <vlan_id>	Create an entry in the MAC to VLAN table for the specific interface. The entry will contain the VLAN ID and MAC address specified in the command. **<mac_ucast>** must be a valid unicast MAC address.

		<vlan_id> identifies the value of the Dot1Q tag which will be appended to the frame. Valid **<vlan_id>** values are from 1 to 4095.
Step 4	end	**(Optional)** Return to Privileged EXEC mode.
Step 5	copy running-config startup-config	**(Optional)** Copy the contents of the running-config to the startup-config.

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# interface GigabitEthernet 1/1-5
FLEX24-10G(config-if)# switchport vlan mac 00-E0-4C-30-0D-65 vlan 10
FLEX24-10G(config-if)# end
FLEX24-10G# copy running-config startup-config
Building configuration...
% Saving 2367 bytes to flash:startup-config
FLEX24-10G#
```

A single MAC to VLAN entry can apply to multiple interfaces. This is accomplished by specifying multiple interfaces when entering Interface Configuration mode in Step 2.

Note: The MAC to VLAN table can contain up to 256 entries.

IP-Based VLANs

IP-based VLANs function in the same way as MAC-based VLANs with the exception that the source IP address of ingress traffic is examined rather than the source MAC address. If the source IP address of ingress traffic matches the IP address in an entry in the IP to VLAN table, a corresponding VLAN ID will be appended to the packet.

A single IP address or an entire network can be contained within a single IP to VLAN entry. The range of addresses is dictated by the subnet mask.

IP to VLAN table entries are created at the interface level as follows.

	Command	**Explanation**
Step 1	configure terminal	Enter Global Configuration mode.
Step 2	interface {*, GigabitEthernet <1/1-24>, 10GigabitEthernet<1/1-2>}	Enter Interface Configuration mode for the interface(s) to apply the IP to VLAN entry to.
Step 3	switchport vlan ip-subnet <ip_address/subnet_mask> vlan <vlan_id> **Example 1: Mapping the entire 192.168.100.0/24 subnet to VLAN 15.** switchport vlan ip-subnet 192.168.100.0/255.255.255.0 vlan 15 **Example 2: Mapping only 192.168.100.50 to VLAN 30.**	Create an entry in the IP to VLAN table for the specific interface. The entry will contain the VLAN ID and IP address specified in the command. **<ip_address/subnet_mask>** must be a valid IP address and subnet mask. To include a single IP address, use a subnet mask of 255.255.255.255.

	switchport vlan ip-subnet 192.168.100.50/255.255.255.255 vlan 30	**<vlan_id>** identifies the value of the Dot1Q tag which will be appended to the frame. Valid **<vlan_id>** values are from 1 to 4095.
Step 4	end	**(Optional)** Return to Privileged EXEC mode.
Step 5	copy running-config startup-config	**(Optional)** Copy the contents of the running-config to the startup-config.

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# interface GigabitEthernet 1/10-15
FLEX24-10G(config-if)# switchport vlan ip-subnet 192.168.100.0/255.255.255.0 vlan 50
FLEX24-10G(config-if)# end
FLEX24-10G# copy running-config startup-config
Building configuration...
% Saving 2885 bytes to flash:startup-config
FLEX24-10G#
```

A single IP to VLAN entry can apply to multiple interfaces. This is accomplished by specifying multiple interfaces when entering Interface Configuration mode in Step 2.

Note: The IP to VLAN table can contain up to 128 entries.

Protocol-Based VLANs

Protocol-based VLANs are configured in a two-step process. First, a Protocol to Group mapping must be created. Once a group containing one or more protocols has been created, the group must be mapped to a VLAN.

Individual protocols are mapped to groups from Global Configuration mode. A protocol is either an EtherType, SNAP OUI/PID, or LLC DSAP/SSAP.

Ethertype: The Ethertype is a 16 byte field in an ethernet frame which indicates the protocol of the payload of the frame.

Valid Ethertype values range from 0x0600 to 0xffff.

LLC: An LLC-Based VLAN can be configured which will match ingress LLC PDUs containing a specified DSAP (Destination Source Access Point) and SSAP (Source Service Access Point). The DSAP and SSAP are both contained within the LLC header.

The DSAP and SSAP are both one-byte strings ranging from 0x00 to 0xff.

SNAP: SNAP is an extension to LLC. The SNAP header is 5 bytes long and contains a 3-byte OUI as well as a 2-byte protocol ID. SNAP based VLANs are configured by specifying the OUI and PID contained within the SNAP header of ingress traffic.

The OUI (Organizationally Unique Identifier) is specified in xx-xx-xx format where each xx is a hexadecimal string.

The PID (Protocol ID) value depends on the OUI value. If the OUI value is 00-00-00, then the PID will be equal to the Ethertype of the frame. If the OUI is not equal to 00-00-00, then the PID will be any value from 0x0000 to 0xffff.

802.2 LLC Header			**SNAP Extension**	
DSAP	**SSAP**	**Control**	**OUI**	**Protocol ID**
1 byte	1 byte	1 or 2 bytes	3 bytes	2 bytes

Creating a Protocol to Group Mapping

Protocols are mapped to Groups from Global Configuration Mode as follows:

<table>
<tr><th></th><th><u>Command</u></th><th><u>Explanation</u></th></tr>
<tr><td>Step 1</td><td>configure terminal</td><td>Enter Global Configuration mode.</td></tr>
<tr><td>Step 2</td><td>vlan protocol {eth2 {<0x600-0xffff> | arp | at | ip | ipx} | llc <dsap> <ssap> | snap {<0x0-0xffffff> | rfc-1042 <0x0000-0xffff> | snap-8021h <0x0000-0xffff>}} group <group_name></td><td>Create a protocol filter and map it to <group_name>.

Multiple filters can be created and mapped to the same group name.

arp, at, ip, and ipx act as shortcuts instead of entering the Ethertype for ARP, Appletalk, IPv4, or IPX, respectively.

A SNAP OUI of rfc-1042 or 8021h can be configured using the rfc-1042 or snap-8021h keywords.

<u>Note:</u> <group_name> must be 16 characters or fewer and can only contain alphanumeric characters.

More detailed information can be found <u>above detailing the individual protocols and parameters.</u></td></tr>
<tr><td>Step 3</td><td>end</td><td>(Optional) Return to Privileged EXEC mode.</td></tr>
<tr><td>Step 4</td><td>copy running-config startup-config</td><td>(Optional) Copy the contents of the running-config to the startup-config.</td></tr>
</table>

<u>Note:</u> A maximum of 128 Group to Protocol mappings can exists at once.

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# vlan protocol eth2 0x88cc group LLDPGroup
FLEX24-10G(config)# vlan protocol llc 0x18 0x00 group LLCSNAPGroup
FLEX24-10G(config)# vlan protocol snap snap-8021h 0x0001 group LLCSNAPGroup
FLEX24-10G(config)# end
```

```
FLEX24-10G# copy running-config startup-config
Building configuration...
% Saving 3026 bytes to flash:startup-config
FLEX24-10G#
```

The second line in the above CLI snippet maps LLDP traffic to the group LLDPGroup.

The third and fourth lines of the above CLI snippet create an LLC and SNAP protocol filter and maps them to the group LLCSNAPGroup.

Mapping a Group to a VLAN

Once a protocol or protocols have been mapped to a group, those groups must then be mapped to a VLAN. Groups are mapped to VLANs at the interface level as follows:

	Command	Explanation
Step 1	configure terminal	Enter Global Configuration mode.
Step 2	interface {*, GigabitEthernet <1/1-24>, 10GigabitEthernet<1/1-2>}	Enter Interface Configuration mode for the interface or interfaces in which to map a protocol to a VLAN.
Step 3	switchport vlan protocol group <group_name> vlan <vlan_id>	Map all protocols contained within **<group_name>** to VLAN **<vlan_id>**
Step 4	end	**(Optional)** Return to Privileged EXEC mode.
Step 5	copy running-config startup-config	**(Optional)** Copy the contents of the running-config to the startup-config.

Note: When mapping a group to a VLAN, the command will be accepted even if the group does not exist. It is important to make sure that the group name is typed correctly.

The below CLI snippet will map the group LLCSNAPGroup, created above, to VLAN 15 on interfaces GigabitEthernet 1/10 – 1/20.

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# interface GigabitEthernet 1/10-20
FLEX24-10G(config-if)# switchport vlan protocol group LLCSNAPGroup vlan 15
FLEX24-10G(config-if)# end
FLEX24-10G# copy running-config startup-config
Building configuration...
% Saving 3176 bytes to flash:startup-config
FLEX24-10G#
```

Verification

MAC-Based VLAN Verification

show vlan mac [address <mac_ucast>]: Displays all entries in the MAC to VLAN table. The output can be filtered to only display certain MAC addresses with the optional **[address <mac_ucast>]** parameter.

```
FLEX24-10G# show vlan mac
```

```
MAC Address        VID   Interfaces
-----------        ---   ----------
00:e0:4c:30:0d:65  10    GigabitEthernet 1/1-5
FLEX24-10G#
```

IP-Based VLAN Verification

show vlan ip-subnet [<ipv4_subnet>]: Display all entries in the IP to VLAN table. Output can be filtered to only display entries in the IP to VLAN table for a specific IPv4 subnet.

```
FLEX24-10G# show vlan ip-subnet
IP Address       Mask Length  VID   Interfaces
----------       -----------  ---   ----------
192.168.101.11   32           11    GigabitEthernet 1/19
192.168.100.0    24           50    GigabitEthernet 1/10-15
FLEX24-10G#
```

Protocol-Based VLAN Configuration

show vlan protocol [eth2 <0x600-0xffff> | arp | at | ip | ipx] [llc <dsap_value> <ssap_value>] [snap {<0x0-0xffffff> <pid>| rfc-1042 <pid> | snap-8021h <pid>}: Displays all protocol groups as well as Group to VLAN mappings. Output can be filtered to only display specific protocols using the optional **eth2**, **llc**¸or **snap** parameters.

```
FLEX24-10G# show vlan protocol
Protocol Type  Protocol (Value)          Group ID
-------------  ------------------------  --------
EthernetII     ETYPE:0x88cc              LLDPGroup
LLC_SNAP       OUI-00:00:f8; PID:0x1     LLCSNAPGroup
LLC_Other      DSAP:0x18; SSAP:0x0       LLCSNAPGroup

Switch #1
---------
Group ID          VID   Ports
----------------  ----  -----
LLCSNAPGroup      12    GigabitEthernet 1/20-21
FLEX24-10G#
```

Chapter 29: IPv4/IPv6 Source Guard

Introduction

IPv4 and IPv6 Source Guard allow for the administrative control of which clients can transmit or receive data to/from a switchport.

A switchport will by default dynamically learn any downstream clients from the switchport and update its MAC address table accordingly.

By configuring IP Source Guard, the switchport can be configured with a maximum number of dynamically learnt clients. Additionally, static bindings can be created which create static entries in the MAC address table.

IP Source Guard operates in a similar fashion to Dynamic ARP Inspection. Where Dynamic ARP Inspection is designed to prevent ARP spoofing attacks, IP Source Guard is designed to prevent IP spoofing attacks.

IP Source Guard uses the DHCP Snooping Database to verify the authenticity of a host's IP address.

Configuration

Enabling IPv4/IPv6 Source Guard on an Interface

IPv4/IPv6 Source Guard is enabled at the interface level as follows:

	Command	Explanation
Step 1	configure terminal	Enter Global Configuration mode.
Step 2	interface {*, GigabitEthernet <1/1-24>, 10GigabitEthernet<1/1-2>}	Enter Interface Configuration mode for the interface in which to enable IP Source Guard on.
Step 3	{ip | ipv6} verify source	Enable IP Source Guard on the interface.
Step 4	{ip | ipv6} verify source limit <0-2>	Set the maximum amount of clients allowed on the interface. By default, the maximum amount of clients is set to unlimited.
Step 5	end	**(Optional)** Return to Privileged EXEC mode.
Step 6	copy running-config startup-config	**(Optional)** Copy the contents of the running-config to the startup-config.

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# interface GigabitEthernet 1/1
FLEX24-10G(config-if)# ip verify source
FLEX24-10G(config-if)# ip verify source limit 1
FLEX24-10G(config-if)# ipv6 verify source
FLEX24-10G(config-if)# ipv6 verify source limit 2
FLEX24-10G(config-if)# end
FLEX24-10G# copy running-config startup-config
```

```
Building configuration...
% Saving 2068 bytes to flash:startup-config
FLEX24-10G#
```

Enabling IPv4/IPv6 Source Guard Globally

IPv4/IPv6 Source Guard must also be enabled globally from Global Configuration. This is done as follows:

	Command	Explanation
Step 1	configure terminal	Enter Global Configuration mode.
Step 2	{ip | ipv6} verify source	Enable IPv4/IPv6 Source Guard globally.
Step 3	end	**(Optional)** Return to Privileged EXEC mode.
Step 4	copy running-config startup-config	**(Optional)** Copy the contents of the running-config to the startup-config.

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# ip verify source
FLEX24-10G(config)# ipv6 verify source
FLEX24-10G(config)# end
FLEX24-10G# copy running-config startup-config
Building configuration...
% Saving 2104 bytes to flash:startup-config
FLEX24-10G#
```

Translating Dynamic Entries to Static Entries

The default behavior for a switchport is to dynamically learn all downstream clients from that interface. These clients are placed in the FLEX24-10G's MAC address table as dynamic entries. By default, a switch will discard any dynamic entry after 300 seconds of not hearing from the client.

Static entries will never expire from the switch's MAC address table.

Translate all dynamic entries to static entries as follows:

	Command	Explanation
Step 1	configure terminal	Enter Global Configuration mode.
Step 2	{ip | ipv6} verify source translate	Translate all dynamic entries to static entries.
Step 3	end	**(Optional)** Return to Privileged EXEC mode.
Step 4	copy running-config startup-config	**(Optional)** Copy the contents of the running-config to the startup-config.

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# ip verify source translate
IP Source Guard:
        Translate 0 dynamic entries into static entries.
FLEX24-10G(config)# end
FLEX24-10G# copy running-config startup-config
Building configuration...
% Saving 1956 bytes to flash:startup-config
FLEX24-10G#
```

Creating a Static IPv4/IPv6 Source Guard Entry

When a static entry has been configured, all traffic containing the source MAC address, and source IP address within the entry, is permitted. Traffic from other hosts on the same interface is denied.

Static entries are configured as follows:

	Command	Explanation
Step 1	configure terminal	Enter Global Configuration mode.
Step 2	ip source binding interface {*, GigabitEthernet <1/1-24>, 10GigabitEthernet<1/1-2>} <vlan_id> <ipv4/ipv6_address> <mac_address>	Create a static IPv4/IPv6 Source Guard Entry. Each entry must contain an interface, VLAN ID, IPv4/IPv6 address, and MAC address. Only traffic which enters the interface with an IP and MAC address matching the IP and MAC address in the entry is allowed.
Step 3	end	**(Optional)** Return to Privileged EXEC mode.
Step 4	copy running-config startup-config	**(Optional)** Copy the contents of the running-config to the startup-config.

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# ip source binding interface GigabitEthernet 1/1 100 192.168.100.2 00-E0-
4C-68-07-55
FLEX24-10G(config)# end
FLEX24-10G# copy running-config startup-config
Building configuration...
% Saving 2188 bytes to flash:startup-config
FLEX24-10G#
```

Verification

show {ip | ipv6} verify source [interface {*, GigabitEthernet <1/1-24>, 10GigabitEthernet<1/1-2>}]: Displays IPv4/IPv6 Source Guard information. Output displays the current state of all switch interfaces but can be filtered to only displays the status of specific interfaces.

```
FLEX24-10G# show ip verify source
IP Source Guard Mode : disabled

Port                      Port Mode    Dynamic Entry Limit
----                      ---------    -------------------
GigabitEthernet 1/1       disabled     unlimited
GigabitEthernet 1/2       disabled     unlimited
GigabitEthernet 1/3       disabled     unlimited
GigabitEthernet 1/4       disabled     unlimited
GigabitEthernet 1/5       disabled     unlimited
GigabitEthernet 1/6       disabled     unlimited
GigabitEthernet 1/7       disabled     unlimited
```

```
GigabitEthernet 1/8       disabled     unlimited
GigabitEthernet 1/9       disabled     unlimited
GigabitEthernet 1/10      disabled     unlimited
GigabitEthernet 1/11      disabled     unlimited
GigabitEthernet 1/12      disabled     unlimited
GigabitEthernet 1/13      disabled     unlimited
GigabitEthernet 1/14      disabled     unlimited
GigabitEthernet 1/15      disabled     unlimited
GigabitEthernet 1/16      disabled     unlimited
GigabitEthernet 1/17      disabled     unlimited
GigabitEthernet 1/18      disabled     unlimited
GigabitEthernet 1/19      disabled     unlimited
GigabitEthernet 1/20      disabled     unlimited
GigabitEthernet 1/21      disabled     unlimited
GigabitEthernet 1/22      disabled     unlimited
GigabitEthernet 1/23      disabled     unlimited
GigabitEthernet 1/24      disabled     unlimited
GigabitEthernet 1/25      disabled     unlimited
10GigabitEthernet 1/1     disabled     unlimited
10GigabitEthernet 1/2     disabled     unlimited
FLEX24-10G# show ipv6 verify source

IPv6 Source Guard Mode : disabled

Port                      Port Mode    Dynamic Entry Limit
----                      ---------    -------------------
GigabitEthernet 1/1       disabled     unlimited
GigabitEthernet 1/2       disabled     unlimited
GigabitEthernet 1/3       disabled     unlimited
GigabitEthernet 1/4       disabled     unlimited
GigabitEthernet 1/5       disabled     unlimited
GigabitEthernet 1/6       disabled     unlimited
GigabitEthernet 1/7       disabled     unlimited
GigabitEthernet 1/8       disabled     unlimited
GigabitEthernet 1/9       disabled     unlimited
GigabitEthernet 1/10      disabled     unlimited
GigabitEthernet 1/11      disabled     unlimited
GigabitEthernet 1/12      disabled     unlimited
GigabitEthernet 1/13      disabled     unlimited
GigabitEthernet 1/14      disabled     unlimited
GigabitEthernet 1/15      disabled     unlimited
GigabitEthernet 1/16      disabled     unlimited
GigabitEthernet 1/17      disabled     unlimited
GigabitEthernet 1/18      disabled     unlimited
GigabitEthernet 1/19      disabled     unlimited
GigabitEthernet 1/20      disabled     unlimited
GigabitEthernet 1/21      disabled     unlimited
GigabitEthernet 1/22      disabled     unlimited
```

```
GigabitEthernet 1/23      disabled     unlimited
  ------------------------------------OUTPUT TRUNCATED------------------------------------
```

show {ip | ipv6} source binding {dhcp-snooping | dhcpv6-snooping} [interface {*, GigabitEthernet <1/1-24>, 10GigabitEthernet<1/1-2>]: Displays all IPv4 or IPv6 bindings learnt via DHCP. Output can be filtered to only display DHCP bindings belonging to specific interfaces.

```
FFLEX24-10G# show ip source binding

Type     Port                    VLAN  IP Address       MAC Address
----     ----                    ----  ----------       -----------
Static   GigabitEthernet 1/1        1  192.168.100.2    00-e0-4c-68-07-55
FLEX24-10G#
```

show {ip | ipv6} source binding interface {*, GigabitEthernet <1/1-24>, 10GigabitEthernet<1/1-2>} [static | [dhcp-snooping | dhcpv6-snooping]: Displays all IPv4 or IPv6 source bindings on a specific interface. Output can be filtered to only display the static bindings or bindings learnt via DHCP.

```
FLEX24-10G# show ip source binding interface GigabitEthernet 1/1

Type     Port                    VLAN  IP Address       MAC Address
----     ----                    ----  ----------       -----------
Static   GigabitEthernet 1/1        1  192.168.100.2    00-e0-4c-68-07-55
FLEX24-10G#
```

show {ip | ipv6} source binding static [interface {*, GigabitEthernet <1/1-24>, 10GigabitEthernet<1/1-2>]]: Displays all static IPv4 or IPv6 source bindings. Output can be filtered to only display static bindings belonging to certain interfaces.

```
FLEX24-10G# show ip source binding static

Type     Port                    VLAN  IP Address       MAC Address
----     ----                    ----  ----------       -----------
Static   GigabitEthernet 1/1        1  192.168.100.2    00-e0-4c-68-07-55
FLEX24-10G#
```

Chapter 30: Quality of Service (QoS)

Introduction

Quality of Service provides a means for network traffic to be manipulated based on priority levels defined by Class of Service.

Class of Service priority levels are embedded within 802.1Q tags. Priority levels allow various types of traffic to be prioritized based on their importance.

For instance, acceptable standards for VoIP are much different than what is deemed acceptable for web traffic. The latency and jitter for a VoIP stream should not exceed 150ms and 30ms respectively. Class of Service priorities can ensure that all packets in a VoIP stream arrive at their destination in less than 150ms by prioritizing them over less crucial traffic.

Terminology

The following terminology is used extensible throughout this chapter. Become familiar with the following definitions before configuring QoS:

CoS (Class of Service): Priority level ranging from 0 to 7 indicating the importance of traffic. Default priority is 0 with 7 being the highest priority.

PCP (Priority Code Point): 3-bit field referring to the 802.1p class of service. The PCP value directly maps to the 802.1p priority.

DEI (Drop Eligibility Indicator): 1-bit field which can work independently or in conjunction with the PCP field. The DEI field marks frames which are eligible to be dropped in the event of network congestion.

DPL (Drop Precedence Level): The Drop Precedence Level works in conjunction with the DSCP field. The fourth of fifth bits of the DSCP value indicate the DPL value.

Fourth Bit	Fifth Bit	DPL
0	0	None
0	1	Low
1	0	Medium
1	1	High

DSCP (Differentiated Service Code Point): 6-byte field ranging from 0 to 63. The DSCP value is used in the IP header for packet classification.

Common DSCP Values

DSCP Decimal Value	Meaning	Drop Probability	Equivalent IP Precedence Value	Service Class
0	Best Effort	N/A	000 (Routine)	Default DSCP Value
8	CS1		1	Low-Priority Data

10	AF11	Low	001 (Priority)	High-Throughput Data
12	AF12	Medium	001 (Priority)	High-Throughput Data
14	AF13	High	001 (Priority)	High-Throughput Data
16	CS2		2	Operations, Administration, Management (OAM)
18	AF21	Low	010 (Immediate)	Low-Latency Data
20	AF22	Medium	010 (Immediate)	Low-Latency Data
22	AF23	High	010 (Immediate)	Low-Latency Data
24	CS3		3	Broadcast Video
26	AF31	Low	011 (Flash)	Multimedia Streaming
28	AF32	Medium	011 (Flash)	Multimedia Streaming
30	AF33	High	011 (Flash)	Multimedia Streaming
32	CS4		4	Real-Time Interactive
34	AF41	Low	100 (Flash Override)	Multimedia Conferencing
36	AF42	Medium	100 (Flash Override)	Multimedia Conferencing
38	AF43	High	100 (Flash Override)	Multimedia Conferencing
40	CS5		5	Signaling
46	Expedited Forwarding	N/A	101 (Critical)	Telephony
48	CS6		6	Network Control
56	CS7		7	

Configuration

There are several ways in which priority levels can be applied to ingress and egress traffic on the FLEX24-10G.

Class of Service Values

Priority Code Point	**Priority**	**Types of Traffic**
001	0	Background
000	1 (default priority)	Best effort
010	2	Excellent effort
011	3	Critical applications
100	4	Video (< 100 ms of latency and jitter)
101	5	Voice (< 10 ms of latency and jitter)
110	6	Internetwork control
111	7	Network control

Interface Wide QoS Port Classifications

Interface Wide Port Classifications classify all traffic on an interface to specific QoS parameters.

	Command	**Explanation**
Step 1	configure terminal	Enter Global Configuration Mode.

Step 2	interface {*, GigabitEthernet <1/1-24>, 10GigabitEthernet<1/1-2>}	Enter Interface Configuration Mode for the interface(s) in which to apply QoS Port Classifications to.
Step 3	qos cos <0-7>	Configure the default CoS value. All frames on the interface are classified to the CoS value. If the interface is VLAN aware, the frame's CoS is mapped from the tag's PCP and DEI value. **Note:** The CoS value can be overridden by a QoS Control List (QCL) entry.
Step 4	qos pcp <0-7>	Configure the default Priority Code Point (PCP) value. All frames are classified to a PCP value. If the interface is VLAN aware, PCP values contained within ingress tagged traffic are preserved. If untagged traffic is found on the interface, the traffic will be classified to the default PCP value.
Step 5	qos dpl <0-3>	Configure the default Drop Precedence Level (DPL) value. All frames are classified to a Drop Precedence Level. If the interface is VLAN aware, the frame's DPL is mapped from the tag's PCP and DEI value. **Note:** The DPL value can be overridden by a QoS Control List (QCL) entry.
Step 6	qos dei <0-1>	Configure the default Drop Eligibility Indicator (DEI). All frames are classified to a DEI. If the interface in VLAN aware, DEI values contained within ingress tagged traffic are preserved.

		If untagged traffic is found on the interface, the traffic will be classified to the default DEI value.
Step 7	qos class <0-7>	Configure the default CoS ID. All ingress traffic is classified to a CoS ID. The CoS ID can be utilized for rewriting of different parts of the frame.
Step 8	qos trust {dscp | tag}	Enable DSCP Based QoS Ingress Port Classification. When DSCP Based QoS Ingress Port Classification is enabled, the switch will use the DSCP in the IP header to determine to correct CoS value.
Step 9	qos wred-group <1-3>	Map the interface to a WRED Group. WRED Groups are configured from Global Configuration mode.
Step 10	end	**(Optional)** Return to Privileged EXEC mode.
Step 11	copy running-config startup-config	**(Optional)** Copy the contents of the running-config to the startup-config.

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# interface GigabitEthernet 1/1
FLEX24-10G(config-if)# qos cos 5
FLEX24-10G(config-if)# qos pcp 2
FLEX24-10G(config-if)# qos dpl 2
FLEX24-10G(config-if)# qos dei 1
FLEX24-10G(config-if)# qos class 5
FLEX24-10G(config-if)# qos trust tag
FLEX24-10G(config-if)# qos wred-group 1
FLEX24-10G(config-if)# end
FLEX24-10G# copy running-config startup-config
Building configuration...
% Saving 3721 bytes to flash:startup-config
FLEX24-10G#
```

WRED Group Configuration

WRED Groups are configured from Global Configuration mode. The FLEX24-10G contains three WRED groups.

Each WRED Group can have its Drop Precedence Level configured for each CoS value.

For example, WRED Group 1 can be modified such that traffic with a CoS and DPL value of 3 and 2 respectively, can have its drop probability configured.

The drop probability is configured via a lower and upper bound. The lower bound must be within 0-100% and the upper bound must be within 1-100%.

Each WRED group has seven queues, and each queue has 3 DPL options. The minimum, maximum, and fill-unit parameters can be modified for each of the 21 possible combinations. For a total of three groups, this equates to 63 possible permutations.

WRED Groups are configured as follows:

	Command	Explanation
Step 1	configure terminal	Enter Global Configuration Mode.
Step 2	qos wred group <1-3> queue <0-7> dpl <1-3> min-fl <0-100> max <1-100> [fill-level]	Modify one of the possible 63 Group-Queue-Entries. **group <1-3>** specifies which WRED group the command with modify. **queue <0-7>** specifies which CoS priority the command will alter. **dpl <1-3>** specifies which Drop Precedence Level to configure the upper and lower bound for. **min-fl <0-100>** and **max <1-100>** configure the lower and upper bound respectively for the drop-probability. The optional **fill-level** keyword indicates that the **max** parameter only applies when the drop probability reaches 100%. By default, **fill-level** is not applied, and the **max** parameter applies when the drop probability is just below 100%.
Step 3	end	**(Optional)** Return to Privileged EXEC mode.
Step 4	copy running-config startup-config	**(Optional)** Copy the contents of the running-config to the startup-config.

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# qos wred group 1 queue 2 dpl 1 min-fl 0 max 75
FLEX24-10G(config)# qos wred group 1 queue 2 dpl 2 min-fl 0 max 90
FLEX24-10G(config)# qos wred group 1 queue 2 dpl 3 min-fl 0 max 100 fill-level
FLEX24-10G(config)# end
FLEX24-10G# copy running-config startup-config
Building configuration...
% Saving 2588 bytes to flash:startup-config
FLEX24-10G#
```

Egress Port Tag Remarking

Egress Port Tag Remarking allows for the remarking of the PCP, and the DEI field within egress traffic.

