ExtremeSwitching

Troubleshooting Ethernet Routing Switch 4900 and 5900 Series

Release 7.7
9035793 Rev.AA
June 2019

Legal Notice

Extreme Networks, Inc. reserves the right to make changes in specifications and other information contained in this document and its website without prior notice. The reader should in all cases consult representatives of Extreme Networks to determine whether any such changes have been made.

The hardware, firmware, software or any specifications described or referred to in this document are subject to change without notice.

Trademarks

Extreme Networks and the Extreme Networks logo are trademarks or registered trademarks of Extreme Networks, Inc. in the United States and/or other countries.

All other names (including any product names) mentioned in this document are the property of their respective owners and may be trademarks or registered trademarks of their respective companies/owners.

For additional information on Extreme Networks trademarks, please see: www.extremenetworks.com/company/legal/trademarks

Open Source Declarations

Some software files have been licensed under certain open source or third-party licenses. End-user license agreements and open source declarations can be found at: www.extremenetworks.com/support/policies/software-licensing

Contents

Chapter 1: About this Document

This section discusses the purpose of this document, the conventions used, ways to provide feedback, additional help, and information regarding other Extreme Networks publications.

Purpose

This document describes the diagnostic tools and utilities available to help you troubleshoot operational and configuration issues on the following platforms:

- Extreme Networks Ethernet Routing Switch 4900 Series
- Extreme Networks Ethernet Routing Switch 5900 Series

This document guides you through some common problems, to achieve a first tier solution to these situations, and advises you what information to compile prior to troubleshooting or calling Extreme Networks for help.

You can configure and display files, view and monitor port statistics, trace a route, run loopback and ping tests, test the switch, and view the address resolution table. Although the diagnostic tools and utilities described are available with both the Command Line Interface (CLI) and Enterprise Device Manager (EDM), this document focuses on using CLI to demonstrate most of the troubleshooting tasks. You can access CLI through either a direct console connection to the switch or by using the Telnet or SSH protocols to connect to the switch remotely.

Conventions

This section discusses the conventions used in this guide.

Text Conventions

The following tables list text conventions that can be used throughout this document.

Table 1: Notice Icons

Icon	Alerts you to...
Important:	A situation that can cause serious inconvenience.
Note:	Important features or instructions.
Tip:	Helpful tips and notices for using the product.
Danger:	Situations that will result in severe bodily injury; up to and including death.
Warning:	Risk of severe personal injury or critical loss of data.
Caution:	Risk of personal injury, system damage, or loss of data.

Table 2: Text Conventions

Convention	Description
Angle brackets (< >)	Angle brackets (< >) indicate that you choose the text to enter based on the description inside the brackets. Do not type the brackets when you enter the command. If the command syntax is `cfm maintenance-domain maintenance-level <0-7>` , you can enter `cfm maintenance-domain maintenance-level 4`.
Bold text	Bold text indicates the GUI object name you must act upon. Examples: • Click **OK**. • On the **Tools** menu, choose **Options**.
Braces ({ })	Braces ({ }) indicate required elements in syntax descriptions. Do not type the braces when you enter the command. For example, if the command syntax is `ip address {A.B.C.D}`, you must enter the IP address in dotted, decimal notation.
Brackets ([ ])	Brackets ([ ]) indicate optional elements in syntax descriptions. Do not type the brackets when you enter the command. For example, if the command syntax is `show clock [detail]`, you can enter either `show clock` or `show clock detail`.

Table continues…

Convention	Description
Ellipses (…)	An ellipsis (…) indicates that you repeat the last element of the command as needed. For example, if the command syntax is `ethernet/2/1 [ <parameter> <value> ]...`, you enter `ethernet/2/1` and as many parameter-value pairs as you need.
Italic Text	Italics emphasize a point or denote new terms at the place where they are defined in the text. Italics are also used when referring to publication titles that are not active links.
`Plain Courier Text`	Plain Courier text indicates command names, options, and text that you must enter. Plain Courier text also indicates command syntax and system output, for example, prompts and system messages. Examples: • `show ip route` • `Error: Invalid command syntax [Failed][2013-03-22 13:37:03.303 -04:00]`
Separator (>)	A greater than sign (>) shows separation in menu paths. For example, in the Navigation tree, expand the **Configuration** > **Edit** folders.
Vertical Line (|)	A vertical line (|) separates choices for command keywords and arguments. Enter only one choice. Do not type the vertical line when you enter the command. For example, if the command syntax is `access-policy by-mac action { allow | deny }`, you enter either `access-policy by-mac action allow` or `access-policy by-mac action deny`, but not both.

Documentation and Training

To find Extreme Networks product guides, visit our documentation pages at:

Current Product Documentation	www.extremenetworks.com/documentation/

Table continues…

Archived Documentation (for earlier versions and legacy products)	www.extremenetworks.com/support/documentation-archives/
Release Notes	www.extremenetworks.com/support/release-notes
Hardware/Software Compatibility Matrices	https://www.extremenetworks.com/support/compatibility-matrices/
White papers, data sheets, case studies, and other product resources	https://www.extremenetworks.com/resources/

Training

Extreme Networks offers product training courses, both online and in person, as well as specialized certifications. For more information, visit www.extremenetworks.com/education/.

Getting Help

If you require assistance, contact Extreme Networks using one of the following methods:

Extreme Portal	Search the GTAC (Global Technical Assistance Center) knowledge base, manage support cases and service contracts, download software, and obtain product licensing, training, and certifications.
The Hub	A forum for Extreme Networks customers to connect with one another, answer questions, and share ideas and feedback. This community is monitored by Extreme Networks employees, but is not intended to replace specific guidance from GTAC.
Call GTAC	For immediate support: 1-800-998-2408 (toll-free in U.S. and Canada) or +1 408-579-2826. For the support phone number in your country, visit: www.extremenetworks.com/support/contact

Before contacting Extreme Networks for technical support, have the following information ready:

- Your Extreme Networks service contract number and/or serial numbers for all involved Extreme Networks products
- A description of the failure
- A description of any action(s) already taken to resolve the problem
- A description of your network environment (such as layout, cable type, other relevant environmental information)
- Network load at the time of trouble (if known)
- The device history (for example, if you have returned the device before, or if this is a recurring problem)
- Any related RMA (Return Material Authorization) numbers

Subscribing to Service Notifications

You can subscribe to email notifications for product and software release announcements, Vulnerability Notices, and Service Notifications.

1. Go to www.extremenetworks.com/support/service-notification-form.
2. Complete the form with your information (all fields are required).
3. Select the products for which you would like to receive notifications.

   Note:
   You can modify your product selections or unsubscribe at any time.
4. Click **Submit**.

Providing Feedback to Us

Quality is our first concern at Extreme Networks, and we have made every effort to ensure the accuracy and completeness of this document. We are always striving to improve our documentation and help you work better, so we want to hear from you! We welcome all feedback but especially want to know about:

- Content errors or confusing or conflicting information.
- Ideas for improvements to our documentation so you can find the information you need faster.
- Broken links or usability issues.

If you would like to provide feedback to the Extreme Networks Information Development team, you can do so in two ways:

- Use our short online feedback form at https://www.extremenetworks.com/documentation-feedback/.
- Email us at documentation@extremenetworks.com.

Please provide the publication title, part number, and as much detail as possible, including the topic heading and page number if applicable, as well as your suggestions for improvement.

Chapter 2: New in this document

The following sections detail what is new in this document.

Timestamp in show command outputs

The output for all CLI show commands includes a timestamp header to indicate when the command output was generated. This information can be helpful when communicating with Support.

For more information, see Timestamp in show command outputs on page 39.

Chapter 3: Troubleshooting Planning

There are some things you can do to minimize the need for troubleshooting and to plan for doing it as effectively as possible.

First, use the Documentation Reference for Ethernet Routing Switch 4900 and 5900 Series to familiarize yourself with the documentation set, so you know where to get information as you need it.

Second, make sure the system is properly installed and maintained so that it operates as expected.

Third, make sure you gather and keep up to date the site map, logical connections, device configuration information, and other data that you will require if you have to troubleshoot.

- A site network map identifies where each device is physically located on your site, which helps locate the users and applications that are affected by a problem. You can use the map to systematically search each part of your network for problems.
- You must know how your devices are connected logically and physically with virtual local area networks (VLAN).
- Maintain online and paper copies of your device configuration information. Ensure that all online data is stored with your site's regular data backup for your site. If your site has no backup system, copy the information about to a backup medium and store the backup offsite.
- Store passwords in a safe place. A good practice is to keep records of your previous passwords in case you must restore a device to a previous software version. You need to use the old password that was valid for that version.
- A good practice is to maintain a device inventory, which lists all devices and relevant information for your network. Use this inventory to easily see the device types, IP addresses, ports, MAC addresses, and attached devices.
- If your hubs or switches are not managed, you must keep a list of the MAC addresses that correlate to the ports on your hubs and switches.
- Maintain a change-control system for all critical systems. Permanently store change-control records.
- A good practice is to store the details of all key contacts, such as support contacts, support numbers, engineer details, and telephone and fax numbers. Having this information available during troubleshooting saves you time.

Fourth, understand the normal network behavior so you can be more effective at troubleshooting problems.

- Monitor your network over a period of time sufficient to allow you to obtain statistics and data to see patterns in the traffic flow, such as which devices are typically accessed or when peak usage times occur.

- Use a baseline analysis as an important indicator of overall network health. A baseline view of network traffic as it typically is during normal operation is a reference that you can compare to network traffic data that you capture during troubleshooting. This speeds the process of isolating network problems.

Chapter 4: Troubleshooting tools

This section describes available troubleshooting tools and their applications.

Port mirroring

With the port mirroring feature you can monitor and analyze network traffic. The port mirroring feature supports both ingress (incoming traffic) and egress (outgoing traffic) port mirroring. After port mirroring is enabled, the ingress or egress packets of the mirrored (source) port are forwarded normally and a copy of the packets is sent from the mirrored port to the mirroring (destination) port. Although you can configure the switch to monitor both ingress and egress traffic, some restrictions apply:

- For Xtx mode, you can only configure one port as the monitor port and one port as the mirrored port (monitoring traffic transmitted by port X).
- For Xrx mode, you can only configure one port as the monitor port and one port as the mirrored port (monitoring traffic received by port X).
- For XrxorXtx mode, you can only configure one port as the monitor port and one port as the mirrored port (monitoring traffic received by port X OR transmitted by port X).
- For XrxYtx mode, you can only configure one port as the monitor port, one port for mirroring traffic received by port X and one port for mirroring traffic transmitted by port Y (monitoring traffic received by port X AND transmitted by port Y).
- For XrxorYtx mode, you can only configure one port as the monitor port, one port for mirroring traffic received by port X and one port for mirroring traffic sent by port Y (monitoring traffic received by port X OR transmitted by port Y).
- For XrxYtxorYrxXtx mode, you can only configure one port as the monitor port, one port for mirroring traffic received/sent by port X and one port for mirroring traffic sent/received by port Y ((traffic received by port X AND transmitted by port Y) OR (monitoring traffic received by port Y AND transmitted by port X)).

You can also monitor traffic for specified MAC addresses.

- For Adst mode, you can only configure one port as the monitor port and destination MAC address A. (monitoring traffic with destination MAC address A).
- For Asrc mode, you can only configure one port as the monitor port and source MAC address A. (monitoring traffic with source MAC address A).

- For AsrcBdst mode, you can only configure one port as the monitor port, source MAC address A and destination MAC address B. (monitoring traffic with source MAC address A and destination MAC address B).
- For AsrcBdstorBsrcAdst mode, you can only configure one port as the monitor port, source MAC address A and destination MAC address B. ((monitoring traffic with source MAC address A and destination MAC address B) OR (source MAC address B and destination MAC address A).
- For AsrcorAdst mode, you can only configure one port as the monitor port, source/destination MAC address A. (monitoring traffic with source OR destination MAC address A).
- For ManytoOneRx, you can only configure one port as the monitor port and up to the rest of the ports as mirrored ports. (monitoring traffic received by all mirrored ports).
- For ManytoOneTx, you can only configure one port as the monitor port and up to the rest of the ports as mirrored ports. (monitoring traffic transmitted by all mirrored ports).
- For ManytoOneRxTx, you can only configure one port as the monitor port and up to the rest of the ports as mirrored ports. (monitoring traffic transmitted AND received by all mirrored ports).

You can observe and analyze packet traffic at the mirroring port using a network analyzer. A copy of the packet can be captured and analyzed. Unlike other methods that are used to analyze packet traffic, the packet traffic is uninterrupted and packets flow normally through the mirrored port.

Port Mirroring Commands

See Configuring System Monitoring on Ethernet Routing Switch 4900 and 5900 Series for port mirroring command information.

Use the port mirroring commands to assist in diagnostics and information gathering.

RSPAN

Remote Switch Port ANalyzer (RSPAN), also known as Remote Port Mirroring, enhances port mirroring by enabling mirrored traffic to be sent to one or more switches or stacks on the network using an intermediate VLAN for forwarding the mirrored traffic.

Considerations

- Switches must support RSPAN VLAN configuration and flood traffic within that VLAN as specified by the characteristics of an RSPAN VLAN.
- The RSPAN VLAN carries port mirroring and SPAN traffic between RSPAN source and destination sessions. All traffic in the RSPAN VLAN is flooded and no MAC address learning occurs on the RSPAN VLAN.
- RSPAN traffic might be terminated on a switch supporting RSPAN.

- The maximum number of RSPAN vlans on a DUT is four
- Configure up to four RSPAN destination instances.
- You cannot use the same vlan or the same interface in another RSPAN instance.

Configuring ports

Install filters to enable port mirroring/ RSPAN source for MAC base modes (Asrc, Adst, AsrcBdst, AsrcBdstOrBsrcAdst, AsrcOrAdst) and port based modes (XrxYtx, XrxYtxOrYrxXtx) port-mirroring. If platform resource limits are reached, the application may not function in these modes. RSPAN only works for unicast traffic for port based modes.

Broadcast/Multicast/UUC traffic does not use hardware filters, it uses a group of workarounds that must be removed in order for RSPAN to work.

Note:

Port-mirroring shows incorrect source/dest mac for routed layer 3 traffic because mirroring is the last operation performed by the ASIC (after routing).

You cannot configure a port under the following conditions:

- A port has 802.1X enabled as an RSPAN destination port
- A port is a member of MLT/DMLT/LAG as an RSPAN destination port
- A port cannot be configured as an RSPAN destination or Mirror To Port (MTP) if it is an RSPAN source / mirrored port for another instance.
- You cannot configure allow-traffic option and RSPAN because the port must be in a enabled and disabled state at the same time.

VLAN considerations

- If a RSPAN VLAN is used in a PMT RSPAN instance, it cannot be deleted. The RSPAN instance must be deleted first.
- RSPAN destination port cannot be removed from the RSPAN VLAN while involved in the RSPAN instance.
- RSPAN destination port membership cannot be changed unless the instance is deleted first.
- A SPBM B-VLAN or spbm-switchedUni VLAN can not be a RSPAN VLAN.
- A RSPAN VLAN cannot be set as a management VLAN.
- Mapping of an RSPAN VLAN over an SPB ISID and transport over an SPB cloud is not supported.

RSPAN Commands

Use the RSPAN commands to assist in diagnostics and information gathering.

See Configuring System Monitoring on Ethernet Routing Switch 4900 and 5900 Series for RSPAN command information.

Port Statistics

Use port statistics commands to display information about received and transmitted packets at the ports. The ingress and egress counts occur at the MAC layer. Count updates occur once every second.

For more information regarding port statistics and commands, see Configuring System Monitoring on Ethernet Routing Switch 4900 and 5900 Series.

Stack Loopback Testing

The stack loopback tests help you determine if the cause of your stacking problem is a bad stack cable or a damaged stack port.

There are two types of stack loopback tests: internal loopback test and external loopback test. The purpose of the internal loopback test is to verify that the stack ports are functional in each switch. The purpose of the external loopback test is to verify that the stack cables are functional.

For accurate results, the internal loopback test must be run before the external loopback test. The stack loopback tests can only be performed on a standalone unit with no traffic running on the unit.

To run the test, first use the **`stack loopback-test internal`** command. To perform the external loopback test, connect the stack uplink port with the stack downlink port. Use the **`stack loopback-test external`** command.

For more detail regarding stack loopback testing, see Configuring System Monitoring on Ethernet Routing Switch 4900 and 5900 Series.

Stack Health Check

Use this feature to run a high-level test to confirm stack operation and stack continuity. The stack health check results give you information about the stacking state of the rear ports of each switch, confirm the total number of switching units in the stack, confirm the number of stacking cables used, and indicate which unit acts as base.

Use CLI and Web-based management to inquire about the stack health status. This feature is not available for standalone switching units.

For detailed information about stack health check, see Configuring System Monitoring on Ethernet Routing Switch 4900 and 5900 Series.

Stack Forced Mode

The switch might enter Stack Forced Mode (if configured as such) after a stack of two units breaks into one or two standalone switches. The Stack Forced Mode operation allows the standalone device that comes out of a broken stack of two to be managed using the previous stack IP address. After a stack of two fails, you have access to a device without the need of a standalone IP address.

The Stack Forced Mode applies to a standalone switch that was part of a stack of two units. When functioning in this mode, the standalone switch keeps the previous stack IP settings (IP address, netmask, gateway), which allows you to reach the device using an IP connection such as Telnet, Web-based management, or Device Manager.

Stack Forced Mode can be configured for each device, regardless of stack or standalone mode. If the Stack Forced Mode is enabled on a stack, it is enabled on all switches in that stack. However, this mode only becomes active after a stack of two fails and one or both switches become standalone.

There are two scenarios in which the stack might be broken. First, one of the two units, base or non-base unit, has failed due to power interruption or other hardware problem. Second, at least one of the stack cables connecting the two units has failed.

In the case of a one-unit failure, the remaining unit keeps the previous stack IP settings. The remaining unit issues a gratuitous ARP packet after entering Stack Forced Mode in order for other devices on the network to update their ARP cache.

After entering Stack Forced Mode, the device sends an SNMP trap informing the administrator that the switch has entered this mode. The trap information contains the switch IP and MAC addresses, which allows you to know if two devices are using the same IP address. The format for this trap is

`Trap: Device is functioning in Forced Stack Mode – MAC: yy:yy:yy:yy:yy:yy`

. The

`yy:yy:yy:yy:yy:yy`

represents the device MAC address.

A device functions in Stack Forced Mode either until the unit is rebooted or until the unit joins a stack.

The Stack Forced Mode feature is configurable using CLI. The commands in Global Configuration Mode are as follows:

- **`stack forced-mode`** enables Stack Forced Mode
- **`no stack forced-mode`** disables Stack Forced Mode
- **`default stack forced-mode`** sets the Stack Forced Mode to the default setting. The default is disabled.

While in PrivExec mode, you can use the **show stack forced-mode** command. Depending on the configuration and if the device is currently functioning in Stack Forced Mode, the output is one of three options:

1. If the Stack Forced Mode is not configured on the device, the output is:

   ```
   Forced-Stack Mode: Disabled

   Device is not currently running in forced stack mode.
   ```

2. If the Stack Forced Mode is configured on the device, but inactive, the output is:

   ```
   Forced-Stack Mode: Enabled

   Device is not currently running in forced stack mode.
   ```

3. If the Stack Forced Mode is configured on the device, and the device is currently running in Stack Forced Mode, the output is:

   ```
   Forced-Stack Mode: Enabled

   Device is currently running in forced stack mode.
   ```

The following is a series of failure scenarios and the description of the Stack Forced Mode behavior. These scenarios assume the following stack setup:

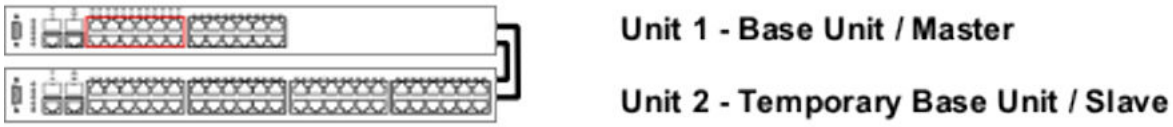


Figure 1: Forced stack mode example setup

In the following scenario, the non-base unit, if functioning in Stack Forced Mode, keeps the previous stack IP address. In this setup it is impossible to keep network connectivity without administrator intervention. Clients connected to the non-base unit lose WAN connectivity.

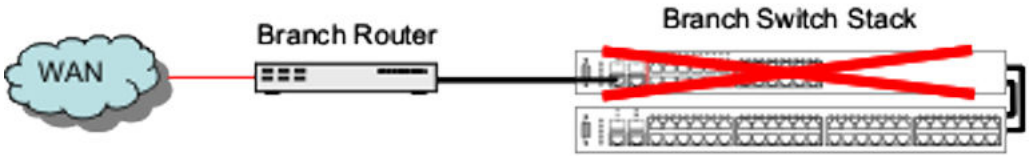


Figure 2: Remote Branch Office - Failure Scenario 1

In the following scenario the non-base unit of a stack of two fails. The previous base unit, if functioning in Stack Forced Mode, keeps the previous stack IP address, and preserves connectivity to the network.

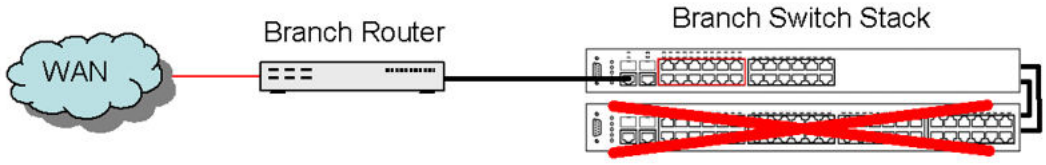


Figure 3: Remote Branch Office - Failure Scenario 2

In the following scenario, while functioning in Stack Forced Mode, both base and non-base units keep using the previous stack IP address. The non-base unit is, however, isolated from the rest of the network. Clients connected to this unit lose WAN connectivity.

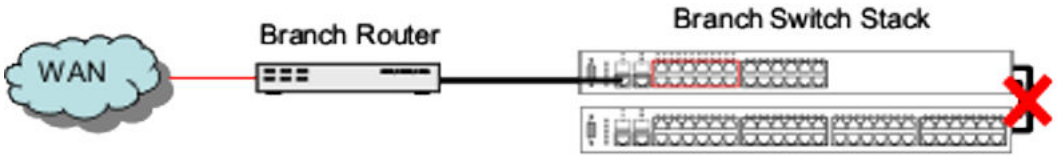


Figure 4: Remote Branch Office – Failure Scenario 3

In the following scenario, the possible failures are identical to Remote Branch Office - Failure Scenarios 1, 2, and 3.

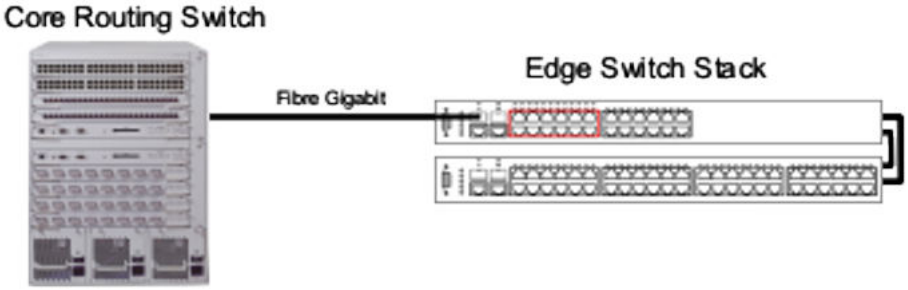


Figure 5: Wiring Closet Deployment 1

In the following scenario, the non-base unit continues to use the stack IP address. A gratuitous ARP is issued by the non-base unit to update ARP caches throughout the network. Clients connected to the non-base unit still have connectivity to the network.

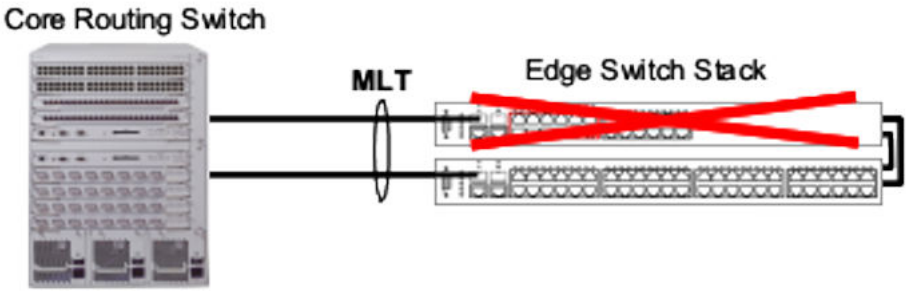


Figure 6: Wiring Closet Deployment 2 – Failure Scenario 1

In the following scenario, the base unit continues to use the stack IP address. It issues an ARP request to update the ARP cache throughout the network. Clients connected to the base unit maintain network connectivity.

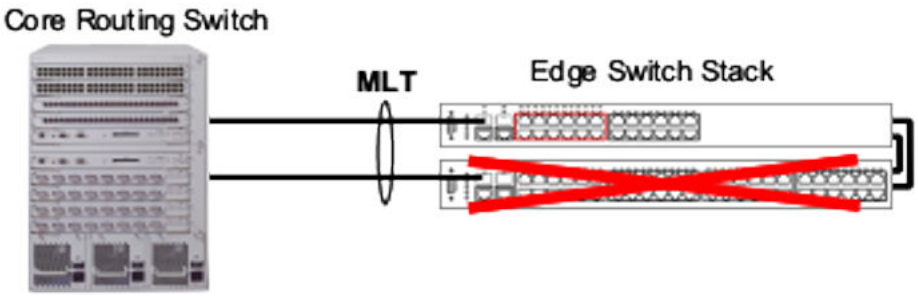


Figure 7: Wiring Closet Deployment 2 – Failure Scenario 2

In the following scenario, if functioning in Stack Forced Mode, both devices use the previous stack IP address. Each device, to detect if the previous stack partner also uses the previous stack IP address, issues an ARP request on that IP address before using it. In the scenario where the stack of two is connected to the router through an MLT, both of these devices continue using the same IP address. If the switch connects to the core routing switch through LACP, the two links are not aggregated and the problem does not arise.

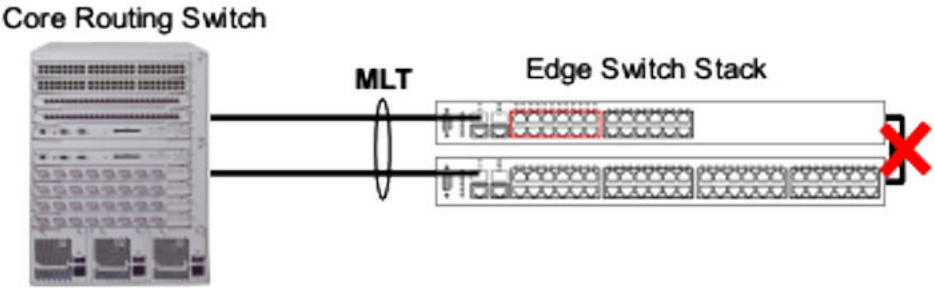


Figure 8: Wiring Closet Deployment 2 – Failure Scenario 3

System Logs

You can use the syslog messaging to manage event messages. The switch syslog software communicates with a server software component named syslogd that resides on your management workstation.

The daemon syslog is a software component that receives and locally logs, displays, prints, or forwards messages that originate from sources that are internal and external to the workstation. For example, syslogd software concurrently handles messages received from applications running on the workstation, as well as messages received from a switch running in a network accessible to the workstation.

For more information about system logging, see Configuring System Monitoring on Ethernet Routing Switch 4900 and 5900 Series.

Syslog messages

Syslog messages for the various states of 802.1X/EAP/NEAP/UBP authentications are introduced to allow more thorough troubleshooting. Logged messages include:

- time of authentication
- MAC authentication success/failure
- IP address associated with MAC authentication
- VLAN and UBP policy assignment

Use the `show logging` command.

```
Switch(config)#sh logging
Type Time                          Idx  Src Message
---- ----------------------------- ---- --- -------
I    00:00:00:15                   1        Web server starts service on port 8
0.
I    00:00:00:17                   2        Successfully loaded configuration files from
block 1
```

Log Messages with Enhanced Secure Mode

Enhanced secure mode allows the system to provide role-based access levels, stronger password requirements, and stronger rules on password length, password complexity, password change intervals, password reuse, and password maximum age use. If you enable enhanced secure mode, the system encrypts the entire log file.

The following actions can be performed when the enhanced secure mode is enabled:

- only individuals in security, emergency and system administrator role can view log files to analyze switch access and configuration activity.
- no user in any access level role can modify log file content.
- default encryption key can be modified only by the security and emergency administrators when they switch to security mode.
- restart or a default boot does not affect the audit log.

Audit file captures the following when the enhanced secure mode enabled:

- identity of each user using the user name, IP and session ID.
- date and time of the access attempts.
- all activities performed on the system.
  - all successful login attempts.
  - invalid user authentication attempt.
  - unauthorized attempts to access system resources.
  - each logout or session termination.
  - all software downloads.

The following table summarizes log file command access based on role-based access levels.

Access level role	Command group	Rights
System security administrator	audit-cmds-group	All show commands for log configurations (show-config).
System administrator	audit-cmds-group	All show commands for log files (show-only).
Application administrator		
Emergency user	audit-cmds-group	All show commands for log configurations (show-config).
All users in all roles	audit-cmds-group	Cannot modify the content of the log files using the following commands: • delete

Backup config file

The backup config file feature is transparent. After writing the configuration file to FLASH, the switch writes to the primary configuration block, updates the CRC16 checksum to the Multi Configuration area, and then saves the same information to the auxiliary configuration block.

After the switch boots, if it detects that the primary configuration file is corrupted (checksum mismatch), it logs a message to the system log. The switch then attempts to load the secondary configuration file if the checksum is correct on the auxiliary configuration block and logs a message to the system log.

If both primary and auxiliary configurations blocks are corrupted, the settings are restored to default and a message is created in the system log.

You can check the system log for messages indicating that a configuration block is corrupted. The following are examples of system logs you may encounter:

- `Error loading primary configuration block <block number>`
- `Error loading backup configuration block <block number>`
- `Backup configuration block <block number> is in use`
- `Configuration files are corrupted. Restored to default`

The following messages are loaded to the engineering log menu:

- `Backup configuration restored from primary configuration block`
- `Backup configuration updated for next active configuration block`

ASCII download log enhancement

The purpose of the ASCII Download Log feature is to log messages for describing the result of the ASCII Configuration File download, especially the failed commands, as informational customer

messages. You can log four hundred customer messages in Dynamic random access memory (DRAM).

The informational messages logged for describing the result of the ASCII Configuration File download are :

- Connection error (ACG_DOWNLOAD_ERROR)—the connection failed and the ASCII configuration file can not be accessed or used. The message contains the cause of the error. The interface you use to start the ASCII file download does not matter. The logged message is the one from CLI. The system logs an ACG_DOWNLOAD_ERROR error message for the following situations:
  - `Transfer Timed Out`
  - `Invalid TFTP Server address`
  - `Configuration failed`
  - `Switch IP not set`
  - `Stack IP not set`
  - `TFTP Server address not set`
  - `Mask not set`
  - `File too large`
  - `Invalid Configuration File`
  - `Invalid Configuration File or File not found`
  - `Error accessing ASCII file, file missing or can’t access USB device`
- Connection error on load on boot (ACG_DOWNLOAD_ERROR_ ON_BOOT)—the connection failed at load on boot and the ASCII Configuration File can not be accessed. The IP and the filename is in the message if you use TFTP server, or the filename if you use USB .The message contains the cause of the error. If the IP number is unknown, the system uses the question mark character (?).
- Success (ACG_DOWNLOAD_OK)—the connection was successful. The ASCII Configuration File can be accessed and it can be used. The IP and the filename is in the message when you use TFTP server , or the filename when you use USB .
- Success on load on boot (ACG_DOWNLOAD_OK_ON_BOOT)—the connection was successful at load on boot. The ASCII Configuration File can be accessed and it can be used. The IP and the filename is in the message if you use a TFTP server usage, or the filename if you use USB .
- Failed command (ACG_CMD_ERR)—a command from the ASCII Configuration File failed. The failed command text line number is in the message. The cause is in the message with the following errors:
  - `Invalid input detected`
  - `Ambiguous command`
  - `Incomplete command`

```
- Permission denied
- Not allowed on slave
```

CPU and Memory Utilization

The CPU utilization provides CPU utilization data for the last 10 seconds, 1 min, 60 minutes, 24 hours, and from system bootup. CPU utilization is provided as a percentage and the information shows how the CPU was loaded for the specific time average.