The FLEX24-10G supports two Tag Remarking modes: Remarked and Mapped.

Remarked overwrites all PCP and DEI values found in the IP header of egress traffic with two administratively set values.

Mapped maps (CoS, DPL) values to (PCP, DEI). Since there are eight possible CoS values and two possible DPL values, 16 (8 x 2) mappings can exist.

By default, all interfaces will not remark the PCP and DEI values found in the IP header of egress traffic.

To restore the Tag Remarking mode to its default state, issue the **no qos tag-remark** command from Interface Configuration mode.

Default Tag Remarking Configuration

	Command	**Explanation**
Step 1	configure terminal	Enter Global Configuration Mode.
Step 2	interface {*, GigabitEthernet <1/1-24>, 10GigabitEthernet<1/1-2>}	Enter Interface Configuration mode for the interface(s) in which to remark PCP and DEI values.
Step 3	qos tag-remark pcp <0-7> dei <0-1>	Remark all egress traffic on the specified interface with the (PCP, DEI) pairing.
Step 4	end	**(Optional)** Return to Privileged EXEC mode.
Step 5	copy running-config startup-config	**(Optional)** Copy the contents of the running-config to the startup-config.

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# interface GigabitEthernet 1/1
FLEX24-10G(config-if)# qos tag-remark pcp 5 dei 1
FLEX24-10G(config-if)#
```

Mapped Tag Remarking Configuration

	Command	**Explanation**
Step 1	configure terminal	Enter Global Configuration Mode.
Step 2	interface {*, GigabitEthernet <1/1-24>, 10GigabitEthernet<1/1-2>}	Enter Interface Configuration mode for the interface(s) in which to remark PCP and DEI values.
Step 3	qos tag-remark mapped	Set the Mapped Tag Remarking mode to Mapped.
	qos map cos-tag cos <0-7> dpl <0-1> pcp <0-7> dei <0-1>	Map a (CoS, DPL) pair to a (PCP, DEI) pair.
Step 4	end	**(Optional)** Return to Privileged EXEC mode.
Step 5	copy running-config startup-config	**(Optional)** Copy the contents of the running-config to the startup-config.

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# interface GigabitEthernet 1/1
FLEX24-10G(config-if)# qos tag-remark mapped
FLEX24-10G(config-if)# qos map cos-tag cos 7 dpl 1 pcp 2 dei 0
FLEX24-10G(config-if)# end
FLEX24-10G# copy running-config startup-config
Building configuration...
% Saving 3826 bytes to flash:startup-config
FLEX24-10G#
```

Queue Policing

Up to eight queues can be configured on each of the FLEX24-10G’s interfaces. Each queue contains a limiter for each interface on the switch.

These queues are used for deficit weighted round robin queueing. Each interface can support eight ingress queues and eight egress queues. The queue number corelates with the CoS value of the traffic which will be found on that queue. For example, only traffic with a CoS value of 0 will be found on Queue 0, traffic with a Cos value of 1 will be found on Queue 1, so on and for forth.

Ingress Queueing

Traffic in queues area handled in one of two ways, Strict Priority or Weighted Round Robin.

Strict Priority: With multiple queues with multiple priorities, traffic from the highest priority queue is always transmitted first. Traffic from lower priority queues must wait until all the traffic from the higher priority queues has been transmitted.

Weighted Round Robin: Each queue is assigned a weight. The weight of the queue corresponds to the amount of bandwidth allowed on that queue.

Eight queues can be configured on the FLEX24-10G and then mapped to individual interfaces. Single queues can be mapped to one or more interfaces. Each queue can be rate restricted with the rate being a value from 25-13128147 kbps.

When a queue has been enabled on an interface, the bandwidth for that queue will not exceed the queue rate on the interface.

Ingress Port Policing

Port Policing applies a bandwidth (rate) limit on an interface or interfaces. When ingress traffic exceeds this limit, the excess traffic is dropped by the switch.

Enabling an Ingress Queue on an Interface

An Ingress Queue limits how much ingress traffic a queue can receive. A queue can be enabled on one or more interfaces from Interface Configuration mode as follows:

	Command	Explanation
Step 1	configure terminal	Enter Global Configuration Mode.
Step 2	interface {*, GigabitEthernet <1/1-24>, 10GigabitEthernet<1/1-2>}	Enter Interface Configuration mode for the interface(s) in which to enable an Ingress Queue on.
Step 3	qos queue-policer queue <0-7> <1-13128147> [kbps | mbps]	Enable an Ingress Queue on the interface and configure the queue with a bandwidth limit. **<0-7>** identifies the queue to be enabled on the interface. By default, the bandwidth limit is set in kbps. When applying the **kbps** keyword, the limit must be within the range of 25 and 13128147. When applying the **mbps** keyword, the limit must be within the range of 1 and 13128.
Step 4	end	**(Optional)** Return to Privileged EXEC mode.
Step 5	copy running-config startup-config	**(Optional)** Copy the contents of the running-config to the startup-config.

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# interface GigabitEthernet 1/1
FLEX24-10G(config-if)# qos queue-policer queue 0 10000 mbps
FLEX24-10G(config-if)# qos queue-policer queue 1 500
FLEX24-10G(config-if)# qos queue-policer queue 2 1000
FLEX24-10G(config-if)# qos queue-policer queue 3 1500
FLEX24-10G(config-if)# qos queue-policer queue 4 2000
FLEX24-10G(config-if)# qos queue-policer queue 5 2500
FLEX24-10G(config-if)# qos queue-policer queue 6 3000
FLEX24-10G(config-if)# qos queue-policer queue 7 3500
FLEX24-10G(config-if)# end
FLEX24-10G# copy running-config startup-config
Building configuration...
% Saving 2605 bytes to flash:startup-config
FLEX24-10G#
```

Egress Queueing

Port Shaping and Scheduling allows for the configuration of any egress queues configured on an interface. By default, no egress queues are enabled on any interfaces.

Up to eight egress queues can be enabled on an interface simultaneously. Each queue's rate can operate based on the line rate or the data rate.

Additionally, each queue's weight can be configured. The queue weight directly corresponds to what percentage of traffic on the switchport will be transmitted on that queue.

Configuring the Egress Port Shaper Data Stream

	Command	**Explanation**
Step 1	configure terminal	Enter Global Configuration mode.
Step 2	interface {*, GigabitEthernet <1/1-24>, 10GigabitEthernet<1/1-2>}	Enter Interface Configuration mode for the interface(s) in which to configure an Egress Port Shaper on.
Step 3	qos shaper <1-13107100> [kbps | mbps] [rate-type {data | line}]	Configure the Port Shaper. By default, the bandwidth limit is set in kbps. When applying the **kbps** keyword, the limit must be within the range of 100 and 13107100. When applying the **mbps** keyword, the limit must be within the range of 1 and 13107. The rate is rounded up to the nearest value supported by the port shaper. **rate-type data:** The rate offered by the physical layer to the data link layer. **rate-type line:** The speed in which bits are sent onto the wire.
Step 4	end	**(Optional)** Return to Privileged EXEC mode.
Step 5	copy running-config startup-config	**(Optional)** Copy the contents of the running-config to the startup-config.

Configuring Port Shapers and Schedulers

Egress Port Shapers limit the amount of egress traffic which a queue can transmit on an interface. Egress Port Shapers are also configured at the interface level as follows:

	Command	**Explanation**
Step 1	configure terminal	Enter Global Configuration Mode.
Step 2	interface {*, GigabitEthernet <1/1-24>, 10GigabitEthernet<1/1-2>}	Enter Interface Configuration mode for the interface(s) in which to enable an Egress Port Shaper on.
Step 3	qos queue-shaper queue <0-7> <1-13107100> [kbps | mbps] [rate-type {data | line}]	Enable an Egress Port Shaper on the interface and configure the shaper with a bandwidth limit. **<0-7>** identifies the queue to be enabled on the interface. By default, the bandwidth limit is set in kbps. When applying the **kbps** keyword, the limit must be within the range of 100 and 13107100. When

		applying the **mbps** keyword, the limit must be within the range of 1 and 13107. The rate is rounded up to the nearest value supported by the queue shaper. **rate-type data:** The rate offered by the physical layer to the data link layer. **rate-type line:** The speed in which bits are sent onto the wire.
Step 4	end	**(Optional)** Return to Privileged EXEC mode.
Step 5	copy running-config startup-config	**(Optional)** Copy the contents of the running-config to the startup-config.

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# interface GigabitEthernet 1/1
FLEX24-10G(config-if)# qos queue-shaper queue 0 10000 mbps
FLEX24-10G(config-if)# qos queue-shaper queue 1 500
FLEX24-10G(config-if)# qos queue-shaper queue 2 1000
FLEX24-10G(config-if)# qos queue-shaper queue 3 1500
FLEX24-10G(config-if)# qos queue-shaper queue 4 2000
FLEX24-10G(config-if)# qos queue-shaper queue 5 2500
FLEX24-10G(config-if)# qos queue-shaper queue 6 3000 rate-type line
FLEX24-10G(config-if)# qos queue-shaper queue 7 3500 rate-type data
FLEX24-10G(config-if)# end
FLEX24-10G# copy running-config startup-config
Building configuration...
% Saving 2625 bytes to flash:startup-config
FLEX24-10G#
```

Port Scheduling is configured by assigning weights to individual queues. The queue weights can be configured as follows:

	Command	**Explanation**
Step 1	configure terminal	Enter Global Configuration mode.
Step 2	interface {*, GigabitEthernet <1/1-24>, 10GigabitEthernet<1/1-2>}	Enter interface configuration mode for the interfaces in which to configure port scheduling
Step 3	qos wrr <1-100> <1-100> [<1-100> <1-100> <1-100> <1-100> <1-100> <1-100>]	Configure each queue with a desired weight. The weight must be a value between 1 and 100. Each <1-100> represents the weight of each queue. Queue 0's weight is configured using the first <1-100>, Queue 1's using the second <1-100>, so on and for forth.

		A minimum of two queues' weights must be configured for the switch to how to divide the traffic among the queues.
Step 4	end	**(Optional)** Return to Privileged EXEC mode.
Step 5	copy running-config startup-config	**(Optional)** Copy the contents of the running-config to the startup-config.

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# interface GigabitEthernet 1/1
FLEX24-10G(config-if)# qos wrr 17 100 10 10 50 50 50 50
FLEX24-10G(config-if)# end
FLEX24-10G# copy running-config startup-config
Building configuration...
% Saving 2625 bytes to flash:startup-config
FLEX24-10G#
```

The above CLI snippet configures the Queues 0 through 7 with the following weights:

Queue	Weight
0	17
1	100
2	10
3	10
4	50
5	50
6	50
7	50

To determine what percentage of egress traffic will be transmitted out each queue, calculate the sum of all the queue weights, and divide each queue weight by the total sum.

Example: Total Sum = 17 + 100 + 10 + 10 + 50 + 50 + 50 + 50 = 337

Queue 1 Percentage = 17/337 = 5.0% of traffic will be transmitted out Queue 1
Queue 2 Percentage = 100/337 = 29.7% of traffic will be transmitted out Queue 2
Queue 3 Percentage = 10/337 = 2.9% of traffic will be transmitted out Queue 3
Queue 4 Percentage = 10/337 = 2.9% of traffic will be transmitted out Queue 4
Queue 5 Percentage = 50/337 = 14.8% of traffic will be transmitted out Queue 5
Queue 6 Percentage = 50/337 = 14.8% of traffic will be transmitted out Queue 6
Queue 7 Percentage = 50/337 = 14.8% of traffic will be transmitted out Queue 7
Queue 8 Percentage = 50/337 = 14.8% of traffic will be transmitted out Queue 8

Percentages do not sum to 100% due to rounding.

With several queues and their weights configured on an interface, the interface will know how to prioritize each queue and how to distribute traffic between the queues.

The FLEX24-10G uses Dynamic Weighted Round Robin to consolidate all active Queue Shapers on an interface into a single data stream.

The single data stream can also have its properties configured such as its data/line rate.

Applying a Bandwidth (Rate) Limit on an Interface

Bandwidth limits are applied at the interface level as follows:

	Command	Explanation
Step 1	configure terminal	Enter Global Configuration Mode.
Step 2	interface {*, GigabitEthernet <1/1-24>, 10GigabitEthernet<1/1-2>}	Enter Interface Configuration mode for the interface in which to apply a bandwidth limit to.
Step 3	qos policer <1-13128147> [fps | kbps | kfps | mbps] [flowcontrol]	Set a bandwidth limit on the specified interface. **fps:** frames per second **kbps:** kilobits per second **kfps:** kiloframes (thousands of frames) per second **mbps:** megabits per second The optional **flowcontrol** keyword enables the transmission of pause frames. Pause frames will pause the transmission of data as opposed to dropping excess traffic.
Step 4	end	**(Optional)** Return to Privileged EXEC mode.
Step 5	copy running-config startup-config	**(Optional)** Copy the contents of the running-config to the startup-config.

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# interface GigabitEthernet 1/1
FLEX24-10G(config-if)# qos policer 55555 flowcontrol
FLEX24-10G(config-if)# int
FLEX24-10G(config-if)# interface GigabitEthernet 1/2
FLEX24-10G(config-if)# qos policer 55555 kfps
% QOS: max rate is 13128 when using kfps
FLEX24-10G(config-if)# qos policer 13000 kfps
FLEX24-10G(config-if)# interface GigabitEthernet 1/3
FLEX24-10G(config-if)# qos policer 55555 mbps
% QOS: max rate is 13128 when using mbps
FLEX24-10G(config-if)# qos policer 13000 mbps flowcontrol
FLEX24-10G(config-if)# end
FLEX24-10G# copy running-config startup-config
Building configuration...
% Saving 2685 bytes to flash:startup-config
FLEX24-10G#
```

Note: When the **flowcontrol** unit is set to either **kfps**, or **mbps**, the quantity must be within the range of 1 to 13128. When the units are set to either **fps**, or **kbps**, the quantity can occupy and value within the range of 10 to 13128147.

Port DSCP Configuration

Port DSCP Configuration allows for the remarking of the DSCP field for ingress traffic.

The DSCP can be modified by two different means, Classification and Translation. Both translation and classification can be enabled on an interface at the same time.

Classification will overwrite the current DSCP value and apply a new value based on the frames CoS and DSCP values.

Translation only examines the frame's existing DSCP value and will translate the current value to a new value based on an administratively set mapping.

Classification Configuration

Interface Classification can possess four different states:

1. **Disabled:** Ingress DSCP Classification is not enabled
2. **DSCP=0:** Classification only occurs when the DSCP value of ingress traffic is equal to 0. Classification will also occur when **qos dscp-translate** has been issued on the interface.
3. **Selected:** Classification only occurs when a frame contains a DSCP value which is contained within a DSCP translation entry. The DSCP translation entry must also have Classification enabled.
4. **Any:** Classify all, regardless of the DSCP value of ingress traffic.

Modifying an Interfaces Classification State

An interface's classification state is modified within interface configuration mode as follows:

	Command	**Explanation**
Step 1	configure terminal	Enter Global Configuration Mode.
Step 2	interface {*, GigabitEthernet <1/1-24>, 10GigabitEthernet<1/1-2>}	Enter Interface Configuration Mode.
Step 3	qos dscp-classify {any | selected | zero}	Modify the interfaces classification state. By default, all interfaces are disabled and do not perform ingress DSCP classification.
Step 4	end	**(Optional)** Return to Privileged EXEC mode.
Step 5	copy running-config startup-config	**(Optional)** Copy the contents of the running-config to the startup-config.

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# interface GigabitEthernet 1/1
FLEX24-10G(config-if)# qos dscp-classify ?
```

```
    any         Classify to new DSCP always
    selected    Classify to new DSCP if classify is enabled for specific DSCP
                value in global DSCP classify map
    zero        Classify to new DSCP if DSCP is 0
FLEX24-10G(config-if)# qos dscp-classify zero
FLEX24-10G(config-if)# end
FLEX24-10G# copy running-config startup-config
Building configuration...
% Saving 4413 bytes to flash:startup-config
FLEX24-10G#
```

Creating a DSCP Translation Entry

DSCP values can be translated on ingress traffic and remapped for egress traffic. Translation entries apply to all switchports.

Ingress Translation

	Command	Explanation
Step 1	configure terminal	Enter Global Configuration Mode.
Step 2	qos map dscp-ingress-translation {<0-63> | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | be | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va} to {<0-63> | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | be | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va}	Create an ingress translation mapping. If ingress traffic matches an ingress translation mapping, the DSCP value will be overwritten based on the contents of the mapping.
Step 3	qos map dscp-classify {<0-63> | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | be | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va}	**(Optional)** Classify a specific DSCP value. When a DSCP value is classified, the value is eligible for classification.
Step 4	end	**(Optional)** Return to Privileged EXEC mode.
Step 5	copy running-config startup-config	**(Optional)** Copy the contents of the running-config to the startup-config.

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# qos map dscp-ingress-translation ?
    <0~63>    Specific DSCP or range
    af11      Assured Forwarding PHB AF11(DSCP 10)
    af12      Assured Forwarding PHB AF12(DSCP 12)
    af13      Assured Forwarding PHB AF13(DSCP 14)
    af21      Assured Forwarding PHB AF21(DSCP 18)
    af22      Assured Forwarding PHB AF22(DSCP 20)
    af23      Assured Forwarding PHB AF23(DSCP 22)
    af31      Assured Forwarding PHB AF31(DSCP 26)
    af32      Assured Forwarding PHB AF32(DSCP 28)
    af33      Assured Forwarding PHB AF33(DSCP 30)
    af41      Assured Forwarding PHB AF41(DSCP 34)
```

```
    af42      Assured Forwarding PHB AF42(DSCP 36)
    af43      Assured Forwarding PHB AF43(DSCP 38)
    be        Default PHB(DSCP 0) for best effort traffic
    cs1       Class Selector PHB CS1 precedence 1(DSCP 8)
    cs2       Class Selector PHB CS2 precedence 2(DSCP 16)
    cs3       Class Selector PHB CS3 precedence 3(DSCP 24)
    cs4       Class Selector PHB CS4 precedence 4(DSCP 32)
    cs5       Class Selector PHB CS5 precedence 5(DSCP 40)
    cs6       Class Selector PHB CS6 precedence 6(DSCP 48)
    cs7       Class Selector PHB CS7 precedence 7(DSCP 56)
    ef        Expedited Forwarding PHB(DSCP 46)
    va        Voice Admit PHB(DSCP 44)
FLEX24-10G(config)# qos map dscp-ingress-translation af22 to 2
FLEX24-10G(config)# end
FLEX24-10G# copy running-config startup-config
Building configuration...
% Saving 4454 bytes to flash:startup-config
FLEX24-10G#
```

Egress Remapping

Egress Remapping is configured similarly to Ingress Translation.

	Command	**Explanation**
Step 1	configure terminal	Enter Global Configuration Mode.
Step 2	qos map dscp-egress-translation {<0-63> | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | be | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va} to {<0-63> | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | be | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va}	Create an egress remapping. If egress traffic matches an egress remapping entry, the DSCP value will be overwritten based on the contents of the mapping.
Step 3	end	**(Optional)** Return to Privileged EXEC mode.
Step 4	copy running-config startup-config	**(Optional)** Copy the contents of the running-config to the startup-config.

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# qos map dscp-egress-translation 22 to 28
FLEX24-10G(config)# end
FLEX24-10G# copy running-config startup-config
Building configuration...
% Saving 4495 bytes to flash:startup-config
FLEX24-10G#
```

DSCP Classification

DSCP Classification allows for a frame's DSCP value to be overwritten based on that same frame's CoS and DPL value.

There are eight unique CoS values and four unique DPL (Drop Precedence Level), creating 32 possible mappings.

Creating a DSCP Classification Entry

DSCP Classification Entries are created from Global Configuration as follows

	Command	Explanation
Step 1	configure terminal	Enter Global Configuration Mode.
Step 2	qos map cos-dscp <0-7> dpl <0-3> dscp {<0-63> | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | be | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va}	Create a DSCP Classification Entry. Traffic found with a CoS of **<0-7>** and a DPL value of **<0-3>** will be given a DSCP value pertaining to the value in the entry.
Step 3	end	**(Optional)** Return to Privileged EXEC mode.
Step 4	copy running-config startup-config	**(Optional)** Copy the contents of the running-config to the startup-config.

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# qos map cos-dscp 2 dpl 2 dscp cs1
FLEX24-10G(config)# end
FLEX24-10G# copy running-config startup-config
Building configuration...
% Saving 4527 bytes to flash:startup-config
FLEX24-10G#
```

DSCP-Based QoS

DSCP-Based QoS performs the opposite operation to DSCP Classification. Where DSCP Classification would examine the CoS and DPL values of ingress traffic and then overwrite the packets DSCP value, DSCP-Based QoS examines the packets DSCP value and overwrites the packets CoS and DPL values.

Creating a DSCP-Based QoS Rule

DSCP-Based QoS Rules and created from Global Configuration as follows:

	Command	Explanation
Step 1	configure terminal	Enter Global Configuration mode.
Step 2	qos map dscp-cos {<0-63> | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | be | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va} cos <0-7> dpl <0-3>	Create a DSCP to (CoS, DPL) mapping.
Step 3	end	**(Optional)** Return to Privileged EXEC mode.
Step 4	copy running-config startup-config	**(Optional)** Copy the contents of the running-config to the startup-config.

Ingress Maps

Ingress Maps consist of one or more map entries. Each map entry consists of a key and an action. The key indicates which fields of the frame will be mapped to the fields specified by the action.

The four possible values for the Map Key are as follows:

1. **PCP:** When the key is set to PCP only frames containing a VLAN tag will match this key.
2. **PCP – DEI:** A key setting of PCP – DEI will only match frames with a specific (PCP,DEI) pairing.
3. **DSCP:** The DSCP value is used as the key for IP frames.
4. **DSCP – PCP – DEI:** For IP frames the DSCP value is used as the key. For non-IP frames the classified (PCP, DEI) pairing is used.

Once the Map Key value has been set the Action must be set. If an ingress frame matches the key, specific QoS values within the frame will be overridden according to the value of the action.

The six configurable Map Action values are as follows:

1. **CoS:** Class of Service Value
2. **DPL:** Drop Precedence Level
3. **PCP:** Priority Code Point
4. **DEI:** Drop Eligible Indicator
5. **DSCP:** Differentiated Service Code Point
6. **CoS ID:** Class of Service ID

Creating an Ingress Map

	Command	**Explanation**
Step 1	configure terminal	Enter Global Configuration Mode.
Step 2	qos map ingress <0-255>	Create an Ingress Map. **<0-255>** represents the Map ID. Up to 256 Map ID's can be present on the switch. **Note:** The prompt will change to FLEX24-10G(config-qos-map-ingress)#
Step 3	key {pcp | pcp-dei | dscp | dscp-pcp-dei}	Set the key value.
Step 4	action {class | cos | dei | dpl | dscp | pcp} [class] [cos] [dei] [dpl] [dscp] [pcp]	Set the action. Only actions which are explicitly specified in the action command are mapped to keys, regardless of the actions(values) specified in Step 5.

		At least one action parameter must be set. Up to six parameters can be specified.
Step 5	map {pcp <0-7> [dei <0-1>] | dscp {<0-63> | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | be | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va}} **to** {class <0-7> | cos <0-7> | dei <0-1> | dpl <0-3> | dscp <0-63> | pcp <0-7>} [class <0-7>] [cos <0-7>] [dei <0-1>] [dpl <0-3>] [dscp <0-63>] [pcp <0-7>]	Configure the mapping between keys and values. The **map** command takes the form of **map {key} to {values}.** If [dei <0-1>] is left out from the key, only mappings for a DEI value of 0 are configured.
Step 6	preset classes <1-8> [color-aware]	Information Below.
Step 7	end	**(Optional)** Return to Privileged EXEC mode.
Step 8	copy running-config startup-config	**(Optional)** Copy the contents of the running-config to the startup-config.

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# qos map ingress 1
FLEX24-10G(config-qos-map-ingress)# key dscp-pcp-dei
FLEX24-10G(config-qos-map-ingress)# action dscp pcp dpl dei cos
FLEX24-10G(config-qos-map-ingress)# map dscp af41 to dscp 55
FLEX24-10G(config-qos-map-ingress)# end
FLEX24-10G# copy running-config startup-config
Building configuration...
% Saving 2101 bytes to flash:startup-config
FLEX24-10G#
```

Preset Classes

Preset Classes create a mapping between multiple PCP values and multiple CoS ID and CoS values. The amount of mappings is entirely dependent on the parameter the administrator provides when executing the command.

color-aware: Creates a map for DEI values 0 and 1. If color-aware is not provided only maps for a DEI of 0 are created.

Example: The below snippet creates eight ingress maps with eight preset classes:

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# qos map ingress 1
FLEX24-10G(config-qos-map-ingress)# preset classes 1
FLEX24-10G(config-qos-map-ingress)# exit
FLEX24-10G(config)# qos map ingress 2
FLEX24-10G(config-qos-map-ingress)# preset classes 2
FLEX24-10G(config-qos-map-ingress)# exit
FLEX24-10G(config)# qos map ingress 3
FLEX24-10G(config-qos-map-ingress)# preset classes 3
```

```
FLEX24-10G(config-qos-map-ingress)# exit
FLEX24-10G(config)# qos map ingress 4
FLEX24-10G(config-qos-map-ingress)# preset classes 4
FLEX24-10G(config-qos-map-ingress)# exit
FLEX24-10G(config)# qos map ingress 5
FLEX24-10G(config-qos-map-ingress)# preset classes 5
FLEX24-10G(config-qos-map-ingress)# exit
FLEX24-10G(config)# qos map ingress 6
FLEX24-10G(config-qos-map-ingress)# preset classes 6
FLEX24-10G(config-qos-map-ingress)# exit
FLEX24-10G(config)# qos map ingress 7
FLEX24-10G(config-qos-map-ingress)# preset classes 7 color-aware
FLEX24-10G(config-qos-map-ingress)# exit
FLEX24-10G(config)# qos map ingress 8
FLEX24-10G(config-qos-map-ingress)# preset classes 8 color-aware
FLEX24-10G(config-qos-map-ingress)# ^Z
FLEX24-10G# show running-config | begin qos map ingress 1
qos map ingress 1
 action class cos dpl
!
qos map ingress 2
 action class cos dpl
 map pcp 4 dei 0 to class 1 cos 1
 map pcp 5 dei 0 to class 1 cos 1
 map pcp 6 dei 0 to class 1 cos 1
 map pcp 7 dei 0 to class 1 cos 1
!
qos map ingress 3
 action class cos dpl
 map pcp 4 dei 0 to class 1 cos 1
 map pcp 5 dei 0 to class 1 cos 1
 map pcp 6 dei 0 to class 2 cos 2
 map pcp 7 dei 0 to class 2 cos 2
!
qos map ingress 4
 action class cos dpl
 map pcp 2 dei 0 to class 1 cos 1
 map pcp 3 dei 0 to class 1 cos 1
 map pcp 4 dei 0 to class 2 cos 2
 map pcp 5 dei 0 to class 2 cos 2
 map pcp 6 dei 0 to class 3 cos 3
 map pcp 7 dei 0 to class 3 cos 3
!
qos map ingress 5
 action class cos dpl
 map pcp 2 dei 0 to class 1 cos 1
 map pcp 3 dei 0 to class 1 cos 1
 map pcp 4 dei 0 to class 2 cos 2
```

```
 map pcp 5 dei 0 to class 2 cos 2
 map pcp 6 dei 0 to class 3 cos 3
 map pcp 7 dei 0 to class 4 cos 4
!
qos map ingress 6
 action class cos dpl
 map pcp 0 dei 0 to class 1 cos 1
 map pcp 2 dei 0 to class 2 cos 2
 map pcp 3 dei 0 to class 2 cos 2
 map pcp 4 dei 0 to class 3 cos 3
 map pcp 5 dei 0 to class 3 cos 3
 map pcp 6 dei 0 to class 4 cos 4
 map pcp 7 dei 0 to class 5 cos 5
!
qos map ingress 7
 key pcp-dei
 action class cos dpl
 map pcp 0 dei 0 to class 1 cos 1
 map pcp 0 dei 1 to class 1 cos 1 dpl 1
 map pcp 1 dei 1 to dpl 1
 map pcp 2 dei 0 to class 2 cos 2
 map pcp 2 dei 1 to class 2 cos 2 dpl 1
 map pcp 3 dei 0 to class 3 cos 3
 map pcp 3 dei 1 to class 3 cos 3 dpl 1
 map pcp 4 dei 0 to class 4 cos 4
 map pcp 4 dei 1 to class 4 cos 4 dpl 1
 map pcp 5 dei 0 to class 4 cos 4
 map pcp 5 dei 1 to class 4 cos 4 dpl 1
 map pcp 6 dei 0 to class 5 cos 5
 map pcp 6 dei 1 to class 5 cos 5 dpl 1
 map pcp 7 dei 0 to class 6 cos 6
 map pcp 7 dei 1 to class 6 cos 6 dpl 1
!
qos map ingress 8
 key pcp-dei
 action class cos dpl
 map pcp 0 dei 0 to class 1 cos 1
 map pcp 0 dei 1 to class 1 cos 1 dpl 1
 map pcp 1 dei 1 to dpl 1
 map pcp 2 dei 0 to class 2 cos 2
 map pcp 2 dei 1 to class 2 cos 2 dpl 1
 map pcp 3 dei 0 to class 3 cos 3
 map pcp 3 dei 1 to class 3 cos 3 dpl 1
 map pcp 4 dei 0 to class 4 cos 4
 map pcp 4 dei 1 to class 4 cos 4 dpl 1
 map pcp 5 dei 0 to class 5 cos 5
 map pcp 5 dei 1 to class 5 cos 5 dpl 1
 map pcp 6 dei 0 to class 6 cos 6
```

```
map pcp 6 dei 1 to class 6 cos 6 dpl 1
map pcp 7 dei 0 to class 7 cos 7
map pcp 7 dei 1 to class 7 cos 7 dpl 1
```

Egress Maps

Egress Maps are configured in much the same way as Ingress Maps. Each map entry consists of a key and an action where the key and the action behave the same way as they would for an Ingress Map.

The key indicates which fields of the frame will be mapped to the fields specified by the action.

The four possible values for the Map Key are as follows:

1. **CoS ID:** The CoS value embedded within frames is used as the key.
2. **CLASS-DPL:** Both the CoS value and the DPL are used together as the key.
3. **DSCP:** The DSCP value is used as the key.
4. **DSCP – DPL:** Both the DSCP and DPL and used together as the key.

Once the Map Key value has been set the Action must be set. If an egress frame matches the key, specific QoS values within the frame will be overridden according to the value of the action.

The three configurable Map Action values are as follows:

1. **PCP:** Priority Code Point
2. **DEI:** Drop Eligibility Indicator
3. **DSCP:** Differentiated Services Code Point

Creating an Egress Map

	Command	**Explanation**
Step 1	configure terminal	Enter Global Configuration Mode.
Step 2	qos map egress <0-511>	Create an Egress Map. **<0-511>** represents the Map ID. Up to 512 Map ID's can be present on the switch. **Note:** The prompt will change to FLEX24-10G(config-qos-map-egress)#
Step 3	key {class | class-dpl | dscp | dscp-dpl}	Set the key value.
Step 4	action {dei | dscp | pcp} [dei] [dscp] [pcp]	Set the action. Only actions which are explicitly specified in the action command are mapped to keys, regardless of the actions(values) specified in Step 5.

		At least one action parameter must be set. Up to six parameters can be specified.
Step 5	map {class <0-7> [dpl <0-3>] | dscp {<0-63> | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | be | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va}} **to** {dei <0-1> | dscp <0-63> | pcp <0-7>} [dei <0-1>] [dscp <0-63>] [pcp <0-7>]	Configure the mapping between keys and values. The **map** command takes the form of **map {key} to {values}.** If [dpl <0-3>] is left out from the key, only mappings for a DPL value of 0 are configured.
Step 6	preset classes <1-8> [color-aware]	Information Below.
Step 7	end	**(Optional)** Return to Privileged EXEC mode.
Step 8	copy running-config startup-config	**(Optional)** Copy the contents of the running-config to the startup-config.

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# qos map egress 1
FLEX24-10G(config-qos-map-egress)# key class
FLEX24-10G(config-qos-map-egress)# action pcp dei
FLEX24-10G(config-qos-map-egress)# map class 2 to dscp 15
FLEX24-10G(config-qos-map-egress)# end
FLEX24-10G# copy running-config startup-config
Building configuration...
% Saving 2166 bytes to flash:startup-config
FLEX24-10G#
```

Preset Classes

Preset Classes also behave in the same manner as with Ingress Maps. With all preset classes the **action dei pcp** command is set. The number of mappings is entirely dependent on the value specified by the administrator when entering the command.

Example: When the following Egress Maps are created and configured via Preset classes:

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# qos map egress 1
FLEX24-10G(config-qos-map-egress)# preset classes 1
FLEX24-10G(config-qos-map-egress)# qos map egress 2
FLEX24-10G(config-qos-map-egress)# preset classes 2
FLEX24-10G(config-qos-map-egress)# qos map egress 3
FLEX24-10G(config-qos-map-egress)# preset classes 3
FLEX24-10G(config-qos-map-egress)# qos map egress 4
FLEX24-10G(config-qos-map-egress)# preset classes 4
FLEX24-10G(config-qos-map-egress)# qos map egress 5
FLEX24-10G(config-qos-map-egress)# preset classes 5
```

```
FLEX24-10G(config-qos-map-egress)# qos map egress 6
FLEX24-10G(config-qos-map-egress)# preset classes 6
FLEX24-10G(config-qos-map-egress)# qos map egress 7
FLEX24-10G(config-qos-map-egress)# preset classes 7
FLEX24-10G(config-qos-map-egress)# qos map egress 8
FLEX24-10G(config-qos-map-egress)# preset classes 8
FLEX24-10G(config-qos-map-egress)#
```

The following Egress Maps will appear in the running-config:

qos map egress 1 action dei pcp map class 1 dpl 0 to pcp 7 map class 1 dpl 1 to pcp 7 map class 1 dpl 2 to pcp 7 map class 1 dpl 3 to pcp 7 map class 2 dpl 0 to pcp 7 map class 2 dpl 1 to pcp 7 map class 2 dpl 2 to pcp 7 map class 2 dpl 3 to pcp 7 map class 3 dpl 0 to pcp 7 map class 3 dpl 1 to pcp 7 map class 3 dpl 2 to pcp 7 map class 3 dpl 3 to pcp 7 map class 4 dpl 0 to pcp 7 map class 4 dpl 1 to pcp 7 map class 4 dpl 2 to pcp 7 map class 4 dpl 3 to pcp 7 map class 5 dpl 0 to pcp 7 map class 5 dpl 1 to pcp 7 map class 5 dpl 2 to pcp 7 map class 5 dpl 3 to pcp 7 map class 6 dpl 0 to pcp 7 map class 6 dpl 1 to pcp 7 map class 6 dpl 2 to pcp 7 map class 6 dpl 3 to pcp 7 map class 7 dpl 0 to pcp 7 map class 7 dpl 1 to pcp 7 map class 7 dpl 2 to pcp 7 map class 7 dpl 3 to pcp 7	qos map egress 2 action dei pcp map class 1 dpl 0 to pcp 4 map class 1 dpl 1 to pcp 4 map class 1 dpl 2 to pcp 4 map class 1 dpl 3 to pcp 4 map class 2 dpl 0 to pcp 7 map class 2 dpl 1 to pcp 7 map class 2 dpl 2 to pcp 7 map class 2 dpl 3 to pcp 7 map class 3 dpl 0 to pcp 7 map class 3 dpl 1 to pcp 7 map class 3 dpl 2 to pcp 7 map class 3 dpl 3 to pcp 7 map class 4 dpl 0 to pcp 7 map class 4 dpl 1 to pcp 7 map class 4 dpl 2 to pcp 7 map class 4 dpl 3 to pcp 7 map class 5 dpl 0 to pcp 7 map class 5 dpl 1 to pcp 7 map class 5 dpl 2 to pcp 7 map class 5 dpl 3 to pcp 7 map class 6 dpl 0 to pcp 7 map class 6 dpl 1 to pcp 7 map class 6 dpl 2 to pcp 7 map class 6 dpl 3 to pcp 7 map class 7 dpl 0 to pcp 7 map class 7 dpl 1 to pcp 7 map class 7 dpl 2 to pcp 7 map class 7 dpl 3 to pcp 7
qos map egress 3 action dei pcp map class 1 dpl 0 to pcp 4 map class 1 dpl 1 to pcp 4 map class 1 dpl 2 to pcp 4 map class 1 dpl 3 to pcp 4 map class 2 dpl 0 to pcp 6 map class 2 dpl 1 to pcp 6 map class 2 dpl 2 to pcp 6	qos map egress 4 action dei pcp map class 1 dpl 0 to pcp 2 map class 1 dpl 1 to pcp 2 map class 1 dpl 2 to pcp 2 map class 1 dpl 3 to pcp 2 map class 2 dpl 0 to pcp 4 map class 2 dpl 1 to pcp 4 map class 2 dpl 2 to pcp 4

<table>
<tr>
<td>
<pre>
 map class 2 dpl 3 to pcp 6
 map class 3 dpl 0 to pcp 7
 map class 3 dpl 1 to pcp 7
 map class 3 dpl 2 to pcp 7
 map class 3 dpl 3 to pcp 7
 map class 4 dpl 0 to pcp 7
 map class 4 dpl 1 to pcp 7
 map class 4 dpl 2 to pcp 7
 map class 4 dpl 3 to pcp 7
 map class 5 dpl 0 to pcp 7
 map class 5 dpl 1 to pcp 7
 map class 5 dpl 2 to pcp 7
 map class 5 dpl 3 to pcp 7
 map class 6 dpl 0 to pcp 7
 map class 6 dpl 1 to pcp 7
 map class 6 dpl 2 to pcp 7
 map class 6 dpl 3 to pcp 7
 map class 7 dpl 0 to pcp 7
 map class 7 dpl 1 to pcp 7
 map class 7 dpl 2 to pcp 7
 map class 7 dpl 3 to pcp 7
</pre>
</td>
<td>
<pre>
 map class 2 dpl 3 to pcp 4
 map class 3 dpl 0 to pcp 6
 map class 3 dpl 1 to pcp 6
 map class 3 dpl 2 to pcp 6
 map class 3 dpl 3 to pcp 6
 map class 4 dpl 0 to pcp 7
 map class 4 dpl 1 to pcp 7
 map class 4 dpl 2 to pcp 7
 map class 4 dpl 3 to pcp 7
 map class 5 dpl 0 to pcp 7
 map class 5 dpl 1 to pcp 7
 map class 5 dpl 2 to pcp 7
 map class 5 dpl 3 to pcp 7
 map class 6 dpl 0 to pcp 7
 map class 6 dpl 1 to pcp 7
 map class 6 dpl 2 to pcp 7
 map class 6 dpl 3 to pcp 7
 map class 7 dpl 0 to pcp 7
 map class 7 dpl 1 to pcp 7
 map class 7 dpl 2 to pcp 7
</pre>
map class 7 dpl 3 to pcp 7
</td>
</tr>
<tr>
<td>
<pre>
qos map egress 5
 action dei pcp
 map class 1 dpl 0 to pcp 2
 map class 1 dpl 1 to pcp 2
 map class 1 dpl 2 to pcp 2
 map class 1 dpl 3 to pcp 2
 map class 2 dpl 0 to pcp 4
 map class 2 dpl 1 to pcp 4
 map class 2 dpl 2 to pcp 4
 map class 2 dpl 3 to pcp 4
 map class 3 dpl 0 to pcp 6
 map class 3 dpl 1 to pcp 6
 map class 3 dpl 2 to pcp 6
 map class 3 dpl 3 to pcp 6
 map class 4 dpl 0 to pcp 7
 map class 4 dpl 1 to pcp 7
 map class 4 dpl 2 to pcp 7
 map class 4 dpl 3 to pcp 7
 map class 5 dpl 0 to pcp 7
 map class 5 dpl 1 to pcp 7
 map class 5 dpl 2 to pcp 7
 map class 5 dpl 3 to pcp 7
 map class 6 dpl 0 to pcp 7
 map class 6 dpl 1 to pcp 7
 map class 6 dpl 2 to pcp 7
 map class 6 dpl 3 to pcp 7
 map class 7 dpl 0 to pcp 7
 map class 7 dpl 1 to pcp 7
 map class 7 dpl 2 to pcp 7
</pre>
</td>
<td>
<pre>
qos map egress 6
 action dei pcp
 map class 0 dpl 0 to pcp 1
 map class 0 dpl 1 to pcp 1
 map class 0 dpl 2 to pcp 1
 map class 0 dpl 3 to pcp 1
 map class 2 dpl 0 to pcp 2
 map class 2 dpl 1 to pcp 2
 map class 2 dpl 2 to pcp 2
 map class 2 dpl 3 to pcp 2
 map class 3 dpl 0 to pcp 4
 map class 3 dpl 1 to pcp 4
 map class 3 dpl 2 to pcp 4
 map class 3 dpl 3 to pcp 4
 map class 4 dpl 0 to pcp 6
 map class 4 dpl 1 to pcp 6
 map class 4 dpl 2 to pcp 6
 map class 4 dpl 3 to pcp 6
 map class 5 dpl 0 to pcp 7
 map class 5 dpl 1 to pcp 7
 map class 5 dpl 2 to pcp 7
 map class 5 dpl 3 to pcp 7
 map class 6 dpl 0 to pcp 7
 map class 6 dpl 1 to pcp 7
 map class 6 dpl 2 to pcp 7
 map class 6 dpl 3 to pcp 7
 map class 7 dpl 0 to pcp 7
 map class 7 dpl 1 to pcp 7
 map class 7 dpl 2 to pcp 7
</pre>
</td>
</tr>
</table>

map class 7 dpl 3 to pcp 7	map class 7 dpl 3 to pcp 7
`qos map egress 7`	`qos map egress 8`
` action dei pcp`	` action dei pcp`
` map class 0 dpl 0 to pcp 1`	` map class 0 dpl 0 to pcp 1`
` map class 0 dpl 1 to pcp 1`	` map class 0 dpl 1 to pcp 1`
` map class 0 dpl 2 to pcp 1`	` map class 0 dpl 2 to pcp 1`
` map class 0 dpl 3 to pcp 1`	` map class 0 dpl 3 to pcp 1`
` map class 2 dpl 0 to pcp 2`	` map class 2 dpl 0 to pcp 2`
` map class 2 dpl 1 to pcp 2`	` map class 2 dpl 1 to pcp 2`
` map class 2 dpl 2 to pcp 2`	` map class 2 dpl 2 to pcp 2`
` map class 2 dpl 3 to pcp 2`	` map class 2 dpl 3 to pcp 2`
` map class 3 dpl 0 to pcp 3`	` map class 3 dpl 0 to pcp 3`
` map class 3 dpl 1 to pcp 3`	` map class 3 dpl 1 to pcp 3`
` map class 3 dpl 2 to pcp 3`	` map class 3 dpl 2 to pcp 3`
` map class 3 dpl 3 to pcp 3`	` map class 3 dpl 3 to pcp 3`
` map class 4 dpl 0 to pcp 4`	` map class 4 dpl 0 to pcp 4`
` map class 4 dpl 1 to pcp 4`	` map class 4 dpl 1 to pcp 4`
` map class 4 dpl 2 to pcp 4`	` map class 4 dpl 2 to pcp 4`
` map class 4 dpl 3 to pcp 4`	` map class 4 dpl 3 to pcp 4`
` map class 5 dpl 0 to pcp 6`	` map class 5 dpl 0 to pcp 5`
` map class 5 dpl 1 to pcp 6`	` map class 5 dpl 1 to pcp 5`
` map class 5 dpl 2 to pcp 6`	` map class 5 dpl 2 to pcp 5`
` map class 5 dpl 3 to pcp 6`	` map class 5 dpl 3 to pcp 5`
` map class 6 dpl 0 to pcp 7`	` map class 6 dpl 0 to pcp 6`
` map class 6 dpl 1 to pcp 7`	` map class 6 dpl 1 to pcp 6`
` map class 6 dpl 2 to pcp 7`	` map class 6 dpl 2 to pcp 6`
` map class 6 dpl 3 to pcp 7`	` map class 6 dpl 3 to pcp 6`
` map class 7 dpl 0 to pcp 7`	` map class 7 dpl 0 to pcp 7`
` map class 7 dpl 1 to pcp 7`	` map class 7 dpl 1 to pcp 7`
` map class 7 dpl 2 to pcp 7`	` map class 7 dpl 2 to pcp 7`
` map class 7 dpl 3 to pcp 7`	` map class 7 dpl 3 to pcp 7`

Quality of Service Control Lists

The FLEX24-10G contains a single Quality of Service Control List (QCL). This single QCL can contain up to 256 Quality of Service Control Entries (QCE's).

QCLs and QCEs are very similar in function and configuration to ACLs and ACEs. It is best to become comfortable using the switch's context-sensitive help when configuring QCEs.

Configuration

QCEs are created and configured from Global Configuration. There are several different QoS parameters which can be used to filter traffic.

To create a QCE, begin the command with **qos qce [update] <1-256>.** The optional **[update]** keyword is used to update a QCE which already exists. **<1-256>** denotes the ID of the QCE.

Quality of Service Control Entries Explained

Interface

The interface parameter is used to enable the QCE on a select number of interfaces. By default, when a QCE is configured, it is enabled on all interfaces.

Parameter Syntax

The set of interfaces in which to enable the QCE on is specified via the use of the **interface** keyword. The syntax of the **interface** command is as follows:

qos qce <1-256> interface {*, GigabitEthernet <1/1-24>, 10GigabitEthernet<1/1-2>}

Source MAC Address

The source MAC address filter is used to filter packets based on their source MAC address. If ingress traffic matches the source MAC address in the QCE, then the action in the QCE is triggered.

Parameter Syntax

The syntax for the Source MAC Address is as follows:

qos qce <1-256> smac {<mac_address> | any}

```
FLEX24-10G(config)# qos qce 1 smac ?
    <mac_addr>    Matched SMAC (XX-XX-XX-XX-XX-XX)
    any           Match any SMAC
FLEX24-10G(config)# qos qce 1 smac
```

Destination MAC Address

The destination MAC address filter is used to filter packets based on their destination MAC address.

Available Destination MAC address types are:

- **Any:** No destination MAC filter is applied.
- **Broadcast:** QCE will only match ingress traffic containing a broadcast destination MAC address.
- **Multicast:** QCE will only match ingress traffic containing a multicast destination MAC address.
- **Unicast:** QCE will only match ingress traffic containing a unicast destination MAC address.
- **Specific:** QCE will only match a specific MAC address set by the administrator.

Parameter Syntax

The syntax for the Destination MAC Address is as follows:

qos qce <1-256> dmac {<mac_address> | any | broadcast | multicast | unicast}

```
FLEX24-10G(config)# qos qce 1 dmac ?
    <mac_addr>     Matched DMAC (XX-XX-XX-XX-XX-XX)
    any            Match any DMAC
    broadcast      Match broadcast DMAC
    multicast      Match multicast DMAC
    unicast        Match unicast DMAC
FLEX24-10G(config)# qos qce 1 dmac
```

(Outer) Tag

The **tag** keyword is used to create a filter which only matches the tag type, VID, DEI, or PCP values located in the outer tag of the frame.

Note: If a frame has multiple tags, the outer tags are the tag located closer to the Ethernet header, while the inner tag is the tag located closer to the frame's payload. If the frame only has a single tag, configure the Outer Tag and neglect the Inner Tag.

Multiple Outer Tag parameters can be configured in a single line. However, for the sake of brevity, each parameter will be explained individually.

Parameter Syntax

Outer Tagged Syntax

The syntax for the Outer Tag type parameter is as follows:

qos qce <1-256> tag type {any | c-tagged | s-tagged | tagged | untagged}

Outer VID Syntax

The syntax for the Outer VID is as follows:

qos qce <1-256> tag vid {<vlan_list> | any}

Outer DEI Value Syntax

The syntax for the Outer DEI Value is as follows:

qos qce <1-256> tag dei {<0-1> | any}

Outer PCP Value Syntax

The syntax for the Outer PCP Value is as follows:

qos qce <1-256> tag pcp {0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 0-1 | 2-3 | 4-5 | 6-7 | 0-3 | 4-7 | any}

Inner Tag/Inner VID/Inner PCP/Inner DEI

The Inner Tag parameter is used to filter ingress traffic by one or more of following frame properties:

- Tagged Status
- Frame VLAN membership
- DEI value
- PCP value

Multiple Ingress Inner Tag parameters can be configured in a single line. However, for the sake of brevity, each parameter will be explained individually.

Note: The Inner Tag/VID/PCP/DEI are the Tag, VID, PCP, and DEI values which are located closest to the payload portion of the frame. This contrasts with the outer TAG, VID, PCP, and DEI values which are located closest to the Ethernet header.

Parameter Syntax

Inner Tagged Syntax

The syntax for the Inner Tag type parameter is as follows:

qos qce <1-256> inner-tag type {any | c-tagged | s-tagged | tagged | untagged}

Inner VID Syntax

The syntax for the Inner VID is as follows:

qos qce <1-256> inner-tag vid {<vlan_list> | any}

Inner DEI Value Syntax

The syntax for the Inner DEI Value is as follows:

qos qce <1-256> inner-tag dei {<0-1> | any}

Inner PCP Value Syntax

The syntax for the Inner PCP Value is as follows:

qos qce <1-256> inner-tag pcp {0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 0-1 | 2-3 | 4-5 | 6-7 | 0-3 | 4-7 | any}

Frame Type

The frame type can be configured to examine ingress packets based on their frame type:

Available frame types are:

- **Any:** Allow all types of frames.

- **Etype:** Specify the specific Ethertype of the frames which you would like to match the QCE. Valid EtherType values are from 0x0600 to 0xFFFF (excluding 0x0800 (IPv4) and 0x86DD (IPv6)).
- **IPv4:** Allow only IPv4 frames. When a frame type of IPv4 has been set, additional filters for the protocol, source IP, destination IP, source port, destination port, fragment status, and DSCP value can also be configured.
- **IPv6:** Allow only IPv6 frames. When a frame type of IPv6 has been set, additional filters for the protocol, source IP, destination IP, source port, destination port, and DSCP value can also be configured.
- **LLC:** Only allow Logical Link Control (LLC) frames. LLC frames act as an interface between layer-2 and layer-3. When a frame type of LLC has been set, additional filters for the SSAP (Source Service Access Point), DSAP (Destination Service Access Point), and Control value can also be set.
- **SNAP:** Allow only SNAP frames. When a frame type of SNAP has been configured, additional filters for the PID (Ethertype) can also be configured.

Parameter Syntax

Frame Type of Ethertype

Configuring a QCE with a frame type of an Ethertype value is done as follows:

	Command	Explanation
Step 1	configure terminal	Enter Global Configuration Mode.
Step 2	qos qce <1-256> frame-type etype [<0x600-0x7ff> | <0x801-0x86dc> | <0x86de-0xffff>}	Set the QCE to filter ingress traffic by Ethertype. If a specific Ethertype value is not provided, the QCE will match any Ethertype value. Ethertype's of 0x800 and 0x86DD are invalid arguments as they are reserved for IPv4 and IPv6 frames respectively.
Step 3	end	**(Optional)** Return to Privileged EXEC mode.
Step 4	copy running-config startup-config	**(Optional)** Copy the contents of the running-config to the startup-config.

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# qos qce 1 frame-type etype 0x88cc
FLEX24-10G(config)# end
FLEX24-10G# copy running-config startup-config
Building configuration...
% Saving 2174 bytes to flash:startup-config
FLEX24-10G#
```

Frame Type of IPv4

Configuring a QCE with a frame type of IPv4 is done as follows:

	Command	**Explanation**
Step 1	configure terminal	Enter Global Configuration Mode.
Step 2	qos qce <1-256> frame-type ipv4 [proto {<0-255> | any | tcp | udp}] [sport {<sport> | any}] [dport {<dport> | any}] [sip {<ip_address>/<subnet_mask> | any}] [dip {<ip_address>/<subnet_mask> | any}] [fragment {any | no | yes}] [dscp {<0-63>-<0-63> | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | be | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va} | any]	Set the QCE to filter ingress traffic by IPv4 frames. Ingress IPv4 frames can be further filtered by protocol, source port, destination port, source IP, destination IP, fragment status, or DSCP value.
Step 3	end	**(Optional)** Return to Privileged EXEC mode.
Step 4	copy running-config startup-config	**(Optional)** Copy the contents of the running-config to the startup-config.

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# qos qce 1 frame-type ipv4 proto tcp sip 192.168.100.2/255.255.255.0
fragment any dscp cs3
FLEX24-10G(config)# end
FLEX24-10G# copy running-config startup-config
Building configuration...
% Saving 2205 bytes to flash:startup-config
FLEX24-10G#
```

Frame Type of IPv6

Configuring a QCE with a frame type of IPv6 is done as follows:

	Command	**Explanation**
Step 1	configure terminal	Enter Global Configuration Mode.
Step 2	qos qce <1-256> frame-type ipv6 [proto {<0-255> | any | tcp | udp}] [sport {<sport> | any}] [dport {<dport> | any}] [sip {<ip_address>/<subnet_mask> | any}] [dip {<ip_address>/<subnet_mask> | any}] [dscp {<0-63>-<0-63> | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | be | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va} | any]	Set the QCE to filter ingress traffic by IPv6 frames. Ingress IPv6 frames can be further filtered by protocol, source port, destination port, source IP, destination IP, or DSCP value.
Step 3	end	**(Optional)** Return to Privileged EXEC mode.
Step 4	copy running-config startup-config	**(Optional)** Copy the contents of the running-config to the startup-config.