The memory utilization provides information about what percentage of the dynamic memory is currently used by the system. Also, the memory utilization shows a low watermark percentage that represents the lowest percentage of the dynamic memory available since system bootup.

This feature is supported by both CLI and Web-based management. For more information about the feature, see Configuring System Monitoring on Ethernet Routing Switch 4900 and 5900 Series.

Show commands

The **`show tech`** command has been enhanced to display more information. The show commands that are incorporated include (but are not limited to) the following:

- show cpu-utilization
- show environmental
- show system verbose
- show stack-info uptime
- show system last-exception unit all
- show stack-cable-info
- show stack health
- show ip
- show ip mgmt all
- show ip netstat
- show ipv6 address
- show ipv6 default-gateway
- show ipv6 interface
- show ipv6 route
- show ipv6 neighbor

- show ip vrrp interface verbose
- show ip ospf
- show ip ospf stats
- show ip ospf interface enabled
- show ip ospf neighbor
- show ip ospf ifstats detail
- show ip rip interface
- show lldp neighbor
- show mlt
- show ip igmp interface
- show ip igmp snooping
- show ip igmp group-ext
- show ip igmp group count
- show license
- show vlan
- show vlan interface info
- show vlan ip
- show spanning-tree mode
- show spanning-tree rstp config
- show spanning-tree rstp port
- show interfaces verbose
- show interfaces gbic-info
- show logging
- show telnet sessions
- show ssh session
- show autotopology nmm-table
- show qos diag
- show flash
- show flash history
- show mac-address-table
- show ip route
- show ip arp

- show ip dhcp-relay
- show ip dhcp-relay fwd-path
- show lacp aggr
- show lacp port
- show energy-saver
- show energy-saver schedule
- show energy-saver interface

Address Resolution Protocol

Address Resolution Protocol (ARP) is the method for finding a host's hardware address when only its Network Layer address is known.

Caution:

Every time an IP interface or link goes up, the driver for that interface will typically send a gratuitous ARP to preload the ARP tables of all other local hosts. A gratuitous ARP will tell us that host just has had a link up event, such as a link bounce, a machine just being rebooted or you are just configuring the interface up. If you see multiple gratuitous ARPs from the same host frequently, it can be an indication of bad Ethernet hardware or cabling resulting in frequent link bounces.

Dynamic ARP inspection

ARP provides IP communication within a Layer 2 broadcast domain by mapping an IP address to a MAC address. A malicious user can attack hosts, switches, and routers connected to the Layer 2 network by poisoning the ARP caches of systems connected to the subnet and by intercepting traffic intended for other hosts on the subnet.

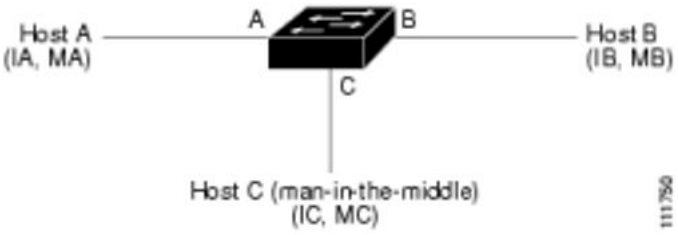


Figure 9: Dynamic ARP inspection

In the preceding figure, hosts A, B, and C are connected to the switch on interfaces A, B, and C, all of which are on the same subnet. Their IP and MAC addresses are shown in parentheses; for example, host A uses IP address IA and MAC address MA. After Host A needs to communicate to

Host B at the IP layer, it broadcasts an ARP request for the MAC address associated with IP address IB. After the switch and Host B receive the ARP request, they populate their ARP caches with an ARP binding for a host with the IP address IA and a MAC address MA. After Host B responds, the switch and Host A populate their ARP caches with a binding for a host with the IP address IB and a MAC address MB.

Host C can poison the ARP caches of the switch (Host A and Host B) by broadcasting forged ARP responses with bindings for a host with an IP address of IA (or IB) and a MAC address of MC. Hosts with poisoned ARP caches use the MAC address MC as the destination MAC address for traffic intended for IA or IB. This means that Host C intercepts that traffic. Because Host C knows the true MAC addresses associated with IA and IB, it can forward the intercepted traffic to those hosts by using the correct MAC address as the destination. Host C has inserted itself into the traffic stream from Host A to Host B, the classic man-in-the-middle attack.

Dynamic ARP inspection is a security feature that validates ARP packets in a network. It intercepts, logs, and discards ARP packets with invalid IP-to-MAC address bindings. This capability protects the network from certain man-in-the-middle attacks.

Dynamic ARP inspection ensures that only valid ARP requests and responses are relayed. The switch performs these activities:

- Intercepts all ARP request and responses on the untrusted ports.
- Verifies that each of these intercepted packets has a valid IP-to-MAC address binding before updating the local ARP cache or before forwarding the packet to the appropriate destination.
- Drops invalid ARP packets.

Dynamic ARP inspection determines the validity of an ARP packet based on valid IP-to-MAC address bindings stored in a trusted database, the DHCP snooping binding database. This database is built by DHCP snooping if DHCP snooping is enabled on the VLANs and on the switch. If the ARP packet is received on a trusted interface, the switch forwards the packet without checks. On untrusted interfaces, the switch forwards the packet only if it is valid.

Dynamic ARP inspection is managed on the base unit. After a new switch joins the stack, the switch receives the Dynamic ARP inspection configuration from the base unit. After a member leaves the stack, all DHCP address bindings associated with the switch are removed.

After a stack merge occurs, all DHCP bindings in the base unit are lost if it is no longer the base unit. With a stack partition, the existing base unit is unchanged, and the bindings belonging to the partitioned switches age out. The new base unit of the partitioned stack begins processing the new incoming DHCP packets

The following CLI commands are used for Dynamic ARP Inspection:

- The **`show ip arp-inspection`** command displays the Dynamic ARP Inspection status.
- The **`ip arp-inspection vlan <VLANID | VLANID range>`** command enables Dynamic ARP Inspection on the specified VLAN or VLANS.
- The **`no ip arp-inspection vlan <VLANID | VLANID range>`** command disables Dynamic ARP inspection for the specified VLAN or VLANS.

MAC Flush

The switch supports MAC Flush. MAC Flush is a direct way to flush out MAC addresses from the MAC table. If the Layer 2 Forwarding Database (FDB) appears corrupted, you can:

- reboot the switch or stack to conduct troubleshooting
- use the MAC Flush command to delete entries in the Layer 2 Forwarding Database
  - individually
  - per port
  - per VLAN
  - across the whole switch

The following CLI commands are used for MAC Flush:

- The **clear mac-address-table** command flushes all MAC addresses from the table.
- The **clear mac-address-table address <H.H.H>** command flushes a single MAC address.
- The **clear mac-address-table interface Ethernet <portlist| ALL>** command flushes all MAC address from a port or list of ports.
- The **clear mac-address-table interface mlt <trunk #>** command flushes all Mac addresses from a given trunk.
- The **clear mac-address-table inteface vlan <vlan #>** command flushes all MAC addresses from a given VLAN.

MLT/DMLT trunk

Enable MLT/DMLT trunk to detect network connectivity issues. The following CLI commands are used for the MLT/DMLT trunk:

- The **show mlt shutdown-ports-on-disable** command is used to verify the MLT status of the trunk.
- The **no mlt shutdown-ports-on-disable enable** command is used to disable member links of the MLT/DMLT trunk. All member links are disable with the exception of the DFL link. This command can be used when you need to perform MTL/DMLT work on the switch.
- The **mlt shutdown-ports-on-disable enalbe** command is used to enable member links of the MLT/DMLT trunk. By having the switch automatically enable all member links in a trunk at once, you significantly reduce the risk of introducing loops and other problems into the network. To ensure that MLT is fully functional and that all links are enabled, you should use the MLT enable command.

SNMP traps for DHCP Snooping, Dynamic ARP Inspection, and IP Source Guard

The switch generates SNMP traps for the following:

- DHCP Snooping
- IP Source Guard
- Dynamic ARP Inspection

The switch generates the following additional trap notifications:

- `send_bsaiArpPacketDroppedOnUntrustedPort_trap`

  - generated when there is an invalid IP/MAC binding

- `send_bsSourceGuardReachedMaxIpEntries_trap`

  - generated when the maximum number of IP entries on a port has been reached

- `send_bsSourceGuardCannotEnablePort_trap`

  - generated when there are insufficient resources available to enable IP source guard checking on a port

- `send_bsDhcpSnoopingBindingTableFull_trap`

  - generated when an attempt is made to add a new DHCP binding entry when the binding table is full

- `send_bsDhcpSnoopingTrap_trap`

  - generated when a DHCP packet is dropped. The following are events which cause a DHCP packet to be dropped:

    - DHCP REQUEST dropped on untrusted port due to Source MAC address not matching DHCP client MAC address.
    - DHCP RELEASE/DECLINE dropped on untrusted port because MAC address is associated to port in DHCP binding table.
    - DHCP REPLY packet dropped with MAC address and IP lease because no corresponding DHCP request was received.
    - DHCP OFFER dropped on untrusted port.
    - DHCP ACK dropped on untrusted port.
    - DHCP NAK dropped on untrusted port.
    - DHCP RELEASEQUERY dropped on untrusted port.

In order to enable or disable SNMP traps, you must enter Global Configuration mode for the switch. The CLI commands for SNMP traps for DHCP Snooping, Dynamic ARP Inspection, and IP Source Guard are:

- **`snmp-server notification-control`** <WORD> - enables the designated trap

- **no snmp-server notification-control** <WORD> - disables the designated trap
- **default snmp-server notification-control** <WORD> - sets designated trap to its defaults
- **show snmp-server notification-control** <WORD> - produces a list of traps and shows whether they are enabled or disabled

<WORD> is one of the following SNMP trap descriptions:

- bsDhcpSnoopingBindingTableFull
- bsDhcpSnoopingTrap
- bsaiArpPacketDroppedOnUntrustedPort
- bsSourceGuardReachedMaxIpEntries
- bsSourceGuardCannotEnablePort

If you enable SNMP traps for DHCP Snooping, Dynamic ARP Inspection, or IP Source Guard, but the switch fails to generate the traps, ensure you have configured the following settings for the respective feature:

- You must globally enable DHCP.
- You must enable ARP Inspection for the management VLAN.
- You must enable IP Source Guard on all ports for which you require the switch to generate SNMP traps.

Dynamic Host Configuration Protocol (DHCP) relay

DHCP and DHCP relay errors are often on the client-side of the communication. In the situation where the DHCP server is not on the same subnet as the client, the DHCP relay configuration may be at fault. If the DHCP snooping application is enabled, then problems may occur if this is improperly configured. For example, the ports that provide connection to the network core or DHCP server are not set as trusted for DHCP snooping.

Auto Unit Replacement

Enable Auto Unit Replacement (AUR) to replace a failed device in a stack.

AUR allows you to replace a failed unit in a stack with a new unit while retaining the configuration of the previous unit. The stack power must be on during unit replacement.

If the model of the replaced unit is different from the previous unit, the unit is allowed to join the stack. However, the configuration of the previous unit cannot be replicated in the new unit.

AUR can be enabled or disabled from CLI and EDM. By default, AUR is enabled.

You can remove entries from the Automatic Unit Replacement (AUR) cache. You can remove the MAC address for a non-operational stack switch from the AUR address cache. A non-operational switch is a unit that is not present in the stack or is in an unknown restore state. Also, you can display MAC address and operational status information for all switches in a stack.

When you remove the MAC address for a non-operational stack switch from the AUR address cache, information about switch hardware type and configuration is maintained on the base unit switch. When the same non-operational switch or a replacement unit is inserted into the stack, AUR performs a hardware type match, and because the switch MAC address was erased, AUR is performed on the inserted switch.

If you attempt to remove the MAC address for an operational switch from the AUR address cache, the base unit switch displays an error message, and the MAC address is not removed.

For more information about AUR, see Configuring System Monitoring on Ethernet Routing Switch 4900 and 5900 Series.

Diagnostic Auto Unit Replacement

Diagnostic Auto Unit Replacement (DAUR) is an AUR enhancement, which enables the switch to update the diagnostic image of the non-base unit with the diagnostic image saved in the base unit of a stack. You must enable AAUR on the stack first.

DAUR updates the diagnostic image on added units in the same way that AAUR updates the agent software.

In an AAUR-enabled stack, the DAUR process starts if a unit with a different diagnostic image is connected to the stack. This process updates all the units in the stack.

When you enable or disable AAUR, you also enable or disable DAUR. There are no commands to separately enable or disable DAUR.

The log file displays the following messages when DAUR completes successfully:

```
I 2 00:02:01:20 18 DAUR - Info: Receive request for diag image, start
transfer

I 2 00:02:01:22 19 DAUR - Info: Diag transfer finished
```

Multicast behavior

IGMP snooping is a technique whereby the switch selectively forwards multicast traffic only onto ports where particular IP multicast streams are expected. The switch can identify those ports by snooping for IGMP communication between routers and hosts.

When IGMP snooping is enabled on a VLAN, the switch treats all multicast IP streams as known multicast, therefore either dropping or sending the streams to host if requested. If a client requests a specific stream, the switch sends the stream only to that client.

With no IGMP snooping configuration, multicast traffic is treated as broadcast.

Multicast VLAN Registration

Multicast VLAN Registration (MVR) is a mechanism that operates across VLANs within a Layer 2 device to improve network performance by eliminating the unnecessary duplication of multicast packets. MVR enhances the existing IGMP infrastructure to maintain the mapping between ports and multicast MAC addresses by analyzing received IGMP messages with the configured MVR group address ranges and forwards the IPv4 multicast traffic across VLANs based on these mappings.

In the IGMP protocol packet IP header, MVR replaces source IP address with the VLAN IP address of the MVR source VLAN. This is assigned prior to forwarding the packet to the upstream multicast router.

When MVR device is connected to a SPBM Multicast environment, IP address must not be assigned on MVR source VLAN. But, when MVR device is connected to a PIM environment, IP address must be assigned on MVR source VLAN.

MVR operates independently of IGMP Snooping so the same VLAN can be enabled for IGMP Snooping and MVR receiver VLAN. However, this is not the case for the MVR source VLAN, as this VLAN should be solely dedicated for the transmission of multicast streams for purpose of MVR bridging. The MVR group ranges define the multicast groups that are distributed under MVR. Multicast groups that fall outside the MVR group ranges operate under IGMP Snooping.

IPv6

IPv6 provides dual-stack configuration that allows both IPv4 and IPv6 protocol stacks to run simultaneously.

Running IPv6 is optional. The IPv6 interface must be enabled on the management VLAN and IPv6 globally enabled on the IPv6 stack.

You can assign a maximum of one IPv6 global unicast address to the interface. The link-local IPv6 address for the interface is automatically configured by the system, but you must configure the default gateway.

The IPv6 protocol runs on the base unit in a stack. The CLI commands must be issued from the base unit console.

The Neighbor Cache replaces the IPv4 ARP cache because ICMPv6-based Neighbor Discovery replaces ARP.

For detailed information about IPv6, see Configuring System Monitoring on Ethernet Routing Switch 4900 and 5900 Series.

Light Emitting Diode (LED) Display

The switch displays diagnostic and operation information through the LEDs on the unit. Familiarize yourself with the interpretation of the LEDs on the device. See the technical document Installing Ethernet Routing Switch 4900 Series or Installing Ethernet Routing Switch 5900 Series for detailed information regarding the interpretation of the LEDs.

Timestamp in show command outputs

The output for all CLI show commands includes a timestamp header to indicate when the command output was generated. This information can be helpful when communicating with Support.

The following command output shows a timestamp example.

```
Switch#show stack-info

================================================================================
        Command Execution Time: 2019-05-15 12:30:52 GMT+00:00
================================================================================
Unit# Switch Model     Pluggable Pluggable Pluggable  Pluggable SW Version
                         Port      Port      Port       Port
----- ---------------- --------- --------- --------- ---------- ----------
1     5928GTS          (25) None (26) None (27) None  (28) None v7.7.0.079
```

Chapter 5: General diagnostic tools

The switch has diagnostic features available through DM, CLI, and Web-based Management. You can use these diagnostic tools to help you troubleshoot operational and configuration issues. You can configure and display files, view and monitor port statistics, trace a route, run loopback and ping tests, test the switch fabric, and view the address resolution table.

This document focuses on using CLI to perform the majority of troubleshooting.

The command line interface is accessed through either a direct console connection to the switch or by using the Telnet or SSH protocols to connect to the switch remotely.

You can use the Web interface in cases where the troubleshooting steps require corroborating information to ensure diagnosis.

CLI Command Modes

CLI command modes provide specific sets of CLI commands. When you log onto the switch, you are in User EXEC mode with limited commands. While in a higher mode, you can access most commands from lower modes, except if they conflict with commands of your current mode.

There are two categories of CLI commands: show commands and configuration commands. Show commands can be used from multiple command modes with the same results; they show the same configuration information regardless of the command mode from which the show command is used. Configuration command results, however, may be dependent on the command mode from which a configuration command is used. For example, an **`enable`** command used in Global Configuration mode will enable a feature globally for all devices, while the same command used from one of the interface command modes will enable a feature for a specific interface only.

Your user authorization credentials determine what commands are available to you in Privileged EXEC mode and all higher level modes. If you have read-only access, you cannot progress beyond User EXEC mode. If you have read-write access, you can progress through all available modes.

The CLI commands for navigating from lower to higher level modes are listed in the following table. To navigate from higher to lower level modes, use the following commands:

- **`exit`** to navigate from a higher level mode to a lower level mode, down to Privileged EXEC mode
- **`end`** from any command mode directly to Privileged EXEC mode

- **disable** to navigate from Privileged EXEC mode to User EXEC mode
- **logout** to terminate the CLI session from any command mode

The following table describes the various command modes, including the CLI commands to access and to exit each mode.

Table 3: CLI command modes

Command mode and sample prompt	Command to access mode	Command to exit mode

User EXEC
`Switch>`
	No entrance command, default mode	`exit`
		or
		`logout`

Privileged EXEC
`Switch#`
	`enable`	`exit`
		or
		`logout`

Global Configuration
`Switch(config)#`
	`configure terminal`	To return to Privileged EXEC mode, enter
		`end`
		or
		`exit`
		To exit CLI completely, enter
		`logout`

Interface Configuration
`Switch(config-if)#`
You can configure the following interfaces:
• Ethernet
• Loopback
• Management
• VLAN
	From Global Configuration mode:
	To configure a port, enter `interface ethernet <port number>`.
	To configure a loopback, enter `interface loopback <loopback number>`.
	To configure a management, enter `interface mgmt <mgmt number>`
	To configure a VLAN, enter `interface vlan <vlan number>`.
		To return to Global Configuration mode, enter
		`Exit`
		To return to Privileged EXEC mode, enter
		`end`
		To exit CLI completely, enter
		`logout`

Router Configuration `Switch(configrouter)#`	From Global or Interface Configuration mode: To configure RIP, enter `router rip`.	To return to Global Configuration mode, enter `exit`.

Table continues…

Command mode and sample prompt	Command to access mode	Command to exit mode
You can configure the following routers: • RIP • OSPF • VRRP • ISIS	To configure OSPF, enter `router ospf`. To configure VRRP, enter `router vrrp`. To configure IS-IS, enter `router isis`.	To return to Privileged EXEC mode, enter `end`. To exit CLI completely, enter `logout`.
Application Configuration `Switch(config-app)`	From Global, Interface or Router Configuration mode, enter `application`.	To return to Global Configuration mode, enter `exit`. To return to Privileged EXEC mode, enter `end`. To exit CLI completely, enter `logout`.
DHCP Guard Configuration `Switch(config-dhcpguard)`	From Global, Interface, Router, Application Configuration mode, enter `ipv6 dhcp guard policy <policy_name>`.	To return to Global Configuration mode, enter `exit`. To return to Privileged EXEC mode, enter `end`. To exit CLI completely, enter `logout`.
RA Guard Configuration `Switch(config-raguard)#`	From Global, Interface, Router, Application Configuration mode, enter `ipv6 nd raguard policy <policy_name>`.	To return to Global Configuration mode, enter `exit`. To return to Privileged EXEC mode, enter `end`. To exit CLI completely, enter `logout`.

Chapter 6: Initial troubleshooting

The types of problems that typically occur with networks involve connectivity and performance. Using the Open System Interconnection (OSI) network architecture layers, and checking each in sequential order, is usually best when troubleshooting. For example, confirm that the physical environment, such as the cables and module connections, is operating without failures before moving up to the network and application layers.

Gather information

Before contacting Technical Support, gather the following information:

- **Default and current configuration of the switch**. To obtain this information, use the **`show running-config`** command.
- **System status**. Obtain this information using the **`show sys-info`** command. Output from the command displays technical information about system status and information about the hardware, software, and switch operation. For more detail, use the **`show tech`** command.
- **Information about past events**. To obtain this information, review the log files using the **`show logging`** command.
- **Information about the FLASH boot image, agent image, or diagnostic image version**. To obtain this information for a single unit or from the base unit, use the **show flash** command. To obtain this information from a specified unit in the stack, use the **show flash unit <1-8>** command.
- The **software version** that is running on the device. To obtain this information, use the **`show sys-info`** or **`show system verbose`** command to display the software version that is running on all devices.
- A **`network topology diagram`**: Get an accurate and detailed topology diagram of your network that shows the nodes and connections. Your planning and engineering function should have this diagram.
- **`Recent changes`**: Find out about recent changes or upgrades to your system, your network, or custom applications (for example, has configuration or code been changed). Get the date and time of the changes, and the names of the persons who made them. Get a list of events that occurred prior to the trouble, such as an upgrade, a LAN change, increased traffic, or installation of new hardware.

- **`Connectivity information`**: To help troubleshoot connectivity problems, you should always provide source and destination IP pairs to facilitate in troubleshooting. Ten pairs is a good rule of thumb (five working pairs and five pairs with connectivity issues). Use the following commands to get connectivity information:
  - **`show tech`**
  - **`show running-config`**
  - **`show port-statistics <port>`**

Chapter 7: Emergency recovery trees

Emergency Recovery Trees (ERT) provide a quick reference for troubleshooting without procedural detail. They are meant to quickly assist you to find a solution for common failures.

Emergency recovery trees

About this task

The following work flow shows the ERTs included in this section. Each ERT describes steps to correct a specific issue; the ERTs are not dependant upon each other.

Procedure

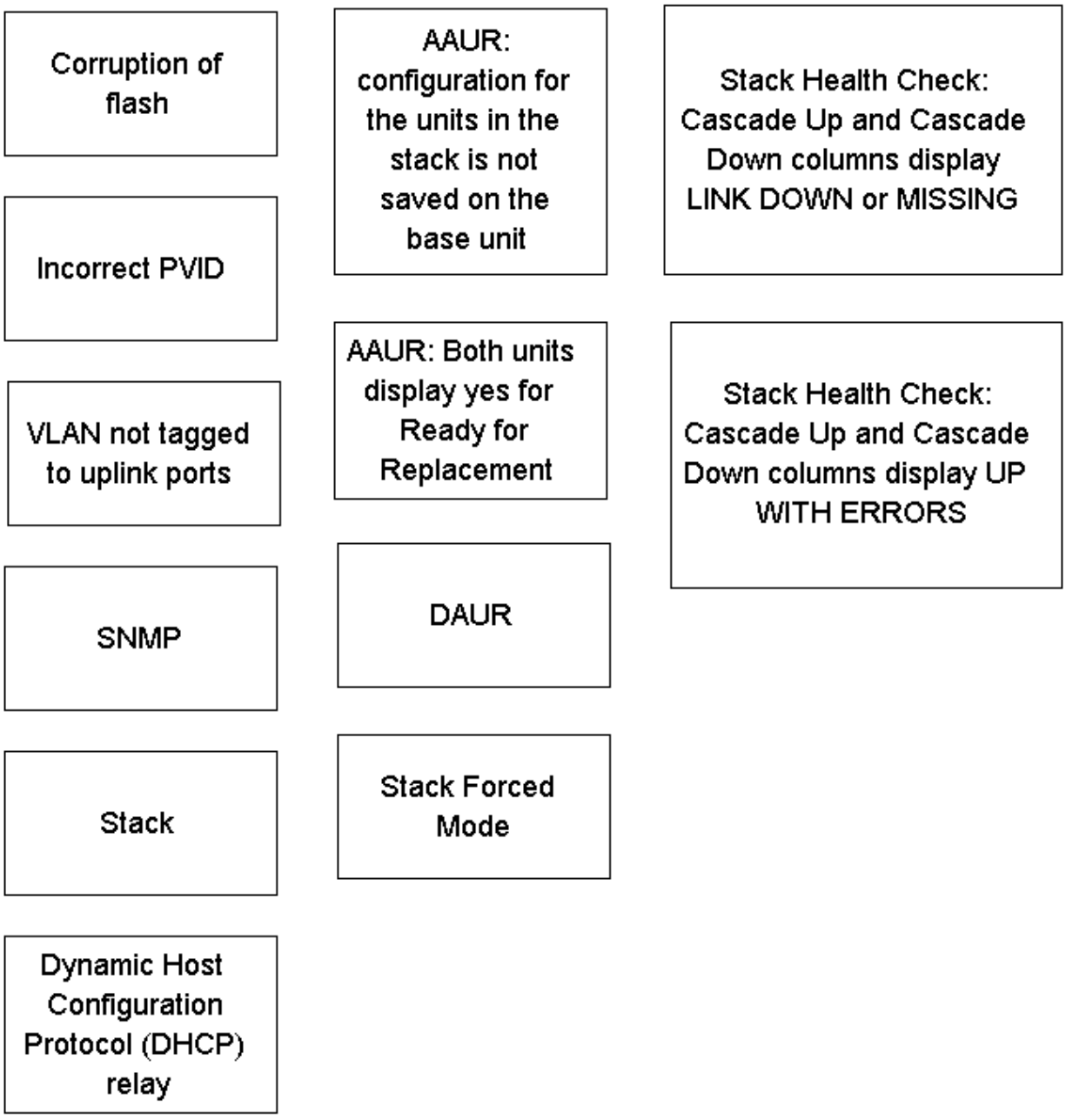


Figure 10: Emergency recovery trees

Corruption of flash

Corruption of the switch configuration file can sometimes occur due to power outage or environmental reasons which can make the configuration of the box corrupt and non-functional. Initializing of the flash is one way to clear a corrupted configuration file and is required before an RMA.

Corruption of flash recovery tree

About this task

The following figure shows the recovery tree for issues related to a corrupted flash.

Procedure

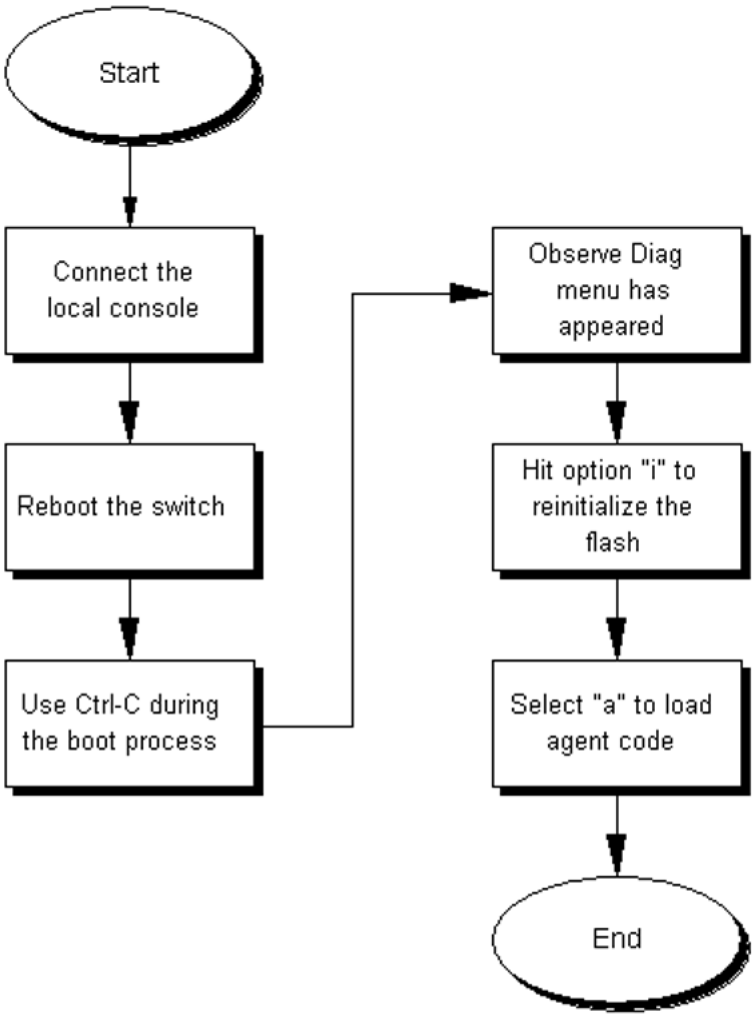


Figure 11: Corruption of flash

Incorrect PVID

An issue can occur where clients cannot communicate to critical servers after their ports are incorrectly put in the wrong VLAN. If the server VLAN is defined as a port based VLAN with a VLAN ID of 3, and the PVID of the port is 2, then loss of communication can occur. This can be verified by checking that the PVID of the ports match the VLAN setting. One way to avoid this problem is to set VLAN configuration control to **`autoPVID`**.

Incorrect PVID recovery tree

About this task

The following figure shows the recovery tree for discovering and correcting issues related to an incorrect PVID.

Procedure

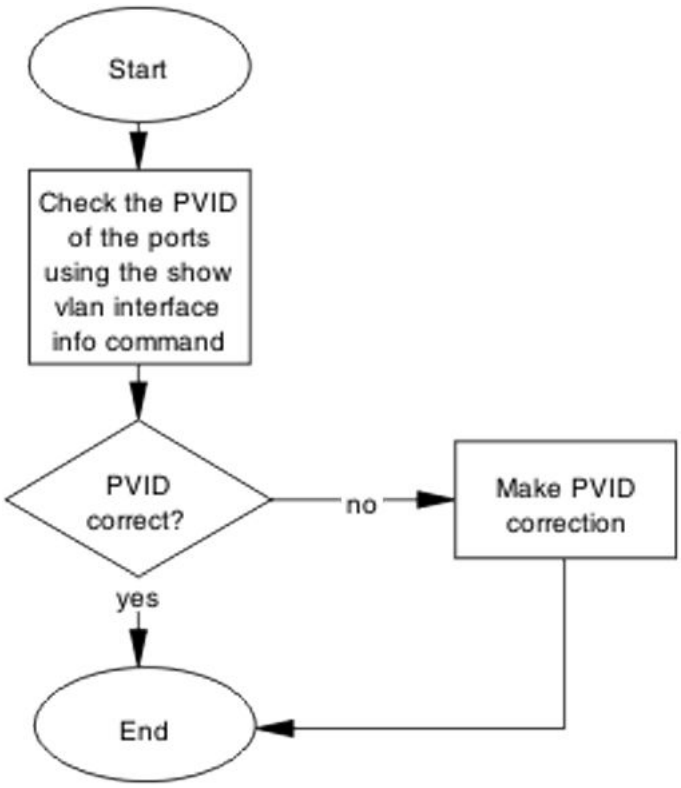


Figure 12: Incorrect PVID

VLAN not tagged to uplink ports

After a ERS 5900 Series switch is connected to an VSP 8600 Series switch and devices in a VLAN on the VSP 8600 Series switch are unable to communicate with devices at the ERS 5900 Series switch in the same VLAN, then it is likely that the uplink ports are not tagged to the VLAN on the ERS 5900 Series switch.

VLAN not tagged to uplink ports recovery tree

About this task

The following figure shows the recovery tree for troubleshooting VLAN communication issues.

Procedure

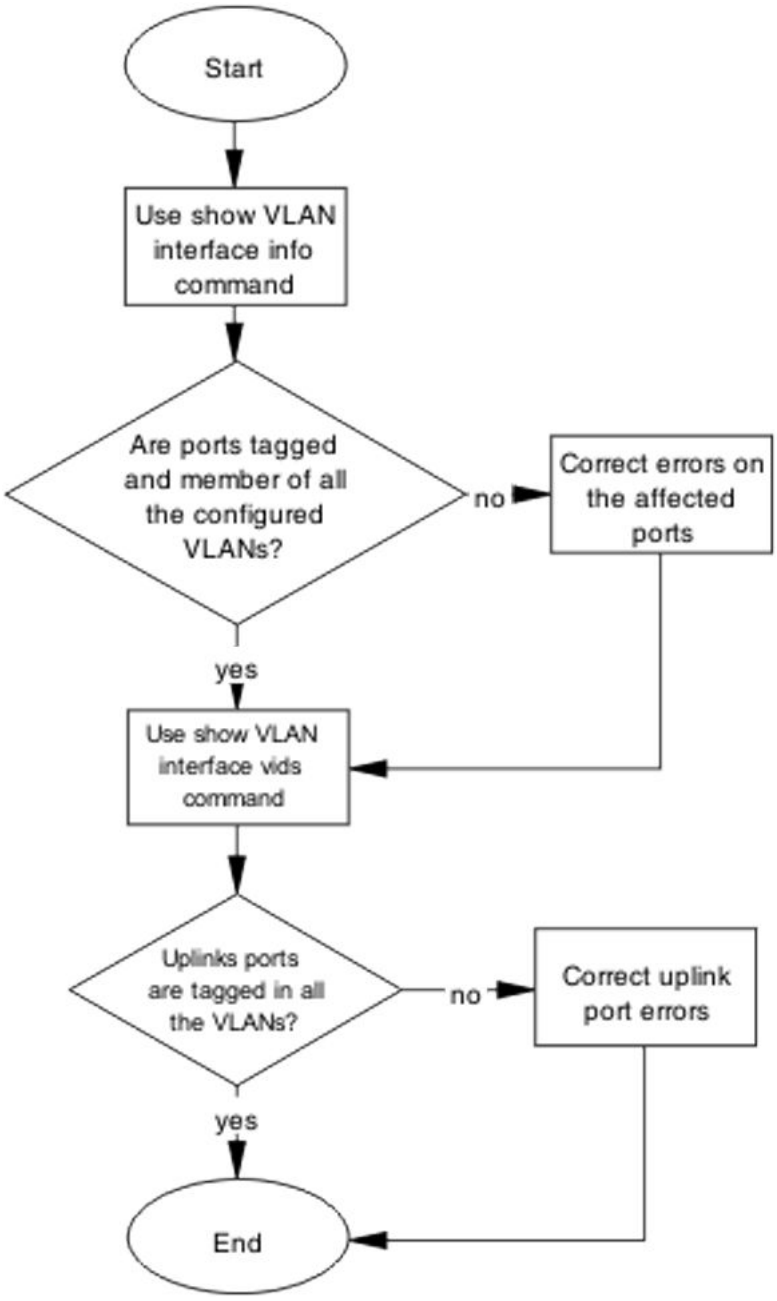


Figure 13: VLAN not tagged to uplink ports

SNMP

SNMP failure may be the result of an incorrect configuration of the management station or its setup. If you can reach a device, but no traps are received, then verify the trap configurations (the trap destination address and the traps configured to be sent).

SNMP recovery tree

About this task

The following figures show the SNMP recovery tree.

Procedure

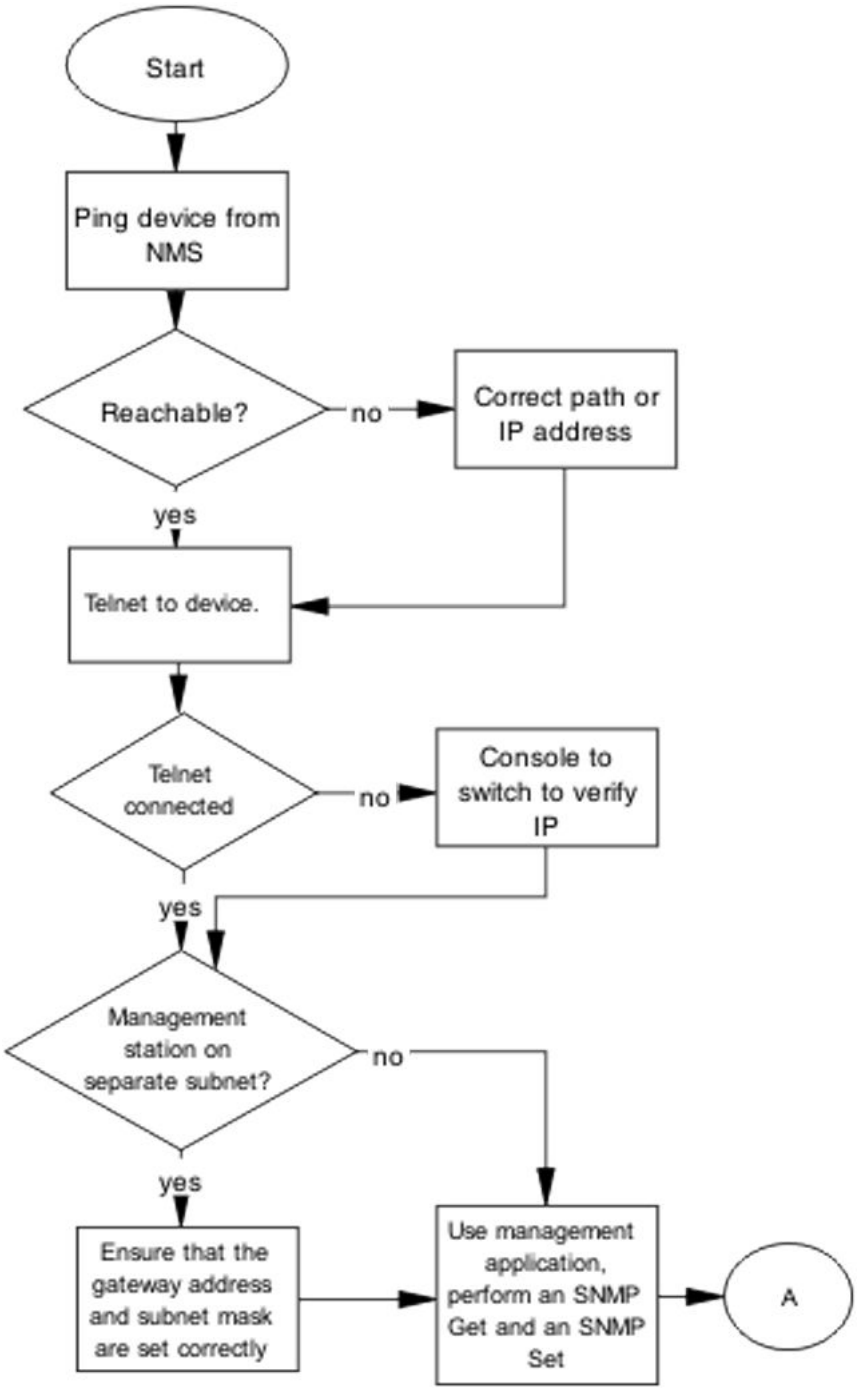


Figure 14: SNMP part 1

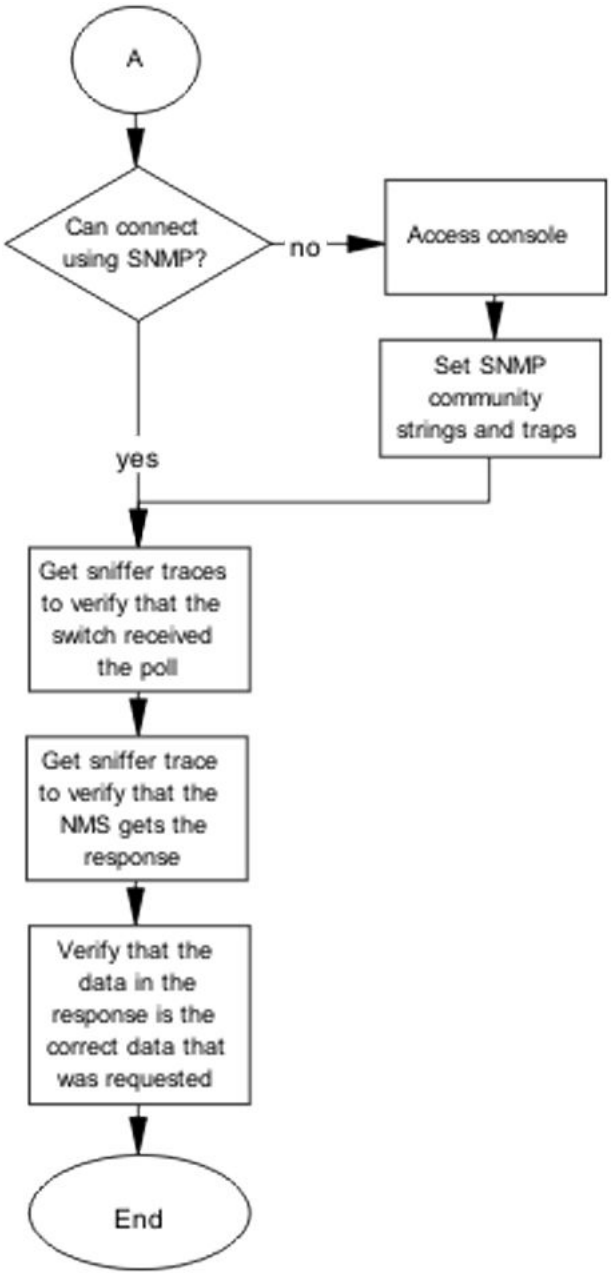


Figure 15: SNMP part 2

Stack

Stack failure can be the result of a communication error between the individual units typically due to stack cabling issues. Failures can also arise after multiple bases are configured.

Several situation may cause stacking problems, for example:

- No units have a base switch set to the on position.
- Multiple units have the base unit set to the on position.
- Incorrect unit has the base unit set to the on position.

Stack recovery tree

About this task

The following figures show the stack recovery tree.

Procedure

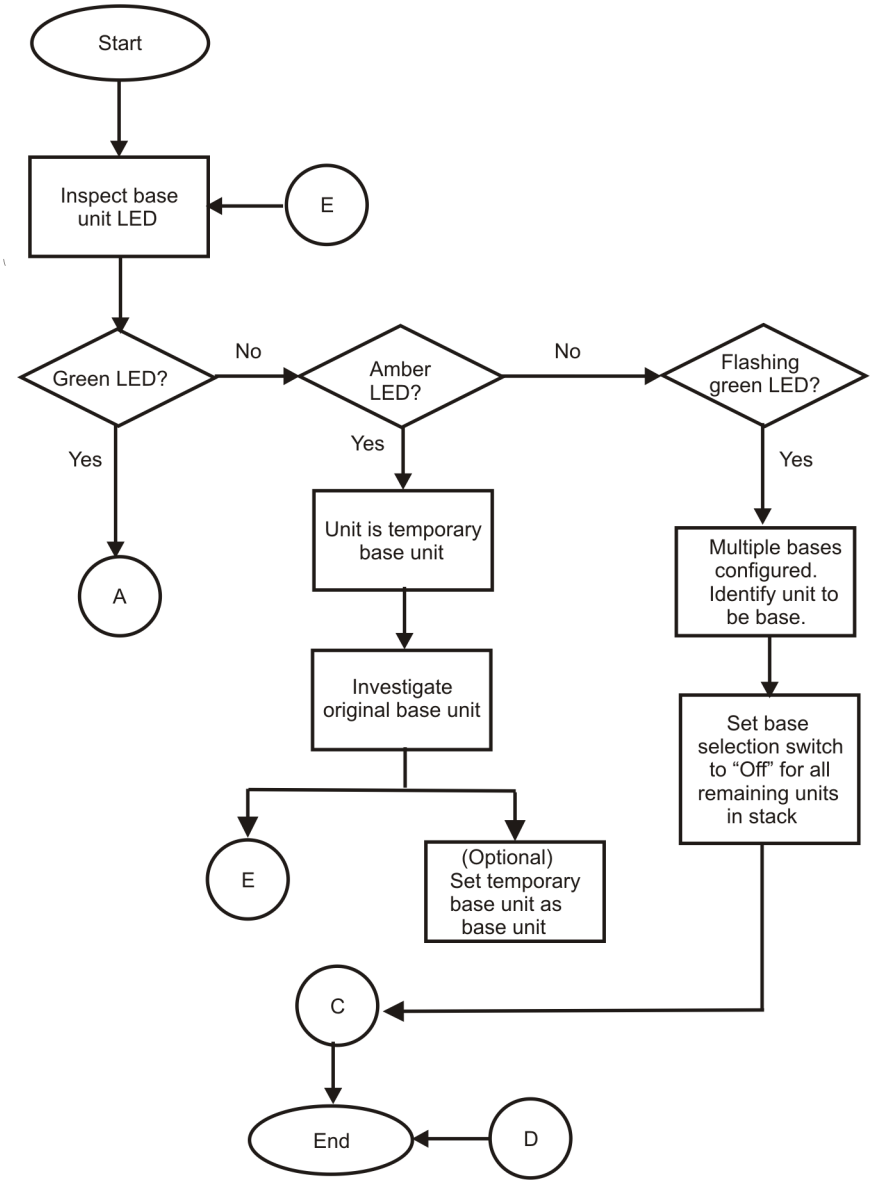


Figure 16: Stack part 1

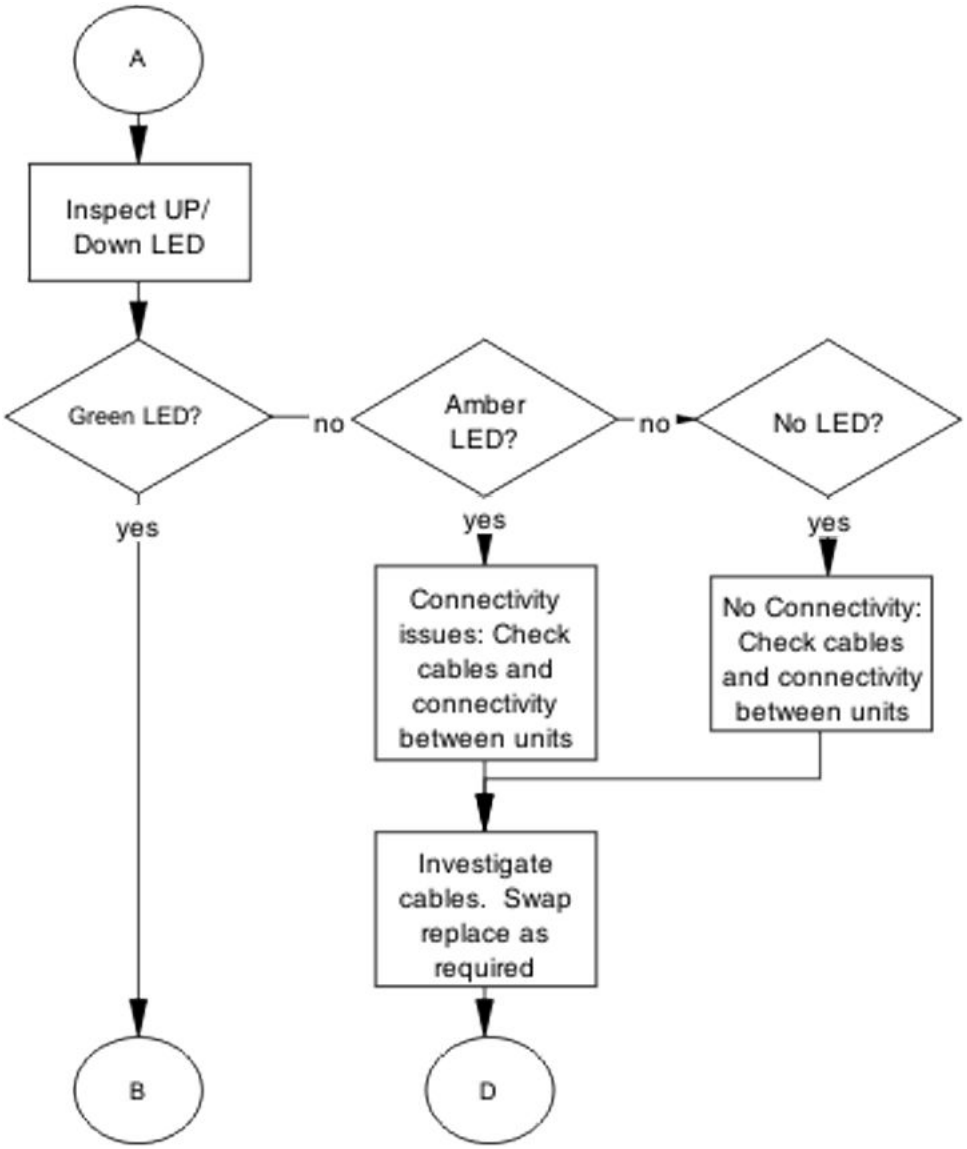


Figure 17: Stack part 2

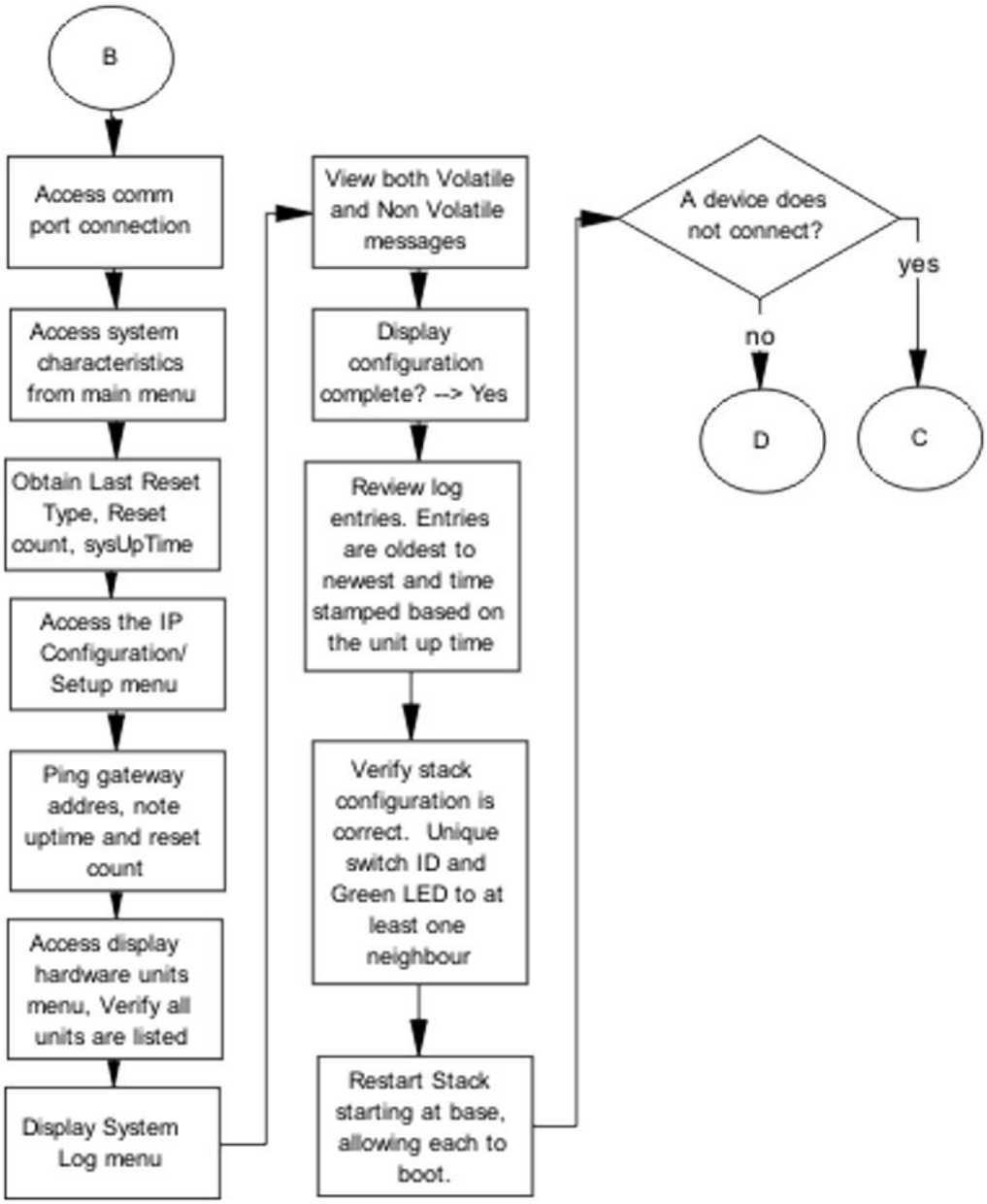


Figure 18: Stack part 3

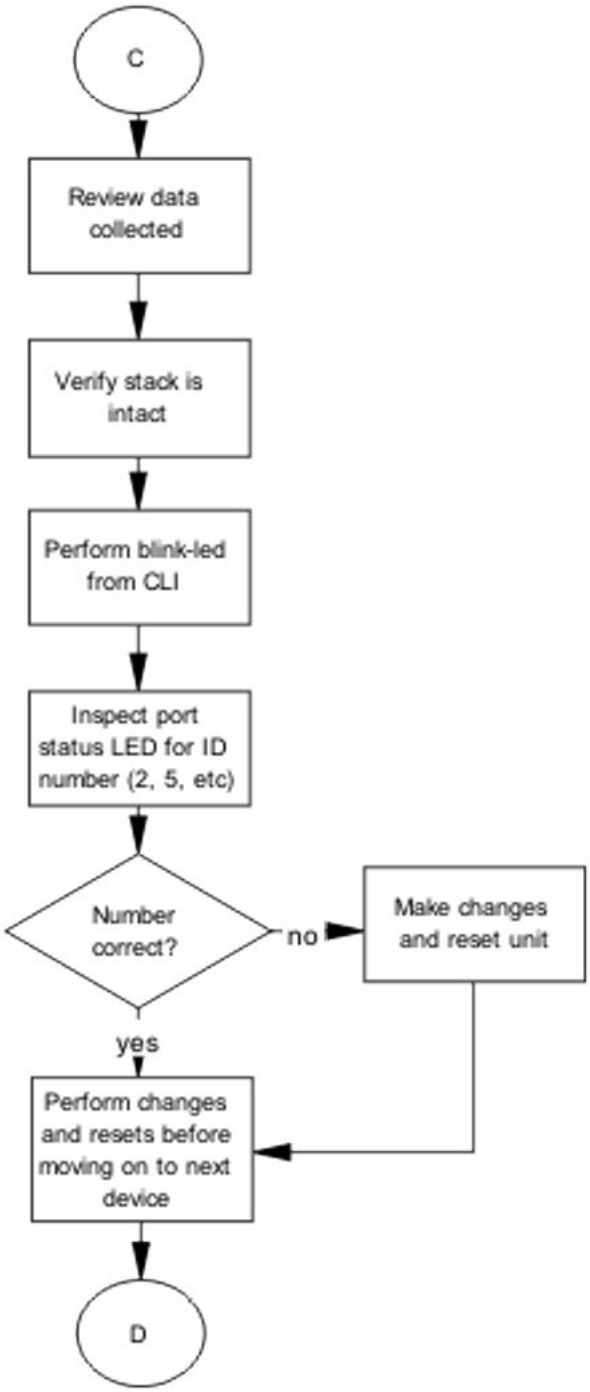


Figure 19: Stack part 4

Dynamic Host Configuration Protocol (DHCP) relay

DHCP and DHCP relay errors are often on the client-side of the communication. In the situation where the DHCP server is not on the same subnet as the client, the DHCP relay configuration may be at fault. If the DHCP snooping application is enabled, then problems may occur if this is improperly configured. For example, the ports that provide connection to the network core or DHCP server are not set as trusted for DHCP snooping.

DHCP recovery tree

About this task

The following figure shows the DHCP relay recovery tree.

Procedure

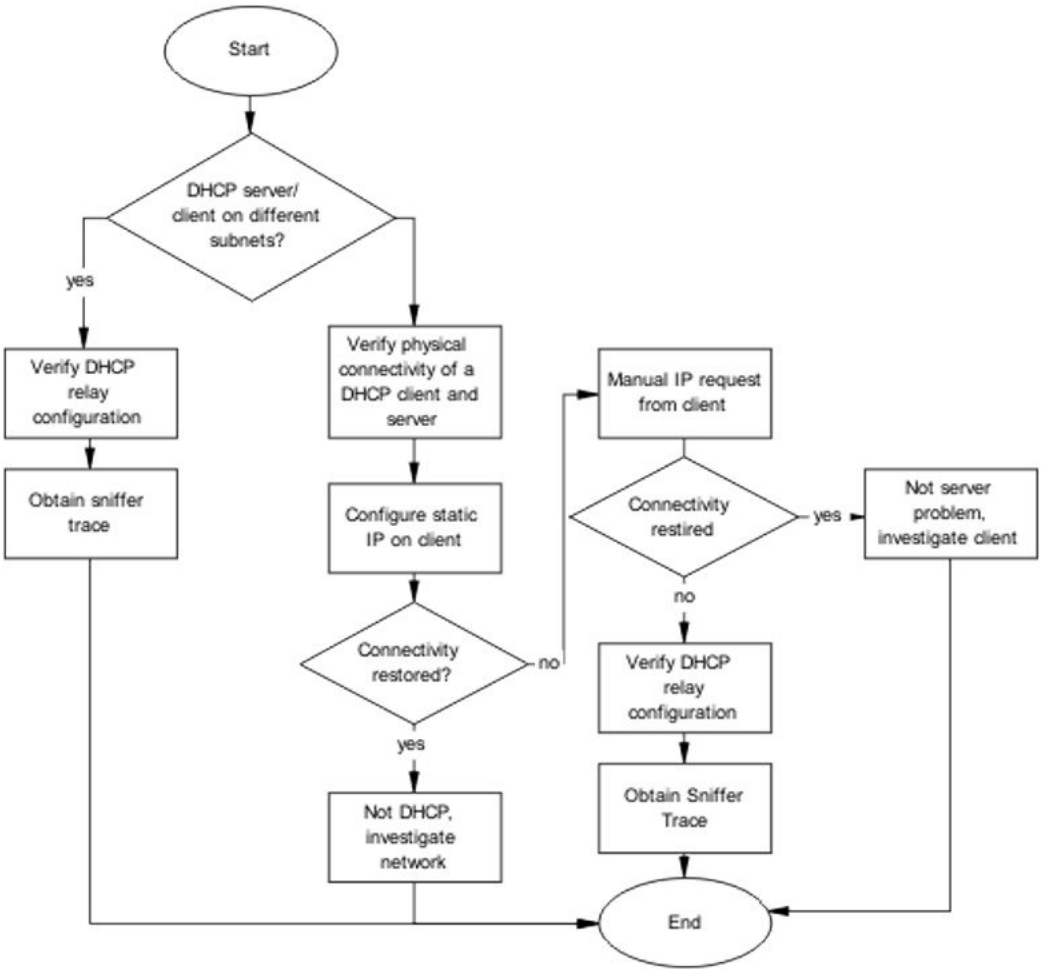


Figure 20: DHCP

AUR: configuration for the units in the stack is not saved on the base unit

Use the recovery tree in this section if configuration for the units in the stack is not saved on the base unit. The typical scenario is that configuration for a unit in a stack is not saved on the base unit because the AUR Auto-Save is disabled. You can manually save the configuration of a non–base unit to the base unit regardless of the state of the AUR feature.

Configuration for the units in the stack is not saved on the base unit recovery tree

About this task

The following figure shows the recovery tree to save configuration for the units in the stack to the base unit. Check that AUR is enabled. If AUR is not enabled, either save the configuration manually or enable AUR.

Procedure

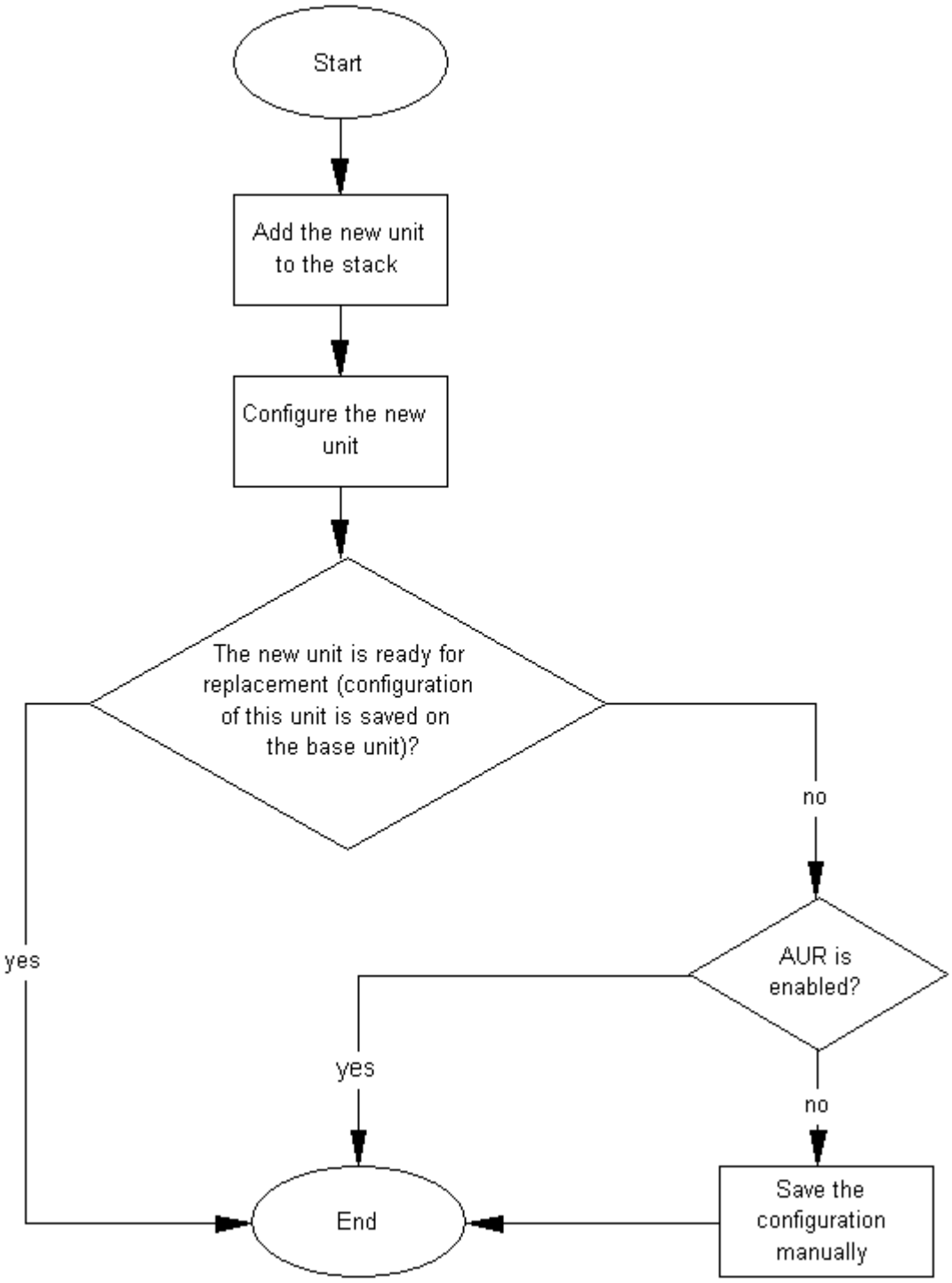


Figure 21: Configuration for the units in the stack is not saved on the base unit

AUR: Both units display yes for Ready for Replacement

Use the recovery tree in this section if both units in a stack of two display "yes" for "Ready for Replacement".