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# qos qce 1 frame-type ipv6 proto udp sip any dip any dscp 0-45
FLEX24-10G(config)# end
FLEX24-10G# copy running-config startup-config
Building configuration...
% Saving 2186 bytes to flash:startup-config
```

```
FLEX24-10G#
```

Frame Type of LLC

Configuring a QCE with a frame type of LLC is done as follows:

<table>
<tr><th></th><th><u>Command</u></th><th><u>Explanation</u></th></tr>
<tr><td>Step 1</td><td>configure terminal</td><td>Enter Global Configuration Mode.</td></tr>
<tr><td>Step 2</td><td>qos qce <1-256> frame-type llc [ssap {<0-0xff> | any}] [dsap {<0-0xff> | any}] [control {<0-0xff> | any}]</td><td>Set the QCE to filter ingress traffic by LLC frames.

<u>SSAP:</u> The SSAP identifies the service access point (SAP) which initiated the PDU.

<u>DSAP:</u> The DSAP identifies the service access point (SAP) for which the PDU is intended.

<u>Control:</u> The control field comes in three varieties:

1. I Frames
2. Supervisory Frames
3. Unnumbered Frames

The last two bits of the control field allow for the identification of the frame.

<table><tr><th><u>Last Two Bits</u></th><th><u>Frame Type</u></th></tr><tr><td>0,0</td><td>I Frame</td></tr><tr><td>0,1</td><td>Supervisory Frame</td></tr><tr><td>1,1</td><td>Unnumbered Frame</td></tr></table>
<u>I Frames:</u> I frames allow for the sequential transfer of PDUs. These PDUs contain information and are transferred between stations. I-frames are made up of a collections NS’s (next-sends) and NR’s (next receives).

The NS indicates the sequence number of the current PDU while the NR indicates the sequence number of the next I-frame which the sender expects to receive.</td></tr>
</table>

	Supervisory Frames: Supervisory frames provide supervisory functions. Examples include: • Acknowledging I Frames • Requesting I Frames • Request for the transmission of I Frames to be paused There are three types of Supervisory frames which are differentiated by the value of the 5th and 6th bit.

5th and 6th Bit	Frame Type
0,0	Receiver Ready (RR)
0,1	Receiver Not Ready (RNR)
1,0	Reject (REJ)

RR: A station will send out an RR frame when it is ready to receive. The RR frame will contain the NR count of the next expected I frame.

RNR: RNR frames indicate that the current station is unable to receive frames. Persistent RNR's can be a result of network congestion.

REJ: Rejection frames are used to request the retransmission of I frames. The NR in the REJ frame indicates the first frame to be retransmitted.

Unnumbered Frames: Unnumbered Frames are 8-bits in length and follow the following format:

M-M-M-P/F-M-M-1-1

The value of the M bits indicates the type of unnumbered frame:

Value of M bits	Frame Type

00011	Disconnect Mode (DM) Response
01000	Disconnect (DISC) Command
01100	Unnumbered Acknowledgement (UA) Response
01111	SABME Command
10001	Frame Reject (FRMR) Response
10111	Exchange Identification (XID) Command or Response
11100	Test Command or Response

DM Response: A station will send a DM Response to indicate that it is in an asynchronous state. In other words, the link is not active.

DISC Command: A station will send a DISC to another station to inform it that it has suspended operation. The remote station will respond to a DISC with either a UA or a DM.

UA Response: A station will send a UA in response to a SABME or DISC frame.

SABME Command: A SABME is used to initiate data transfer while the current station is in asynchronous balanced mode. When a station receives a SABME command message, it will reset its NS and NR counts.

FRMR Response: A FRMR Response is used to indicate an error in an incoming PDU from another station. All frames which arrive after the FRMR are ignored until the station receives a DISC

		or SABME from the remote station. **XID Command/Response:** XID messages are used to share characteristics of one station to another. When a station receives a XID Command it will respond with a XID response. **TEST:** Test messages are used for path discovery between stations. When a station receives a TEST command it will reply with a TEST response.
Step 3	end	**(Optional)** Return to Privileged EXEC mode.
Step 4	copy running-config startup-config	**(Optional)** Copy the contents of the running-config to the startup-config.

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# qos qce 1 frame-type llc ssap any dsap 0x55 control any
FLEX24-10G(config)# end
FLEX24-10G# copy running-config startup-config
Building configuration...
% Saving 2175 bytes to flash:startup-config
FLEX24-10G#
```

Frame Type of SNAP

Configuring a QCE with a frame type of SNAP is done as follows:

	Command	**Explanation**
Step 1	configure terminal	Enter Global Configuration Mode.
Step 2	qos qce <1-256> frame-type snap [<0-0xffff>]	Set the QCE to filter ingress traffic by SNAP frames. The optional **<0-0xfff>** is used to specify the Ethertype of the SNAP frames.
Step 3	end	**(Optional)** Return to Privileged EXEC mode.
Step 4	copy running-config startup-config	**(Optional)** Copy the contents of the running-config to the startup-config.

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# qos qce 1 frame-type snap 0x88cc
FLEX24-10G(config)# end
FLEX24-10G# copy running-config startup-config
Building configuration...
% Saving 2173 bytes to flash:startup-config
```

```
FLEX24-10G#
```

Action

The Action Parameter configures which QoS parameters will be overwritten when this QCE matches ingress traffic.

The available action parameter are as follows:

- CoS
- DPL
- DSCP
- Ingress-Map
- PCP-DEI
- Policy

Parameter Syntax

The syntax for the Action parameter is as follows:

qos qce <1-256> action {cos {<0-7> | default} | [dpl {<0-3> | default}] | [dscp {<0-63> | af11 | af12 | af13 | af21 | af22 | af23 | af31 | af32 | af33 | be | cs1 | cs2 | cs3 | cs4 | cs5 | cs6 | cs7 | ef | va}] | [pcp-dei {<0-7> | default}] | [policy {<0-127> | default}] | [ingress-map {<0-255> | default}]}

At least one of the available action parameters must be specified.

Next

The next keyword places the current QCE which is being configured in a specific location in the QCE list.

Parameter Syntax

The syntax for the Next parameter is as follows:

qos qce <1-256> next <qce_id>

<qce_id> must already be configured on the switch. When QCE with ID **<1-256>** is created, the QCE will precede QCE with ID **<qce_id>.**

<u>**Example:**</u> By creating two QCEs (QCE1 and QCE 2), by default QCE 1 appears first in the QCE list. Creating QCE 2 with the **next 1** parameter will change the order of the QCE list such that QCE 2 appears first.

See below:

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# qos qce 1 frame-type ipv4
FLEX24-10G(config)# qos qce 2 frame-type ipv4 next 1
FLEX24-10G(config)# do show qos qce
```

```
static qce 2:
=============
 port: 1-27
 key parameters:
  dmac: any
  smac: any
  tag:
   type: any
   vid: any
   pcp: any
   dei: any
  inner tag:
   type: any
   vid: any
   pcp: any
   dei: any
  frametype: ipv4
   proto: any
   sip: any
   dip: any
   dscp: any
   frag: any
 action parameters:
  cos: default
  dpl: default
  dscp: default
  tag: default
  policy: default
  ingress-map: default

static qce 1:
=============
 port: 1-27
 key parameters:
  dmac: any
  smac: any
  tag:
   type: any
   vid: any
   pcp: any
   dei: any
  inner tag:
   type: any
   vid: any
   pcp: any
   dei: any
  frametype: ipv4
   proto: any
```

```
   sip: any
   dip: any
   dscp: any
   frag: any
 action parameters:
  cos: default
  dpl: default
  dscp: default
  tag: default
  policy: default
  ingress-map: default
FLEX24-10G(config)#
```

Last

The **last** keyword, when included, places the QCE at the bottom of the QCE list. By default, QCEs are placed in the execution order in the order they are created.

Example: Refer to the below snippet to see how the **last** keyword behaves.

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# qos qce 1 frame-type ipv4
FLEX24-10G(config)# qos qce 2 frame-type ipv6
FLEX24-10G(config)# do show qos qce

static qce 1:
=============
 port: 1-27
 key parameters:
  dmac: any
  smac: any
  tag:
   type: any
   vid: any
   pcp: any
   dei: any
  inner tag:
   type: any
   vid: any
   pcp: any
   dei: any
  frametype: ipv4
   proto: any
   sip: any
   dip: any
   dscp: any
   frag: any
 action parameters:
```

```
  cos: default
  dpl: default
  dscp: default
  tag: default
  policy: default
  ingress-map: default

static qce 2:
=============
 port: 1-27
 key parameters:
  dmac: any
  smac: any
  tag:
   type: any
   vid: any
   pcp: any
   dei: any
  inner tag:
   type: any
   vid: any
   pcp: any
   dei: any
  frametype: ipv6
   proto: any
   sip: any
   dip: any
   dscp: any
 action parameters:
  cos: default
  dpl: default
  dscp: default
  tag: default
  policy: default
  ingress-map: default
FLEX24-10G(config)#
```

When two QCEs are created, QCE 1 followed by QCE 2, QCE 1 will be checked against ingress traffic before QCE 2.

By updating QCE 1, and appending **last** to the command, the QCE order will be changed as follows:

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# qos qce update 1 last
FLEX24-10G(config)# do show qos qce

static qce 2:
=============
 port: 1-27
```

```
  key parameters:
   dmac: any
   smac: any
   tag:
    type: any
    vid: any
    pcp: any
    dei: any
   inner tag:
    type: any
    vid: any
    pcp: any
    dei: any
   frametype: ipv6
    proto: any
    sip: any
    dip: any
    dscp: any
  action parameters:
   cos: default
   dpl: default
   dscp: default
   tag: default
   policy: default
   ingress-map: default

 static qce 1:
 =============
  port: 1-27
  key parameters:
   dmac: any
   smac: any
   tag:
    type: any
    vid: any
    pcp: any
    dei: any
   inner tag:
    type: any
    vid: any
    pcp: any
    dei: any
   frametype: ipv4
    proto: any
    sip: any
    dip: any
    dscp: any
    frag: any
```

```
 action parameters:
  cos: default
  dpl: default
  dscp: default
  tag: default
  policy: default
  ingress-map: default
FLEX24-10G(config)#
```

Now QCE 2 will be checked against ingress traffic before QCE 1.

Storm Policing

Storm Policers are used to configured bandwidth restrictions either globally or on a per interface basis. These policers are applied to a frame type (Unicast, Multicast, and Broadcast frames).

Storm Policers are designed to prevent broadcast storms and only apply to frames whose VLAN ID and Destination MAC address are not present in the switch's MAC Address Table. When a switch receives a frame whose destination MAC address is not in the Mac Address Table, the frame is flooded out all interfaces except the one it was received on.

Configuring a Global Storm Policer

Global Storm Policers are configured from Global Configuration as follows:

	Command	Explanation
Step 1	configure terminal	Enter Global Configuration Mode.
Step 2	qos storm {broadcast <1-13128147> [fps | kbps | kfps | mbps] | multicast <1-13128147> [fps | kbps | kfps | mbps] | unicast <1-13128147> [fps | kbps | kfps | mbps]}	Create a Storm Policer. When a Storm Policer is created, the frame type, and rate limit must be specified. If no unit is specified for the rate, the switch will default to using fps. When the units are set to fps or kbps, the rate must be within the range of 10 to 13128147. When the rate is set to kfps or mbps, the rate must be within the range of 1 to 13128.
Step 3	end	**(Optional)** Return to Privileged EXEC mode.
Step 4	copy running-config startup-config	**(Optional)** Copy the contents of the running-config to the startup-config.

```
FLEX24-10G# configure terminal
-10G(config)# qos storm broadcast 55555 kbps
FLEX24-10G(config)# end
FLEX24-10G# copy running-config startup-config
```

```
Building configuration...
% Saving 2281 bytes to flash:startup-config
FLEX24-10G#
```

Configuring a Storm Policer on an Interface

Storm Policers at the interface level are configured from Interface Configuration mode as follows:

	Command	Explanation
Step 1	configure terminal	Enter Global Configuration Mode.
Step 2	interface {*, GigabitEthernet <1/1-24>, 10GigabitEthernet<1/1-2>}	Enter Interface Configuration Mode for interface(s) in which to enable a Storm Policer on.
Step 3	qos storm {broadcast <1-13128147> [fps | kbps | kfps | mbps] | multicast <1-13128147> [fps | kbps | kfps | mbps] | unicast <1-13128147> [fps | kbps | kfps | mbps]}	Create a Storm Policer on the specified interface. When a Storm Policer is created, the frame type, and rate limit must be specified. If no unit is specified for the rate, the switch will default to using fps. When the units are set to fps or kbps, the rate must be within the range of 10 to 13128147. When the rate is set to kfps or mbps, the rate must be within the range of 1 to 13128.
Step 4	end	**(Optional)** Return to Privileged EXEC mode.
Step 5	copy running-config startup-config	**(Optional)** Copy the contents of the running-config to the startup-config.

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# interface GigabitEthernet 1/1
FLEX24-10G(config-if)# qos storm unicast 10000 mbps
FLEX24-10G(config-if)# end
FLEX24-10G# copy running-config startup-config
Building configuration...
% Saving 2311 bytes to flash:startup-config
FLEX24-10G#
```

Verification

The FLEX24-10G offers the following QoS related show commands:

show qos interface {*, GigabitEthernet <1/1-24>, 10GigabitEthernet<1/1-2>}: Displays the entire QoS configuration for an interface or set of interfaces. Even if no QoS policies have been configured on an interface, the output will display the default settings which would normally be hidden from the running-config.

```
FLEX24-10G# show running-config interface GigabitEthernet 1/1
Building configuration...
interface GigabitEthernet 1/1
!
end
FLEX24-10G#

FLEX24-10G# show qos interface GigabitEthernet 1/1
interface GigabitEthernet 1/1
 qos cos 0
 qos pcp 0
 qos dpl 0
 qos dei 0
 qos class 0
 qos trust tag disabled
 qos map tag-cos pcp 0 dei 0 cos 1 dpl 0
 qos map tag-cos pcp 0 dei 1 cos 1 dpl 1
 qos map tag-cos pcp 1 dei 0 cos 0 dpl 0
 qos map tag-cos pcp 1 dei 1 cos 0 dpl 1
 qos map tag-cos pcp 2 dei 0 cos 2 dpl 0
 qos map tag-cos pcp 2 dei 1 cos 2 dpl 1
 qos map tag-cos pcp 3 dei 0 cos 3 dpl 0
 qos map tag-cos pcp 3 dei 1 cos 3 dpl 1
 qos map tag-cos pcp 4 dei 0 cos 4 dpl 0
 qos map tag-cos pcp 4 dei 1 cos 4 dpl 1
 qos map tag-cos pcp 5 dei 0 cos 5 dpl 0
 qos map tag-cos pcp 5 dei 1 cos 5 dpl 1
 qos map tag-cos pcp 6 dei 0 cos 6 dpl 0
 qos map tag-cos pcp 6 dei 1 cos 6 dpl 1
 qos map tag-cos pcp 7 dei 0 cos 7 dpl 0
 qos map tag-cos pcp 7 dei 1 cos 7 dpl 1
 qos trust dscp disabled
 qos policer mode: disabled, rate: 500 kbps
 qos queue-policer queue 0 mode: disabled, rate: 500 kbps
 qos queue-policer queue 1 mode: disabled, rate: 500 kbps
 qos queue-policer queue 2 mode: disabled, rate: 500 kbps
 qos queue-policer queue 3 mode: disabled, rate: 500 kbps
 qos queue-policer queue 4 mode: disabled, rate: 500 kbps
 qos queue-policer queue 5 mode: disabled, rate: 500 kbps
 qos queue-policer queue 6 mode: disabled, rate: 500 kbps
 qos queue-policer queue 7 mode: disabled, rate: 500 kbps
 qos port shaper: disabled, rate: 500 kbps, mode: line-rate
 qos queue-shaper queue 0: disabled, rate: 500 kbps, mode: line-rate
 qos queue-shaper queue 1: disabled, rate: 500 kbps, mode: line-rate
 qos queue-shaper queue 2: disabled, rate: 500 kbps, mode: line-rate
```

```
 qos queue-shaper queue 3: disabled, rate: 500 kbps, mode: line-rate
 qos queue-shaper queue 4: disabled, rate: 500 kbps, mode: line-rate
 qos queue-shaper queue 5: disabled, rate: 500 kbps, mode: line-rate
 qos queue-shaper queue 6: disabled, rate: 500 kbps, mode: line-rate
 qos queue-shaper queue 7: disabled, rate: 500 kbps, mode: line-rate
 qos wrr mode: disabled
 qos tag-remark classified
 qos map cos-tag cos 0 dpl 0 pcp 1 dei 0
 qos map cos-tag cos 0 dpl 1 pcp 1 dei 1
 qos map cos-tag cos 1 dpl 0 pcp 0 dei 0
 qos map cos-tag cos 1 dpl 1 pcp 0 dei 1
 qos map cos-tag cos 2 dpl 0 pcp 2 dei 0
 qos map cos-tag cos 2 dpl 1 pcp 2 dei 1
 qos map cos-tag cos 3 dpl 0 pcp 3 dei 0
 qos map cos-tag cos 3 dpl 1 pcp 3 dei 1
 qos map cos-tag cos 4 dpl 0 pcp 4 dei 0
 qos map cos-tag cos 4 dpl 1 pcp 4 dei 1
 qos map cos-tag cos 5 dpl 0 pcp 5 dei 0
 qos map cos-tag cos 5 dpl 1 pcp 5 dei 1
 qos map cos-tag cos 6 dpl 0 pcp 6 dei 0
 qos map cos-tag cos 6 dpl 1 pcp 6 dei 1
 qos map cos-tag cos 7 dpl 0 pcp 7 dei 0
 qos map cos-tag cos 7 dpl 1 pcp 7 dei 1
 qos dscp-translate disabled
 qos dscp-classify disabled
 qos dscp-remark disabled
 qos storm unicast mode: disabled, rate: 500 kbps
 qos storm broadcast mode: disabled, rate: 500 kbps
 qos storm unknown mode: disabled, rate: 500 kbps
 qos wred-group 1
 qos ingress-map disabled
 qos egress-map disabled

FLEX24-10G#
```

show qos maps [cos-dscp] [dscp-classify] [dscp-cos] [dscp-egress-translation] [dscp-ingress-translation] [egress] [ingress]: Display all QoS mappings on the FLEX24-10G. Output can be filtered to only include certain mapping types.

```
FLEX24-10G# show qos maps
qos map dscp-cos:
=================
DSCP       Trust     Cos  Dpl
---------  --------  ---  ---
0  (BE)    disabled  0    0
1          disabled  0    0
2          disabled  0    0
3          disabled  0    0
```

```
4          disabled  0    0
5          disabled  0    0
6          disabled  0    0
7          disabled  0    0
8  (CS1)   disabled  0    0
9          disabled  0    0
10 (AF11)  disabled  0    0
11         disabled  0    0
12 (AF12)  disabled  0    0
13         disabled  0    0
14 (AF13)  disabled  0    0
15         disabled  0    0
16 (CS2)   disabled  0    0
17         disabled  0    0
18 (AF21)  disabled  0    0
19         disabled  0    0
20 (AF22)  disabled  0    0
21         disabled  0    0
22 (AF23)  disabled  0    0
23         disabled  0    0
24 (CS3)   disabled  0    0
25         disabled  0    0
26 (AF31)  disabled  0    0
27         disabled  0    0
28 (AF32)  disabled  0    0
29         disabled  0    0
30 (AF33)  disabled  0    0
31         disabled  0    0
32 (CS4)   disabled  0    0
33         disabled  0    0
34 (AF41)  disabled  0    0
35         disabled  0    0
36 (AF42)  disabled  0    0
37         disabled  0    0
38 (AF43)  disabled  0    0
39         disabled  0    0
40 (CS5)   disabled  0    0
41         disabled  0    0
42         disabled  0    0
43         disabled  0    0
44         disabled  0    0
45         disabled  0    0
46 (EF)    disabled  0    0
47         disabled  0    0
48 (CS6)   disabled  0    0
49         disabled  0    0
50         disabled  0    0
51         disabled  0    0
```

```
52         disabled  0    0
53         disabled  0    0
54         disabled  0    0
55         disabled  0    0
56 (CS7)   disabled  0    0
57         disabled  0    0
58         disabled  0    0
59         disabled  0    0
60         disabled  0    0
61         disabled  0    0
62         disabled  0    0
63         disabled  0    0

qos map dscp-ingress-translation:
=================================
DSCP       Translated DSCP
---------  ---------------
0  (BE)    0  (BE)
1          1
2          2
3          3
4          4
5          5
6          6
7          7
8  (CS1)   8  (CS1)
9          9
10 (AF11)  10 (AF11)
11         11
12 (AF12)  12 (AF12)
13         13
14 (AF13)  14 (AF13)
15         15
16 (CS2)   16 (CS2)
17         17
18 (AF21)  18 (AF21)
19         19
20 (AF22)  20 (AF22)
21         21
22 (AF23)  22 (AF23)
23         23
24 (CS3)   24 (CS3)
25         25
26 (AF31)  26 (AF31)
27         27
28 (AF32)  28 (AF32)
29         29
30 (AF33)  30 (AF33)
```

```
31          31
32 (CS4)    32 (CS4)
33          33
34 (AF41)   34 (AF41)
35          35
36 (AF42)   36 (AF42)
37          37
38 (AF43)   38 (AF43)
39          39
40 (CS5)    40 (CS5)
41          41
42          42
43          43
44          44
45          45
46 (EF)     46 (EF)
47          47
48 (CS6)    48 (CS6)
49          49
50          50
51          51
52          52
53          53
54          54
55          55
56 (CS7)    56 (CS7)
57          57
58          58
59          59
60          60
61          61
62          62
63          63

qos map dscp-classify:
======================
DSCP        Classify
---------   --------
0  (BE)     disabled
1           disabled
2           disabled
3           disabled
4           disabled
5           disabled
6           disabled
7           disabled
8  (CS1)    disabled
9           disabled
```

```
10 (AF11)  disabled
11         disabled
12 (AF12)  disabled
13         disabled
14 (AF13)  disabled
15         disabled
16 (CS2)   disabled
17         disabled
18 (AF21)  disabled
19         disabled
20 (AF22)  disabled
21         disabled
22 (AF23)  disabled
23         disabled
24 (CS3)   disabled
25         disabled
26 (AF31)  disabled
27         disabled
28 (AF32)  disabled
29         disabled
30 (AF33)  disabled
31         disabled
32 (CS4)   disabled
33         disabled
34 (AF41)  disabled
35         disabled
36 (AF42)  disabled
37         disabled
38 (AF43)  disabled
39         disabled
40 (CS5)   disabled
41         disabled
42         disabled
43         disabled
44         disabled
45         disabled
46 (EF)    disabled
47         disabled
48 (CS6)   disabled
49         disabled
50         disabled
51         disabled
52         disabled
53         disabled
54         disabled
55         disabled
56 (CS7)   disabled
57         disabled
```

```
58         disabled
59         disabled
60         disabled
61         disabled
62         disabled
63         disabled

qos map cos-dscp:
=================
Cos  DSCP DP0   DSCP DP1   DSCP DP2   DSCP DP3
---  ---------  ---------  ---------  ---------
0    0  (BE)    0  (BE)    0  (BE)    0  (BE)
1    0  (BE)    0  (BE)    0  (BE)    0  (BE)
2    0  (BE)    0  (BE)    0  (BE)    0  (BE)
3    0  (BE)    0  (BE)    0  (BE)    0  (BE)
4    0  (BE)    0  (BE)    0  (BE)    0  (BE)
5    0  (BE)    0  (BE)    0  (BE)    0  (BE)
6    0  (BE)    0  (BE)    0  (BE)    0  (BE)
7    0  (BE)    0  (BE)    0  (BE)    0  (BE)

qos map dscp-egress-translation:
================================
DSCP       Remap
---------  ---------
0  (BE)    0  (BE)
1          1
2          2
3          3
4          4
5          5
6          6
7          7
8  (CS1)   8  (CS1)
9          9
10 (AF11)  10 (AF11)
11         11
12 (AF12)  12 (AF12)
13         13
14 (AF13)  14 (AF13)
15         15
16 (CS2)   16 (CS2)
17         17
18 (AF21)  18 (AF21)
19         19
20 (AF22)  20 (AF22)
21         21
22 (AF23)  22 (AF23)
23         23
```

```
24 (CS3)   24 (CS3)
25         25
26 (AF31)  26 (AF31)
27         27
28 (AF32)  28 (AF32)
29         29
30 (AF33)  30 (AF33)
31         31
32 (CS4)   32 (CS4)
33         33
34 (AF41)  34 (AF41)
35         35
36 (AF42)  36 (AF42)
37         37
38 (AF43)  38 (AF43)
39         39
40 (CS5)   40 (CS5)
41         41
42         42
43         43
44         44
45         45
46 (EF)    46 (EF)
47         47
48 (CS6)   48 (CS6)
49         49
50         50
51         51
52         52
53         53
54         54
55         55
56 (CS7)   56 (CS7)
57         57
58         58
59         59
60         60
61         61
62         62
63         63

ingress map: 1, key: dscp-pcp-dei, action: cos dpl pcp dei dscp
egress map: 1, key: class, action: pcp dei
FLEX24-10G#
```

show qos qce [<1-256>]: Displays all QCE in the order which they are checked against ingress traffic. Output can be filtered to only display a single QCE by specifying the QCE ID.

```
FLEX24-10G# show qos qce

static qce 1:
=============
 port: 1-27
 key parameters:
  dmac: any
  smac: any
  tag:
   type: any
   vid: any
   pcp: any
   dei: any
  inner tag:
   type: any
   vid: any
   pcp: any
   dei: any
  frametype: snap 0x88cc
 action parameters:
  cos: default
  dpl: default
  dscp: default
  tag: default
  policy: default
  ingress-map: default
FLEX24-10G#
```

show qos storm: Displays QoS Storm Policing information.

```
FLEX24-10G# show qos storm
qos storm:
==========
Unicast  : disabled      10 fps
Multicast: disabled      10 fps
Broadcast: disabled      10 fps
Storm detected: FALSE
FLEX24-10G#
```

show qos wred: Displays Weighted Random Early Detection group information.

```
FLEX24-10G# show qos wred
qos wred:
=========
Group  Queue  Dpl  Mode      Min Fl  Max Dp or Fl
-----  -----  ---  --------  ------  ----------------------
    1      0    1  disabled    0 %     50 % Drop Probability
    1      0    2  disabled    0 %     50 % Drop Probability
    1      0    3  disabled    0 %     50 % Drop Probability
```

```
1      1    1  disabled     0 %     50 % Drop Probability
1      1    2  disabled     0 %     50 % Drop Probability
1      1    3  disabled     0 %     50 % Drop Probability
1      2    1  disabled     0 %     50 % Drop Probability
1      2    2  disabled     0 %     50 % Drop Probability
1      2    3  disabled     0 %     50 % Drop Probability
1      3    1  disabled     0 %     50 % Drop Probability
1      3    2  disabled     0 %     50 % Drop Probability
1      3    3  disabled     0 %     50 % Drop Probability
1      4    1  disabled     0 %     50 % Drop Probability
1      4    2  disabled     0 %     50 % Drop Probability
1      4    3  disabled     0 %     50 % Drop Probability
1      5    1  disabled     0 %     50 % Drop Probability
1      5    2  disabled     0 %     50 % Drop Probability
1      5    3  disabled     0 %     50 % Drop Probability
1      6    1  disabled     0 %     50 % Drop Probability
1      6    2  disabled     0 %     50 % Drop Probability
1      6    3  disabled     0 %     50 % Drop Probability
1      7    1  disabled     0 %     50 % Drop Probability
1      7    2  disabled     0 %     50 % Drop Probability
1      7    3  disabled     0 %     50 % Drop Probability
2      0    1  disabled     0 %     50 % Drop Probability
2      0    2  disabled     0 %     50 % Drop Probability
2      0    3  disabled     0 %     50 % Drop Probability
2      1    1  disabled     0 %     50 % Drop Probability
2      1    2  disabled     0 %     50 % Drop Probability
2      1    3  disabled     0 %     50 % Drop Probability
2      2    1  disabled     0 %     50 % Drop Probability
2      2    2  disabled     0 %     50 % Drop Probability
2      2    3  disabled     0 %     50 % Drop Probability
2      3    1  disabled     0 %     50 % Drop Probability
2      3    2  disabled     0 %     50 % Drop Probability
2      3    3  disabled     0 %     50 % Drop Probability
2      4    1  disabled     0 %     50 % Drop Probability
2      4    2  disabled     0 %     50 % Drop Probability
2      4    3  disabled     0 %     50 % Drop Probability
2      5    1  disabled     0 %     50 % Drop Probability
2      5    2  disabled     0 %     50 % Drop Probability
2      5    3  disabled     0 %     50 % Drop Probability
2      6    1  disabled     0 %     50 % Drop Probability
2      6    2  disabled     0 %     50 % Drop Probability
2      6    3  disabled     0 %     50 % Drop Probability
2      7    1  disabled     0 %     50 % Drop Probability
2      7    2  disabled     0 %     50 % Drop Probability
2      7    3  disabled     0 %     50 % Drop Probability
3      0    1  disabled     0 %     50 % Drop Probability
3      0    2  disabled     0 %     50 % Drop Probability
      ------------------------------OUTPUT TRUNCATED------------------------------
```

Chapter 31: sFlow

Introduction

sFlow (sampled flow) provides a means for network monitoring via frame export at Layer 2. A successful sFlow configuration requires the use of a sFlow collector located elsewhere on the network.

The sFlow collector must have network connectivity to the FLEX24-10G.

The sFlow collector is a central server which receives the exported frames for analysis and reporting.

Once sFlow has been configured, the configuration is not saved in non-volatile memory, meaning that after a switch reboot, the sFlow configuration will be lost.

Configuration

Directing the FLEX24-10G to the sFlow Collector

Once an sFlow collector has been configured on the network, the FLEX24-10G must be pointed to the collector. This is performed as follows:

	Command	Explanation
Step 1	configure terminal	Enter Global Configuration mode.
Step 2	sflow collector-address {<domain_name> | <ipv4_address> | <ipv6_ucast>}	Specify the IP address, or hostname of the sFlow collector.
Step 3	sflow collector-port <1-65535>	**(Optional)** Specify the port in which the sFlow collector listens for sFlow datagrams. By default, the sFlow port is set to UDP port 6434.
Step 4	sflow max-datagram-size <200-1468>	**(Optional)** Specify the MTU (in bytes) of sFlow datagrams. The default maximum datagram size is 1400 bytes. The upper bound for this value is set to 1468 bytes because any value larger than 1468 bytes has the possibility of being fragmented.
Step 5	sflow timeout <0-2147483647>	**(Optional)** Configure the sFlow timeout. The sFlow timeout is the number of seconds remaining before the sFlow collector is considered invalid. By default, the timeout is set to 0 seconds.

```
FLEX24-10G# configure terminal
```

```
FLEX24-10G(config)# sflow collector-address 192.168.100.15
FLEX24-10G(config)# sflow collector-port 5500
FLEX24-10G(config)# sflow max-datagram-size 1450
FLEX24-10G(config)# sflow timeout 600
FLEX24-10G(config)# end
FLEX24-10G# copy running-config startup-config
Building configuration...
% Saving 2188 bytes to flash:startup-config
FLEX24-10G#
```

sFlow Agent Configuration

The agent's IP address by default is set to 127.0.0.1 and is embedded within sFlow datagrams. The agent's IP address should be unique as it will identify the agent over extended periods of time.

The agent can be configured with either an IPv4 or IPv6 address as follows:

	Command	Explanation
Step 1	configure terminal	Enter Global Configuration mode.
Step 2	sflow agent-ip {ipv4 <ip_address> | ipv6 <ipv6_address>}	Configure the IP address which will be embedded within sFlow datagrams.
Step 3	end	**(Optional)** Return to Privileged EXEC mode.
Step 4	copy running-config startup-config	**(Optional)** Copy the contents of the running-config to the startup-config.

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# sflow agent-ip ipv4 192.168.100.1
FLEX24-10G(config)# end
FLEX24-10G# copy running-config startup-config
Building configuration...
% Saving 1958 bytes to flash:startup-config
FLEX24-10G#
```

sFlow Interface Configuration

Flow sampling can be configured at the interface level. Flow sampling takes a sample of all packets transmitted/received on the interface. The packets which are members of the sample are then sent to the sFlow collector.

Configuring a sFlow Flow Sampler

An sFlow Flow Sampler will sample on average 1/Nth of the packets on the interface. The value of N is configured by the administrator from Global Configuration mode as follows:

	Command	Explanation
Step 1	configure terminal	Enter Global Configuration mode.
Step 2	interface {*, GigabitEthernet <1/1-24>, 10GigabitEthernet<1/1-2>}	Enter Interface Configuration mode for the interface in which to enable a flow sampler on.

Step 3	sflow sampling-rate [<1-32767>]	Configure the sampling rate. **<1-32767>** specifies the denominator of the 1/N fraction which marks the percentage of packets to be exported to the sFlow collector. **Example:** If the user enters **sflow sampling-rate 5**, 20% (1/5) of the packets transmitted/received on the interface will be sent to the sFlow collector.
Step 4	sflow max-sampling-size [<14-200>]	Specifies the maximum number of bytes to transmit per sample. **Note:** To ensure no frames are dropped, the maximum datagram size should be approximately 100 bytes larger than the maximum header size. If the maximum datagram size is not large enough, samples may be dropped. By default, the max-sampling-size is set to 128 bytes.
Step 5	sflow counter-poll-interval [<1-3600>]	Specify the frequency, in seconds, in which counter poller samplers are sent to the sFlow collector. Counter samplers contain interface counters and are more efficient than SNMP polling when monitoring several interfaces.
Step 6	end	**(Optional)** Exit Interface Configuration mode and return to Privileged EXEC mode.
Step 7	copy running-config startup-config	**(Optional)** Copy the contents of the running-config to the startup-config.

The below CLI snippet will export on average every 50th packet to the sFlow collector and will also export a counter poller sample every 300 seconds (5 minutes).

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# interface GigabitEthernet 1/1
FLEX24-10G(config-if)# sflow sampling-rate 50
FLEX24-10G(config-if)# sflow max-sampling-size 150
FLEX24-10G(config-if)# sflow counter-poll-interval 300
FLEX24-10G(config-if)# end
FLEX24-10G# copy running-config startup-config
Building configuration...
% Saving 1958 bytes to flash:startup-config
FLEX24-10G#
```

Verification

show sflow: Displays general sFlow configuration information.

```
FLEX24-10G# show sflow

Agent Configuration:
====================

Agent Address: 192.168.100.1

Receiver Configuration:
=======================

Owner        : <none>
Receiver     : 0.0.0.0
UDP Port     : 6343
Max. Datagram: 1400 bytes
Time left    : 0 seconds

No enabled collectors (receivers). Skipping displaying per-port info.
FLEX24-10G#
```

show sflow statistics receiver: Displays receiver information such as transmission successes and error counters, number of flow samples, and the number of counter samples.

```
FLEX24-10G# show sflow statistics receiver
Tx Successes     Tx Errors        Flow Samples     Counter Samples
---------------  ---------------  ---------------  ---------------
              0                0                0                0
FLEX24-10G#
```

show sflow statistics samplers [interface {*, GigabitEthernet <1/1-24>, 10GigabitEthernet<1/1-2>}]: Displays interface specific sFlow statistics. Output can be filtered to only include certain interfaces with the optional **interface** keyword.

```
FLEX24-10G# show sflow statistics samplers

Per-Port Statistics:
====================

Interface              Flow Samples     Counter Samples
---------------------- ---------------- ----------------
GigabitEthernet 1/1                   0                0
GigabitEthernet 1/2                   0                0
GigabitEthernet 1/3                   0                0
GigabitEthernet 1/4                   0                0
GigabitEthernet 1/5                   0                0
```

```
GigabitEthernet 1/6                    0                 0
GigabitEthernet 1/7                    0                 0
GigabitEthernet 1/8                    0                 0
GigabitEthernet 1/9                    0                 0
GigabitEthernet 1/10                   0                 0
GigabitEthernet 1/11                   0                 0
GigabitEthernet 1/12                   0                 0
GigabitEthernet 1/13                   0                 0
GigabitEthernet 1/14                   0                 0
GigabitEthernet 1/15                   0                 0
GigabitEthernet 1/16                   0                 0
GigabitEthernet 1/17                   0                 0
GigabitEthernet 1/18                   0                 0
GigabitEthernet 1/19                   0                 0
GigabitEthernet 1/20                   0                 0
GigabitEthernet 1/21                   0                 0
GigabitEthernet 1/22                   0                 0
GigabitEthernet 1/23                   0                 0
GigabitEthernet 1/24                   0                 0
GigabitEthernet 1/25                   0                 0
10GigabitEthernet 1/1                  0                 0
10GigabitEthernet 1/2                  0                 0
FLEX24-10G#
```

Chapter 32: IP Routing

Introduction

Traditional switches operate at Layer 2 (Data Link) of the OSI model. Traffic belonging to one VLAN would be unable to travel to another VLAN without the use of a layer 3 device, typically a router.

Layer 3 switches have become quite popular and allow switches to route traffic between VLANs as well as within VLANs. This is known as inter-VLAN routing. With a layer 3 switch, a router is not a requirement to achieve a completely functional network where hosts in different VLANs can communicate with each other.

Configuration

For the FLEX24-10G to be able to perform inter-VLAN routing, IP routing must be enabled. Enabling IP routing on the FLEX24-10G is quite straightforward. Only a single command needs to be executed from Global Configuration mode.

Enabling IP Routing

IP Routing is enabled from Global Configuration mode as follows:

	Command	**Explanation**
Step 1	configure terminal	Enter Global Configuration mode.
Step 2	ip routing	Enable IP Routing.
Step 3	end	**(Optional)** Return to Privileged EXEC mode.
Step 4	copy running-config startup-config	**(Optional)** Copy the contents of the running-config to the startup-config.

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# ip routing
FLEX24-10G(config)# end
FLEX24-10G# copy running-config startup-config
Building configuration...
% Saving 2241 bytes to flash:startup-config
FLEX24-10G#
```

With IP Routing enabled, the FLEX24-10G is now a Layer 3 switch capable of routing traffic from one VLAN to another.

Adding an IPv4 Route

Static IPv4 routes to external networks can be configured from Global Configuration mode as follows:

	Command	**Explanation**
Step 1	configure terminal	Enter Global Configuration mode.

Step 2	ip route <ipv4_address> <subnet_mask> <gateway>	Create an IPv4 static route. **<ipv4_address>** represents the network address and **<subnet_mask>** represents the subnet mask of the network. **<gateway>** represents the next-hop address to get to the network. This command will throw an error if an invalid network address and subnet mask is entered, or if the gateway is local to the switch.
Step 3	end	**(Optional)** Return to Privileged EXEC mode.
Step 4	copy running-config startup-config	**(Optional)** Copy the contents of the running-config to the startup-config.

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# ip route 10.10.10.0 255.255.255.0 192.168.100.75
FLEX24-10G(config)# ip route 10.0.0.0 255.255.0.0 192.168.100.1
% Failed to add IPv4 route: Invalid next hop address (it's this router).
FLEX24-10G(config)# end
FLEX24-10G# copy running-config startup-config
Building configuration...
% Saving 2490 bytes to flash:startup-config
FLEX24-10G#
```

Notice the error thrown on line four of the above CLI snippet. This error is produced because the IP address of the gateway is located on the local router.

Adding an IPv6 Route

IPv6 routes are configured in much the same way as IPv4 routes.

	Command	**Explanation**
Step 1	configure terminal	Enter Global Configuration mode.
Step 2	ipv6 route <ipv6_subnet> {<ipv6_unicast_adddress> | interface vlan <vlan_id> <ipv6_linklocal>}	Create an IPv6 static route. **<ipv6_subnet>** represents the IPv6 network in which the route is pointing to. There are two options for specifying the next hop address: 1. Specifying an IPv6 unicast address. 2. Specifying the VLAN interface and IPv6 link local address.
Step 3	end	**(Optional)** Return to Privileged EXEC mode.

Step 4	copy running-config startup-config	**(Optional)** Copy the contents of the running-config to the startup-config.

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# ipv6 route 2001:DB8::/32  interface vlan 1 fe80::1
FLEX24-10G(config)# end
FLEX24-10G# copy running-config startup-config
Building configuration...
% Saving 2650 bytes to flash:startup-config
FLEX24-10G#
```

Verification

show ip route: Displays the IPv4 routing table.

```
FLEX24-10G# show ip route
10.10.10.0/24 via 192.168.100.75 <UP GATEWAY>
192.168.50.0/24 via 192.168.100.10 <UP GATEWAY>
192.168.100.0/24 via VLAN1 <UP>
FLEX24-10G#
```

show ipv6 route: Displays the IPv6 routing table.

```
FLEX24-10G# show ipv6 route
2001::/64 via VLAN1 <UP>
2001::/128 via VLAN1 <UP>
2001::3/128 via VLAN1 <UP>
2001:db8::/32 via fe80::1 <UP GATEWAY>
fe80::/64 via VLAN1 <UP>
fe80::/128 via VLAN1 <UP>
fe80::224:63ff:fe04:2a80/128 via VLAN1 <UP>
FLEX24-10G#
```

Chapter 33: MVRP/GVRP

Introduction

MVRP and GVRP are protocols used to distribute VLANs from one switch to another. The Multiple Registration Protocol (MVRP) is the successor to the GARP VLAN Registration Protocol (GVRP).

From a basic level, MVRP allows network devices such as switches and bridges to exchange information with each other. Information commonly exchanged via MVRP is VLAN identities and multicast group memberships.

GVRP Configuration

Like many other features on the FLEX24-10G, GVRP must be enabled globally and on the specific interface which the administrator would like to participate in GVRP functions.

Enabling GVRP Globally

GVRP is enabled globally from Global Configuration mode as follows:

	Command	**Explanation**
Step 1	configure terminal	Enter Global Configuration mode.
Step 2	gvrp	Enable GVRP globally.
Step 3	gvrp time {join-time <1-20> | leave-time <60-300> | leave-all-time <1000-5000>}	**(Optional)** Configure the various GVRP timers. **Join Time:** The join time is the maximum amount of time the switch will wait before sending VLAN advertisements out GVRP enable interfaces. **<1-20>** specifies the join time in hundreds of a second. By default, the join time is 200 milliseconds. **Leave Time:** The leave time is the amount of time a GVRP enabled interface will wait before removing itself from the VLAN indicated in the leave message. **<60-300>** specifies the leave time in centiseconds. By default, the leave time is set to 600ms (60 centiseconds). The leave time must be at least 3 times the join time.

		<u>Leave All Time:</u> The leave all time is the minimum frequency in which the switch sends leave all messages from all GVRP enabled interfaces. **<1000-5000>** specifies the leave all time in milliseconds. By default, the leave all time is set to 1000ms (1 second). When a switchport receives a leave all packet, the switchport is instructed to change the state of all its VLANs to "Leaving". The VLANs are left unless a Join message is received before the Leave All timer expires.
Step 4	gvrp max-vlans <1-4094>	**(Optional)** Specify the maximum number of VLANs in which GVRP will support. By default, this value is set to 20, however, GVRP can support up to 4094 VLANs. The setting cannot be changed while GVRP is running.
Step 5	end	**(Optional)** Return to Privileged EXEC mode.
Step 6	copy running-config startup-config	**(Optional)** Copy the contents of the running-config to the startup-config.

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# gvrp
FLEX24-10G(config)# gvrp time join-time 2 leave-time 100 leave-all-time 3000
FLEX24-10G(config)# gvrp max-vlans 100
%% Failed to configure the number of VLANs managed by GVRP.
% (The GARP application is currently enabled - disable it in order to configure its
parameters.)
FLEX24-10G(config)# no gvrp
FLEX24-10G(config)# gvrp max-vlans 100
FLEX24-10G(config)# gvrp
FLEX24-10G(config)# end
FLEX24-10G# copy running-config startup-config
Building configuration...
% Saving 2018 bytes to flash:startup-config
FLEX24-10G#
```

Enabling GVRP at the Interface Level

GVRP is enabled on an interface from Interface Configuration mode as follows:

	<u>Command</u>	**<u>Explanation</u>**
Step 1	configure terminal	Enter Global Configuration mode.

Step 2	interface {*, GigabitEthernet <1/1-24>, 10GigabitEthernet<1/1-2>}	Enter Interface Configuration mode for the interface in which to enable GVRP on.
Step 3	gvrp	Enable GVRP.
Step 4	end	**(Optional)** Return to Privileged EXEC mode.
Step 5	copy running-config startup-config	**(Optional)** Copy the contents of the running-config to the startup-config.

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# interface GigabitEthernet 1/1
FLEX24-10G(config-if)# gvrp
FLEX24-10G(config-if)# end
FLEX24-10G# copy running-config startup-config
Building configuration...
% Saving 2038 bytes to flash:startup-config
FLEX24-10G#
```

MVRP Configuration

A complete MVRP configuration also consists of MVRP being enabled globally and at the interface level.

Enabling MVRP Globally

MVRP is enabled globally from Global Configuration mode as follows:

	Command	Explanation
Step 1	configure terminal	Enter Global Configuration mode.
Step 2	mvrp	Enable MVRP globally.
Step 4	mvrp managed vlan {<vlan_list> | add <vlan_list> | all | except <vlan_list> | none | remove <vlan_list>}	**(Optional)** Specify the VLANs in which to manage via MVRP. By default, VLANs 1-4094 are managed.
Step 5	end	**(Optional)** Return to Privileged EXEC mode.
Step 6	copy running-config startup-config	**(Optional)** Copy the contents of the running-config to the startup-config.

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# mvrp
FLEX24-10G(config)# mvrp managed vlan 10,20,30
FLEX24-10G(config)# end
FLEX24-10G# copy running-config startup-config
Building configuration...
% Saving 2070 bytes to flash:startup-config
FLEX24-10G#
```

Enabling MVRP at the Interface Level

As with GVRP, MVRP must also be enabled at the Interface level. Where as with GVRP, the Join, Leave, and Leave All timers were configured from Global Configuration, the same three timers for MVRP are configured from Interface Configuration.

	Command	**Explanation**
Step 1	configure terminal	Enter Global Configuration mode.
Step 2	interface {*, GigabitEthernet <1/1-24>, 10GigabitEthernet<1/1-2>}	Enter Interface Configuration mode for the interface in which to enable MVRP on.
Step 3	mvrp	Enable MVRP.
Step 4	mrp timers {join-time <1-20> | leave-time <60-300> | leave-all-time <1000-5000> | default}	**(Optional)** Configure the various MVRP timers. **Join Time:** The join time is the maximum amount of time the switch will wait before sending VLAN advertisements out MVRP enable interfaces. **<1-20>** specifies the join time in hundreds of a second. By default, the join time is 200 milliseconds. **Leave Time:** The leave time is the amount of time a MVRP enabled interface will wait before removing itself from the VLAN indicated in the leave message. **<60-300>** specifies the leave time in centiseconds. By default, the leave time is set to 600ms (60 centiseconds). The leave time must be at least 3 times the join time. **Leave All Time:** The leave all time is the minimum frequency in which the switch sends leave all messages from all MVRP enabled interfaces. **<1000-5000>** specifies the leave all time in milliseconds. By default, the leave all time is set to 1000ms. When a switchport receives a leave all packet, the switchport is instructed to change the state of all its VLANs to "Leaving". The VLANs are left unless a Join message is received before the Leave All timer expires. **Default:** The **default** keyword resets all MRP timers to their default values.
Step 5	mrp periodic	**(Optional)** Enable periodic transmission. When periodic transmission is enabled, each MRP member starts its own timer on startup. When the

		timer expires all stored MRP messages are sent in the least possible amount of MRP frames. Periodic transmission reduces the number of MRP frames sent. By default, periodic transmission is not enabled. When disabled, MRP members send messages when the Leave All timer expires or when the member receives a Leave All from another host.
Step 6	end	**(Optional)** Return to Privileged EXEC mode.
Step 7	copy running-config startup-config	**(Optional)** Copy the contents of the running-config to the startup-config.

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# interface GigabitEthernet 1/1
FLEX24-10G(config-if)# mvrp
FLEX24-10G(config-if)# mrp timers join-time 20 leave-time 100 leave-all-time 2500
FLEX24-10G(config-if)# mrp periodic
FLEX24-10G(config-if)# end
FLEX24-10G# copy running-config startup-config
Building configuration...
% Saving 2150 bytes to flash:startup-config
FLEX24-10G#
```

Verification

show mrp status [[all] interface {*, GigabitEthernet <1/1-24>, 10GigabitEthernet<1/1-2>}]: Displays the MRP statistics for all interfaces. The optional **all**, and **interface** keywords modify the output to include output for all MRP applications or only include output for specific interfaces.

```
FLEX24-10G# show mrp status
GigabitEthernet 1/1 :
---------------------
MRP Appl  FailedRegistrations  LastPduOrigin
--------  -------------------  -------------
MVRP      0                    00-00-00-00-00-00

GigabitEthernet 1/2 :
---------------------
MRP Appl  FailedRegistrations  LastPduOrigin
--------  -------------------  -------------
MVRP      0                    00-00-00-00-00-00

GigabitEthernet 1/3 :
---------------------
MRP Appl  FailedRegistrations  LastPduOrigin
--------  -------------------  -------------
```

```
MVRP      0                    00-00-00-00-00-00

GigabitEthernet 1/4 :
---------------------
MRP Appl  FailedRegistrations  LastPduOrigin
--------  -------------------  -------------
MVRP      0                    00-00-00-00-00-00
         ------------------------------OUTPUT TRUNCATED------------------------------
```

show mrp status [[mvrp] interface {*, GigabitEthernet <1/1-24>, 10GigabitEthernet<1/1-2>}]: Displays the MRP statistics for all interfaces. The optional **mvrp** keyword restricts the output to include MRP statistics for only MVRP applications. As expected, output can also be restricted to include only specific interfaces.

```
FLEX24-10G# show mrp status mvrp
GigabitEthernet 1/1 :
---------------------
MRP Appl  FailedRegistrations  LastPduOrigin
--------  -------------------  -------------
MVRP      0                    00-00-00-00-00-00

GigabitEthernet 1/2 :
---------------------
MRP Appl  FailedRegistrations  LastPduOrigin
--------  -------------------  -------------
MVRP      0                    00-00-00-00-00-00

GigabitEthernet 1/3 :
---------------------
MRP Appl  FailedRegistrations  LastPduOrigin
--------  -------------------  -------------
MVRP      0                    00-00-00-00-00-00

GigabitEthernet 1/4 :
---------------------
MRP Appl  FailedRegistrations  LastPduOrigin
--------  -------------------  -------------
MVRP      0                    00-00-00-00-00-00
         ------------------------------OUTPUT TRUNCATED------------------------------
```

There are no show commands relating to GVRP.

Chapter 34: Remote Monitoring (RMON)

Introduction

Maintaining a healthy network is a requirement is any network regardless of the size. In enterprise environments with many network devices the ability to monitor the health of each device will ensure a proactive approach to network administration.

It is much more desirable to replace a dying network device before it fails rather than reacting to a failed device and a potential network outage.

Remote Monitoring allows the specific aspects of the switch to be monitored. Alerts can then be raised when a certain threshold is reached. When an alarm is raised an event can be triggered in the form of an SNMP trap, SYSLOG log, or both.

RMON Alarm Configuration

Alarms are configured from Global Configuration mode. There are twelve different variables which can be monitored. These variables are the following:

Variable	Description
ifInDiscards	The number of inbound packets that are discarded even when the packets are normal.
ifInErrors	The number of inbound packets that contained errors preventing them from being delivered to a higher-layer protocol.
ifInNUcastPkts	The number of broadcast and multicast packets delivered to a higher-layer protocol.
ifInOctets	The total number of octets received on the interface, including framing characters.
ifInUcastPkts	The number of unicast packets delivered to a higher-layer protocol.
ifInUnknownProtos	The number of inbound packets that were discarded because of an unknown or unsupported protocol.
ifOutDiscards	The number of outbound packets that are discarded even when the packets are normal.
ifOutErrors	The number of outbound packets that could not be transmitted because of errors.
ifOutNUcastPkts	The number of broadcast and multicast packets that request to transmit.
ifOutOctets	The number of octets transmitted out of the interface, including framing characters.
ifOutQLen	The length of the output packet queue (in packets).

ifOutUcastPkts	The number of unicast packets that request to transmit.

Alarms are configured from Global Configuration mode as follows:

	Command	Explanation
Step 1	configure terminal	Enter Global Configuration mode.
Step 2	rmon alarm <1-65535> {ifInDiscards | ifInErrors | ifInNUcastPkts | ifInOctets | ifInUcastPkts | ifInUnknownProtos | ifOutDiscards | ifOutErrors | ifOutNUcastPkts | ifOutOctets | ifOutQLen | ifOutUcastPkts} <interface_index> <1-2147483647> {absolute | delta} rising-threshold <-2147483648-2147483647> <0-65535> falling-threshold <-2147483648-2147483647> <0-65535> [both | falling | rising]	Configure the RMON alarm. **<1-65535>** represents the entry ID. **<interface_index>** represents the value of the statistic during the last sampling period. **<1-2147483647>** represents the interval in seconds for sampling and comparing the rising and falling threshold. **{absolute | delta}** represents the sampling method of the selected variable and calculating the value to be compared against the thresholds. **absolute** obtains the sample directly. **delta** calculates the difference between samples. Delta is the default setting. **rising-threshold <-2147483648-2147483647> <0-65535>** configures the rising threshold and rising index. • **<-2147483648-2147483647>** represents the value in which, when exceeded, the alarm condition is met. • When the alarm condition is met, event **<0-65535>** will be triggered. **falling-threshold <-2147483648-2147483647> <0-65535>** configures the falling threshold and falling index. • **<-2147483648-2147483647>** represents the value in which, when less than, the alarm condition is met.

		• When the alarm condition is met, event **<0-65535>** will be triggered. When the value of the monitored variable is less than the falling-threshold or higher than the rising-threshold, the alarm condition is met.
Step 3	end	**(Optional)** Return to Privileged EXEC mode.
Step 4	copy running-config startup-config	**(Optional)** Copy the contents of the running-config to the startup-config.

RMON Event Configuration

Event entries are also configured from Global Configuration mode.

	Command	Explanation
Step 1	configure terminal	Enter Global Configuration mode.
Step 2	rmon event <1-65535> [description <event_description> | log [description <event_description> | trap <snmp_community_string> [description <event_description>]]| trap [<snmp_community_string> | description <event_description> | log]]	Create an RMON event entry. **<1-65535>** is the event index. **description <event_description>** helps identify the event. **<event_description>** is a string from 0 to 127 characters, inclusive. The **log** and **trap** keywords indicate whether an SNMP log entry and/or SNMP trap should be created when the event is triggered.
Step 4	end	**(Optional)** Return to Privileged EXEC mode.
Step 5	copy running-config startup-config	**(Optional)** Copy the contents of the running-config to the startup-config.