Both units display yes for Ready for Replacement recovery tree

About this task

In a stack of two units, you enter the **`show stack auto-unit-replacement`** command and both units display as ready for replacement (only the non–base unit should be ready for replacement in a stack of two units). The following figure shows the recovery tree to correct the issue.

Procedure

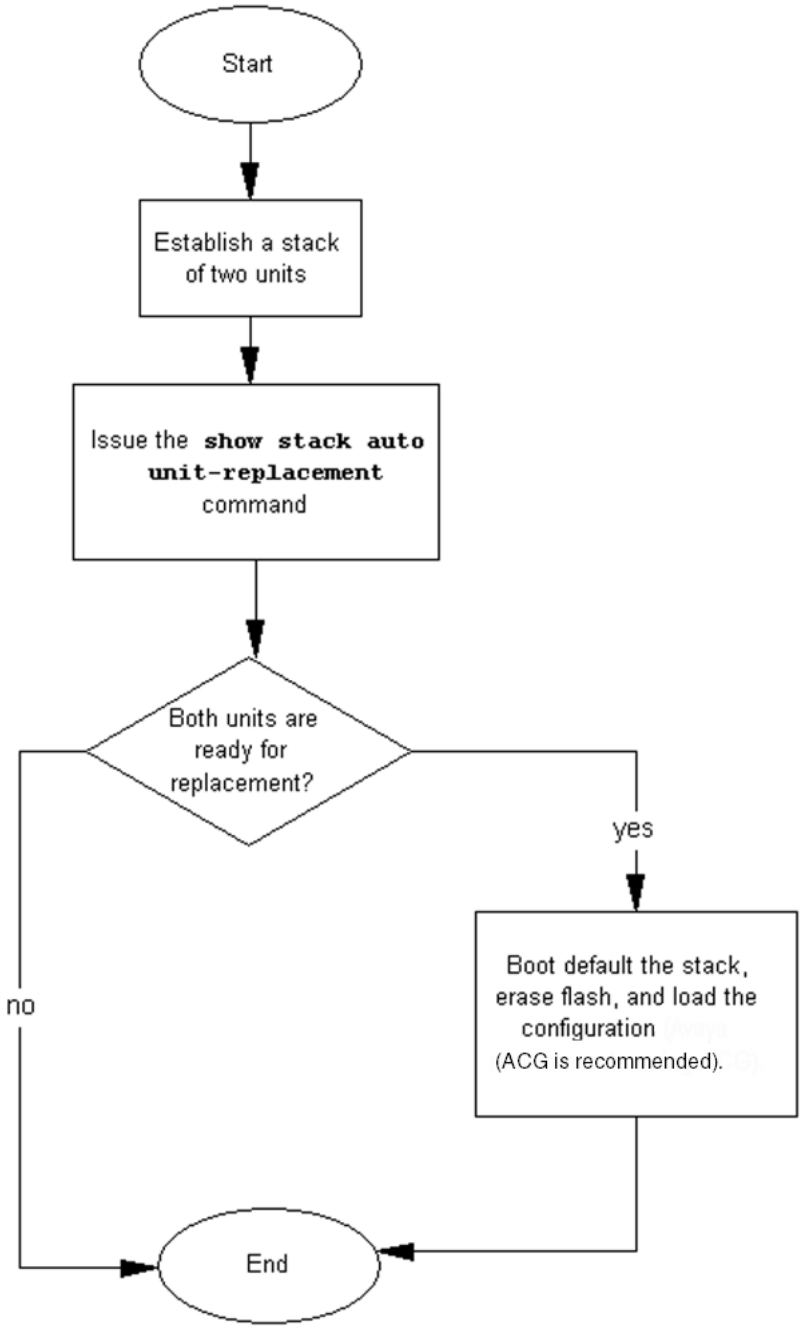


Figure 22: Both units display yes for Ready for Replacement

Stack Forced Mode

If you enable the Stack Forced Mode feature and a stack of two units breaks, the standalone switch that results from that broken stack of two is managed using the previous stack IP address. Use the recovery tree in this section if you cannot access the standalone switch using the stack IP address.

You cannot access a switch at the stack IP address using ping, Telnet, SSH, Web, or DM recovery tree

About this task

If you cannot access a standalone switch in a broken stack of two units, even though you had enabled the Stack Forced Mode feature, check that the standalone device still has a physical connection to the network. The following figure shows the recovery tree for this scenario.

Procedure

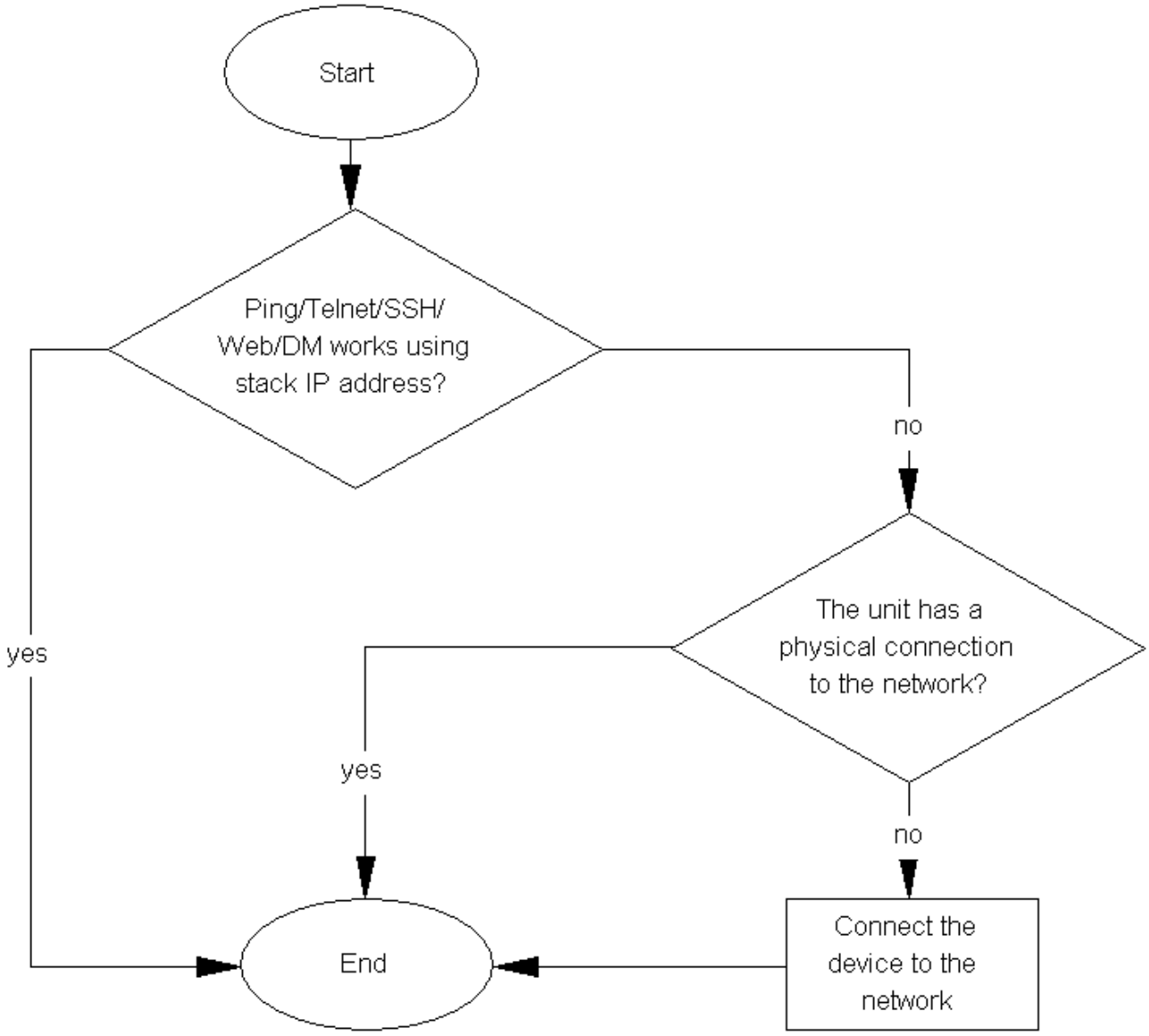


Figure 23: Ping/Telnet/SSH/Web/DM do not work when you use the stack IP address

Stack Health Check: Cascade Up and Cascade Down columns display LINK DOWN or MISSING

Use the recovery tree in this section if the output from the switch displays "LINK DOWN" or "MISSING" in the Cascade Up or Cascade Down columns when you issue the **`show stack health`** command.

Cascade Up and Cascade Down columns display LINK DOWN or MISSING recovery tree

About this task

The following figure shows the recovery tree to use if the output from the switch displays "LINK DOWN" or "MISSING" in the Cascade Up or Cascade Down columns when you issue the show **stack health** command.

Procedure

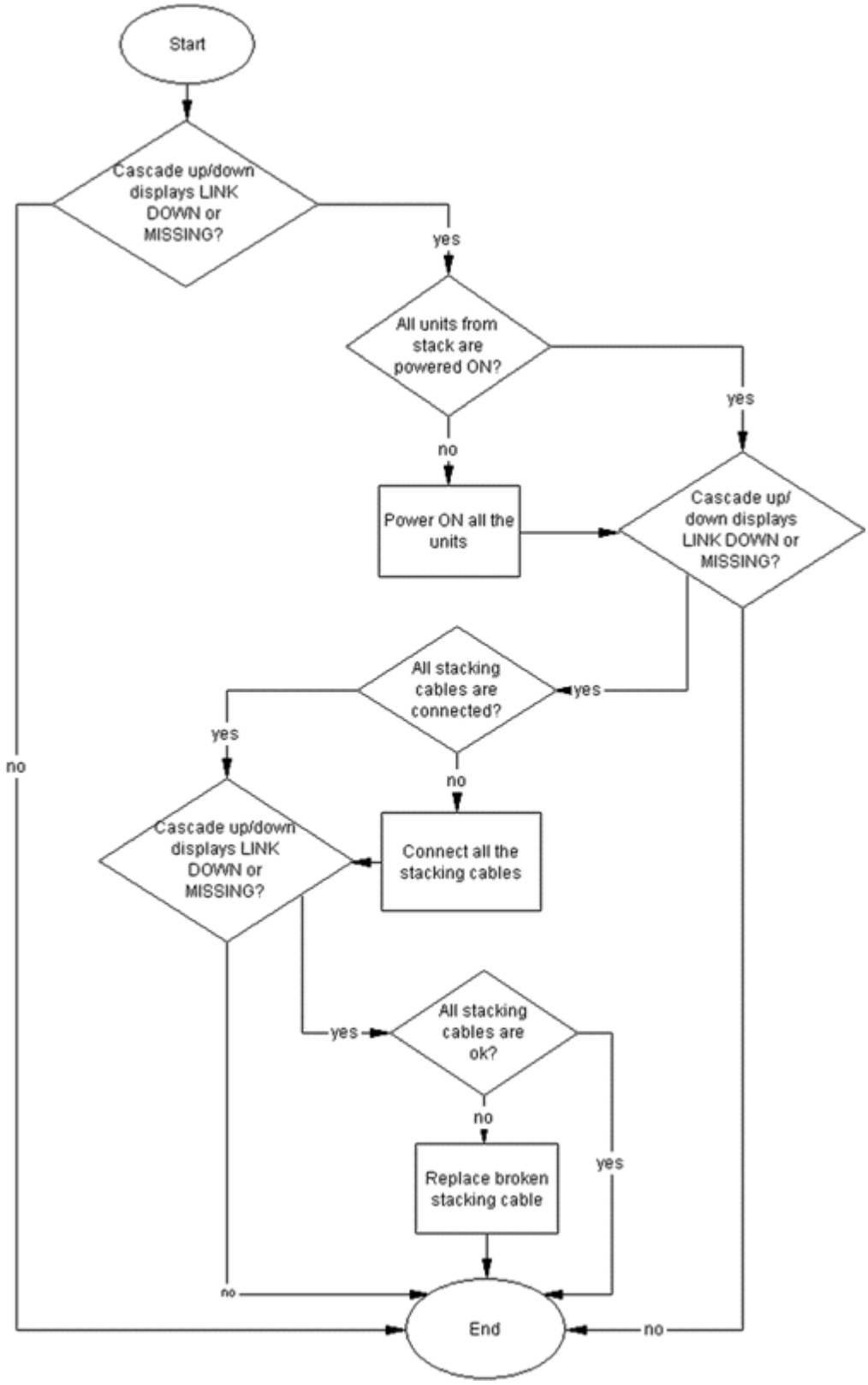


Figure 24: Stack Health Check: Cascade Up and Cascade Down columns display LINK DOWN or

MISSING

Stack Health Check: Cascade Up and Cascade Down columns display UP WITH ERRORS

Use the recovery tree in this section if the switch displays “UP WITH ERRORS” in the Cascade Up and Cascade Down columns when you issue the **`show stack health`** command.

Cascade Up and Cascade Down columns display UP WITH ERRORS recovery tree

About this task

The following figure shows the recovery tree to use if the output from the switch displays "UP WITH ERRORS" in the Cascade Up and Cascade Down columns when you issue the **`show stack health`** command.

Procedure

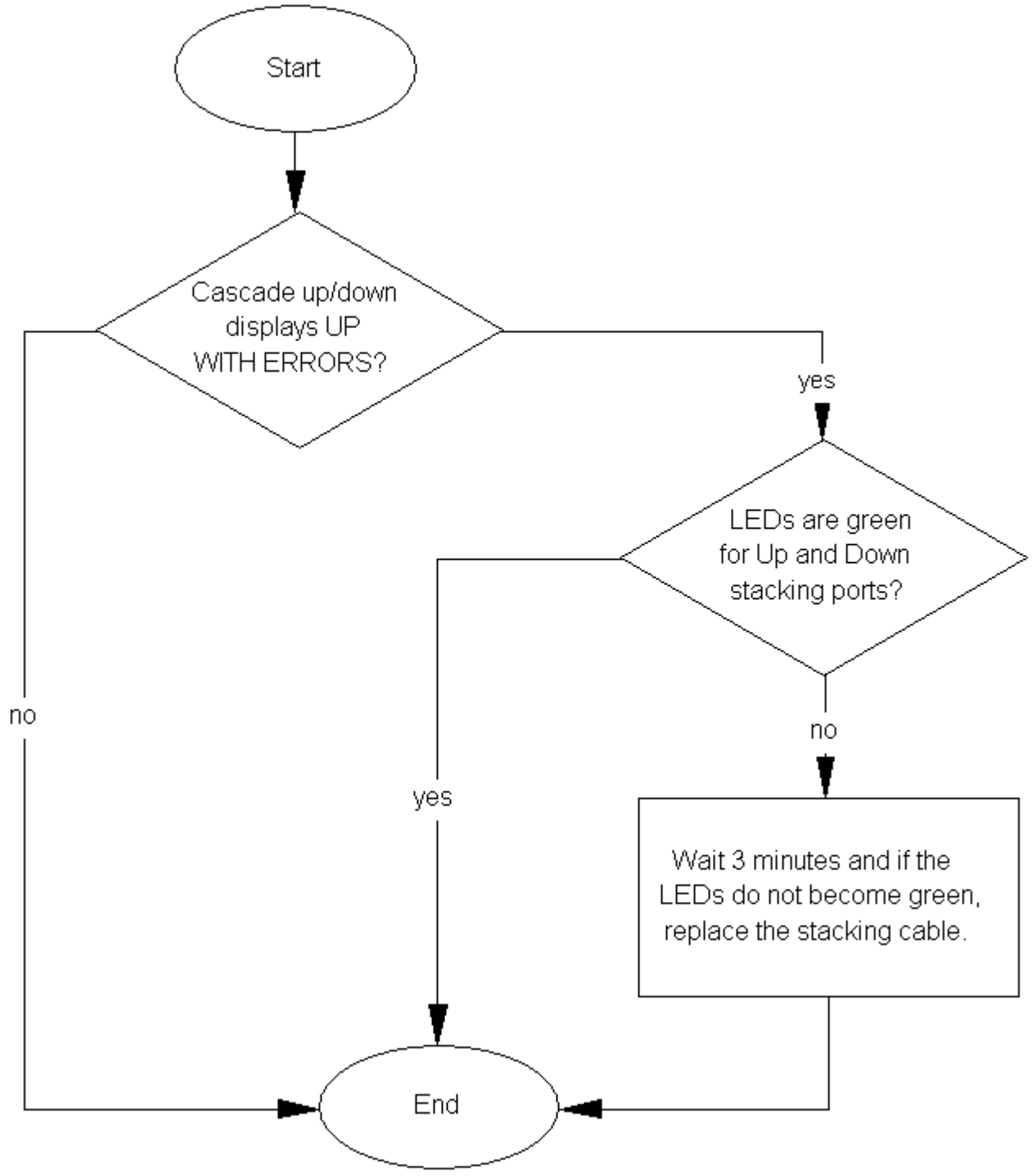


Figure 25: Stack Health Check: Cascade Up and Cascade Down columns display UP WITH ERRORS

Chapter 8: General troubleshooting of hardware

Use this section for hardware troubleshooting.

Work flow: General troubleshooting of hardware

About this task

The following work flow assists you to determine the solution for some common hardware problems.

Procedure

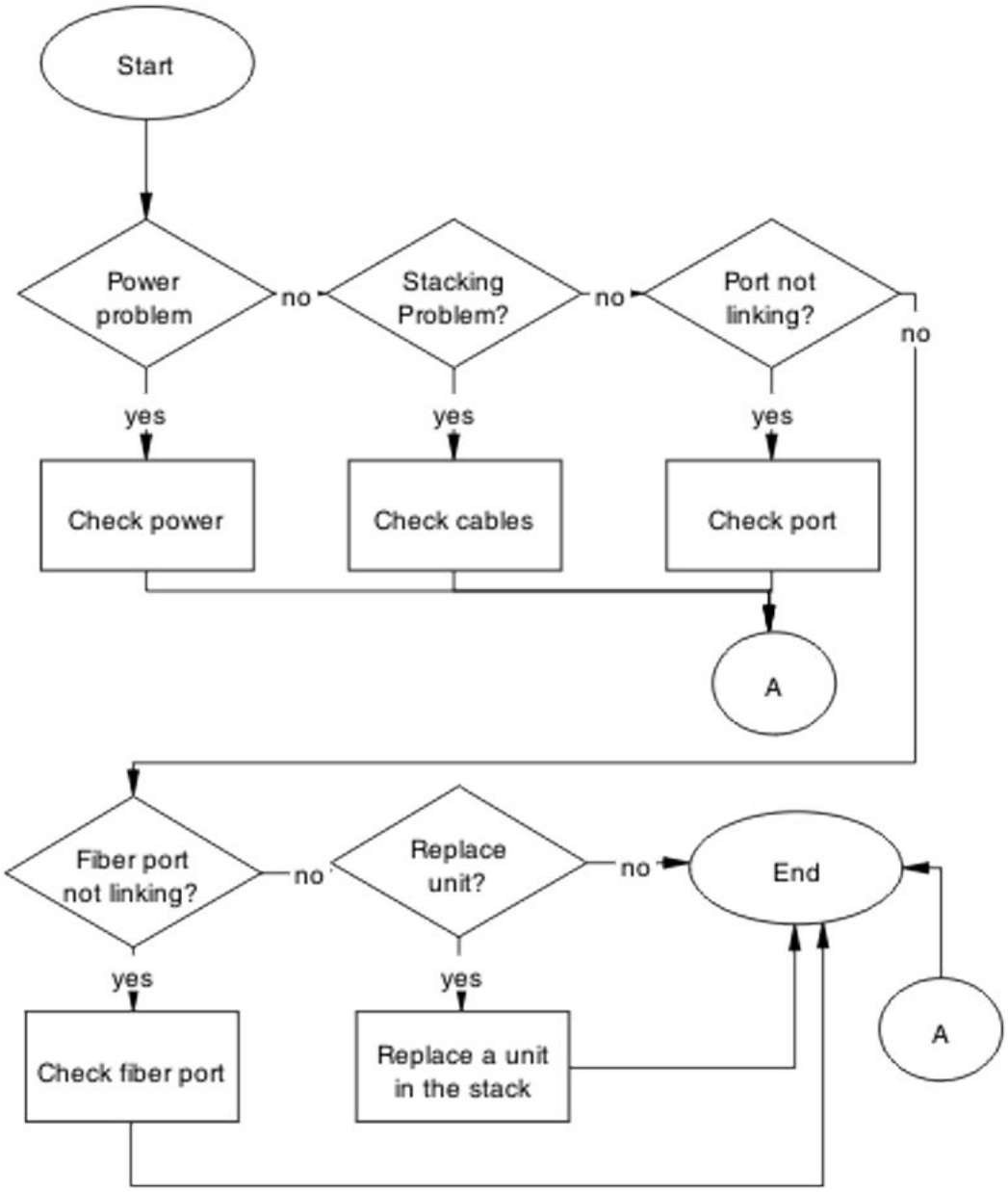


Figure 26: General troubleshooting of hardware

Check power

Confirm power is being delivered to the device. The switch utilizes a universal Power Supply Unit (PSU) that operates with voltages between 90v and 260v AC.

Task flow: Check power

About this task

The following task flow assists you to confirm that the switch is powered correctly.

Procedure

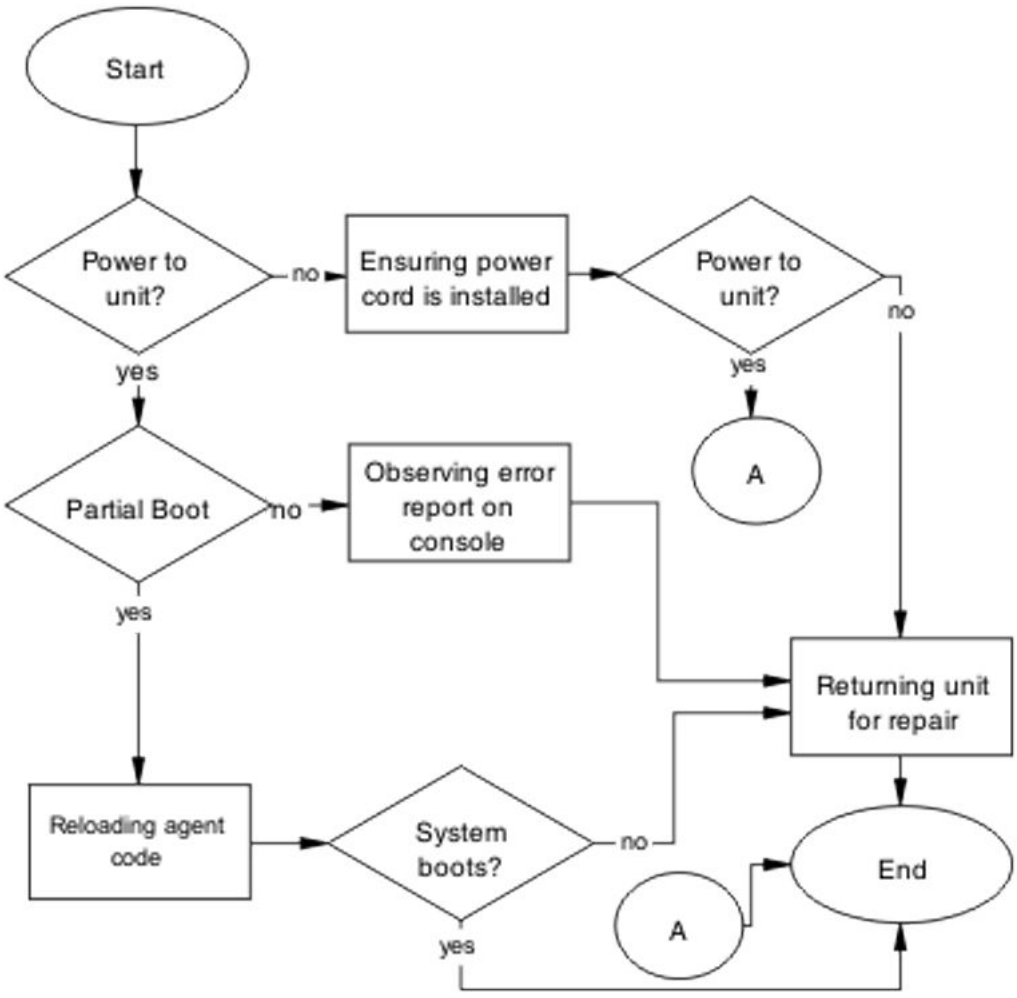


Figure 27: Check power

Ensuring the Power Cord is Installed

About this task

Confirm the power cord is properly installed for the device. All power cords are to be firmly seated. It is important to note that some power cords utilize power interruption features such as an in-line fuse. Ensure the cords are free from damage and are fully operational.

See the technical document Installing Ethernet Routing Switch 4900 Series or Installing Ethernet Routing Switch 5900 Series for power cord standards and details.

Observing an error report on the console

About this task

Interpret the message that is sent to the console after a failure.

Procedure

1. View the console information and note the details for the RMA.
2. Note the LED status for information:
   - Status LED blinking amber: Power On Self Test (POST) failure
   - Power LED blinking: corrupt flash

Reloading the Agent Code

About this task

Reload the agent code on the switch to eliminate corrupted or damaged code that causes a partial boot of the device.

Caution:

Ensure you have adequate backup of your configuration prior to reloading software.

Know the current version of your software before reloading it. Loading incorrect software versions may cause further complications.

Procedure

1. Use the **`show sys-info`** command to view the software version.
2. See Release Notes for Ethernet Routing Switch 4900 and 5900 Series for information about software installation.

Replacing the Power Cord

About this task

The power cord should be replaced to ensure the power problem is not with the cord itself. Ensure you use the same cord model as provided by Extreme Networks. Some power cords have a fuse built into them. Ensure you replace a fused cord with the same cord model that has the same power rating.

Procedure

1. Remove the power cord from the unit.
2. Replace the power cord with another power cord of the same type.

Returning the unit for repair

About this task

Return a unit to Extreme Networks for repair.

Contact Extreme Networks for return instructions.

Check Cables

Confirm the stacking cables are correctly connected. Review the Installing Ethernet Routing Switch 4900 Series or Installing Ethernet Routing Switch 5900 Series stacking section for cable requirements.

Task flow: Check cables

About this task

The following task flow assists you to confirm the stacking cables on the switch are installed correctly.

Procedure

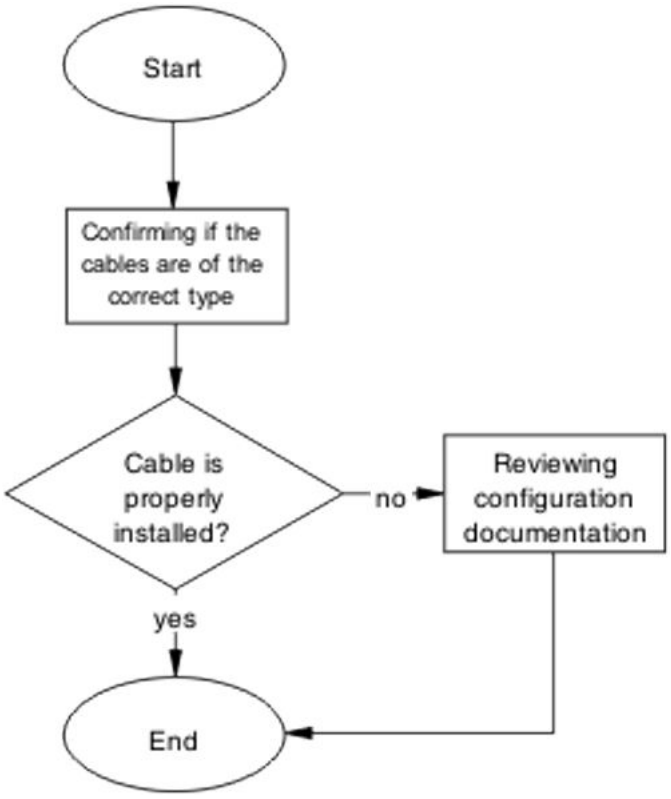


Figure 28: Check cables

Confirming if the cables are the correct type

About this task

To create a stack connection, order the appropriate switch cascade cables to ensure fail-safe stacking. A 1.5 foot stacking cable is included with the switch. For stacking three or more units (maximum eight units in a stack), order the 5-foot (1.5 m), 10-foot (3.0 m), 14-foot (4.3 m), or 16.4-foot (4.9 m) cables as applicable.

Reviewing Stacking Configuration Documentation

About this task

Review the stacking configuration documentation to confirm the correct stacking cabling requirements.

Review the stacking procedure and diagram for your stack configuration (cascade up or down) in the stacking section of Installing Ethernet Routing Switch 4900 Series or Installing Ethernet Routing Switch 5900 Series.

Check port

Confirm that the port and the Ethernet cable connecting the port are in proper configuration.

Task flow: Check port

About this task

The following task flow assists you to check the port and Ethernet cables.

Procedure

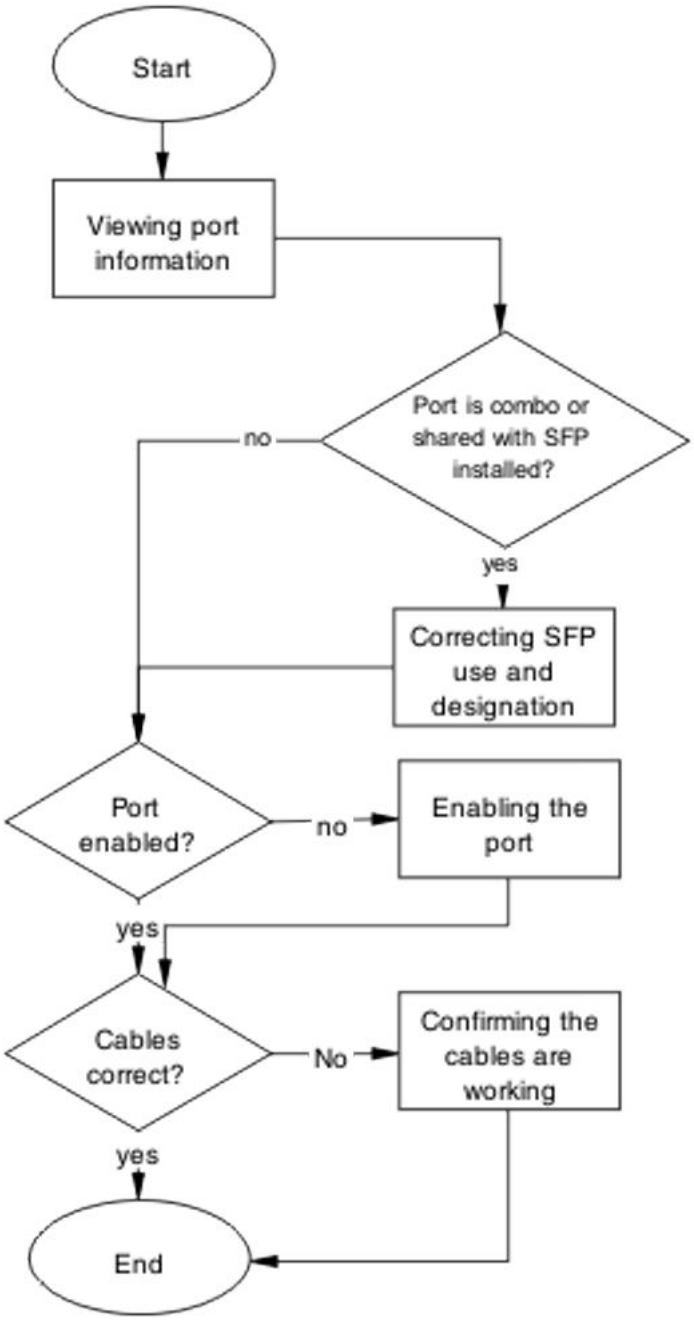


Figure 29: Check port

Viewing port information

About this task

Review the port information to ensure that the port is enabled.