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# rmon event 1 log trap description This is a test event
FLEX24-10G(config)# end
FLEX24-10G# copy running-config startup-config
Building configuration...
% Saving 2230 bytes to flash:startup-config
FLEX24-10G#
```

Interface Specific RMON Commands

Both statistics and alarm entries are created from Interface Configuration mode as follows:

Creating a Statistics Entry

	Command	Explanation
Step 1	configure terminal	Enter Global Configuration mode.
Step 2	interface {*, GigabitEthernet <1/1-24>, 10GigabitEthernet<1/1-2>}	Enter Interface Configuration mode for the interface in which to configure a statistics entry on.
Step 3	rmon collection stats <1-65535>	Configure the RMON statistics entry. **<1-65535>** represents the entry ID.
Step 4	end	**(Optional)** Return to Privileged EXEC mode.
Step 5	copy running-config startup-config	**(Optional)** Copy the contents of the running-config to the startup-config.

```
FLEX24-10G# configure terminal
FLEX24-10G(config)# interface GigabitEthernet 1/1
FLEX24-10G(config-if)# rmon collection stats 1
FLEX24-10G(config-if)# end
FLEX24-10G# copy running-config startup-config
Building configuration...
% Saving 2230 bytes to flash:startup-config
FLEX24-10G#
```

Creating an History Entry

	Command	Explanation
Step 1	configure terminal	Enter Global Configuration mode.
Step 2	interface {*, GigabitEthernet <1/1-24>, 10GigabitEthernet<1/1-2>}	Enter Interface Configuration mode for the interface in which to configure a history entry on.
Step 3	rmon collection history <1-65535> [buckets <1-65535> | interval <1-3600>]	Configure the RMON history entry. **<1-65535>** represents the entry ID. **buckets <1-65535>** represents the requested buckets of intervals. By default, 50 buckets is used. **interval <1-1800>** specifies the length of time in seconds to sam
Step 4	end	**(Optional)** Return to Privileged EXEC mode.
Step 5	copy running-config startup-config	**(Optional)** Copy the contents of the running-config to the startup-config.

Verification

show rmon alarm [<1-65535>]: Displays all RMON alarms. Output can also be filtered to only display entry <1-65535>.

show rmon event [<1-65535>]: Displays all RMON events. Output can also be filtered to only display entry <1-65535>.

```
FLEX24-10G# show rmon event

Event ID :     1
----------------
      Description     : This is a test event
      Type            : logandtrap
      LastSent        : 0d 00:00:00
FLEX24-10G#
```

show rmon history [<1-65535>]: Displays all RMON history entries. Output can also be filtered to only display entry <1-65535>.

```
FLEX24-10G# show rmon history

History ID :     1
------------------
    Data Source         : .1.3.6.1.2.1.2.2.1.1.1000001
    Data Bucket Request : 65000
    Data Bucket Granted : 50
    Data Interval       : 1800
FLEX24-10G#
```

show rmon statistics [<1-65535>]: Displays all RMON statistics entries. Output can also be filtered to only display entry <1-65535>.

```
FLEX24-10G# show rmon statistics

Statistics ID :     1
---------------------
    Data Source : .1.3.6.1.2.1.2.2.1.1.1000001
    etherStatsDropEvents          : 0
    etherStatsOctets              : 0
    etherStatsPkts                : 0
    etherStatsBroadcastPkts       : 0
    etherStatsMulticastPkts       : 0
    etherStatsCRCAlignErrors      : 0
    etherStatsUndersizePkts       : 0
    etherStatsOversizePkts        : 0
    etherStatsFragments           : 0
    etherStatsJabbers             : 0
    etherStatsCollisions          : 0
    etherStatsPkts64Octets        : 0
```

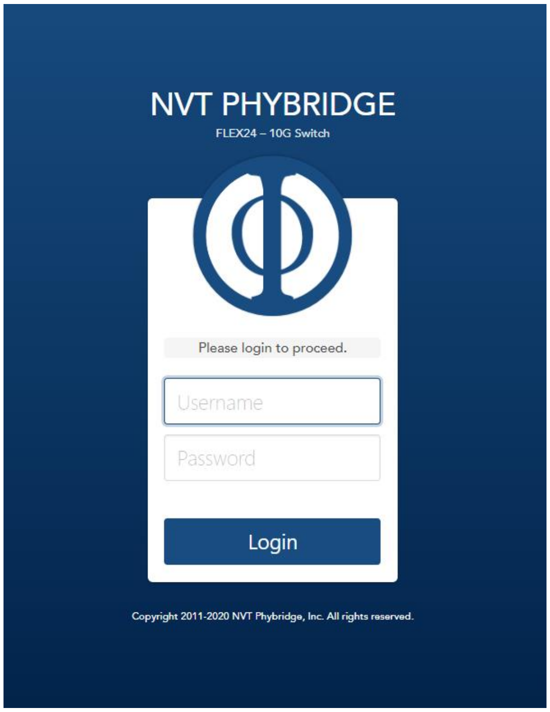
```
    etherStatsPkts65to127Octets   : 0
    etherStatsPkts128to255Octets  : 0
    etherStatsPkts256to511Octets  : 0
    etherStatsPkts512to1023Octets : 0
    etherStatsPkts1024to1518Octets: 0
FLEX24-10G#
```

Chapter 35: WEB Graphical User Interface (GUI)

Introduction

The landing page of the Web GUI is as below.

The default username and password are both admin.



The four tabs of the Web GUI are **SYSTEM**, **ETHERNET**, **VLAN**, and **ADMIN**.

SYSTEM – Contains current real-time system information.

ETHERNET – Contains the uplink and downlink interfaces. Interfaces can be modified as well as PoE settings. SVI configuration is also done here.

VLAN – Contains the current VLAN configuration. VLANs can be created/modified/deleted here. Additionally, an interface's mode can be toggled from this tab. Private VLANs and Port Isolation settings are also found here.

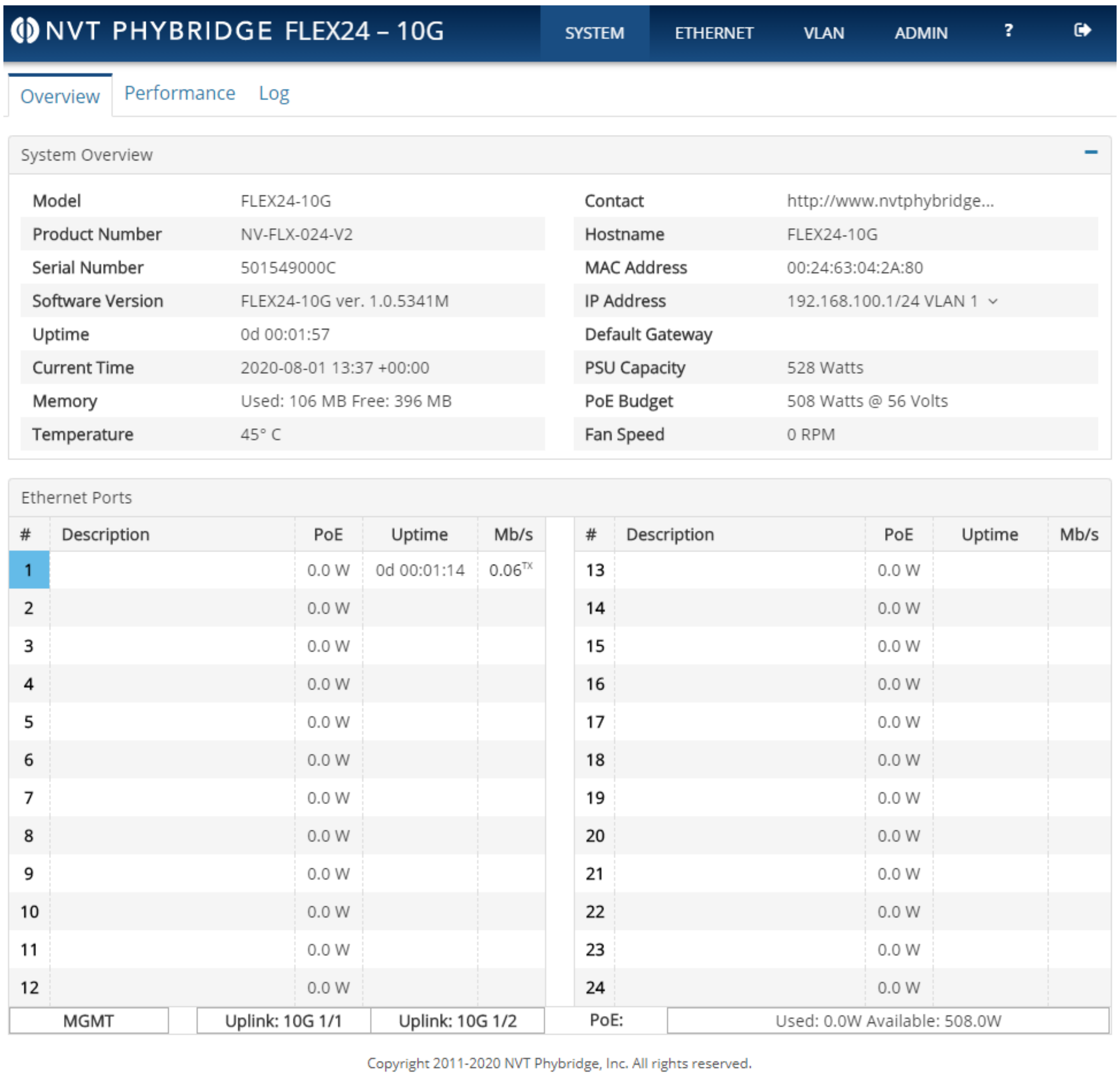
ADMIN – Contains the configuration of system wide settings as well as running-config/startup-config modifications. The switch's firmware can also be upgraded here. The configuration of each service can be configured from the Services subtab.

System

The System tab contains the following subtabs:

- Overview
- Performance
- Log

Overview



<u>System Overview</u>: Provides an overview of the switch's statistics. The System Overview panel can be minimized/maximized by clicking on the -/+ on the top right corner.

Parameter	**Description**
Model	Switch model name
Product Number	Switch product number
Serial Number	Switch serial number

Software Version	Current software version
Uptime	System uptime. This timer updates in real time and is the amount of time the switch has been running.
Current time	System time of the switch. This can either be set by the administrator or by an authoritative time server.
Memory	Displays the currently used and free system memory. Updates in real-time.
Temperature	Displays the system temperature in degrees Celsius. Updates in real-time.
Contact	Displays NVT Phybridge customer support contact information. This field can be edited from the Admin tab.
Hostname	Displays the switch's hostname. The hostname can be edited from the Admin tab.
MAC Address	Displays the CPU's MAC address.
IP Address	Displays all SVI's and their associated IP addresses.
Default Gateway	Displays the switch's default gateway. All network traffic whose destination is not in the routing table will be forwarded to this address.
PSU Capacity	Displays the maximum capacity of the power supply.
PoE Budget	Displays the available power remaining at the current voltage.
Fan Speed	Displays the fan speed of the chassis fans.

Ethernet Ports: Provides real time switchport information.

Interface-ID: Identifier to identify the switchport. Hovering over the interface-id will display the interface's speed, linkdowns, downstream MAC addresses, and bandwidth information. Single click to toggle interface power, double click to reset interface. When resetting an interface, a confirmation window will appear.

Description: Interface description set by an administrator. The description can be set from the Ethernet > Downlink ports panel.

PoE: Current PoE consumption in Watts. The PoE consumption is represented as a horizontal bar graph where the entire width of the field represents 100%. This value updates in real-time.

Uptime: Switchport uptime/downtime. When the link goes down the timer will be displayed in red and begin incrementing. Time format is the following: dd hh:mm:ss.

Mb/s: Current interface bandwidth. The field either displays the Tx or Rx value, whichever is larger.

This field also behaves as a horizonal bar graph similarly to the PoE field.

The Management and Uplink interfaces are displayed as buttons at the bottom on the Ethernet Ports panel.

Interface status can be easily identified by the colour and shading of the interface-id field. Details below:

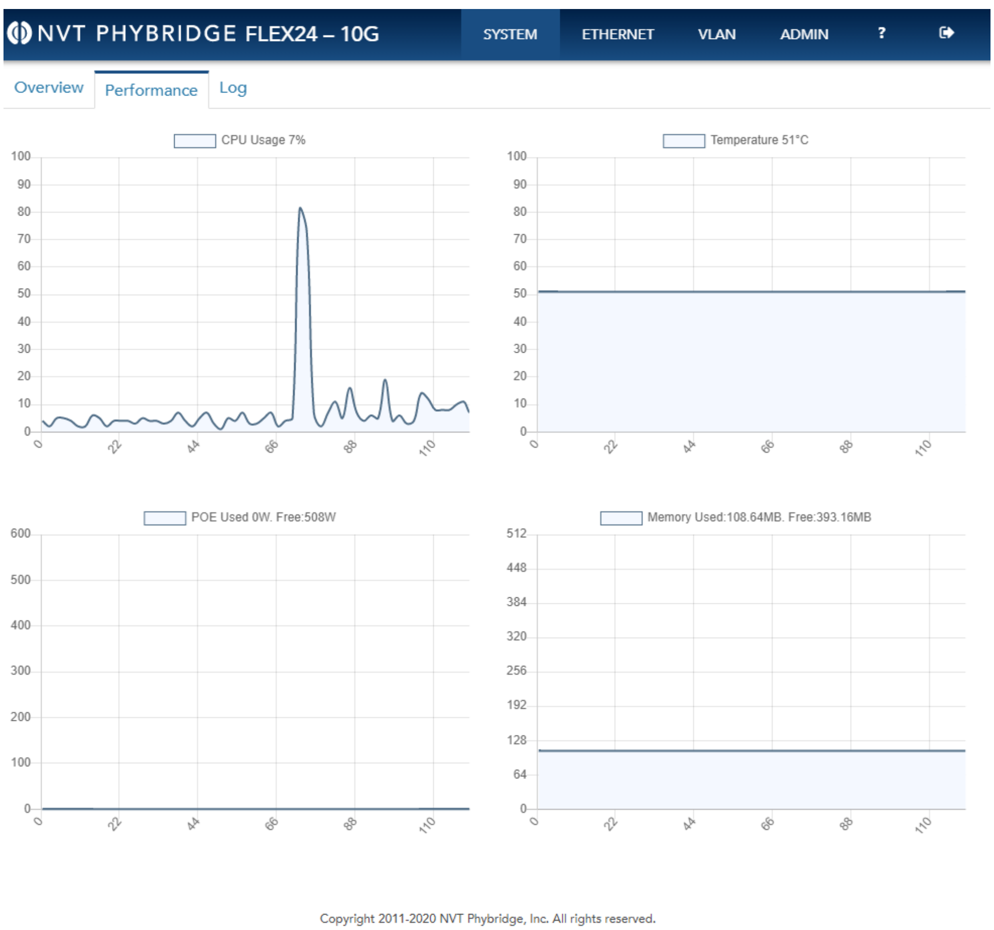
Colour	Port Status
19	Port is available with power; nothing is attached to the port.
6	Port communication is disabled, PoE power is still supplied if enabled in PoE.
20	Adapter is attached to the port; an IP device is connected to the adapter. You can lock the port to the currently connected IP device, on the Ethernet > Downlink Ports page. When locked, appears beside the MAC Address.
Number changes from black to red	The port number gradually changes from black to red if there are link down events. Black = 0 Link Down Events. Red = 250 Link Down Events

Performance

The performance subtab contains four line graphs providing historical information from the previous 120 seconds.

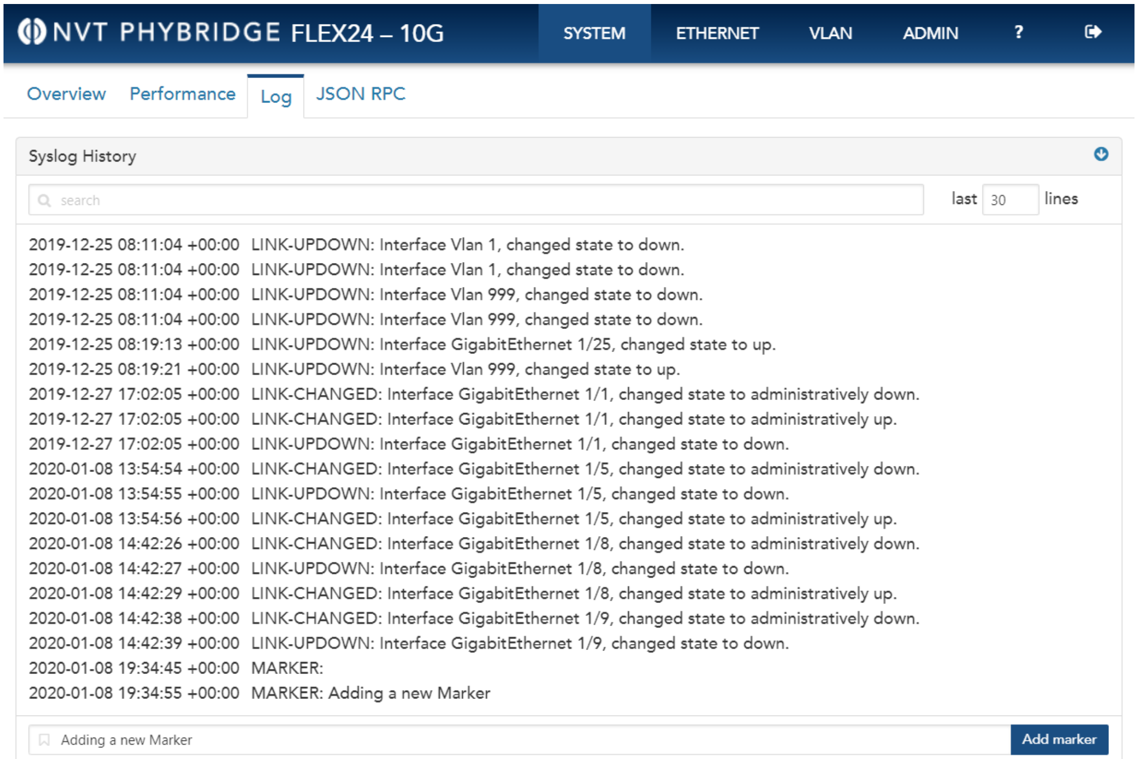
The following are displayed in their own graph: CPU Usage (%), System Temperature (°C), PoE Usage (W), System Memory Usage (MB).

Peaks and valleys are normal and expected on the CPU Usage and PoE graphs.



Log

The log subtab tracks system events.



Searching Log Entries

The log can be searched by typing keywords into the search bar. As keywords are entered the log output screen will automatically update to display entries containing those specific keywords.

Selecting the Number of Events to Display

The last **<*x*>** lines field is used to display the ***x*** most recent log messages, where ***x*** is the value entered into the field.

When the mouse if hovered over the field an up and down arrow will appear. These up and down arrows increase/decrease the last lines value in increments of 10.

Adding Markers to the Log

Markers can be added to the bottom of the log for troubleshooting purposes. Any number of markers can be added at a time and each marker can have its own unique description.

To add a marker, click the Add marker button. If no text is entered into the text box, the marker will not contain a description.

Downloading the Log File

The syslog can be downloaded by clicking the button at the top right corner of the syslog history panel.

The filename for the exported file uses the convention *log<date>.txt*

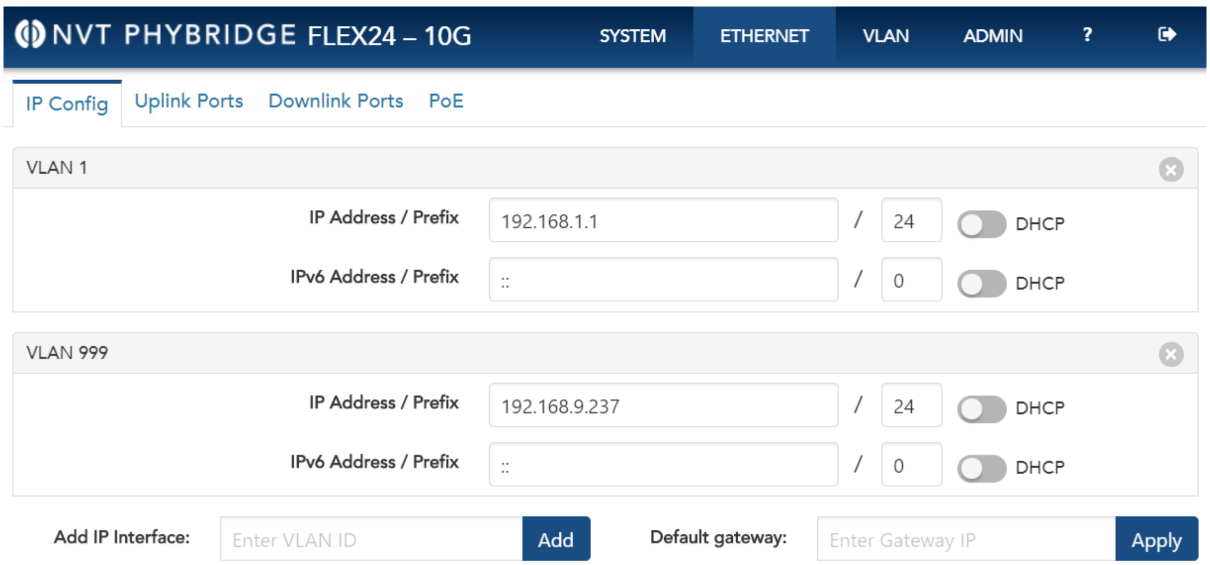
Example: A log file created on June 30th, 2020 would have the file name log20200630.txt.

Ethernet

The Ethernet tab contains the following subtabs:

- IP Config
- Uplink Ports
- Downlink Ports
- PoE

IP Config



The IP Config subtab allows for the management of switched virtual interfaces (SVI's) and the assignment of IP addresses. An SVI can either be statically assigned an IP address from an administrator or obtain an address from a DHCP server.

Adding an IP Interface

To add an IP interface, enter the VLAN number in the **Add IP Interface** field and click Add

Once an IP interface has been created, the interface will have its own panel on the IP Config subtab. The interface's IPv4/IPv6 address and prefix can then be configured.

If the DHCP toggle is enabled, the interface will attempt to receive an address from a DHCP server.

Note: Adding an IP interface for a VLAN which does not exist will not create the VLAN. The VLAN will still need to be created from the VLAN tab. The IP interface will still be created successfully even when its associated VLAN does not exist.

Once edits are made to a VLAN interface an Apply button will appear on the same line. Click Apply for the changes to take effect.

Deleting an VLAN’s IP Interface

VLAN interfaces are deleted by clicking the button in the associated VLAN panel.

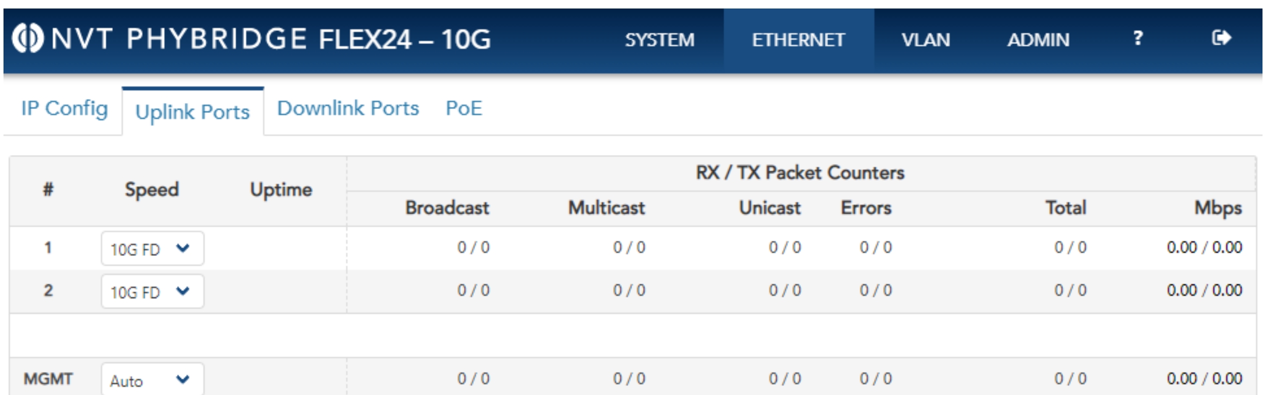
Note: Deleting a VLAN’s IP interface will not delete the associated VLAN.

Setting the Default Gateway

The default gateway can be set by entering an IPv4/IPv6 address into the **Default Gateway** field and clicking Apply

All network traffic whose destination network belongs to a different network segment will be sent to the default gateway.

Uplink Ports



The Uplink Ports subtab allows for the monitoring of the 10G fiber SFP+ interfaces and the management interface.

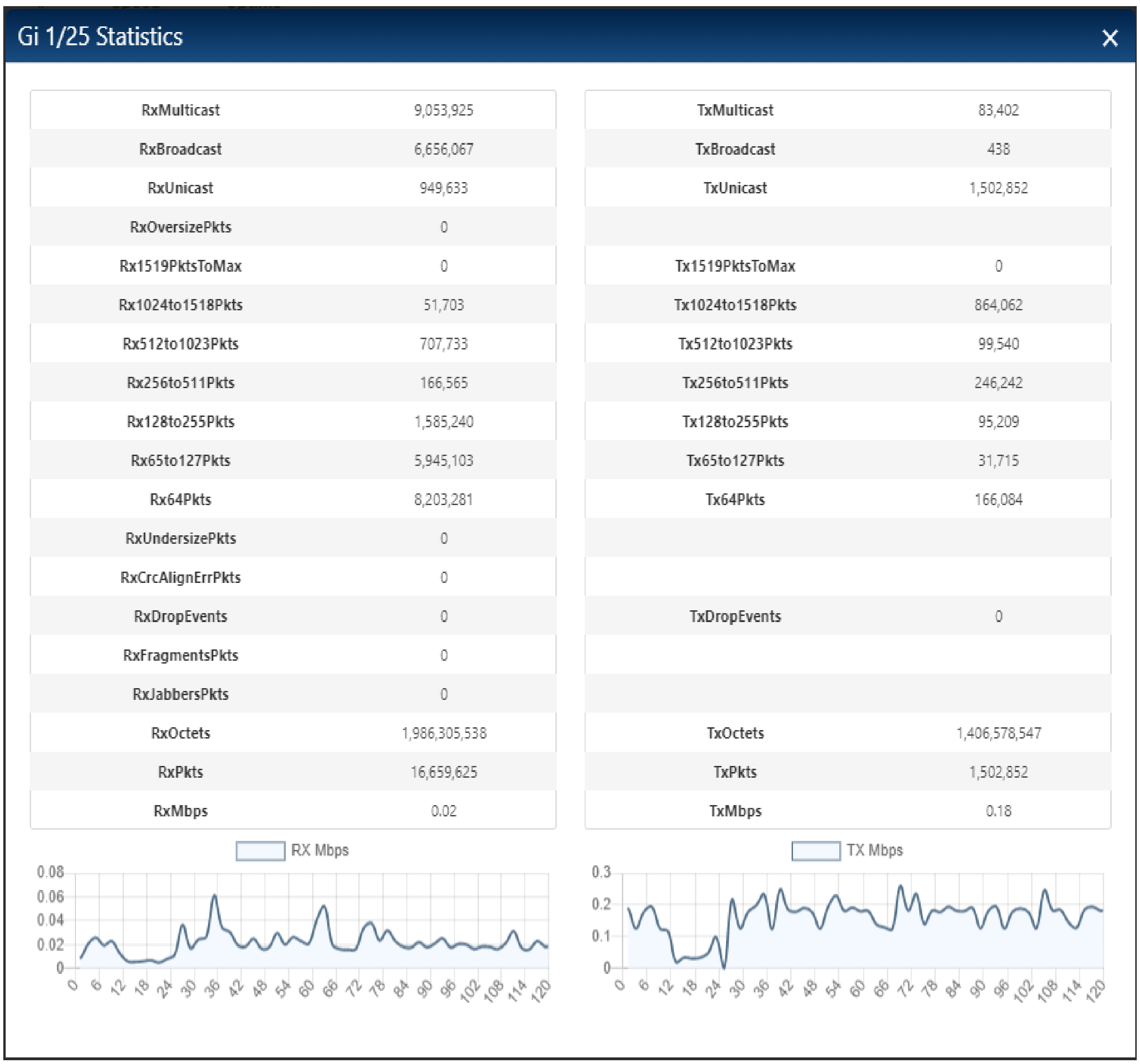
The main panel on the Uplink Ports subtab contains the following information:

Column Header	Description
#	A blue background indicates an active link; a solid grey background indicates the interface is disabled. Hovering over the interface number will display the interface-id and a button to toggle the interface on or off.
Speed	Drop-down box to control the interface’s speed. By default, 10G 1/1 and 10G 1/2 are set to 10Gbps full duplex.
Uptime	If a link has been established, the interface uptime will be displayed as a counter in a black font. If an established link goes done, the counter will turn red and begin to increment from 0.

RX/TX Packet Counters	**Broadcast**	Displays the interface's broadcast transmission and receive counters.
	Multicast	Displays the interface's multicast transmission and receive counters.
	Unicast	Displays the interface's unicast transmission and receive counters.
	Errors	Displays the interface's error packet counters.
	Total	Displays the interface's total transmission and receive packet counters.
	Mbps	Displays the interface's real-time bandwidth information.

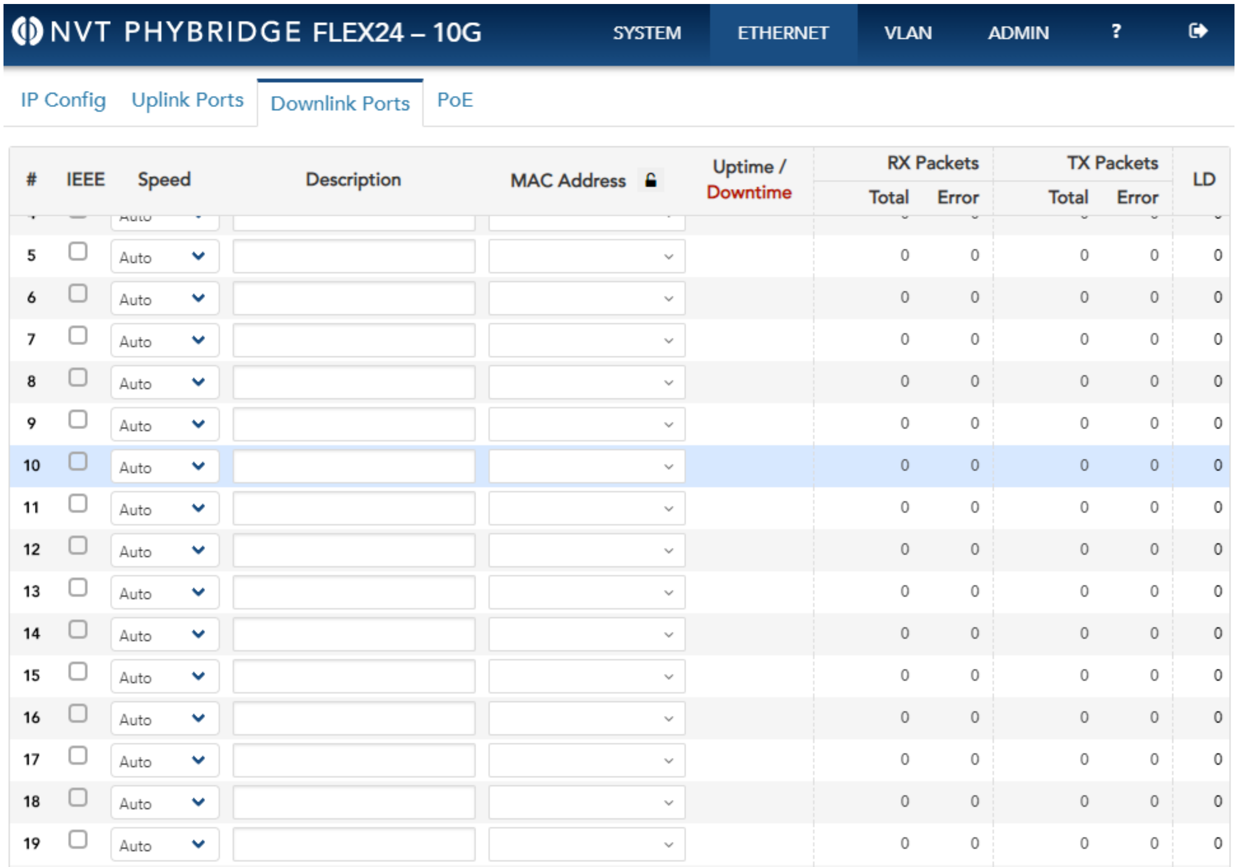
When hovering the mouse over any of the RX/TX Packet Counters values a Show full stats button will appear.

Clicking the Show full stats button will open a new window displaying verbose packet counter information.


Gi 1/25 Statistics

RxMulticast	9,053,925	TxMulticast	83,402
RxBroadcast	6,656,067	TxBroadcast	438
RxUnicast	949,633	TxUnicast	1,502,852
RxOversizePkts	0		
Rx1519PktsToMax	0	Tx1519PktsToMax	0
Rx1024to1518Pkts	51,703	Tx1024to1518Pkts	864,062
Rx512to1023Pkts	707,733	Tx512to1023Pkts	99,540
Rx256to511Pkts	166,565	Tx256to511Pkts	246,242
Rx128to255Pkts	1,585,240	Tx128to255Pkts	95,209
Rx65to127Pkts	5,945,103	Tx65to127Pkts	31,715
Rx64Pkts	8,203,281	Tx64Pkts	166,084
RxUndersizePkts	0		
RxCrcAlignErrPkts	0		
RxDropEvents	0	TxDropEvents	0
RxFragmentsPkts	0		
RxJabbersPkts	0		
RxOctets	1,986,305,538	TxOctets	1,406,578,547
RxPkts	16,659,625	TxPkts	1,502,852
RxMbps	0.02	TxMbps	0.18

Downlink Ports



The Downlink Ports subtab allows for monitoring of the 24 Gigabit Ethernet interfaces.

The main panel of the Downlink Ports subtab contains the following information:

Column header	Description
#	A blue background indicates an active link; a solid grey background indicates the interface is disabled. Hovering over the interface number will display the interface-id and port speed. A button will also be present to enable/disable the interface. If the link is active, a reset button will also be present.
IEEE	The IEEE checkbox enables/disables long reach on the interface: • When checked, the interface supports up to 1Gbps full duplex but does not support long reach. • When cleared, the interface supports up to 100Mbps full duplex and supports long reach.
Speed	Drop-down box to control the interface's speed. By default, all Gigabit interfaces are set to autonegotiate speed with the remote device.
Description	Interface description. By default, this field is empty but can be configured at the administrator's descretion.

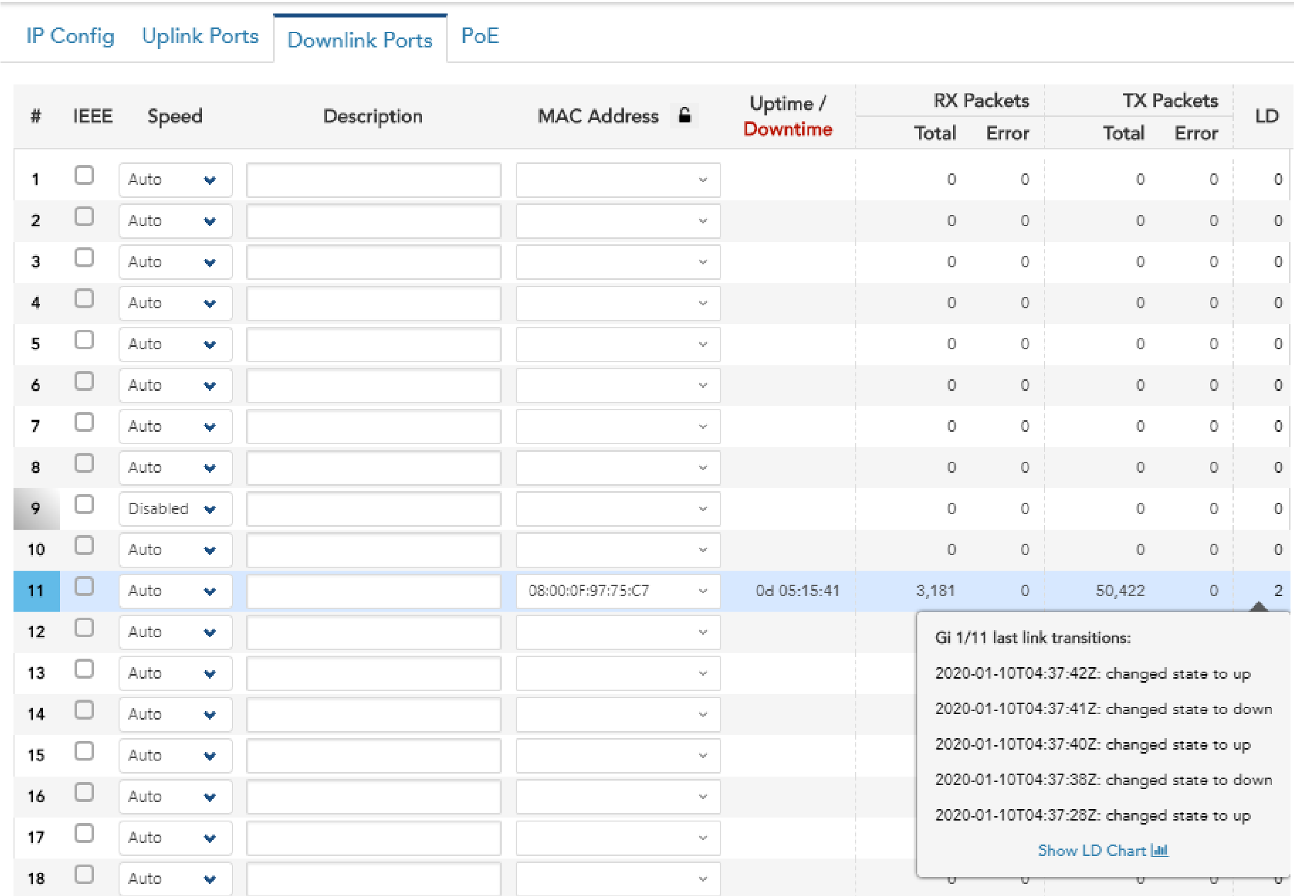
MAC Address		The MAC address column displays all MAC addresses found downstream from the interface. The first MAC address will be displayed without user intervention. Clicking the drop-down will reveal the remaining MAC addresses (if there are any). MAC addresses can be locked/unlocked by clicking the next to the address. A new MAC address can be locked by manual typing in the address and clicking the button. **Note:** Locking a single MAC address will causes all other downstream devices on the same switchport to lose communication with the switch.
Uptime/Downtime		Length of time in which a connection has been established with an adapter/endpoint. Uptime is displayed in black while downtime is displayed in red.
RX Packets	**Total**	Total number of packets received on the interface. Updates in real-time. A breakdown by packet type can be seen by hovering the mouse over the total packet counter.
	Error	Total number of error packets received on the interface. Updates in real-time. The error number should be very small in comparison to the total number.
TX Packets	**Total**	Total number of packets trasmitted on the interface. Updates in real-time. A breakdown by packet type can be seen by hovering the mouse over the total packet counter.
	Error	Total number of error packets transmitted on the interface. Updates in real-time. The error number should be very small in comparison to the total number.
LD		Number of linkdowns on the interface. A linkdown occurs when the adapter/endpoint loses it connection with the switch. A high number of linkdowns may indicate a cabling problem.

Hovering over any of the RX/TX Packet Counters will reveal a Show full stats button.

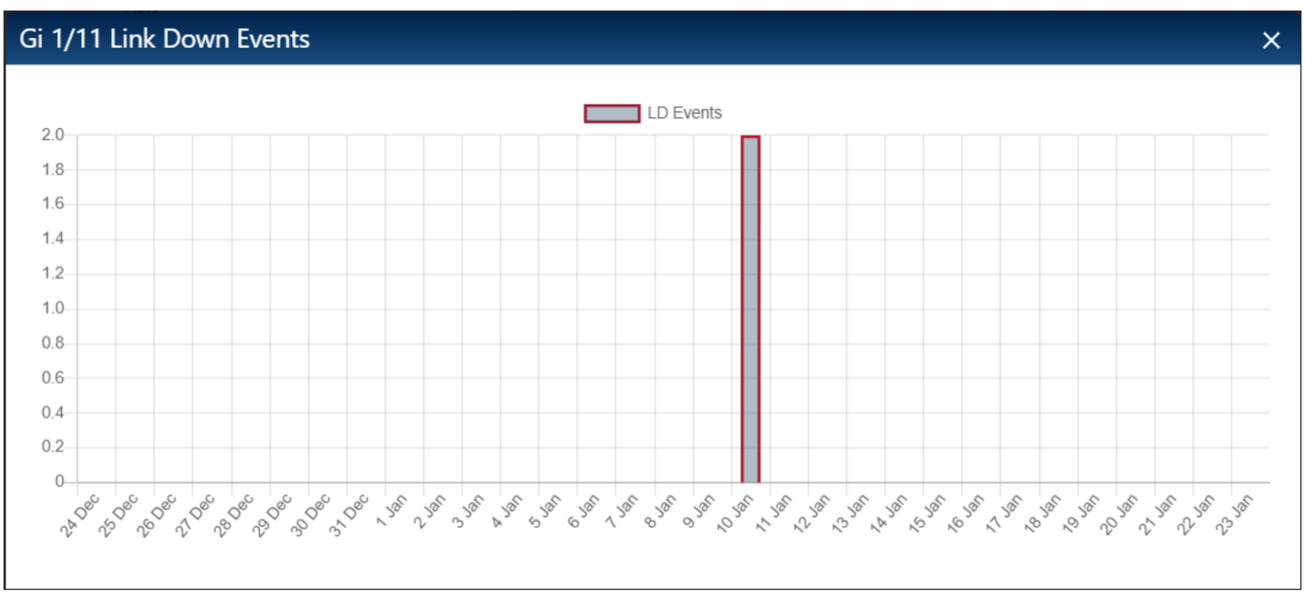
Clicking the Show full stats button will open a new window displaying verbose packet counter information. Image above.

Hovering the mouse over the LD (Linkdown) counter will reveal a Show LD Chart button as well as listing the most recent linkdown events.

Clicking the Show LD Chart button will open a new window showing a 30-day linkdown history for the interface. Image below:

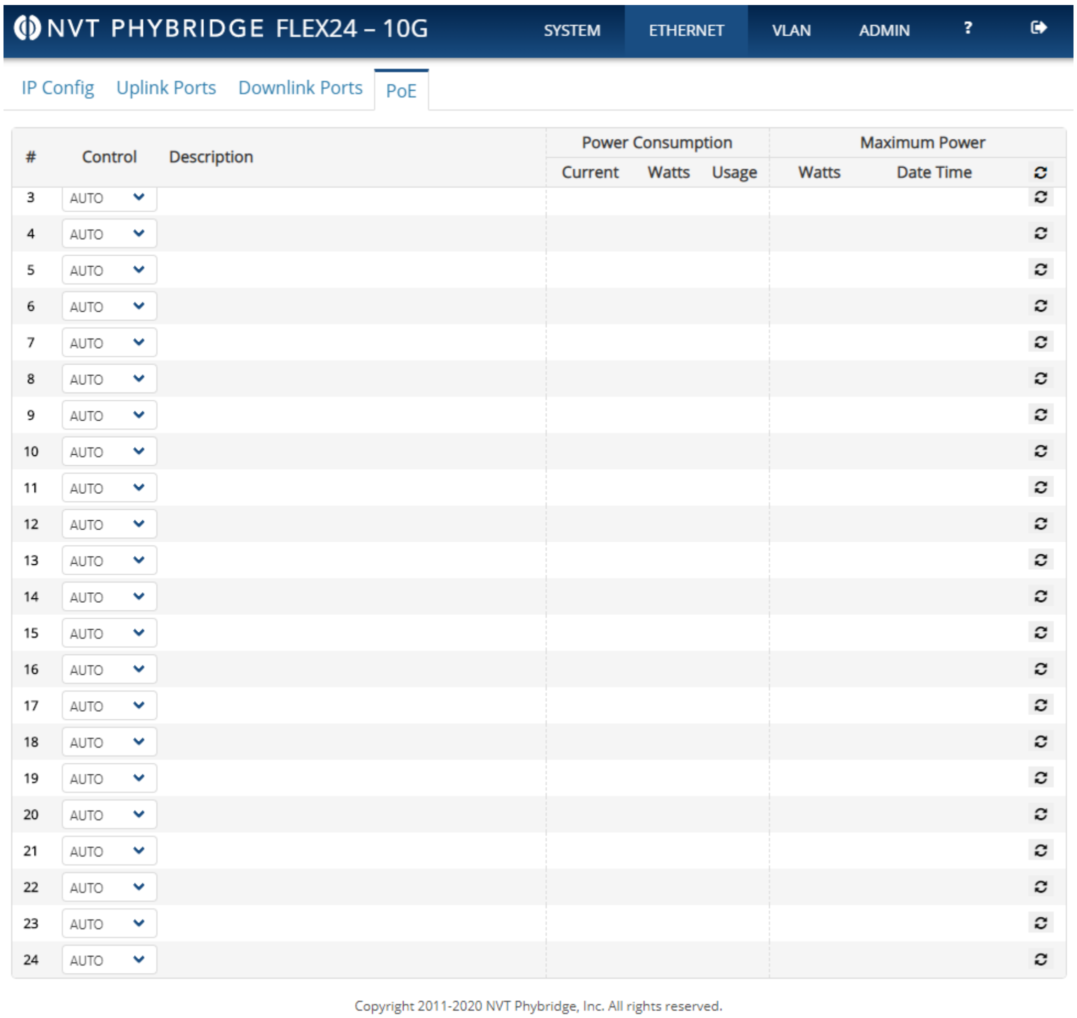


#	IEEE	Speed	Description	MAC Address	Uptime / Downtime	RX Packets Total	RX Packets Error	TX Packets Total	TX Packets Error	LD
1		Auto				0	0	0	0	0
2		Auto				0	0	0	0	0
3		Auto				0	0	0	0	0
4		Auto				0	0	0	0	0
5		Auto				0	0	0	0	0
6		Auto				0	0	0	0	0
7		Auto				0	0	0	0	0
8		Auto				0	0	0	0	0
9		Disabled				0	0	0	0	0
10		Auto				0	0	0	0	0
11		Auto		08:00:0F:97:75:C7	0d 05:15:41	3,181	0	50,422	0	2
12		Auto								
13		Auto								
14		Auto								
15		Auto								
16		Auto								
17		Auto								
18		Auto								



Note: None of the changes made on the Ethernet tab are permanent until the running configuration has been saved from the **Admin > Setup** subtab.

PoE



The PoE tab displays real-time PoE statistics for all 24 Gigabit Ethernet interfaces on the FLEX24-10G.

The main panel on the PoE subtab contains the following information:

Column	Description
#	A blue background indicates an active link; a solid grey background indicates the interface is disabled. Hovering over an active link will display the interface-id and the interface speed. Interfaces can be enabled/disabled by single-clicking the interface number.

Control		Drop-down box to set the interface's PoE mode. The FLEX24-10G supports the following PoE modes: • **Off:** PoE is disabled. • **Manual:** PoE is always provided to the remote device. • **Semi:** PoE negotiation takes place. If the endpoint requires PoE, the interface will output full power to the endpoint regardless of the endpoint's power requirements. • **Auto:** Automatically negotiate PoE with remote device.
Description		Interface description. The description is set from the Ethernet > Downlink Ports subtab.
Power Consumption	**Current**	Current power consumption of the interface in milliamps (mA).
	Watts	Current power consumption of the interface in watts (W).
	Usage	Current power comsumption represented as a percentage.
Maximum Power	**Watts**	Amount of power provided when the interface provided maximum power. Value is displayed in watts (W).
	Date	Datestamp for when the interface provided maximum power.
	Time	Timestamp for when the interface provided maximum power.
		Reset maximum power statistics. The entries in the maximum power column can be cleared on a per interface basis or for all interfaces at once.

VLAN

The VLAN tab contains the following subtabs:

- VLAN Table
- Trunk VLAN
- Private VLAN
- Port Isolation

VLAN Table

Note: Do not use VLAN 0. There is potential in the VLAN specification to interpret the standard VLAN 0 in different ways, which will lead to incompatibility between different vendors.