Procedure

1. Use the **show interfaces <port>** command to display the port information.
2. Note the port status.

Correcting SFP Use and Designation

About this task

Use the procedure in this section if you have a combo or shared port that has an SFP installed and the corresponding SFP is active, but the copper port is not.

For more information about transceiver use and designation, see Extreme Networks Pluggable Transceivers Installation Guide.

Enabling the port

About this task

Enable the port.

Procedure

1. Go to interface specific mode using the **interface ethernet <port>** command.
2. Use the **no shutdown** command to change the port configuration.
3. Use the **show interfaces <port>** command to display the port.
4. Note the port administrative status.

Confirming the cables are working

About this task

Ensure that the cables connected to the port are functioning correctly.

Procedure

1. Go to interface specific mode using the **interface ethernet <port>** command.
2. Use the **no shutdown** command to change the port configuration.
3. Use the **show interfaces <port>** command to display the port.
4. Note the operational and link status of the port.

Check fiber port

Confirm the fiber port is working and the cable connecting the port is the proper type.

Task flow: Check fiber port

About this task

The following task flow assists you to confirm that the fiber port cable is functioning and is of the proper type.

Procedure

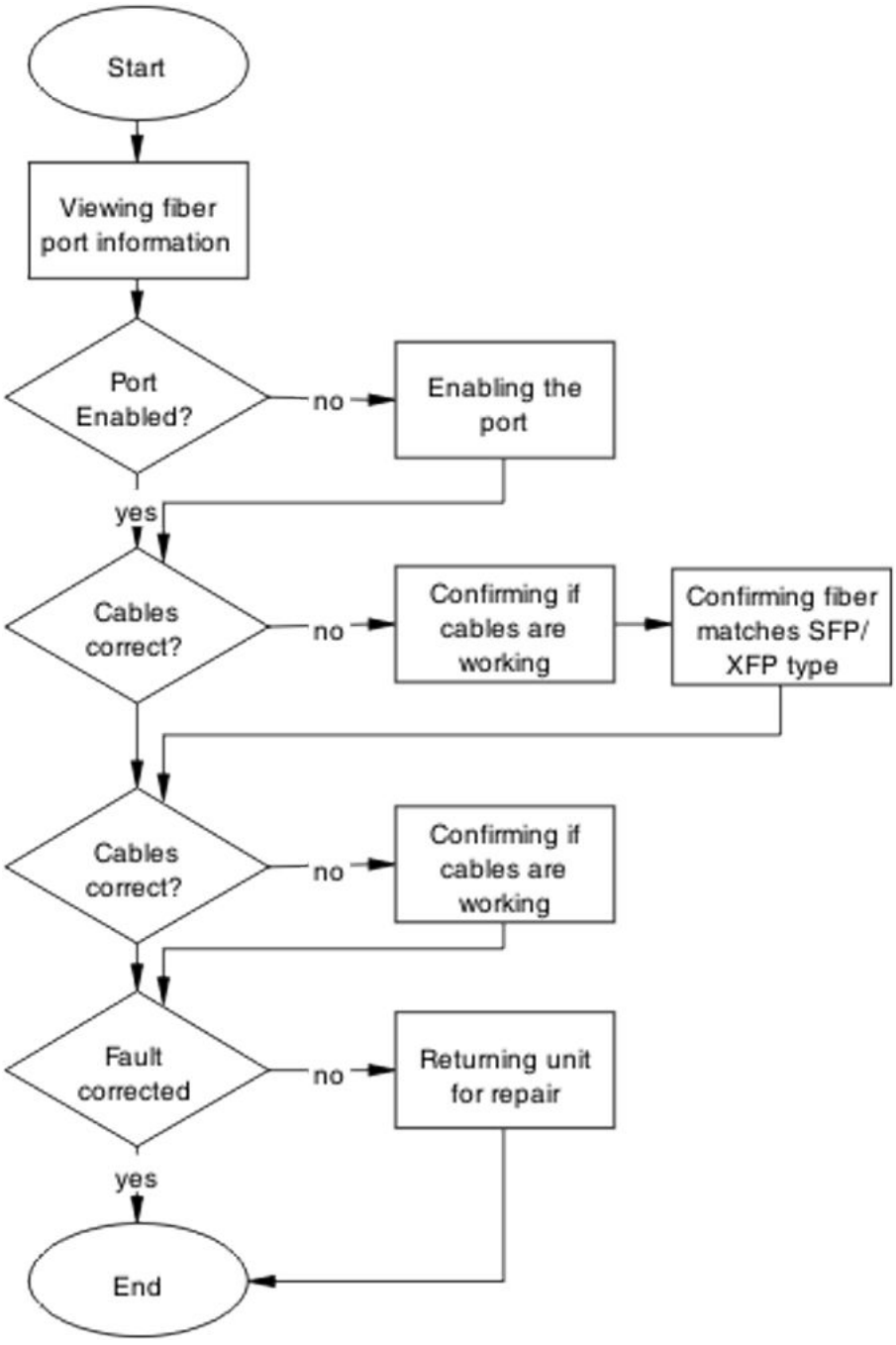


Figure 30: Check fiber port

Viewing fiber port information

About this task

Review the port information to ensure the port is enabled.

Procedure

1. Use the **show interfaces <port>** command to display the port information.
2. Note the port status.

Enabling the port

About this task

Ensure the port on the switch is enabled.

Procedure

1. Use the **no shutdown** command to change the port configuration.
2. Use the **show interfaces <port>** command to display the port information.
3. Note the port status.

Confirming if cables are working

About this task

Confirm that the cables are working on the port.

Procedure

1. Use the **no shutdown** command to change the port configuration.
2. Use the **show interfaces <port>** command to display the port.
3. Note the port operational and link status.

Confirming fiber matches SFP/XFP type

About this task

Ensure the fiber is the correct type and that the SFP or XFP is installed.

Procedure

1. Inspect the fiber cables to ensure they are the correct type.
2. For more information about the SFP GBICs, see Installing Gigabit Interface Converters, SFPs, and CWDM SFP Gigabit Interface Converters (312865).

Returning the unit for repair

About this task

Return unit to Extreme Networks for repair.

Contact Extreme Networks for return instructions and RMA information.

Replace a Unit in the Stack

Remove the defective unit and insert the replacement.

Caution:

Due to physical handling of the device and your physical proximity to electrical equipment, review and adhere to all safety instructions and literature included with the device and in Installation Job Aid for Ethernet Routing Switch 5900 Series.

The Auto Unit Replacement (AUR) feature allows replacement of a failed unit in a stack with a new unit, while retaining the configuration of the previous unit. The stack power must be on during unit replacement.

After replacing the base unit, another unit in the stack becomes the designated temporary base unit. The replacement base unit does not resume as the base unit automatically. The replacement base unit must be configured as the base unit.

The replacement unit to the stack must be running the same software and firmware versions as the previous unit but with a different MAC address.

Important:

If the stack is only of two switches, the remaining switch enters Stack Forced Mode if that feature is enabled. Review the section Stack Forced Mode on page 23 regarding this feature.

Important:

Different versions of the software and diagnostic images have different behaviors for the software and diagnostic images.

Task flow: Replace a unit in the stack

About this task

The following task flow assists you to replace one of the switches in a stack. This is only appropriate if old software is used or AAUR is disabled. If AAUR is available (and it is turned on by default in such cases), then the procedures to verify software are not required.

Procedure

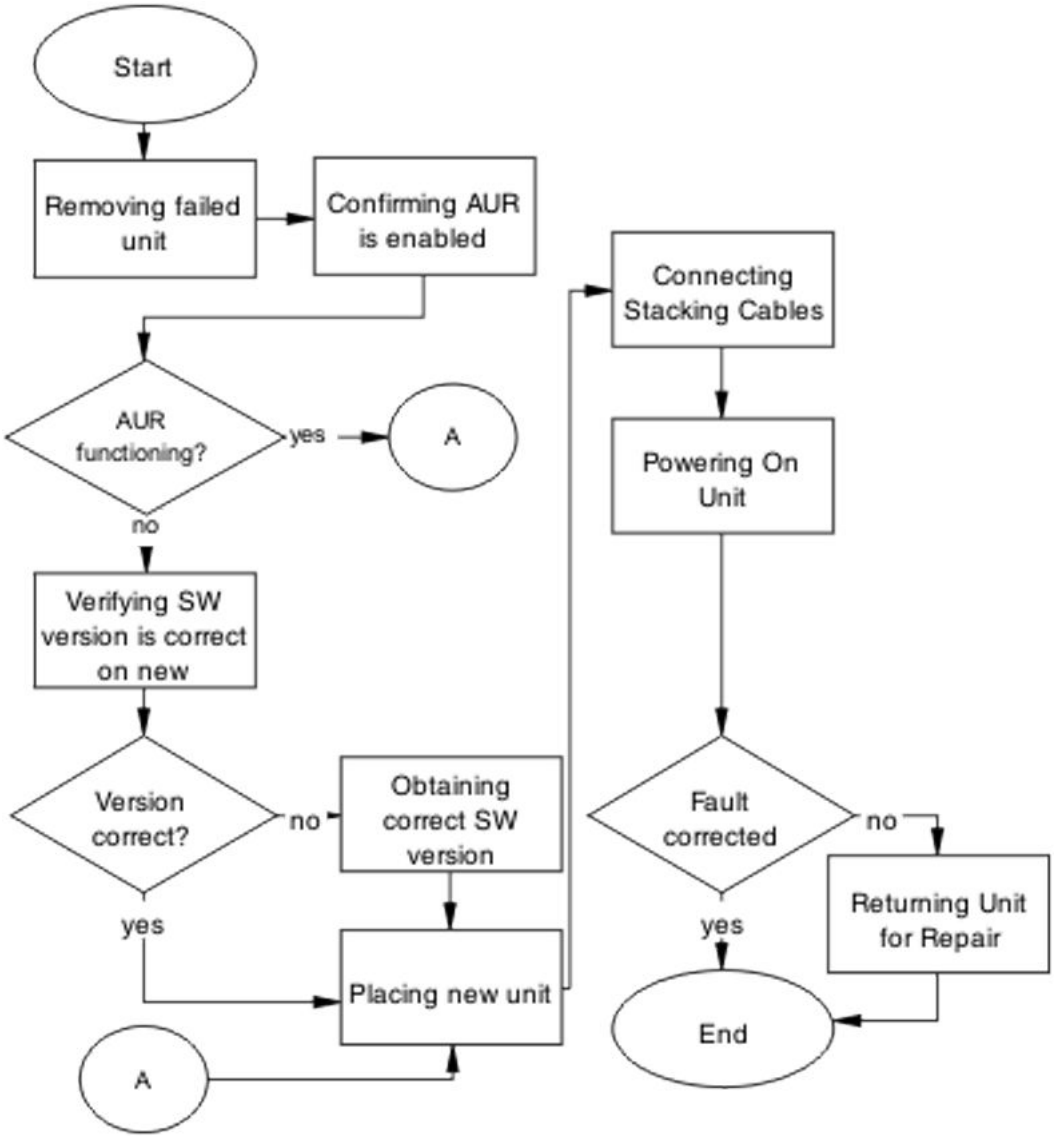


Figure 31: Replace a unit in the stack

Removing a failed unit

About this task

Remove the failed unit from the stack.

Procedure

1. Maintain power to the stack. Do not power down the stack.

2. Remove the failed device.

Confirming AUR is enabled

About this task

Confirm AUR is enabled in the stack.

Procedure

1. Enter the **`show stack auto-unit-replacement`** command to show AUR configuration.
2. Enter the **`stack auto-unit-replacement config save enable`** command to enable AUR.
3. Enter the **`stack auto unit replacement auto-restore enable`** command to configure AUR to automatically restore the configuration to the new unit.

Removing a MAC address from the AUR cache

About this task

Remove the MAC address for a non-operational stack switch from the AUR address cache.

Procedure

1. Enter the `show stack auto-unit-replacement mac-addresses` command to display the MAC addresses and operational status for all switches within a stack.
2. Enter the `stack auto-unit-replacement remove-mac-address unit <1-8>` command to remove the MAC address.
3. Enter the `show stack auto-unit-replacement mac-addresses` command to verify that the MAC address for the non-operational switch is removed from the AUR address cache.

Verifying the software version is correct on the new device

About this task

Verify that the new device to be inserted in the stack has the identical software version.

Procedure

1. Connect the new device to the console, independent of stack connection.
2. Use the **`show sys-info`** command to view the software version.

Obtaining the Correct Software Version

About this task

Obtain and install the correct software version.

Caution:

Ensure you have adequate backup of your configuration prior to reloading software.

Know the Release number of your software before loading it. Loading incorrect software versions may cause further complications.

Procedure

See Release Notes for Ethernet Routing Switch 4900 and 5900 Series for software installation information.

Placing a New Unit

About this task

Place the new unit in the stack where the failed unit was connected.

Place the device in the stack in accordance with procedures outlined in Installing Ethernet Routing Switch 4900 Series or Installing Ethernet Routing Switch 5900 Series.

Connecting Stacking Cables

About this task

Reconnect the stacking cables to correctly stack the device.

Procedure

1. Review the stacking section in Installing Ethernet Routing Switch 4900 Series or Installing Ethernet Routing Switch 5900 Series for cabling details.
2. Connect the cables in accordance with physical stack requirements.

Powering on the unit

About this task

Energize the unit after it is connected and ready to integrate.

Prerequisite There is no requirement to reset the entire stack. The single device being replaced is the only device that you must power on after integration to the stack.

Procedure

1. Connect the power to the unit.
2. Allow time for the new unit to join the stack and for the configuration of the failed unit to be replicated on the new unit.
3. Confirm that the new unit has reset itself. This confirms that replication has completed.

Returning the unit for repair

About this task

Return the unit to Extreme Networks for repair.

Contact Extreme Networks for return instructions.

Chapter 9: Troubleshooting ADAC

Automatic Detection and Automatic Configuration (ADAC) can encounter detection and configuration errors that can be easily corrected.

ADAC clarifications

ADAC VLAN settings are dynamic and are not saved to nonvolatile memory. After ADAC is enabled, all VLAN settings you manually made on ADAC uplink or telephony ports are dynamic and are not saved to non-volatile memory. After the unit is reset, these settings are lost. ADAC detects the ports again and re-applies the default settings for them.

You must manually create a VLAN to be used as the voice VLAN and then set this VLAN as the ADAC voice VLAN using the command **adac voice-vlan x**.

After the VLAN number is reserved as the ADAC voice VLAN using the **`adac voice-vlan x`** command, even if the ADAC administrative status is disabled or ADAC is in UTF mode, the VLAN number cannot be used by anyone else in regular VLAN creation.

If you enable the LLDP detection mechanism for telephony ports, then LLDP itself has to be enabled on the switch. Otherwise, ADAC cannot detect phones using the LLDP detection mechanism.

Work flow: Troubleshooting ADAC

About this task

The following work flow assists you to identify the type of problem you are encountering.

Procedure

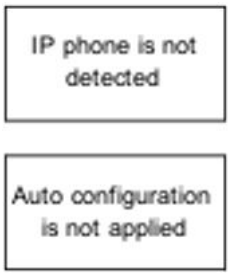


Figure 32: Troubleshooting ADAC

IP phone is not detected

Correct an IP phone that is not being detected by ADAC.

Work flow: IP phone not detected

About this task

The following work flow assists you to resolve detection issues.

Procedure

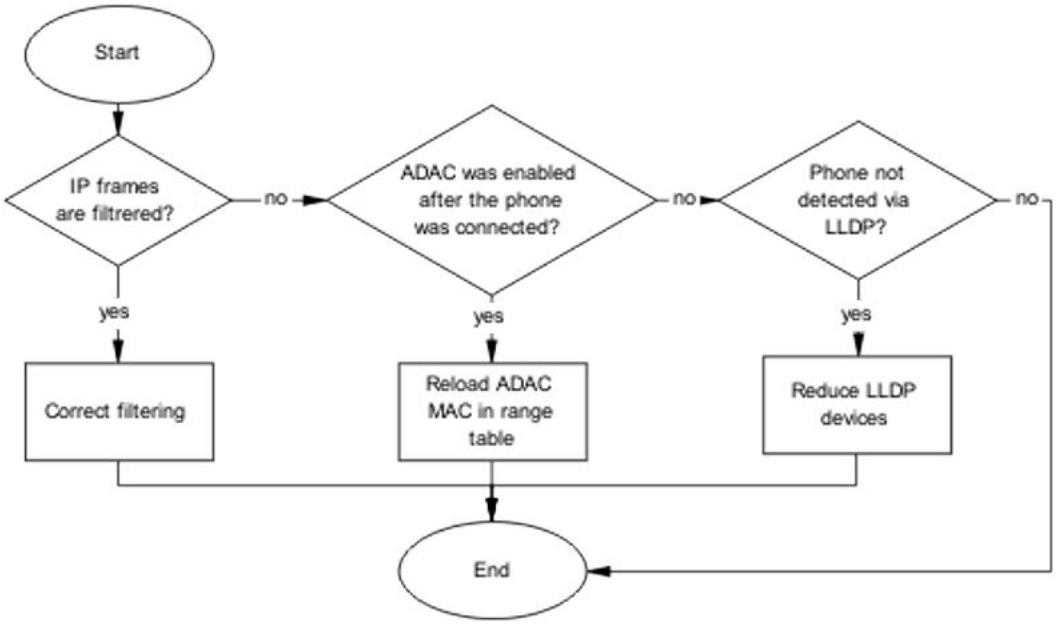


Figure 33: IP phone not detected

Correct filtering

Configure the VLAN filtering to allow ADAC.

Task flow: Correct filtering

About this task

The following task flow assists you to correct the filtering.

Procedure

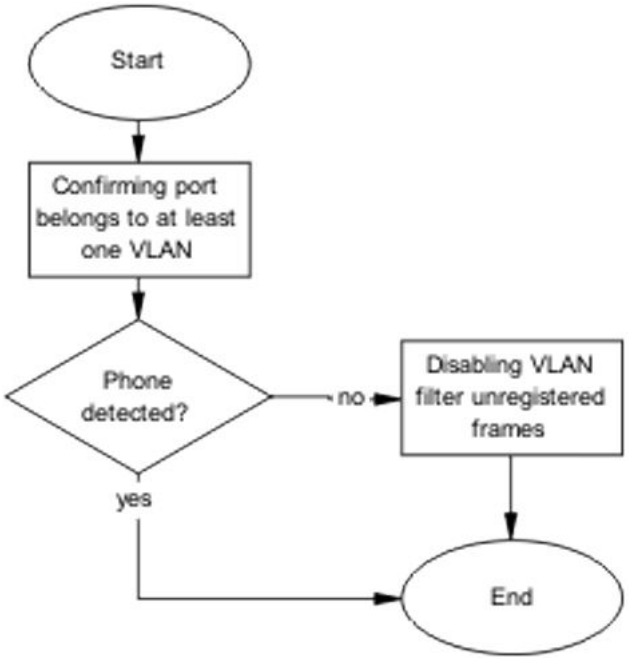


Figure 34: Correct filtering

Confirming port belongs to at least one VLAN

About this task

View information to ensure that the port belongs to a VLAN.

Procedure

1. Use the **`show vlan interface info <port>`** command to view the details.
2. Note the VLANs listed with the port.

Disabling the VLAN filtering of unregistered frames

About this task

Change the unregistered frames filtering of the VLAN.

Procedure

1. Use the **`vlan ports <port> filter-unregistered-frames disable`** command to view the details.
2. Ensure no errors after command execution.

Reload ADAC MAC in range table

Ensure the ADAC MAC address is properly loaded in the range table.

Task flow: Reload ADAC MAC in range table

About this task

The following task flow assists you to place the ADAC MAC address in the range table.

Procedure

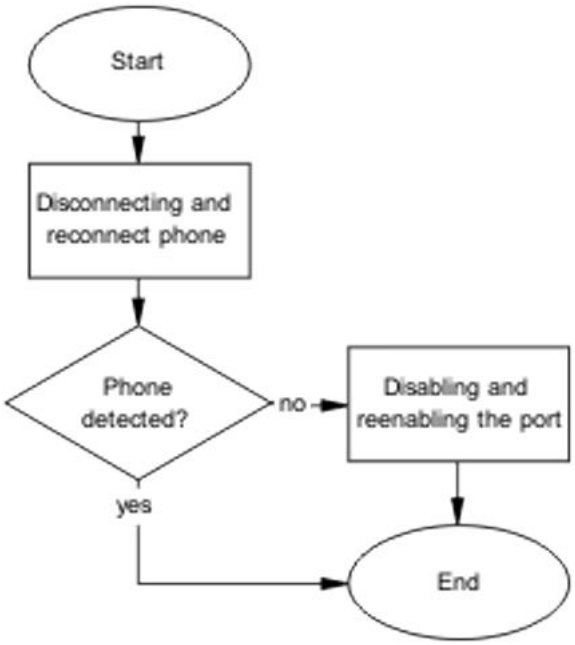


Figure 35: Reload ADAC MAC in range table

Disconnecting and reconnecting phone

About this task

Remove the phone and then reconnect it to force a reload of the MAC address in the range table.

Procedure

1. Follow local procedures to disconnect the phone.

2. Follow local procedures to reconnect the phone.

Disabling and enabling the port

About this task

Disable ADAC on the port and then enable it to detect the phone. After disabling and re-enabling the port administratively, the MAC addresses already learned on the respective port are aged out.

Procedure

1. Use the **`no adac enable <port>`** command to disable ADAC.
2. Use the **`adac enable <port>`** command to enable ADAC.

Reduce LLDP devices

Reduce the number of LLDP devices. More than 16 devices may cause detection issues.

Task flow: Reduce LLDP devices

About this task

The following task flow assists you to reduce the number of LLDP devices on the system.

Procedure

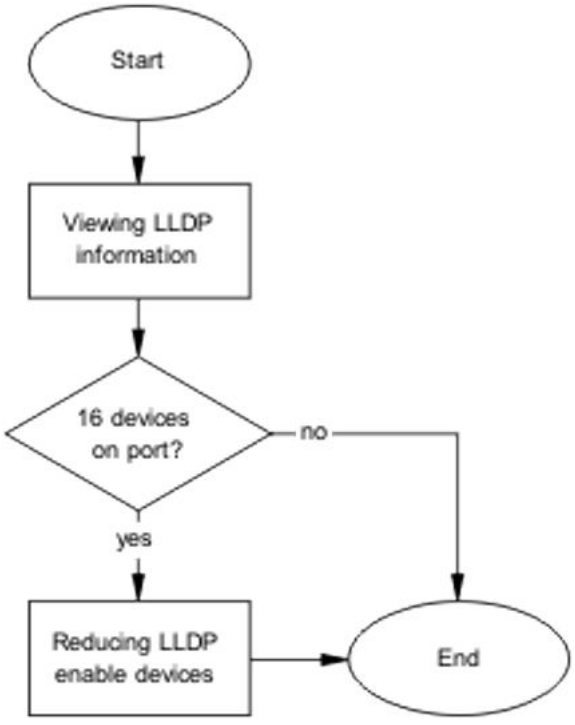


Figure 36: Reduce LLDP devices

Viewing LLDP information

About this task

Display the LLDP devices that are connected to a port.

Procedure

1. Use the **`show lldp port 1 neighbor`** command to identify the LLDP devices.
2. Note if there are more than 16 LLDP-enabled devices on the port.

Reducing LLDP enabled devices

About this task

Reduce the number of LLDP devices on the system.

Procedure

1. Follow local procedures and SOPs to reduce the number of devices connected.
2. Use the **`show adac in <port>`** command to display the ADAC information for the port to ensure there are less than 16 devices connected.

Auto configuration is not applied

Correct some common issues that may interfere with auto configuration of devices.

Task flow: Auto configuration is not applied

About this task

The following task flow assists you to solve auto configuration issues.

Procedure

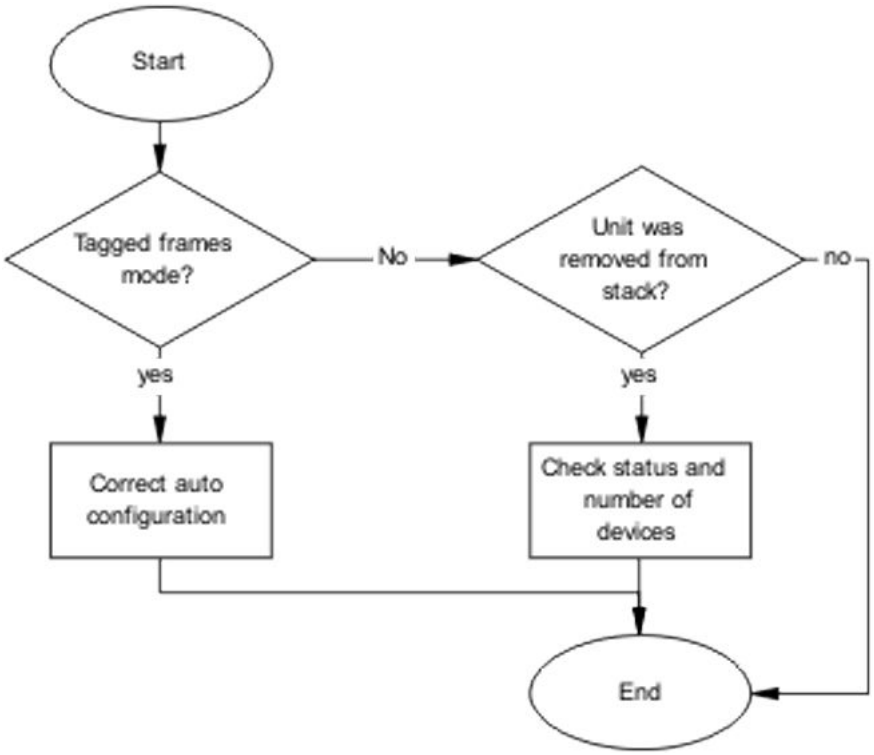


Figure 37: Auto configuration is not applied

Correct auto configuration

Tagged frames mode may be causing a problem. In tagged frames mode, everything is configured correctly, but auto configuration is not applied on a telephony port.

Task flow: Correct auto configuration

About this task

The following task flow assists you to correct auto configuration.

Procedure

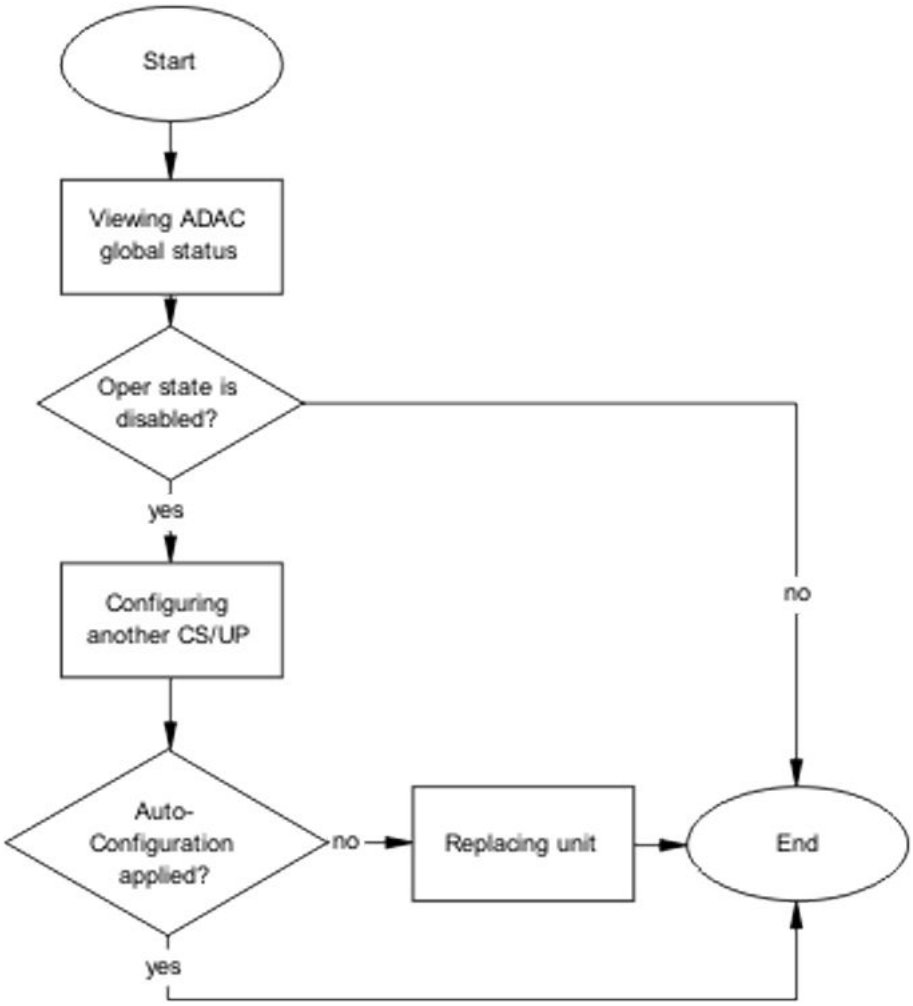


Figure 38: Correct auto configuration

Viewing ADAC global status

About this task

Display the global status of ADAC.

Procedure

1. Use the **`show adac`** command to display the ADAC information.
2. Note if the oper state is showing as disabled.

Configuring another call server and uplink port

About this task

Configuring another call server and uplink port can assist the auto configuration.

Procedure

1. Use the **`adac uplink-port <port>`** command to assign the uplink port.
2. Use the **`adac call-server-port <port>`** command to assign the call server port.

Replacing the Unit

About this task

Replace the unit to replicate configuration if AUR is enabled.

Procedure

1. Follow the replacement guidelines in Configuring Systems on Ethernet Routing Switch 4900 and 5900 Series.
2. Refer to the unit replacement section in the Troubleshooting Hardware section of this document.

Check status and number of devices

Auto configuration can stop being applied after a unit is removed from the stack.

Task flow: Check status and number of devices

About this task

The following task flow assists you to correct the auto configuration.

Procedure

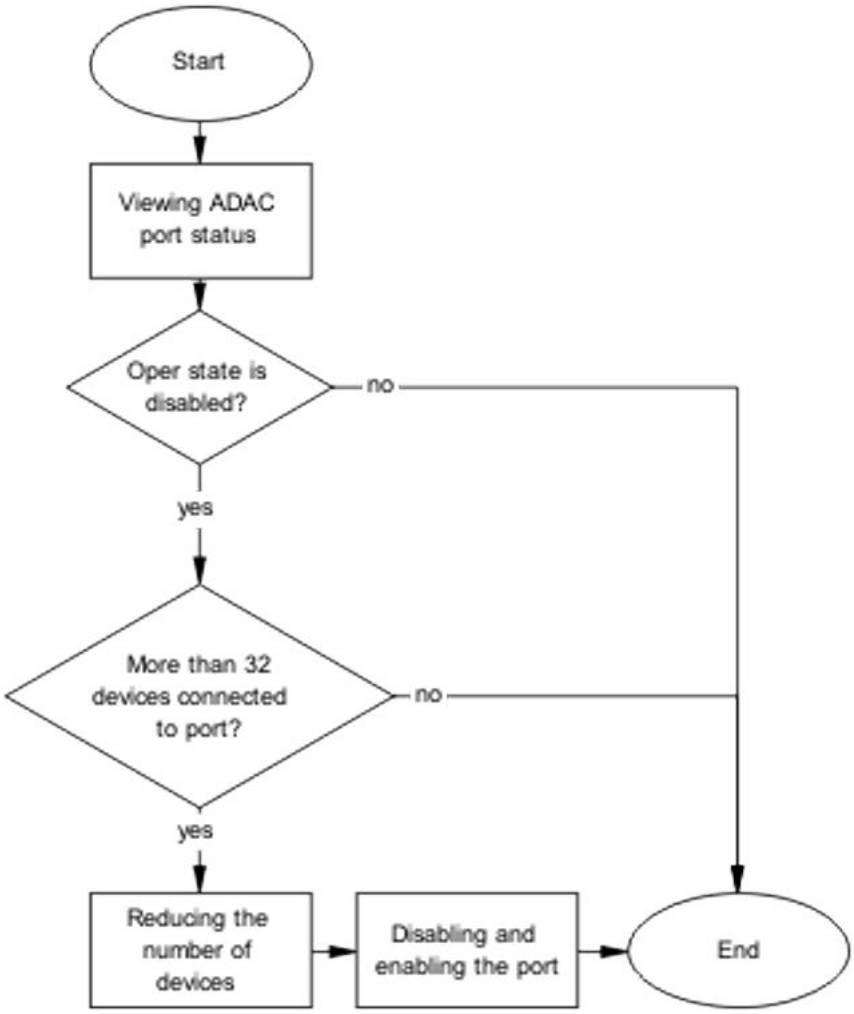


Figure 39: Check status and number of devices

Viewing ADAC port status

About this task

Display the status of ADAC on the port.