By default, the FLEX24-10G contains two VLANs, VLAN 1 and VLAN 1001. All 24 GigabitEthernet interfaces are members of VLAN 1 while the management interface is a member of VLAN 1001.

The following operations can be performed from the VLAN Table subtab:

- Creating a VLAN
- Access port assignment to a VLAN
- Deleting a VLAN

Adding a VLAN

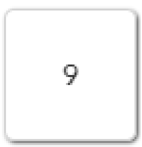
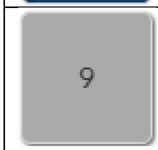
Additional VLANs are created by entering a VLAN ID into the **Add VLAN** field and clicking Add

A new panel will appear for the VLAN you just created. Click Apply edits to finalize the creation of the VLAN.

<u>Note:</u> VLANs will not be reflected in the switch's running-config untill the Apply edits button is clicked.

Assigning an Access Port to a VLAN

When a VLAN is first created, no interfaces are a member of that VLAN. To assign an access port to a VLAN, click the interface box pertaining to the interface in question. The interface's background will change from white to blue.

Background	**Description**
	Interface 9 is not an access port.
	Interface 9 is an access port.
	Interface 9 is a trunk port.

The interface's background will transition from blue to white in the VLAN which the interface was previously a member of.

If the interface is a trunk interface, a dialog window will appear with the following message:

The port is in trunk mode.

Click 'OK' to be redirected to VLAN > Trunk VLAN page

The trunk toggle will have to be toggled off before an interface's VLAN membership can be changed.

Click Select All to assign all Gigabit Ethernet and 10 Gigabit Ethernet interfaces as access ports.

Click Apply edits to save the changes to the switch's running-config.

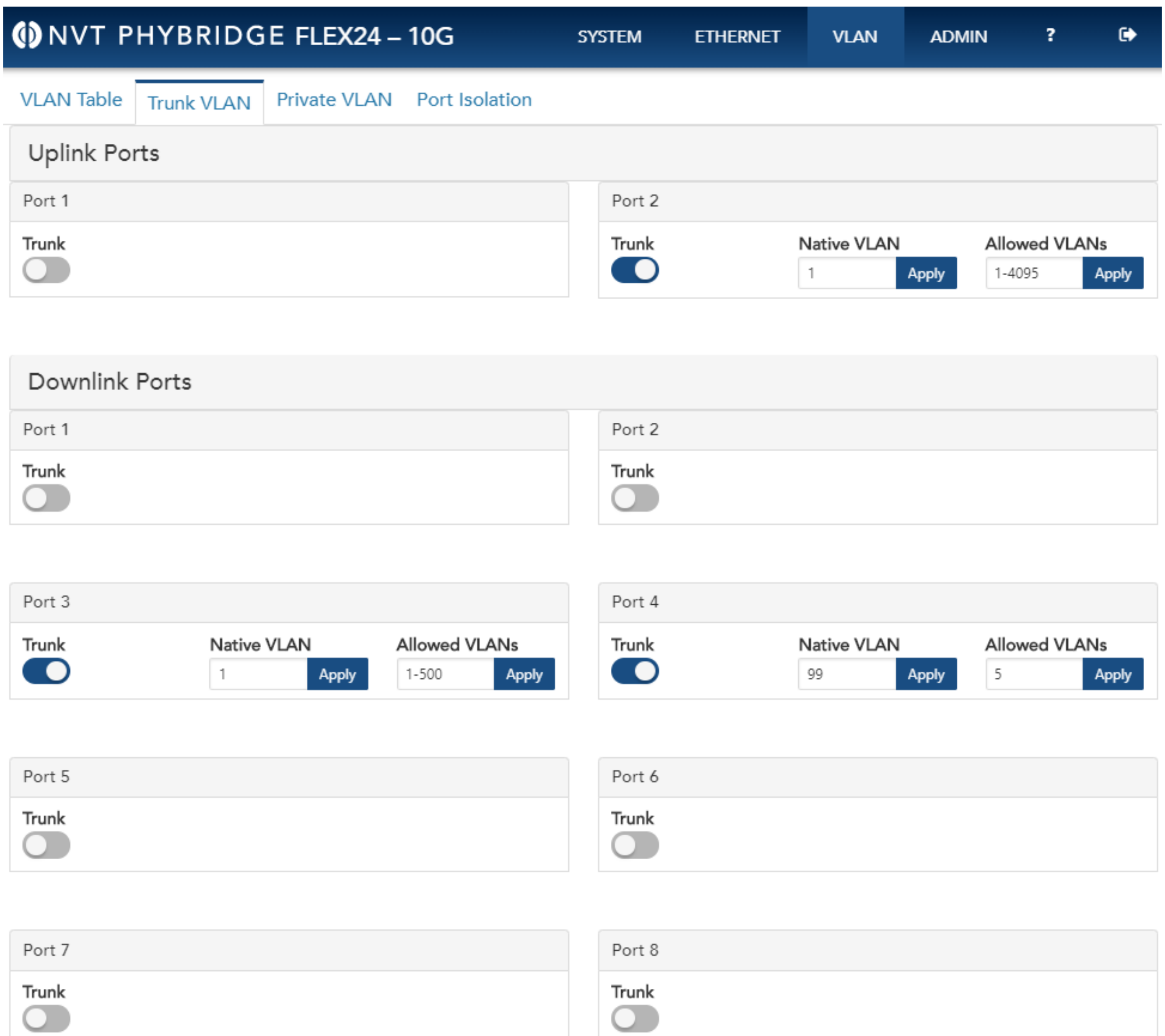
Deleting a VLAN

To delete a VLAN, click the ⊗ button on the VLAN panel in which you would like to delete. To finalize the deletion, click Apply edits

If the user navigates to another page in the WEB GUI before clicking Apply edits, the changes will not be saved.

Note: Applying the edits will not save the changes to the switch's startup-config. To overwrite the startup-config with the running-config the Save button must be clicked from the **Admin > Setup** tab.

Trunk VLAN



The Trunk VLAN subtab allows the administrator to create trunk ports. A trunk port is an interface which carries traffic belonging to more than one VLAN.

Creating a Trunk Interface

A trunk interface is created by toggling the Trunk toggle for the interface you would like to make a trunk.

Editing the Native VLAN on a Trunk Port

Traffic belonging to the native VLAN will travel across the trunk port untagged. All other traffic will contain a dot1q tag. This tag is used to identify the VLAN in which a frame belongs to.

When a trunk is initially created, the native VLAN is VLAN 1. To change the trunk port's native VLAN enter the VLAN ID into the **Native VLAN** field and click Apply.

<u>Note:</u> A VLAN does not have to exist for it be a native VLAN for a trunk interface. The switch will accept assigning a non-existent VLAN to a trunk's native VLAN.

Editing Allowed VLANs on a Trunk Port

When a trunk is initially created, all VLANs (VLANs 1-4095) are permitted across the trunk. It is often undesirable to allow all VLANs across a trunk port.

To change the VLANs allowed on a trunk, enter a set of VLANs into the **Allowed VLANs** field and click Apply

A set of VLANs can be denoted as a consecutive range (i.e. 5-10), non-consecutive list (2, 4, 6, 8), or a combination of the two.

Acceptable VLAN ranges:

- 2,3,4
- 2-4
- 2,3,4,5-10
- 2,3,4,5,6,7,8,9,10
- 2-10

Unacceptable VLAN Ranges:

- VLAN 2,3,4

Strings are not accepted, only natural numbers, commas, and hyphens.

<u>Note:</u> Changes are not saved to the switch's startup-config until the Save button has been clicked from the **Admin > Setup** page. Changes not stored in the startup-config will be lost in the event of a system reboot.

Private VLAN

Private VLANs can be thought of as sub-VLANs. Interfaces in a private VLAN can only communicate with interfaces in the same private VLAN.

An interface can be a member of more than one Private VLAN. PVLANs are only significant on the local switch. Frames are not tagged with a PVLAN ID.

The Private VLAN subtab allows for the management of Private VLANs (PVLANs). From this screen the following actions can be performed:

- Adding a Private VLAN
- Assigning interfaces to a Private VLAN
- Removing interfaces from a Private VLAN
- Deleting a Private VLAN

Adding a PVLAN

By default, the FLEX24-10G only contains one PVLAN (PVLAN 1). All interfaces are a member of this PVLAN.

To create a new PVLAN, enter the PVLAN ID into the **Add VLAN** field and click 

A new panel will appear for the PVLAN which was just created. When a new PVLAN is created, no interfaces will be a member of the PVLAN. This is reflected by the solid white background for each interface.

Assigning an Interface to a PVLAN

To assign an interface to a PVLAN, click the interface to be added to the PVLAN. The background of that interface will change from solid white to solid blue.

An interface can be a member of more than one PVLAN. Click Select All to assign all interfaces to the PVLAN.

An Apply edits button will appear at the top and bottom of the Private VLAN list. Click this button to save the changes to the switch’s running-config.

Removing Interfaces from a PVLAN

An interface with a solid blue background is a member of a specific PVLAN.

To remove that interface from the PVLAN, click the interface, it’s background should change from solid blue to solid white.

An Apply edits button will appear at the top and bottom of the Private VLAN list. Click this button to save the changes to the switch’s running-config.

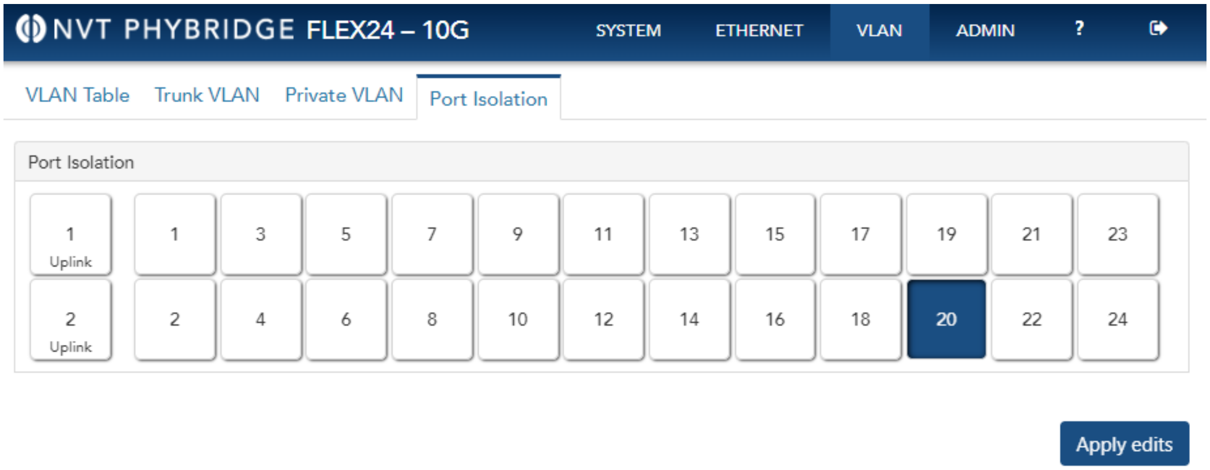
Deleting a PVLAN

To delete a PVLAN, click the button for the PVLAN which you would like to delete. The entire PVLAN panel will be removed.

An Apply edits button will appear at the top and bottom of the Private VLAN list. Click this button to save the changes to the switch’s running-config.

Note: Changes are not saved to the switch’s startup-config until the Save button has been clicked from the **Admin > Setup** page. Changes not stored in the startup-config will be lost in the event of a system reboot.

Port Isolation



Port Isolation is configured from the Port Isolation subtab. Isolated ports cannot communicate with any other isolated ports. Isolated ports are able to communicate with non-isolated ports.

Port Isolation provides a means to ensure that two or more ports will never be able to communicate with one another.

Configuring Port Isolation

By default, none of the interfaces on the FLEX24-10G are isolated ports.

To create an isolated port, click the interface in which you would like to make isolated, it's background will transition from solid white to solid blue.

An Apply edits button will appear below the Port Isolation panel. Click this button to save the changes to the switch's running-config.

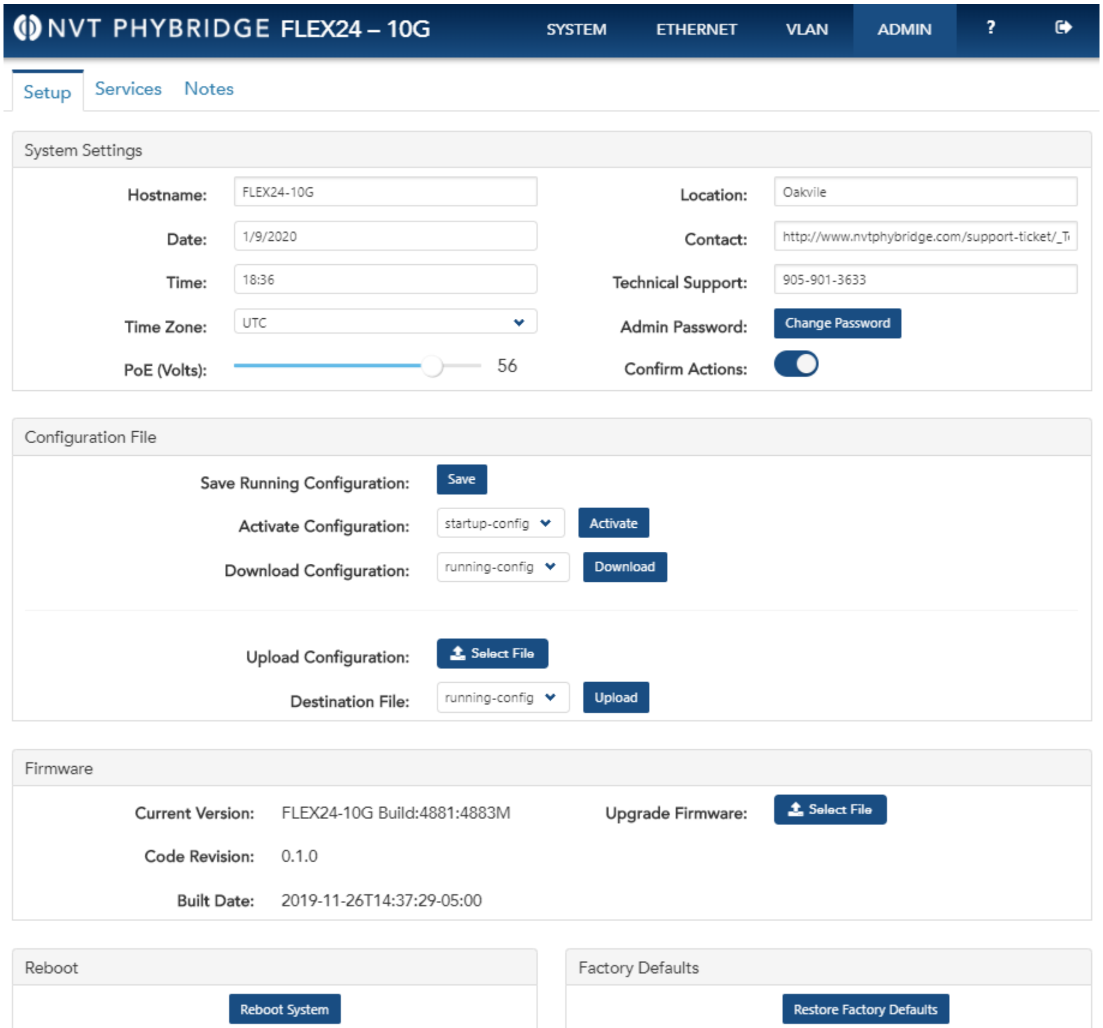
Note: Changes are not saved to the switch's startup-config until the Save button has been clicked from the **Admin > Setup** page. Changes not stored in the startup-config will be lost in the event of a system reboot.

Admin

The Admin tab contains the following subtabs:

- Setup
- Services
- Notes

Setup



The **System Settings** panel allows the administrator to configure switch wide settings.

The following parameters can be configured from the System Settings panel:

Parameter	Description
Hostname	System hostname.
Date	System date. When the cursor is placed in this field a calendar will appear allowing the user to select the date.
Time	System date in 24-hour format. Placing the cursor in this field will present a drop-down allowing the user to specify the system time.
Time Zone	Time zone specified using UTC offset. The time zone is selected by clicking the correct UTC offset from the drop-down menu.
PoE (Volts)	PoE available to endpoint devices. The PoE slider can be set to any integer between 48 and 58 Volts inclusive. By default, the PoE is set to 56 Volts.
Location	System location.

Contact	System contact information. By default, the contact is set to the NVT Phybridge technical support website, and telephone number.
Technical Support	Technical support contact. By default, the NVT Phybridge technical support phone number appears in this field.
Admin Password	Switch admin password. By default, the admin password is “admin”, but this can be changed. The user will be prompted for the current switch password before being allowed to enter a new password. Upon a successful password change, the user will be logged out of the GUI and taken to the GUI login page.
Confirm Actions	When the **Confirm Actions** toggle is enabled, a confirmation window will appear before changes are applied.

The Configuration File panel allows the administrator to import/export a configuration file to and from the switch. Additionally, the startup-config can be overwritten with the current entries of the running config.

The Configuration File panel contains the following options:

Option	Description
Save Running Configuration	Copy the contents of the running-config to the startup-config.
Activate Configuration	Load a specific configuration file from the switch’s memory. The available configuration files which can be loaded are the following: • default-config • startup-config Click Activate to activate the configuration selected from the drop-down menu.
Download Configuration	Export the switch’s configuration. One of the following configurations can be exported and downloaded to the user’s local computer: • running-config • default-config • startup-config Click Download to download the configuration as a .txt file.
Upload Configuration	Browse your local machine’s file system for a configuration file to upload to the switch. Clicking the Select File button will open a new dialog window of the user’s file system.

	Find the new configuration file and click "Open". The Select File button will be replaced with the file name of the configuration.
Destination File	Upload the configuration file from the "Upload Configuration" step. The configuration file will replace the configuration displayed in the drop-down menu. The configuration file can either replace the running-config or the startup-config. Click Upload to upload the configuration. **Note:** If running-config is selected, the changes are applied immediately. Click Save to ensure the changes survive a reboot. If startup-config is selected, the changes will not be applied immediately but instead are applied after a system reboot.

The Firmware panel displays information regarding the switch's current firmware. A newer firmware image can also be uploaded from this panel.

The Firmware panel provides the following information:

Panel Entry	Description
Current Version	Displays the current firmware version.
Code Revision	Displays the current firmware code revision.
Build Date	Displays the firmware build date.
Upgrade Firmware	Upgrade the switch's firmware. A new firmware version is uploaded by clicking Select File and opening a genuine firmware file. The firmware filename and an Upgrade button will appear. Click Upgrade to upgrade the switch firmware. The upgrade progress is displayed as a blue bar at the bottom on the Firmware panel.

Rebooting the Switch

The switch can be rebooted from the Reboot panel.

To reboot the system, click Reboot System

A new dialog window will appear. Click OK to confirm. The switch will reboot.

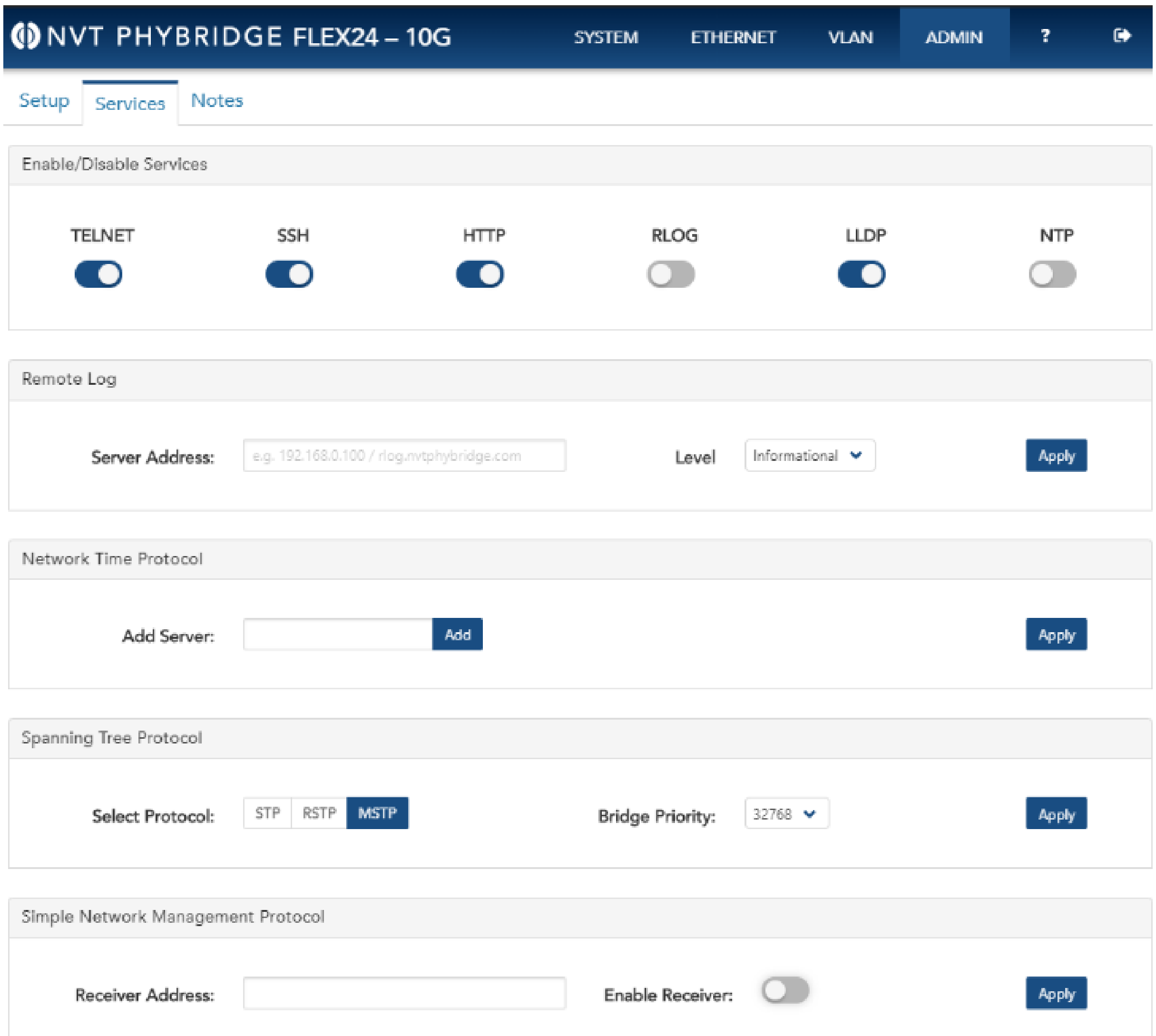
Factory Defaulting the Switch

The switch can be factory defaulted from the Factory Defaults panel by clicking the Restore Factory Defaults button.

A new dialog window will appear. Click OK to confirm. The switch's running-config will be overwritten with the default-config.

For a factory default to survive a reboot, the startup-config must be overwritten with the switch's running-config. This is done by clicking Save from the Configuration File panel.

Services



The Services subtab is where all the system services can be managed. The FLEX24-10G contains the following services:

- TELNET
- SSH
- HTTP
- REMOTE SYSLOG
- LLDP
- NTP

Enabling/Disabling a Service

Services are enabled/disabled from the Enable/Disable Services panel. When a service is enabled, it will be started when the switch powers on.

To enable a service, toggle the slider to the ON position. Likewise, to disable a service, toggle the slider to an OFF position.

Position	**Meaning**
	Service is enabled
	Service is disabled

Note: If the HTTP service is disabled from the WEB GUI, the connection to the GUI will be terminated immediately.

Remote Log Configuration

The Remote Log panel allows the switch's syslog messages to be sent to an external syslog server.

Enter the syslog server's IP address/domain name into the **Server Address** field.

The **Level** drop-down controls the severity of log message to send to the syslog server. All messages with a priority equal to or higher will be sent to the syslog server.

Log Levels

Priority (Highest to Lowest)	**Describer**
0	Emergency (Highest Priority)
1	Alert
2	Critical
3	Error
4	Warning
5	Notification
6	Informational
7	Debugging (Lowest Priority)

Click Apply to apply the changes.

Network Time Protocol (NTP)

The FLEX24-10G can be configured with up to five NTP servers.

To add an NTP server, enter the server's IP address/domain name into the **Add Server** field and click Add

To remove an NTP server, click the ⊗ next to the IP address/domain name you would like to delete.

Click Apply to save the changes to the switch's running-config.

Spanning Tree Protocol (STP)

Spanning Tree Protocol (STP) can be configured from the Spanning Tree Protocol panel.

By default, Multiple Spanning Tree Protocol is enabled on the FLEX24-10G with a bridge priority of 32768.

The FLEX24-10G supports the following Spanning Tree modes:

- Spanning Tree Protocol
- Rapid Spanning Tree Protocol
- Multiple Spanning Tree Protocol

To change the Spanning Tree protocol, click the protocol you would like to enable. The protocol button will turn solid blue.

To change the bridge priority, click the **Bridge Priority** drop-down. All the available priorities are listed in increments of 4096. Select the desired protocol and click Apply to apply the changes to the switch's running-config.

Note: Enabling STP in a live network will cause service disruptions to end users while the network is converging. To avoid impacting users, changes to STP should be conducted outside of business hours or during a scheduled maintenance period. Consult the MCD Resiliency Guidelines for information on how to optimally configure STP/RSTP/MSTP.

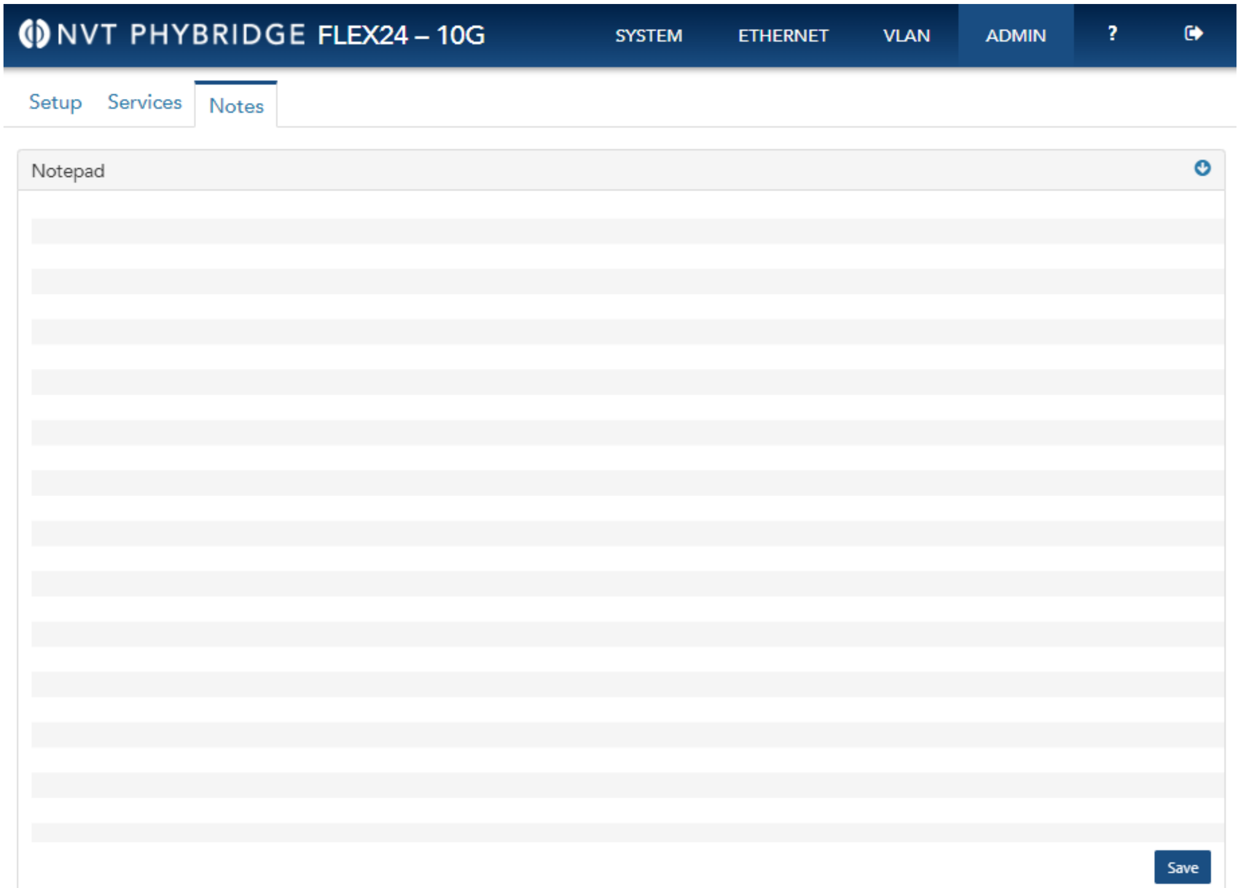
Simple Network Management Protocol (SNMP)

The FLEX24-10G supports SNMP in the sense that system events can be exported to an external SNMP server.

To configure an SNMP server, enter the server's IP address/domain name into the **Receiver Address** field and click Apply to apply the changes.

The receiver must also be enabled for SNMP traps to be sent to the SNMP server. To enable the receiver, enable the toggle switch ( ).

Notes



The Notes subtab contains a Notepad which allows for the saving of notes. These notes are shared between all users with WEB GUI access.

To enter a note, click anywhere in the Notepad panel and begin typing.

To save the Notepad, click the Save button located to the bottom right of the Notepad.

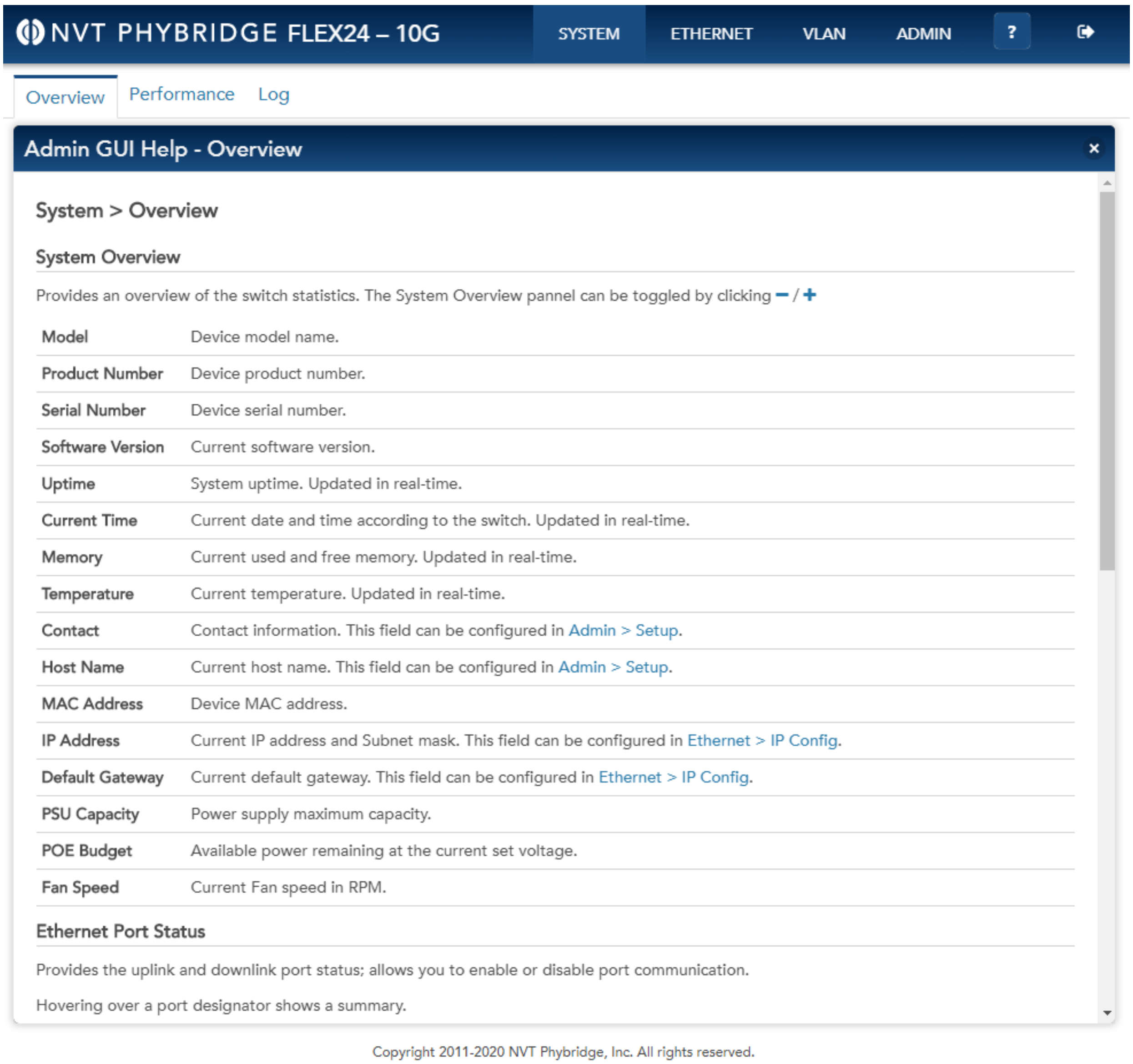
To download the Notepad, click the button located to the top right of the Notepad. A notepad.txt file will be downloaded.

Help

The WEB GUI also contains Help pages specific to each tab and subtab in the GUI.

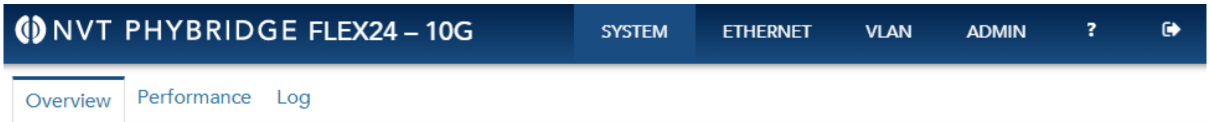
The display the Help pages click the ? located on the top navigation bar. The information displayed in the Help window will be specific to the last screen.

For example, if the user is on the System > Overview screen and then clicks the ? button, the help window for the System > Overview screen will be displayed.



The help pages contain links which link to other pages in the GUI. Clicking one of these links will take the user to another page.

The GUI can also be navigated while the help pages are displayed. Both the main tab navigation bar and subtab navigation bar remain visible the help screen is displayed.



Use the navigation bars to change the actively displayed help screen.