Procedure

1. Use the **`show adac in <port>`** command to display the ADAC information for the port.
2. Note if the oper state is disabled and the number of devices connected.

Reducing the number of devices

About this task

Reduce the number of LLDP devices on the system.

Procedure

1. Follow local procedures and Standard Operating Procedures to reduce the number of devices connected.
2. Use the **`show adac in <port>`** command to display the ADAC information for the port to ensure that less than 32 devices are connected.

Disabling and enabling the port

About this task

Administratively disable and enable the port to initialize the configuration.

Procedure

1. Use the **`no adac enable <port>`** command to disable ADAC.
2. Use the **`adac enable <port>`** command to enable ADAC.

Chapter 10: Troubleshooting authentication

Authentication issues can interfere with device operation and function. The following work flow shows common authentication problems.

Work flow: Troubleshooting authentication

About this task

The following work flow shows typical authentication problems. These work flows are not dependant upon each other.

Procedure

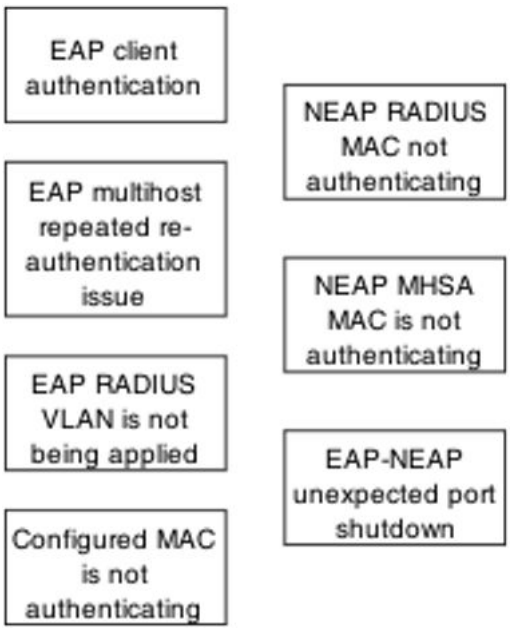


Figure 40: Troubleshooting authentication

Change RADIUS Password

Before you begin

- Enable MS-CHAPv2 encapsulation on the switch in order to change the RADIUS password. Follow the steps in Configuring Security on Ethernet Routing Switch 4900 and 5900 Series.
- Use this feature in conjunction with password fallback. Follow the steps in Configuring Systems on Ethernet Routing Switch 4900 and 5900 Series.
- Ensure the RADIUS server is configured properly. Follow the steps in Configuring Systems on Ethernet Routing Switch 4900 and 5900 Series .

Note:

If the server is not reachable after waiting one to two minutes to try again, use the following command: `radius reachability use-radius`.

About this task

The feature is used to validate RADIUS credentials to allow CLI, Telnet, and SSH access to the switch. Change the password using one of two methods:

- Enter one of the following commands: `cli password serial radius` or `cli password telnet radius`. If the password has expired, you are prompted to enter and confirm a new password.
- Enter new CLI command described in the procedure below.

Procedure

Enter the following CLI command: `cli password change`

Example

```
Switch(config)#cli password change
Changing password for user: admin-test
Enter old password              : **********
Enter New Password           : ********
Re-enter New Password      : ********
```

Troubleshooting Fail Open VLAN Continuity Mode

The Fail Open VLAN Continuity Mode feature introduces a new mode of operation for EAP/ NEAP clients when the RADIUS server(s) become unreachable.

When Fail Open VLAN Continuity Mode is enabled, if the RADIUS client does not receive any response from the RADIUS server, the EAP or Non-EAP MACs are not flushed. The RADIUS reachability is triggered, and the port is copied to Fail Open VLAN.

Display Fail Open VLAN continuity mode status

```
4xxx(config)#show eapol multihost
[...]
Fail Open VLAN:  Enabled
Fail Open VLAN ID:  1000
Fail Open VLAN Continuity Mode:  Enabled
```

Verify functionality

Verify Fail Open VLAN Continuity Mode is functioning properly by using syslog when the RADIUS server is down and a client is reauthenticated.

```
4xxx(config)#show logging sort-reverse
[...]
I    00:00:29:57                   43       No Response from RADIUS Server port 14
mac 1c:bd:b9:e5:cb:42, FOV continuity activated; RADIUS Reachability Triggered
[...]
```

Limitations

It is recommended that the RADIUS Reachability to be set on Use RADIUS.

If Use ICMP is used and the RADIUS server is reachable, but the RADIUS Server Service is stopped, an ICMP packet is sent for every authentication. If there are many EAP/Non-EAP clients in the setup, this flood with ICMP packets can be disturbing. This is a corner case and can be avoided using RADIUS packets for reachability, as recommended, or starting RADIUS Server Service if Use ICMP is used for reachability. This situation appears because with Fail Open Continuity Mode enabled, the RADIUS Reachability mechanism is triggered when no response is received from the RADIUS Server.

EAP client authentication

This section provides troubleshooting guidelines for the EAP and NEAP features on the switch.

Work flow: EAP client is not authenticating

About this task

The following work flow assists you to determine the cause and solution of an EAP client that does not authenticate as expected.

Procedure

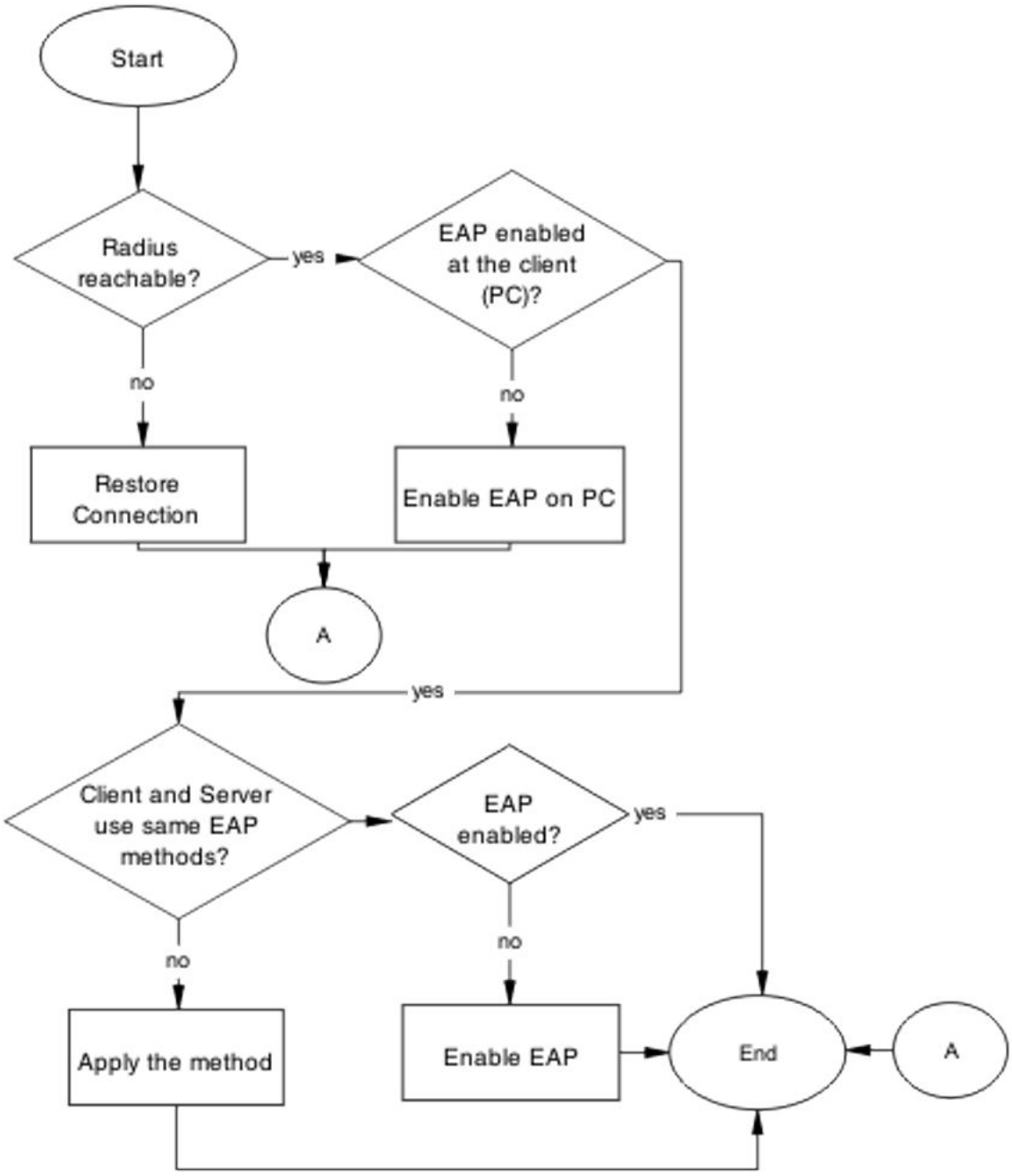


Figure 41: EAP client is not authenticating

Restore RADIUS connection

Ensure that the RADIUS server has connectivity to the device.

Task flow: Restore RADIUS connection

About this task

The following task flow assists you to restore the connection to the RADIUS server.

Procedure

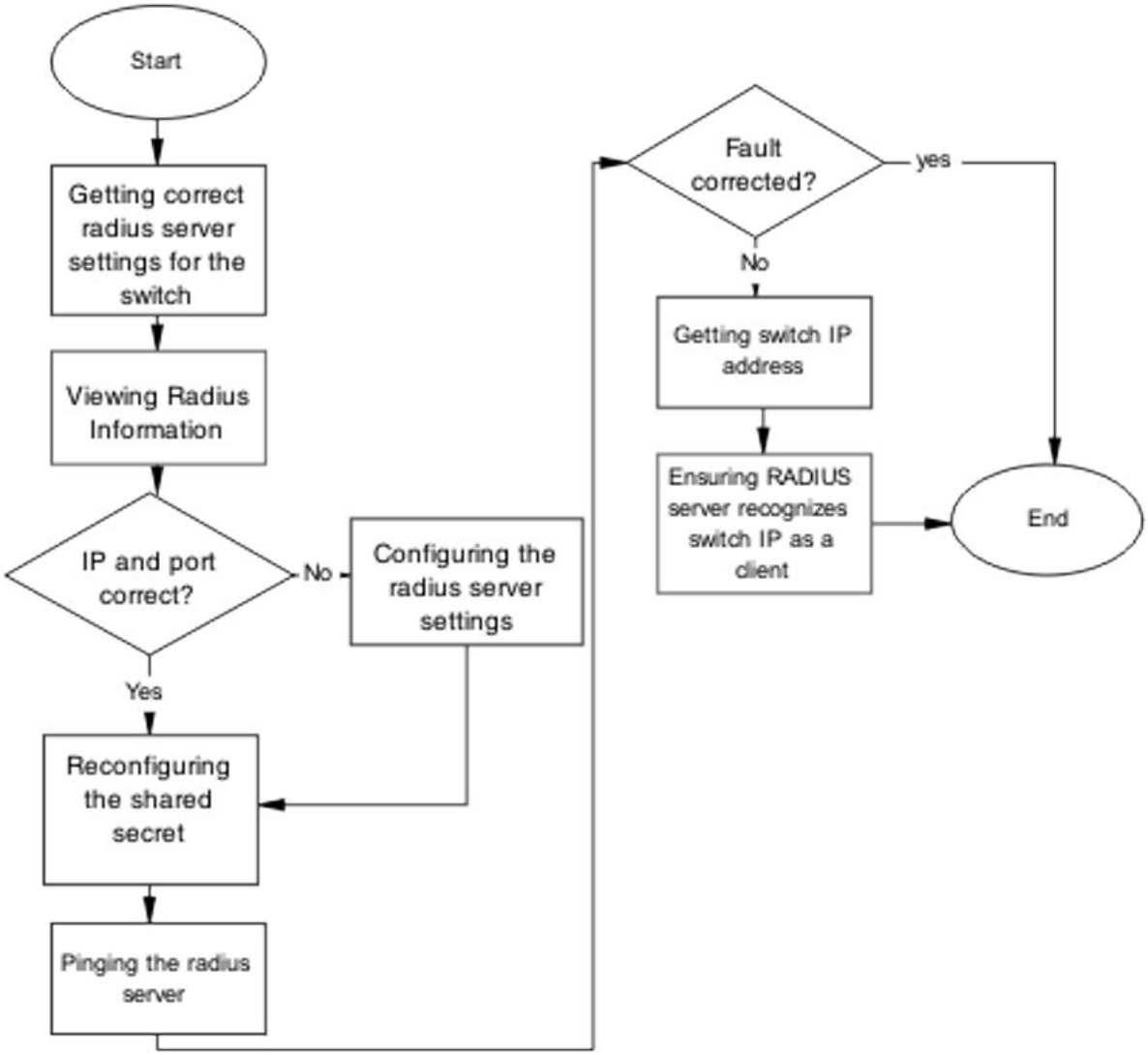


Figure 42: Restore RADIUS connection

Getting correct RADIUS server settings for the switch

About this task

This section provides troubleshooting guidelines for obtaining the RADIUS server settings.

Procedure

1. Obtain network information for the RADIUS server from the Planning and Engineering documentation.
2. Follow vendor documentation to set the RADIUS authentication method MD5.

Viewing RADIUS information

About this task

Review the RADIUS server settings in the device. The default server port is 1812/UDP. Older servers may use 1645/UDP, and other older servers do not support UDP at all

Procedure

1. Use the **`show radius-server`** command to view the RADIUS server settings.
2. Refer to the vendor documentation for server configuration.

Configuring the RADIUS server settings

About this task

The RADIUS server settings must be correct for the network.

Follow vendor documentation to set the RADIUS server settings.

Reconfiguring the shared secret

About this task

Reset the shared secret in case there was any corruption.

Procedure

1. Use the **`radius server host key`** command.
2. Refer to the vendor documentation for server configuration.

Pinging the RADIUS server

About this task

Ping the RADIUS server to ensure connection exists.

Procedure

1. Use the **`ping <server IP>`** command to ensure connection.
2. Observe no packet loss to confirm connection.

Enable EAP on the PC

The PC must have an EAP-enabled device that is correctly configured.

Task flow: Enable EAP on the PC

About this task

The following task flow assists you to ensure the PC network card has EAP enabled.

Procedure

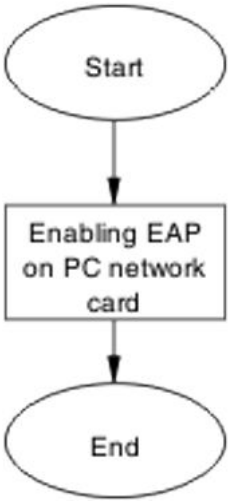


Figure 43: Enable EAP on the PC

Enabling EAP on PC network card

About this task

The PC must have the correct hardware and configuration to support EAP.

Procedure

1. See vendor documentation for the PC and network card.
2. Ensure the network card is enabled.
3. Ensure the card is configured to support EAP.

Apply the method

Ensure you apply the correct EAP method.

Task flow: Apply the method

About this task

The following task flow assists you to apply the correct EAP method.

Procedure

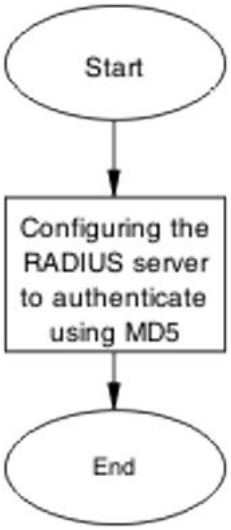


Figure 44: Apply the method

Configuring the RADIUS server

About this task

Configure the RADIUS server to authenticate using MD5.

Procedure

1. Obtain network information for the RADIUS Server from Planning and Engineering.
2. Save the information for later reference.

Enable EAP globally

Enable EAP globally on the switch.

Task flow: Enable EAP globally

About this task

The following task flow assists you to enable EAP globally on the switch.

Procedure

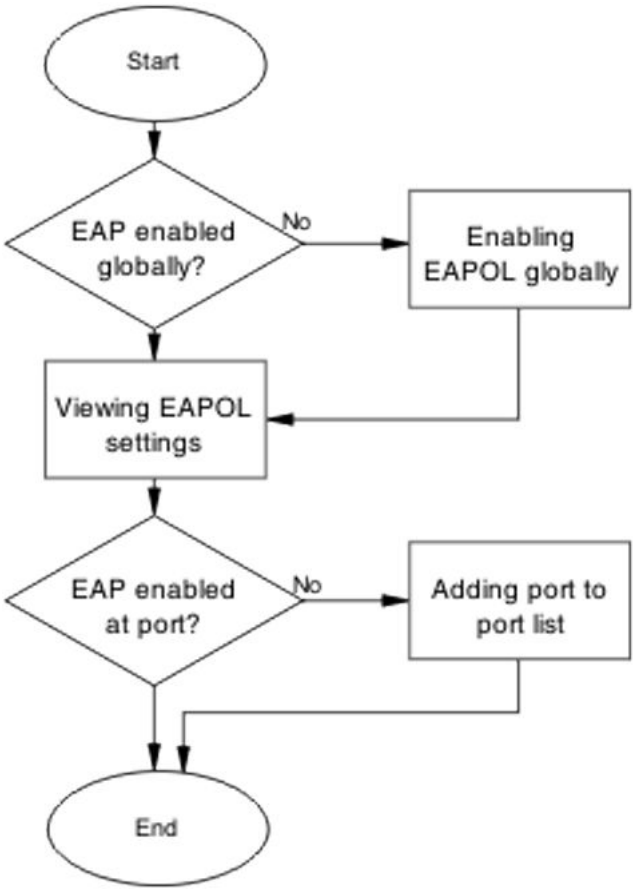


Figure 45: Enable EAP globally

Enabling EAP globally

About this task

Enable EAP globally on the switch.

Procedure

1. Use the **`eapol enable`** command to enable EAP globally on the switch.
2. Ensure that there are no errors after command execution.

Viewing EAPOL settings

About this task

Review the EAPOL settings to ensure EAP is enabled.

Procedure

1. Use the **`show eapol port <port#>`** command to display the information.
2. Observe the output.

Setting EAPOL port administrative status to auto

About this task

Set the EAPOL port administrative status to auto.

Procedure

1. Use the **`eapol status auto`** command to change the port status to auto.
2. Ensure that there are no errors after the command execution.

EAP multihost repeated re-authentication issue

Eliminate the multiple authentication of users.

Task flow: EAP multihost repeated re-authentication issue

About this task

The following work flow assists you to determine the cause and solution of an EAP multihost that authenticates repeatedly.

Procedure

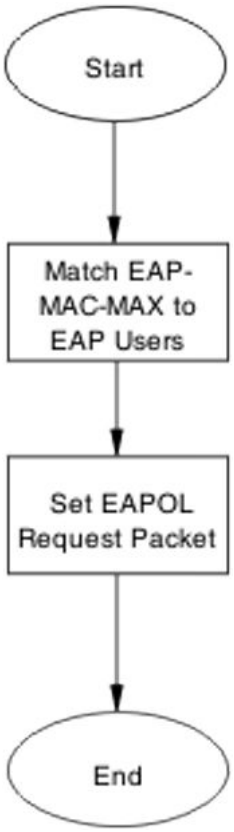


Figure 46: EAP multihost repeated re-authentication issue

Match EAP-MAC-MAX to EAP users

When the number of authenticated users reaches the allowed maximum, lower the eap-mac-max to the exact number of EAP users that may soon enter to halt soliciting EAP users with multicast requests.

Task flow: Match EAP-MAC-MAX to EAP users

About this task

The following task flow assists you to match the EAP-MAC-MAX to the number of EAP users.

Procedure

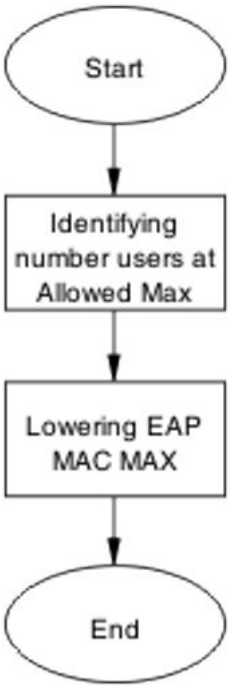


Figure 47: Match EAP-MAC-MAX to EAP users

Identifying number of users at allowed max

About this task

Obtain the exact number of EAP users that may soon enter when the number of authenticated users reaches the allowed max.

Procedure

Use the **`show eapol multihost status`** command to display the authenticated users.

Lowering EAP max MAC

About this task

Lower the eap-mac-max value to match the users.

Procedure

1. Use the **`eapol multihost eap-mac-max`** command to set the mac-max value.
2. Ensure that there are no errors after execution.

Set EAPOL request packet

Change the request packet generation to unicast.

Task flow: Set EAPOL request packet

About this task

The following task flow assists you to set the EAPOL request packet to unicast.

Procedure

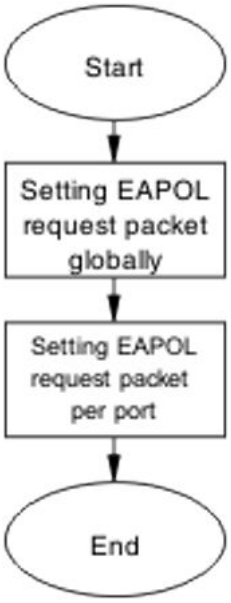


Figure 48: Set EAPOL request packet

Setting EAPOL request packet globally

About this task

Globally change the EAPOL request packet from multicast to unicast.

Procedure

1. Use the **`eapol multihost eap-packet-mode unicast`** command to set the EAPOL request packet to unicast.
2. Ensure that there are no errors after execution.

Setting EAPOL request packet for a port

About this task

Change the EAPOL request packet from multicast to unicast for a specific port.

Procedure

1. Enter the Interface Configuration mode.
2. Use the **`eapol multihost eap-packet-mode unicast`** command to set the EAPOL request packet to unicast for the interface.

EAP RADIUS VLAN is not being applied

Ensure that the RADIUS VLAN is applied correctly to support EAP.

Work flow: EAP RADIUS VLAN is not being applied

About this task

The following work flow assists you to determine the cause and solution of the RADIUS VLAN not being applied.

Procedure

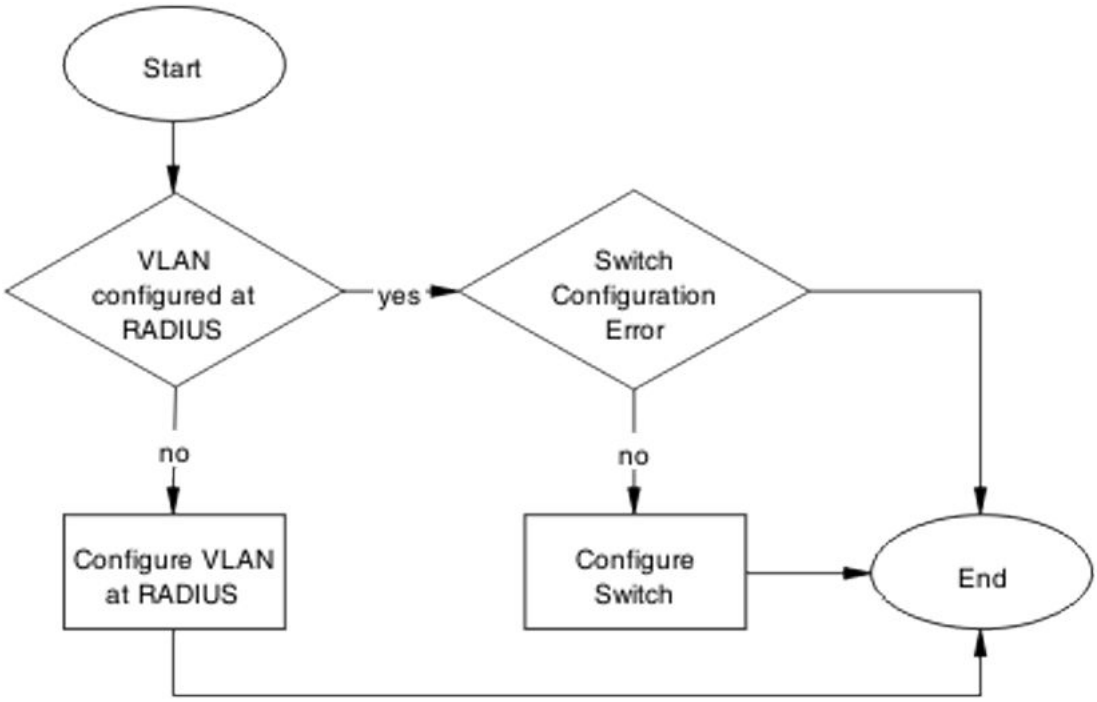


Figure 49: EAP Radius VLAN is not being applied

Configure VLAN at RADIUS

Correct any discrepancies in VLAN information at the RADIUS server.

Task flow: Configure VLAN at RADIUS

About this task

The following task flow assists you to ensure the VLAN is configured at the RADIUS server.

Procedure

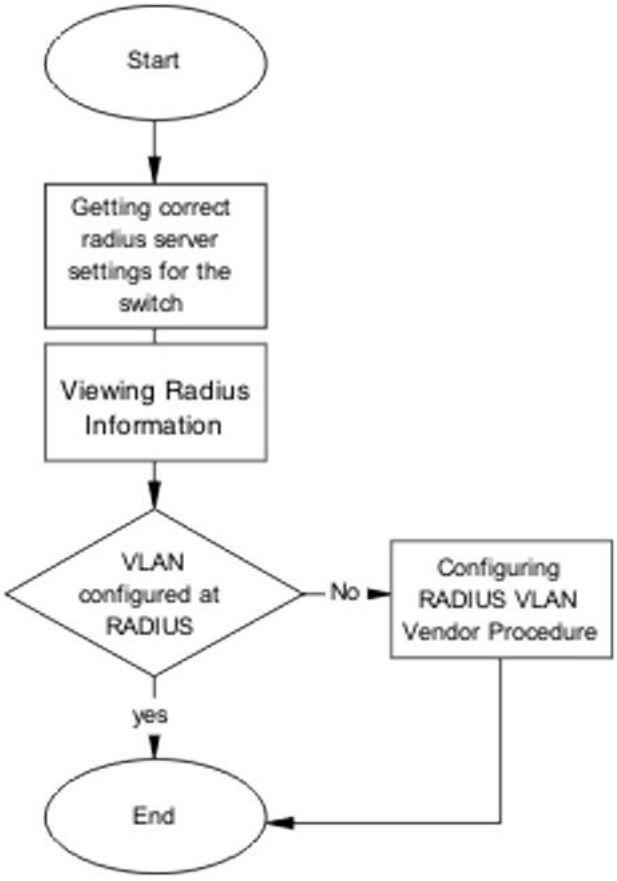


Figure 50: Configure VLAN at RADIUS

Getting correct RADIUS server settings

About this task

This section provides troubleshooting guidelines to obtain the correct RADIUS server settings.

Procedure

1. Obtain network information from Planning and Engineering documentation to locate server information.
2. Obtain network information for the RADIUS server.

Viewing RADIUS information

About this task

Obtain the RADIUS information to identify its settings.

Use vendor documentation to obtain settings display.

Configuring RADIUS

About this task

Configure the RADIUS server with the correct VLAN information. Use vendor documentation to make the required changes.

There are three attributes that the RADIUS server sends back to the NAS (switch) for RADIUS-assigned VLANs. These attributes are the same for all RADIUS vendors:

- Tunnel-Medium-Type – 802
- Tunnel-Pvt-Group-ID – <VLAN ID>
- Tunnel-Type – Virtual LANs (VLAN)

Configure the switch

The VLAN must be configured correctly on the switch.

Task flow: Configure switch

About this task

The following task flows assist you to configure the VLAN on the device.

Procedure

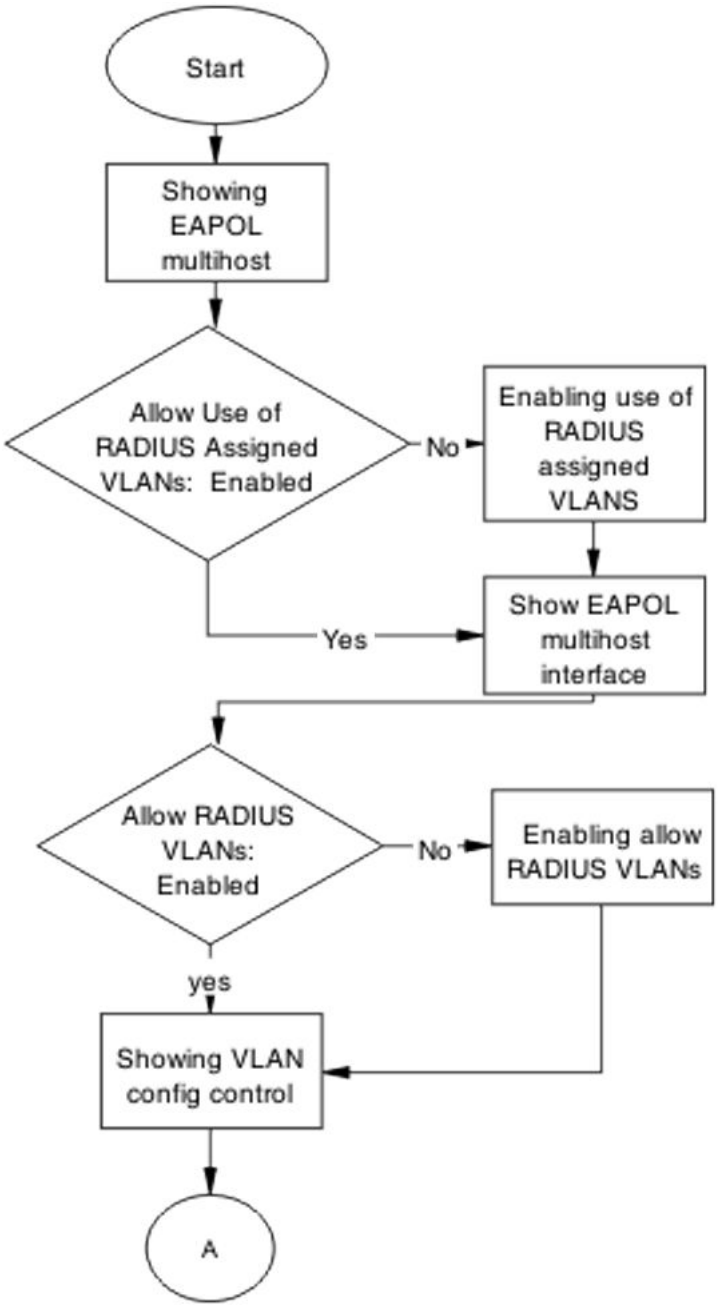


Figure 51: Configure switch task part 1

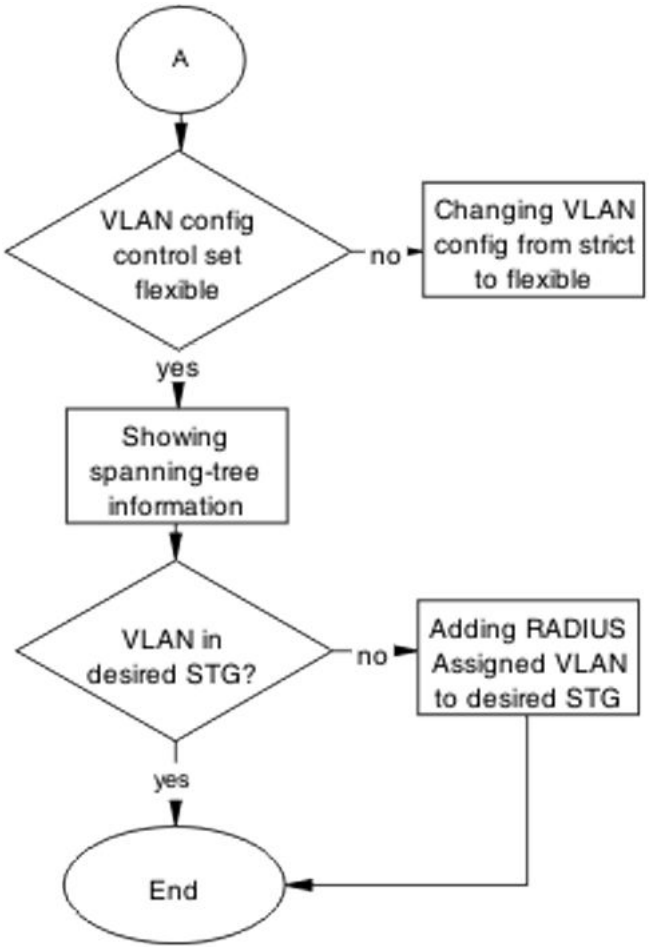


Figure 52: Configure switch task part 2

Showing EAPOL multihost

About this task

Identify the EAPOL multihost information.

Procedure

1. Use the **`show eapol multihost`** command to display the multihost information.
2. Note the state of Allow Use of RADIUS Assigned VLANs.

Enabling use of RADIUS assigned VLANs

About this task

Change the "allow RADIUS assigned VLAN" setting to "enable".

Procedure

1. Use the **`eapol multihost use-radius-assigned-vlan`** command to allow the use of VLAN IDs assigned by RADIUS.
2. Ensure that there are no errors after execution.

Showing EAPOL multihost interface

About this task

Display the EAPOL interface information.

Procedure

1. Use the **`show eapol multihost interface <port#>`** command to display the interface information.
2. Note the status of ALLOW RADIUS VLANs.

Showing VLAN config control

About this task

Display the VLAN config control information.

Procedure

1. Use the **`show vlan config control`** command to display information.
2. Identify if the config control is set to strict.

Changing VLAN config from strict to flexible

About this task

Set the VLAN config control to flexible to avoid complications with strict.

Procedure

1. Use the **`vlan config control flexible`** command to set the VLAN config control to flexible.
2. Ensure that there are no errors after execution.

Showing spanning tree

About this task

View the VLANs added to the desired STG.

If the RADIUS-assigned VLAN and the original VLAN are in the same STG, the EAP-enabled port is moved to the RADIUS-assigned VLAN after EAP authentication succeeds.

Procedure

1. Use the **`show spanning-tree stp <1-8> vlans`** command to display the information.
2. Identify if the RADIUS-assigned VLAN and the original VLAN are in the same STG.

Adding RADIUS assigned VLAN to desired STG

About this task

Configure the VLAN that was assigned by RADIUS to the correct Spanning Tree Group.

Procedure

1. Use the **`spanning-tree stp <1-8> vlans`** command to make the change.
2. Review the output to identify that the change was made.

Configured MAC is not authenticating

Correct a MAC to allow authentication.

Work flow: Configured MAC is not authenticating

About this task

The following work flow assists you to determine the cause and solution of a configured MAC that does not authenticate as expected.

Procedure

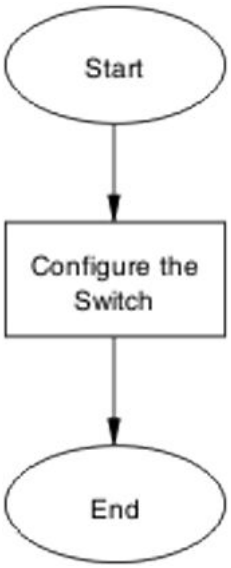


Figure 53: Configured MAC is not authenticating

Configure the switch

Configure the switch to ensure the correct settings are applied to ensure the MAC is authenticating.

Task flow: Configure the switch

About this task

The following task flows assist you to ensure that the MAC is authenticating on the switch.

Procedure

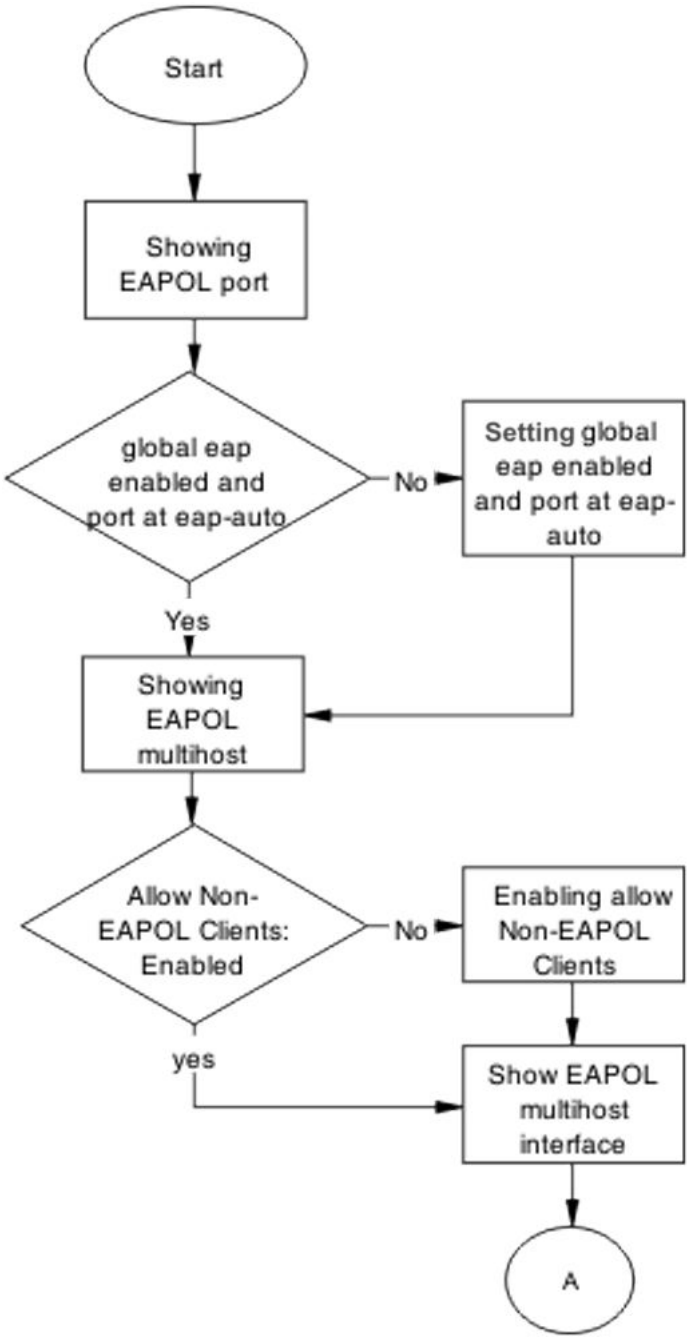


Figure 54: Configure the switch part 1

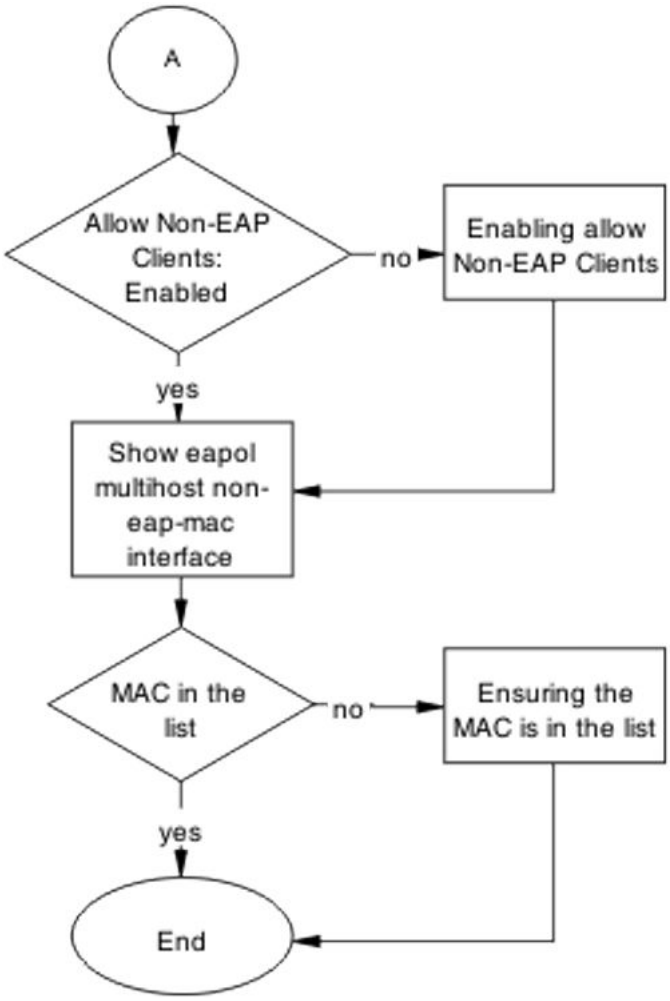


Figure 55: Configure the switch part 2

Showing the EAPOL port

About this task

Display the EAPOL port information

Procedure

1. Use the **`show eapol port <port>`** command to display the port information.
2. Ensure that EAP is enabled globally, and that the port EAP status is set to auto.

Setting global EAP enabled and port at eap-auto

About this task

Make corrections to ensure that EAP is enabled globally, and that the port EAP status is set to auto.

Procedure

1. Use the **`eapol enable`** command to enable EAP globally.

2. Use the **eapol status auto** command to change port status to auto.

Showing EAPOL multihost

About this task

Display the EAPOL multihost information.

Procedure

1. Enter the **show eapol multihost** command to display the information.
2. Ensure that Allow Non-EAPOL clients is enabled.

Enabling allow non-EAPOL clients

About this task

Correct the non-EAPOL client attribute.

Procedure

1. Use the **eapol multihost allow-non-eap-enable** command to allow non-EAPOL clients.
2. Ensure that there are no errors after execution.

Showing EAPOL multihost interface

About this task

Display the EAPOL multihost interface information.

Procedure

1. Enter the **show eapol multihost interface <port#>** command to display the information.
2. Ensure that allow Non-EAPOL clients is enabled.
3. Ensure that the multihost status is enabled.

Showing EAPOL multihost non-eap-mac interface

About this task

Display the EAPOL multihost interface information.

Procedure

1. Enter the **show eapol multihost non-eap-mac interface <port>** command to display the information.
2. Note that the MAC address is in the list.

Ensuring MAC is in the list

About this task

Add the MAC address to the list if it was omitted.

Procedure

1. Use the **`show eapol multihost non-eap-mac status <port>`** command to view MAC addresses.
2. Use the **`eapol multihost non-eap-mac <port> <H.H.H>`** command to add a MAC address to the list.

Non-EAP RADIUS MAC not authenticating

Correct a non-EAP RADIUS MAC that is not authenticating.

Work flow: Non-EAP RADIUS MAC not authenticating

About this task

The following work flow assists you to determine the cause of and solution for a RADIUS MAC that does not authenticate.

Procedure

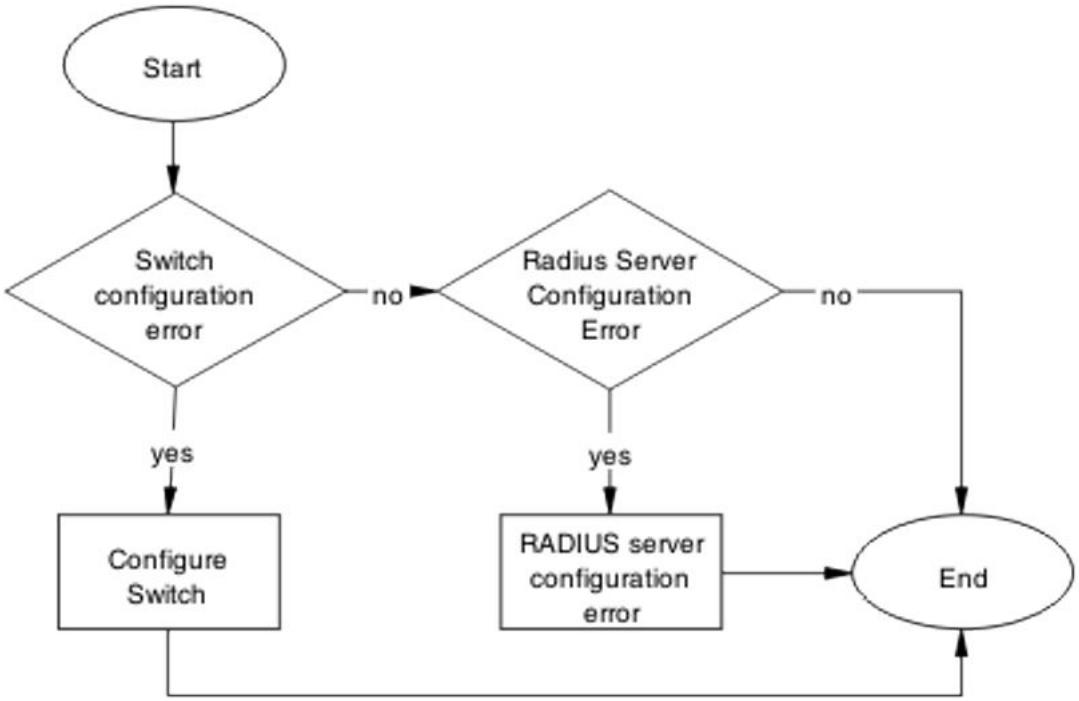


Figure 56: NEAP RADIUS MAC not authenticating

Configure switch

Correct the switch configuration to correct the issue with RADIUS MAC.

Task flow: Configure switch

About this task

The following task flows assist you to configure the switch to correct the RADIUS MAC issue.

Procedure

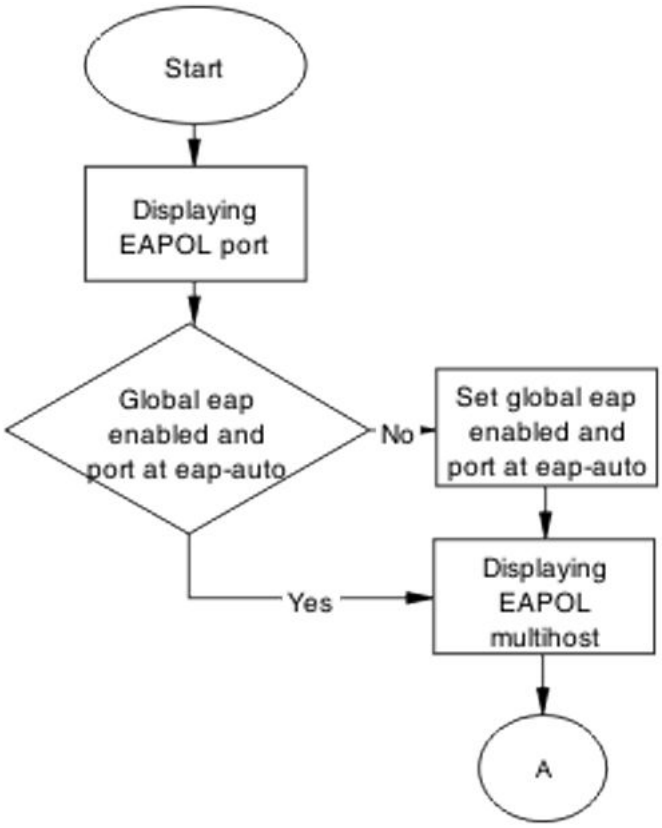


Figure 57: Configure switch part 1

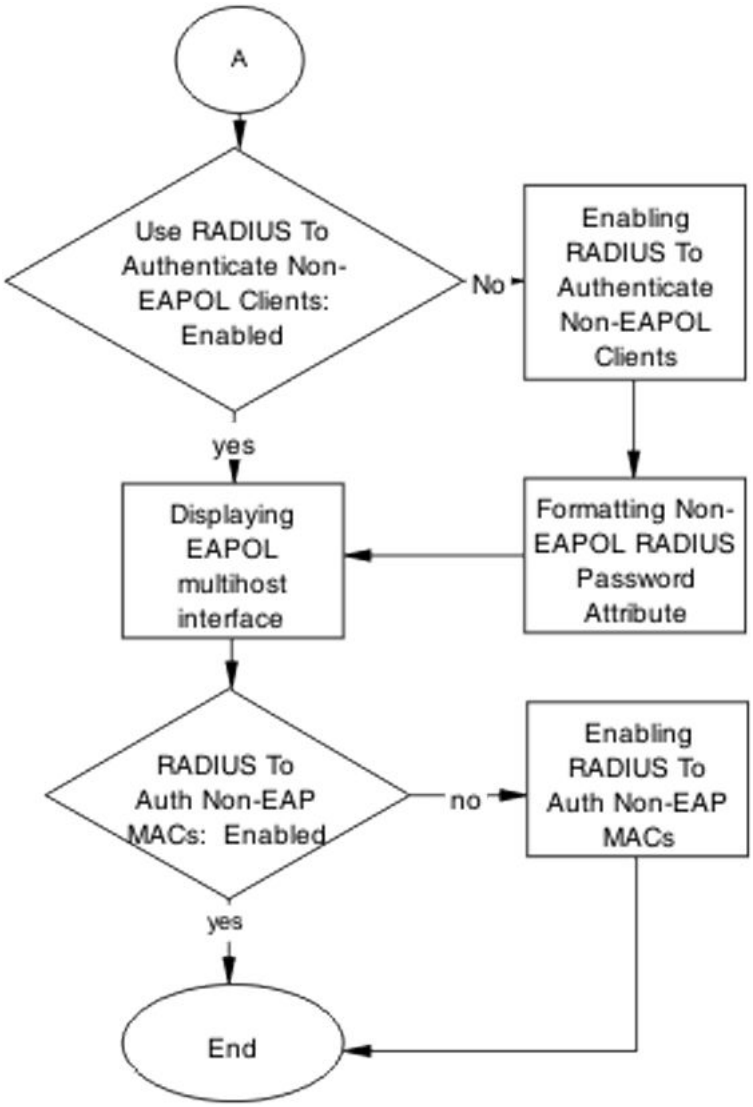


Figure 58: Configure switch part 2

Displaying the EAPOL port

About this task

Review the EAPOL port information.

Procedure

1. Enter the **`show eapol port <port#>`** command to display the information.
2. Ensure that global EAP is enabled and port status is set to eap-auto.

Setting global eap enabled and port at eap-auto

About this task

Make required changes to enable EAP globally and to set the port status to auto.

Procedure

1. Use the **`eapol enable`** command to enable EAP globally.
2. Use the **`eapol status auto`** command to change port status to auto.

Displaying EAPOL multihost

About this task

Review the EAPOL multihost information.

Procedure

1. Enter the **`show eapol multihost`** command to display the information.
2. Note the following:
   - Use RADIUS To Authenticate NonEAPOL Clients is enabled.
   - Non-EAPOL RADIUS password attribute format is **IpAddr.MACAddr.PortNumber**

Enabling RADIUS to authenticate non-EAPOL clients

About this task

Make the required changes on the RADIUS server to authenticate non-EAP clients.

Apply changes to the RADIUS server using vendor documentation.

Formatting non-EAPOL RADIUS password attribute

About this task

Make the required changes to the password format on the RADIUS server.

The RADIUS server is to have the format changed to IpAddr.MACAddr.PortNumber.

Displaying EAPOL multihost interface

About this task

Review the EAPOL multihost information.

Procedure

1. Enter the **`show eapol multihost interface <port#>`** command to display the information.
2. Verify the following:
   - Use RADIUS To Authenticate Non EAP MACs is enabled.

Enabling RADIUS To Auth non-EAP MACs

About this task

Make the required changes on the RADIUS server to authenticate non-EAP clients.

Apply any changes to the RADIUS server using vendor documentation.

RADIUS server configuration error

The RADIUS server requires that the correct MAC address and password for the switch to be configured.

Task flow: RADIUS server configuration error

About this task

The following task flow assists you to configure the RADIUS server with the correct MAC and password.

Procedure

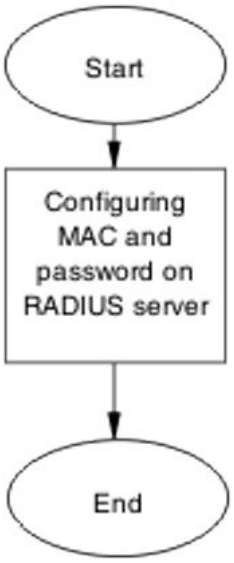


Figure 59: RADIUS server configuration error

Configuring MAC and password on RADIUS server

About this task

The RADIUS server requires that the MAC and password for the switch be correct. If it is incorrect, the switch may not authenticate.

See the vendor documentation for the RADIUS server for details.

Non-EAP MHSA MAC is not authenticating

Ensure that the switch is configured correctly.

Work flow: Non-EAP MHSA MAC is not authenticating

About this task

The following work flow assists you to determine the solution for an MHSA MAC that is not authenticating.

Procedure

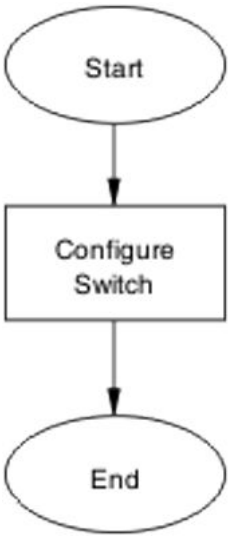


Figure 60: Non-EAP MHSA MAC is not authenticating

Configure switch

Configure the switch to enable MHSA.

Task flow: Configure switch

About this task

The following task flows assist you to enable MHSA on the switch.

Procedure

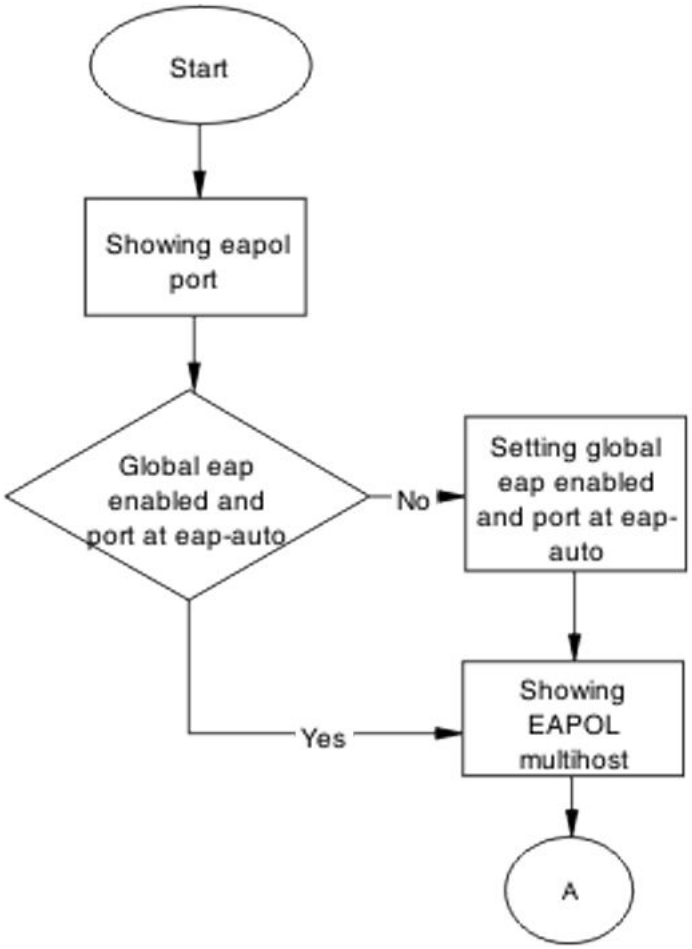


Figure 61: Configure switch part 1

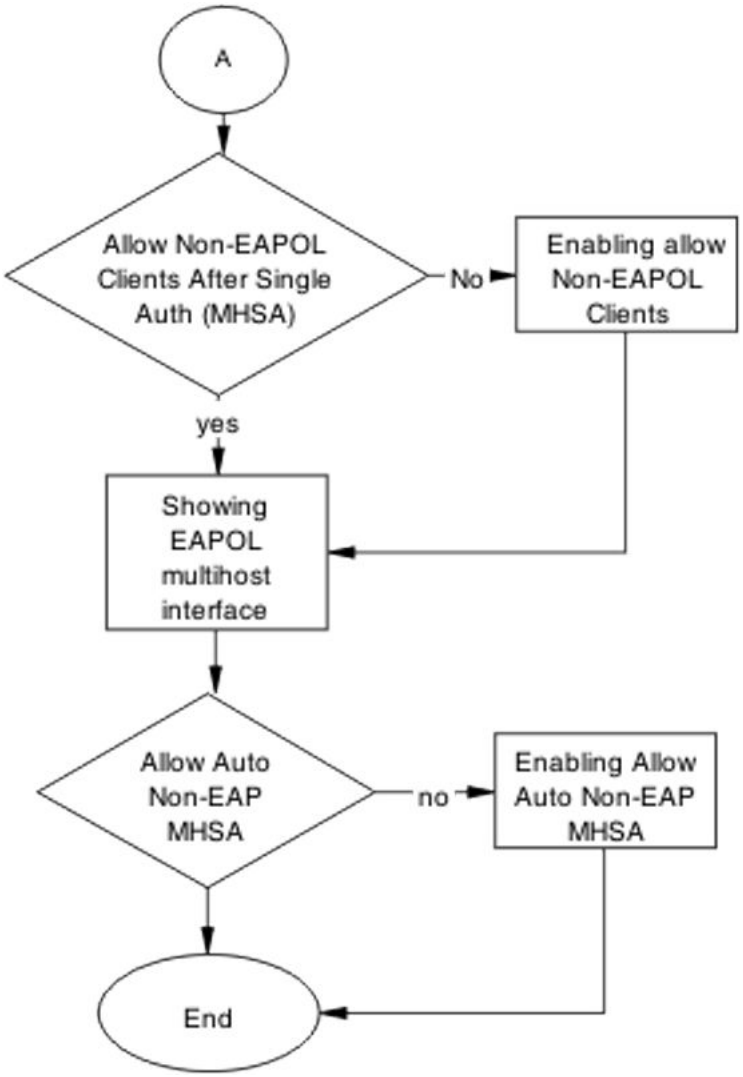


Figure 62: Configure switch part 2

Showing EAPOL port

About this task

Review the EAPOL port information.

Procedure

1. Enter the **`show eapol port <port#>`** command to display the information.
2. Ensure that global EAP is enabled and that the port status is eap-auto.

Setting global EAP enabled and port at eap-auto

About this task

Make the required changes to ensure that EAP is enabled globally and that the port status is set to auto.

Procedure

1. Use the **eapol enable** command to enable EAP globally.
2. Use the **eapol status auto** command to change port status to auto.

Showing EAPOL multihost

About this task

Review the EAPOL multihost information.

Procedure

1. Enter the **show eapol multihost** command to display the information.
2. Note the following:
   - Use RADIUS To Authenticate NonEAPOL Clients is enabled.

Formatting non-EAPOL RADIUS password attribute

About this task

Make the required changes on the RADIUS server to the password format.

Use vendor documentation to make required changes on RADIUS server to change the format to IpAddr.MACAddr.PortNumber.

Enabling RADIUS to authenticate non-EAPOL clients

About this task

Make the required changes on the RADIUS server to authenticate non-EAP clients.

Apply changes to the RADIUS server using vendor documentation.

Showing EAPOL multihost interface

About this task

Review the EAPOL multihost information.

Procedure

1. Enter the **show eapol multihost interface <port#>** command to display the information.
2. Note the following:
   - Allow Auto Non-EAP MHSA: Enabled

Enabling RADIUS to auth non-EAP MACs

About this task

Make the required changes on the RADIUS server to authenticate non-EAP clients.

Apply changes to the RADIUS server using vendor documentation.

EAP–non-EAP unexpected port shutdown

Identify the reason for the port shutdown and make configuration changes to avoid future problems.

Work flow: EAP–non-EAP unexpected port shutdown

About this task

The following work flow assists you to determine the solution for EAP–non-EAP ports experiencing a shutdown.

Procedure

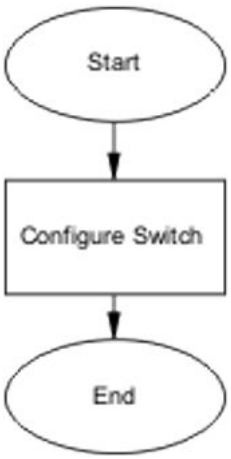


Figure 63: EAP-NEAP unexpected port shutdown

Configure switch

Configure ports to allow more unauthorized clients.

Task flow: Configure switch

About this task

The following task flow assists you to allow an increased number of unauthorized clients on the ports.

Procedure

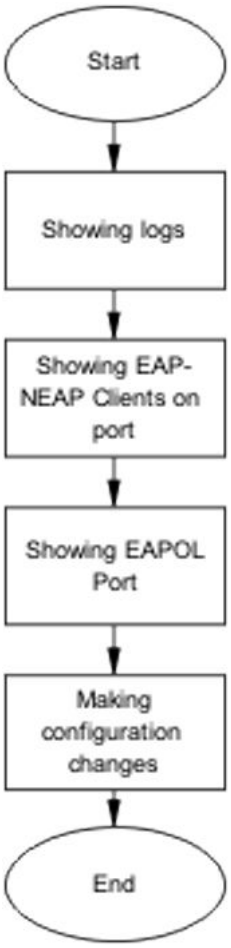


Figure 64: Configure switch

Showing logs

About this task

Display log information to provide additional information.

Procedure

1. Use the **`show logging`** command to display the log.
2. Observe the log output and note anomalies.

Showing EAP–non-EAP clients on port

About this task

Display EAP–non-EAP client information on the port to provide additional information.

Procedure

1. Use the **`show mac-address-table`** command to show the clients on the port.
2. Observe the log output and note anomalies.

Showing EAPOL port information

About this task

Display EAPOL port information for additional information.

Procedure

1. Use the **`show eapol port <port#>`** command to display the port information.
2. Observe the log output and note anomalies.

Making changes

About this task

This section provides troubleshooting guidelines for changing the EAP settings. It assists in the cleanup of old MAC addresses.

Procedure

1. Use the **`eap status unauthorized`** command to set the administrative state of the port to forced unauthorized.
2. Use the **`eapol status auto`** command to change to eap-auto.
3. In the Interface Configuration Mode, use the **`shut/no shut`** commands.

Non-EAP is not a member of a VLAN

If no VLAN is pre-existing on the port, authentication cannot happen because a RADIUS request has not been sent by the switch. NEAP authentication will not occur for a port with no VLAN, but an EAP client on a similarly configured port can be authenticated.

Limitations

- Verify a port with Non-EAP authentication is assigned to at least one VLAN at all times.
- If Non-EAP is not member of a VLAN:
  - Enable Non-EAP authentication on a port that isn't in a VLAN.
  - The port already has Non-EAP authentication enabled, but you want to remove it from all vlans.

    In both cases, the port is added to vlan 1.
- The feature will not take action if vlan 1 and the previous vlan are in different stages.

Non-EAP freeform password

When you configure the RADIUS password, you can also use the following commands:

- `show eapol multihost non-eap-pwd-fmt`—this command shows the password fields and padding.
- `show eapol multihost non-eap-pwd-fmt key`—this command prints the key used. The password is printed in cleartext only when password security is not enabled. Otherwise, the password is printed as a string of asterisks.

Using Trace

Use trace to observe the status of a software module at a given time. Follow the steps in Configuring System Monitoring on Ethernet Routing Switch 4900 and 5900 Series.

Note:

If the trace level is set to a higher level (*Warning* or above), a large number of messages are displayed in CLI. This may cause subsequent commands to not be displayed properly, and the actions of those commands may be executed with a slight delay.

EAP and Non-EAP Separation

Use the EAP/ NEAP separation command to disable EAP clients without disabling NEAP clients. For more information, see Configuring Security on Ethernet Routing Switch 4900 and 5900 Series.

Display EAP Protocol Status

Display EAP protocol status on the interface:

```
4xxx(config)#show eapol multihost interface X
[...]
EAPOL Protocol:  Disabled
[…]
or
4xxx(config)#show eapol multihost interface X
[...]
EAPOL Protocol:  Enable
[…]
```

802.3at LLDP based Discovery

PWR+ devices support the IEEE 802.3at-2009 standard for an Link Layer Discovery Protocol (LLDP) configuration with a Powered Device (PD). The LLDP support for PoE+ is added by extending the existing standard LLDP DOT3 Power via MDI TLV defined by the IEEE 802.1ab with the new fields and values defined in the IEEE 802.3at-2009 standard. Information for power

negotiation between PD and Power Sourcing Equipment (PSE) is described in Power via MDI, which is the optional TLV.

The PoE PD communicates through the Data Link Layer (DLL) classification instead of Physical Layer (high power mode). Hence, the PoE+ capable devices can deliver power greater than 15.4 watts for each port.

You can configure the PoE PD detection type (802.3at or 802.3at_and_legacy) to support a DLL classification for communication. The Data Link Layer classification provides finer power resolution and the ability for PSE and PD to participate in dynamic power allocation. The allocated power to the PD can change one or more times during PD operation.

Before you begin

Follow the steps in Configuring Systems on Ethernet Routing Switch 4900 and 5900 Series.

Procedure

1. Check the LLDPDUs are enabled for transmission and reception on the PoE+ enabled port:

   ```
   show lldp [port <portlist> | all][local-sys-data {dot1 | dot3 | detail | med }]
   ```

2. Check the LLDP DOT3 Power-via-MDI TLV is enabled for transmission in LLDPDUs on the PoE+ enabled port:

   ```
   show lldp [port <portlist> | all][local-sys-data {dot1 | dot3 | detail | med }][rx-stats] [tx-stats] [pdu-tlv-size] [tx-tlv {dot1 | dot3 | med | vendor-specific}]
   ```

3. Display the LLDP DOT3 Power-via-MDI TLV local port data:

   ```
   show lldp [port <portlist> | all][local-sys-data {dot1 | dot3 | detail | med }]
   ```

4. Display the LLDP DOT3 Power-via-MDI TLV neighbor data (for example, a PoE+ endpoint device, like an IP phone). If a neighbor does not support this extended TLV, the supplementary information is not displayed.

   ```
   show lldp [port <portlist> | all] [neighbor {dot1 | dot3 | detail | med }
   ```

5. Display the PoE+ main status. Check that PD Detect type is 802.3at or 802.3at and Legacy:

   ```
   show poe-main-status
   ```

6. Check the PoE port status. It should deliver power. Note the PoE classification for the endpoint device detected on the port, and the power limit set for the port:

   ```
   show poe-port-status [<portlist>]
   ```

7. Display the port PoE power measurement:

   ```
   show poe-power-measurement
   ```

Example

```
(config)#sho lldp port 7 tx-tlv dot3
--------------------------------------------------------------------------------
                            LLDP port dot3 tlvs
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
Port    MacPhy         MdiPower      Link         MaxFrameSize
      ConfigStatus     Support      Aggregation
--------------------------------------------------------------------------------
```

```
7       false         true          false         false
-------------------------------------------------------------------------------
```

```
(config)#sho lldp port 7 tx-tlv dot3
-------------------------------------------------------------------------------
                            LLDP port dot3 tlvs
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
Port    MacPhy        MdiPower      Link         MaxFrameSize
      ConfigStatus    Support      Aggregation
-------------------------------------------------------------------------------
7       false         true          false         false
-------------------------------------------------------------------------------
```

```
(config)#sho lldp port 7 local-sys-data dot3
-------------------------------------------------------------------------------
                       LLDP local-sys-data chassis
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
        ChassisId: MAC address        84:83:71:0a:f8:00
        SysName:
        SysCap:    rB / B             (Supported/Enabled)
        SysDescr:
Ethernet Routing Switch 4826GTS-PWR+  HW:10       FW:5.6.2.1   SW:v5.7.0.114
-------------------------------------------------------------------------------
                       LLDP local-sys-data port
-------------------------------------------------------------------------------
Port:  7
 Dot3-MAC/PHY Auto-neg: supported/enabled       OperMAUtype:  1000BaseTFD
 PSE MDI power:         supported/enabled       Port class:   PSE
 PSE power pair:        signal/not controllable Power class:  0
   PSE: Type: Type 2 PSE    Source: Primary     Priority: Low
   PSE: PD  requested power:  23.0 Watts
   PSE: PSE allocated power:  23.0 Watts
 LinkAggr: not aggregatable/not aggregated      AggrPortID:   0
                                                MaxFrameSize: 9216
 PMD auto-neg:          10Base(T, TFD), 100Base(TX, TXFD), (FdxA)Pause,
                        1000Base(TFD)
-------------------------------------------------------------------------------
Sys capability: O-Other; R-Repeater; B-Bridge; W-WLAN accesspoint; r-Router;
T-Telephone; D-DOCSIS cable device; S-Station only.
```

```
(config)#sho lldp port 7 neighbor dot3
-------------------------------------------------------------------------------
                            LLDP neighbor
-------------------------------------------------------------------------------
Port: 7     Index: 4                  Time: 0 days, 00:53:04
        ChassisId: MAC address        00:10:18:82:0b:bd
        PortId:    MAC address        00:10:18:82:0b:bf
 PSE MDI power:         not supported/disabled  Port class:   PD
 PSE power pair:        spare/not controllable  Power class:  4
   PD: Type: Type 2 PD     Source: PSE         Priority: Low
   PD: PD  requested power:  23.0 Watts
   PD: PSE allocated power:  23.0 Watts
-------------------------------------------------------------------------------
Sys capability: O-Other; R-Repeater; B-Bridge; W-WLAN accesspoint; r-Router;
T-Telephone; D-DOCSIS cable device; S-Station only.
Total neighbors: 3
```

```
(config)# show poe-main-status
PoE Main Status - Stand-alone
-------------------------------------------------
Available DTE Power        : 855 Watts
DTE Power Status           : Normal
DTE Power Consumption      : 5 Watts
DTE Power Usage Threshold  : 80 %
```

```
PD Detect Type              : 802.3at and Legacy
Power Source Present        : AC Only
Primary Power Status        : Present and operational
Redundant Power Status      : Not Present
IP Phone Priority           : N/A
IP Phone Power Limit        : N/A
```

```
(config)#show poe-port-status 7
      Admin      Current                              Limit
Port  Status     Status              Classification   (Watts)  Priority
----  -------    ------------------  --------------   -------  --------
7     Enable     Delivering Power          4          32       Low
```

```
show poe-power-measurement 21
Port  Volt(V)  Current(mA)   Power(Watt)
----  -------  -----------   ---------------
21    53.7     108           5.800
```

Run Scripts

You can use the scripts to configure the parameters for an Ethernet Routing Switch. The scripts can be executed in a default or verbose mode. In this release, run scripts are available in non-verbose and verbose mode for IP Office, and verbose mode for Link Layer Discovery Protocol (LLDP) and Auto Detect Auto Configuration (ADAC).

Follow the steps in Configuring Systems on Ethernet Routing Switch 4900 and 5900 Series.

- Run the scripts on a default configuration, otherwise previous settings may conflict with the script settings and errors may occur.
- Do not run other commands while a script is in progress, especially when the script is run via SNMP (the EDM version), because this will slow down the execution and EDM may time out while waiting for a response.
- When using CLI, the scripts show confirmation messages for the settings that are made.
- If a setting cannot be made, the currently running script stops and an error message is shown.
- The script also logs messages and sends traps to indicate whether it has been successfully executed or an error was encountered. The final configuration can be verified with the ”show running” command.
- Error messages examples:

```
% Error setting VLAN attributes
% Error setting Switch Management IP and network mask % Error configuring 802.1AB
% Error creating Voice VLAN
% Error setting uplink ports
% Error enabling IP Routing
```

Link-state Tracking

Link-state tracking (LST) binds the link state of multiple interfaces. The Link-state tracking feature identifies the upstream and downstream interfaces. The associations between these two interfaces form link-state tracking group.

Follow the steps in Configuring Systems on Ethernet Routing Switch 4900 and 5900 Series.

Guidelines

Follow these guidelines when using Link-state tracking:

- The maximum number of upstream members is 8.
- The maximum number of downstream members is 384.
- Valid interfaces are ports and trunks (MLT / LAG).
- An interface can belong only to a single link-state tracking group.
- A trunk-member port cannot be added to a link-state tracking group by itself.
- Only enabled MLTs can be tracking group members.
- A trunk which is a tracking group member cannot be disabled.
- Ports with link aggregation enabled cannot be added to a tracking group.
- The user is prevented from enabling link aggregation on a tracking group member port.
- Only LAGs with static trunk ids are valid tracking group members.
- A tracking group member LAG cannot be associated with another LACP key, nor can its key binding be removed.
- A LACP key bound with a tracking group member cannot be associated with another set of ports.
- Operational state for interfaces or tracking groups is not saved in binary / ASCII configuration, they are dynamically determined during switch operation.

Retrieving LST Group Information

LST group information is accessible through CLI:

```
4526GTS(config)#show link state detail
Link State Group:     1
Status:               Enabled
VLACP Upstream State: Active on Ports : 2,4
                                Trunks : 1
Operational Status:   Up
Upstream Ports:       1(Up)    2(Down)    3(Down)    4(Down)
Upstream Trunks:      1(Down)
Downstream Ports:     11(Up)   12(Down)   13(Down)   14(Up)
Downstream Trunks:    2(Down)
```

Chapter 11: Troubleshooting IPv6

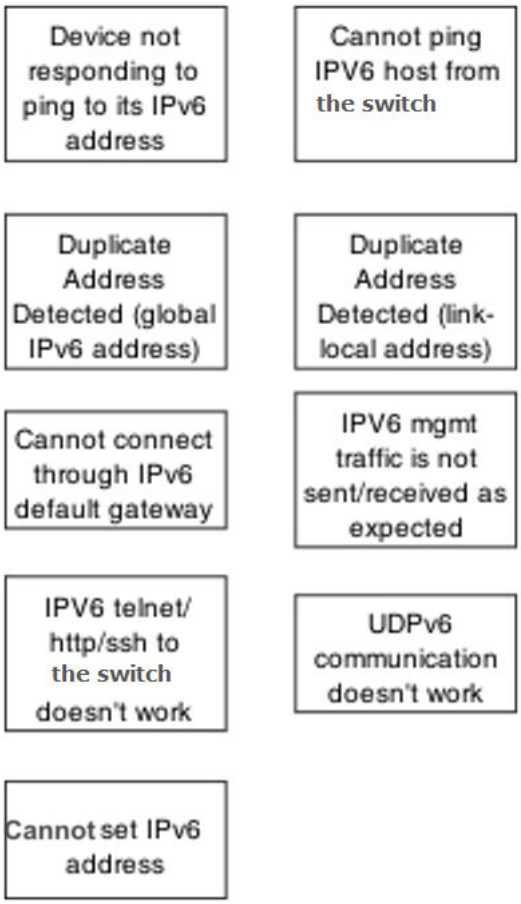
This chapter contains details about how to troubleshoot common IPv6 problems you may encounter.

Troubleshooting IPv6 work flow

About this task

This workflow will assist you to identify common scenarios related to IPv6 that you can troubleshoot.

Procedure



Device not responding to ping to its IPv6 address

When you ping the IPv6 address from another host, the ping fails.

Device not responding to ping to its IPv6 address task flow

About this task

Use these task flows to restore the connectivity through IPv6.

Procedure

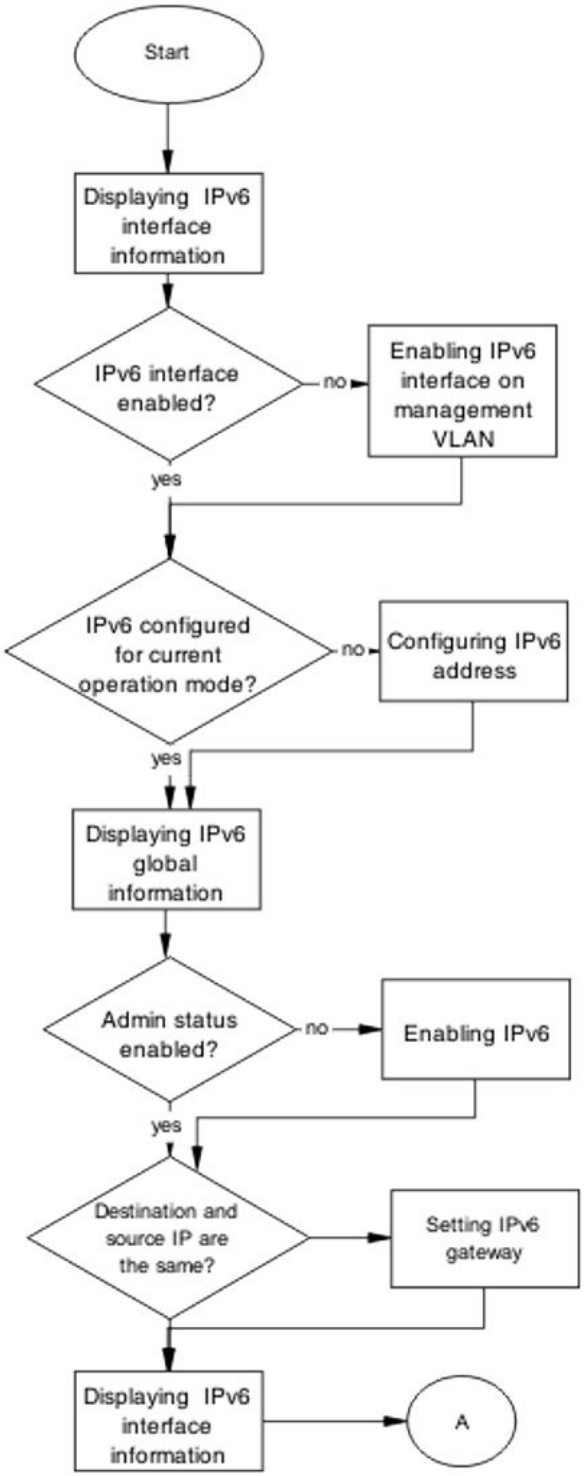


Figure 65: Task flow: Device not responding to ping to its IPv6 address part 1

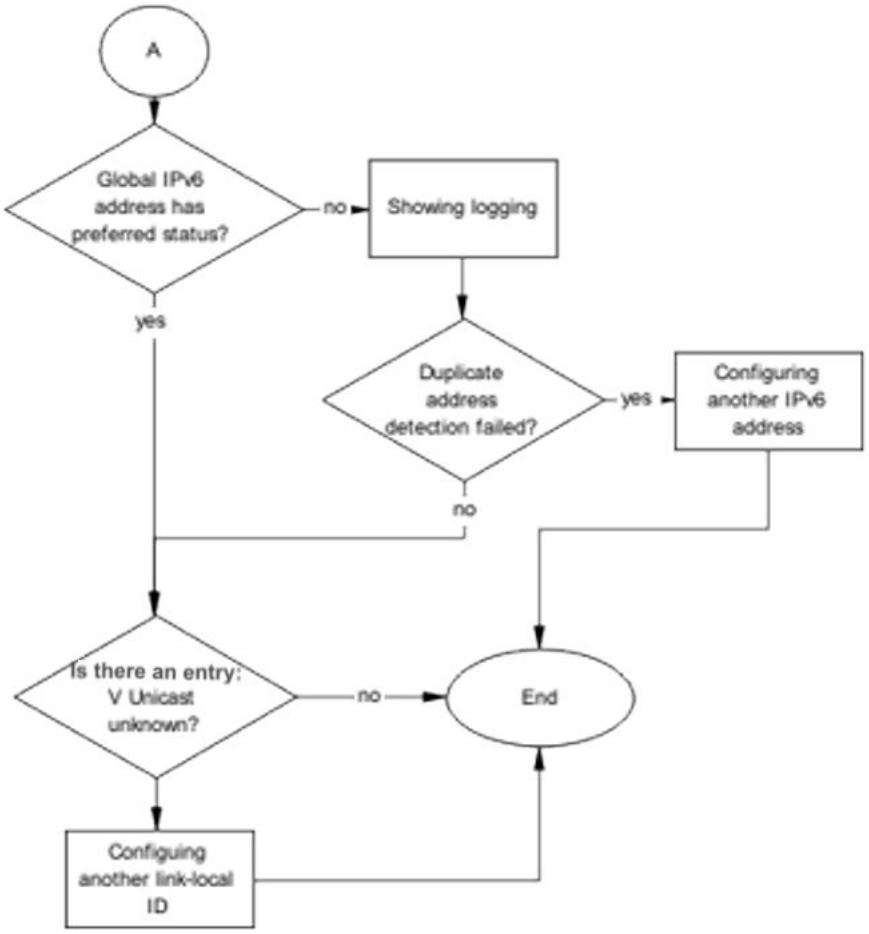


Figure 66: Task flow: Device not responding to ping to its IPv6 address part 2

Displaying IPv6 interface information

About this task

Use the procedure in this section to verify that the IPv6 global admin status is enabled.

Procedure

1. Use the **`show ipv6 global`** command to display the IPv6 global status.
2. Use the **`show ipv6 interface`** command to display the IPv6 interface status.
3. Ensure the admin-status is set to enabled.

Enabling IPv6 interface on management VLAN

About this task

Use this procedure to enable IPv6 on the management VLAN. The operational state becomes active about 30 seconds from boot, synchronized with the time when the IPv4 configured address is in use.

Procedure

1. Use the **`show vlan mgmt`** command to show the management VLAN.
2. Use the **`interface vlan <Number>`** command to configure the management VLAN.
3. Use the **`ipv6 interface enable`** command to enable IPv6 on the management VLAN.
4. Ensure the admin-status is set to enabled.

Configuring IPv6 address

About this task

Use the procedure in this section to configure an IPv6 address for the device.

Procedure

1. Use the **`ipv6 address switch <IPv6 address>`** command to assign an IPv6 address to the switch.
2. Ensure the command completes without error.

Displaying IPv6 global information

About this task

Use the procedure in this section to display IPv6 global information for the device.

Procedure

1. Use the **`show ipv6 global`** command to display the IPv6 global information.
2. Ensure that admin status is enabled.

Enabling IPv6

About this task

Use the procedure in this section to enable IPv6 on the device.

Procedure

1. Use the **ipv6 enable** command to enable IPv6 globally.
2. Ensure that the command completes.

Setting IPv6 gateway

About this task

Use the procedure in this section to set the IPv6 gateway.

Procedure

1. Use the **ipv6 default-gateway <IPv6 address>** command to set the default gateway address.
2. Ensure that the command completes.

Displaying IPv6 interface information

About this task

Use the procedure in this section to display the IPv6 interface information.

Procedure

1. Use the **show ipv6 interface** command to display the IPv6 interface information.
2. Observe that the global IPv6 address has preferred status.

Showing logging

About this task

Use the procedure in this section to display logging information.

Procedure

1. Use the **show logging** command to display logging information.
2. Look for a message that states that duplicate address detection failed.

Configuring another IPv6 address

About this task

Use the procedure in this section to configure a new IPv6 address.

Procedure

1. Use the **`IPv6 address <ipv6_address/prefix_length>`** command to configure a new IPv6 address.
2. Return to the beginning of the task flow if the issue is not resolved.

Configuring another link-local ID

About this task

Use the procedure in this section to configure a new link-local ID.

Procedure

Use the **`IPv6 interface link-local <WORD 0-19>`** command to configure a new link-local ID.

Cannot ping IPV6 host from device console

When you ping an IPv6 address from the device, the ping fails.

Cannot ping IPV6 host from device console task flow

About this task

Use this task flow to restore the connectivity through IPv6.

Procedure

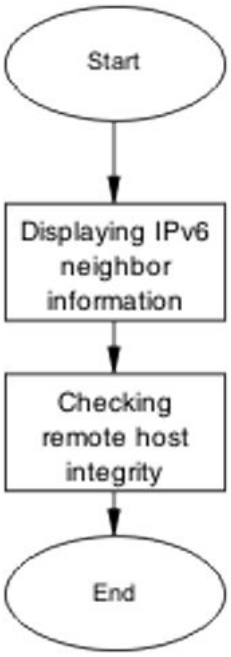


Figure 67: Task flow: Cannot ping IPV6 host from device console

Displaying IPv6 neighbor information

About this task

Use the procedure in this section to show the IPv6 neighbor information.

Procedure

1. Use the **`show ipv6 neighbor <IPv6 address>`** command to display the details of the IPv6 neighbor.
2. Identify if the state is INCOMPLETE.

Checking remote host integrity

About this task

Use the procedure in this section to check the IPv6 integrity of the remote host.

Procedure

1. Use vendor documentation to ensure the remote host is configured correctly for IPv6.
2. Check cabling to ensure that no physical problem exists.

Duplicate address detected (global IPv6 address)

The global address was found to be a duplicate, indicating that another node in the link scope already has the same address.

Duplicate address detected (global IPv6 address)

About this task

Use this task flow to restore the connectivity through IPv6.

Procedure

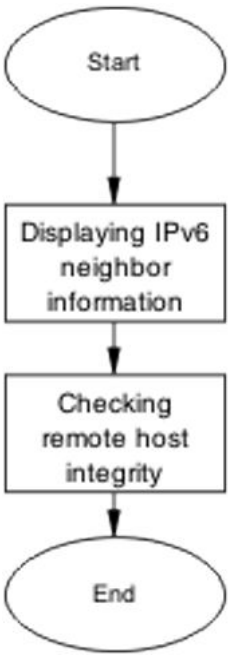


Figure 68: Task flow: Duplicate Address Detected (global IPv6 address)

Displaying IPv6 neighbor information

About this task

Use the procedure in this section to show the IPv6 neighbor information.

Procedure

1. Use the **`show ipv6 neighbor <IPv6 address>`** command to display the details of the IPv6 neighbor.
2. Identify if the state is INCOMPLETE.

Checking remote host integrity

About this task

Use the procedure in this section to check the IPv6 integrity of the remote host.

Procedure

1. Use vendor documentation to ensure the remote host is configured correctly for IPv6.
2. Check cabling to ensure that no physical problem exists.

Duplicate address detected (link-local address)

The global address was found to be a duplicate, indicating that another node in the link scope already has the same address.

Duplicate address detected (link-local address)

About this task

Use this task flow to restore the connectivity through IPv6.

Procedure

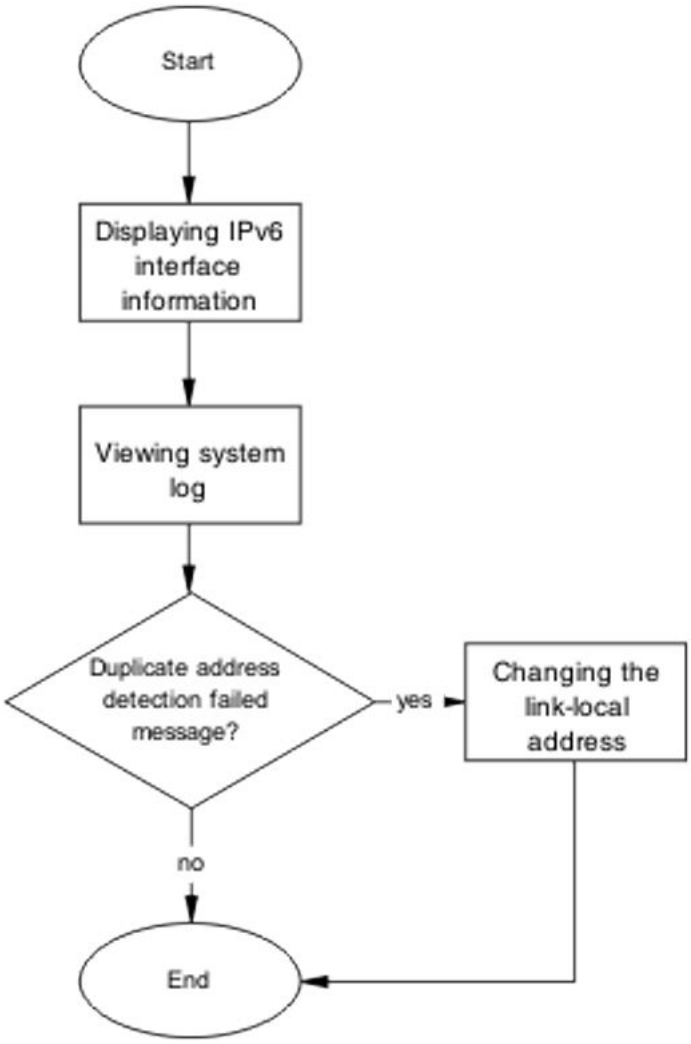


Figure 69: Task flow: Duplicate Address Detected (link-local address)

Displaying IPv6 interface information

About this task

Use the procedure in this section to show the IPv6 interface information.

Procedure

1. Use the **`show ipv6 interface <IPv6 address>`** command to display the details of the IPv6 neighbor.
2. Identify if the state is UNKNOWN.

Viewing the system log

About this task

Use the procedure in this section to view the system log.

Procedure

1. Use the **`show logging`** command to display the system log.
2. Identify an entry: "Duplicate address detection failed."

Changing the link-local address

About this task

Use the procedure in this section to change the 64-bit identifier for the link-local address.

Procedure

1. Use the **`ipv6 interface link-local <IPv6 address>`** command to set the 64-bit identifier.
2. Use the **`show ipv6 interface`** command to view the interface details.
3. Confirm that the unknown multicast address is displayed.

Cannot connect through IPv6 default gateway

This taskflow assists you to correct connections from outside the local subnet (routed) to or from the device through its IPv6 default gateway.

Cannot connect through IPv6 default gateway

About this task

Use this task flow to restore the connectivity through IPv6.

Procedure

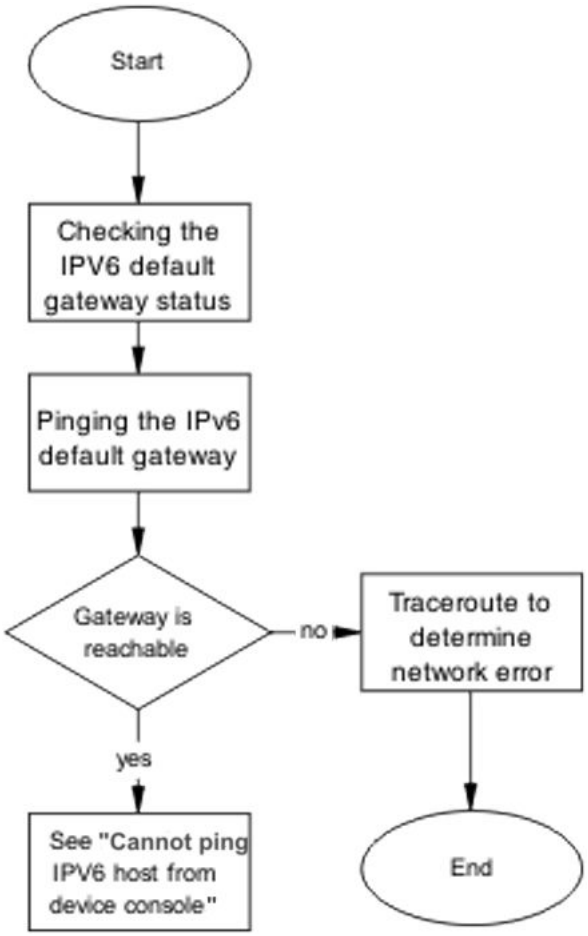


Figure 70: Task flow: Cannot connect through IPv6 default gateway

Checking the IPV6 default gateway status

About this task

Use the procedure in this section to check the IPv6 default gateway status.

Procedure

1. Use the **`show ipv6 default-gateway`** command to display the status of the gateway.
2. Confirm that the status is ReachableInRtm.

Pinging the IPv6 default gateway

About this task

Use the procedure in this section to ping the default gateway.

Procedure

1. Use the **`ping <gaterway address>`** command to ping the 64-bit address of the default gateway.
2. Identify if the host is reachable.

Using traceroute to determine network error

About this task

Use the procedure in this section to identify the route to the gateway.

Procedure

1. Use the **`traceroute <IPv6 address>`** command to identify the route to the gateway.
2. Use the traceroute documentation to interpret the output.

IPv6 management traffic is not sent/received as expected

This taskflow assists you to correct issues with IPv6 management traffic that is not correctly sent or received.

IPv6 management traffic is not sent/received as expected

About this task

Use this task flow to correct issues with IPv6 management traffic that is not correctly sent or received.

Procedure

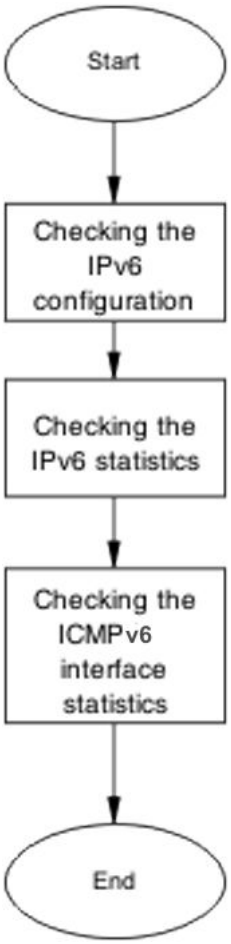


Figure 71: Task flow: IPv6 management traffic is not sent/received as expected

Checking the IPv6 configuration

About this task

Use the procedure in this section to check the IPv6 configuration.

Procedure

Use the **`show ipv6 default-gateway`** command to display the status of the gateway.

Checking the IPv6 statistics

About this task

Use the procedure in this section to view the IPv6 statistics.

Procedure

1. Use the **`show ipv6 interface statistics`** command to show the interface statistics.
2. Observe the command output.

Checking the ICMPv6 statistics

About this task

Use the procedure in this section to view the ICMPv6 statistics.

Procedure

1. Use the **`show ipv6 interface icmpstatistics`** command to display the ICMPv6 statistics.
2. Observe the command output.

IPv6 management traffic over SPB is not sent or received as expected

Use the procedure in this section to verify whether conditions required for IPv6 management over SPB are met.

Procedure

1. Use the `show i-sid` command to verify that the management VLAN is also a C-VLAN.
2. Use the `show ipv6 global` command to verify that the IPv6 global admin status is enabled.
3. Use the `show ipv6 interface` command to verify the IPv6 interface state. The Operational state must be UP.
4. Use the `show ipv6 address interface` command to verify the IPv6 address state. The address must be in PREF state.
5. Use the `show log` command to ensure the duplicate address detection state is not FAIL for the link-local or global address.
6. Use the `show qos diag` to verify that IPv6-over-SPBM filters are installed properly.

IPV6 telnet/http/ssh to device does not work

This taskflow assists you to correct IPv6 connectivity for Telnet, Web, or SSH protocols.

IPV6 telnet/http/ssh to device does not work

About this task

Use this task flow to correct IPv6 connectivity for Telnet, Web, or SSH protocols.

Procedure

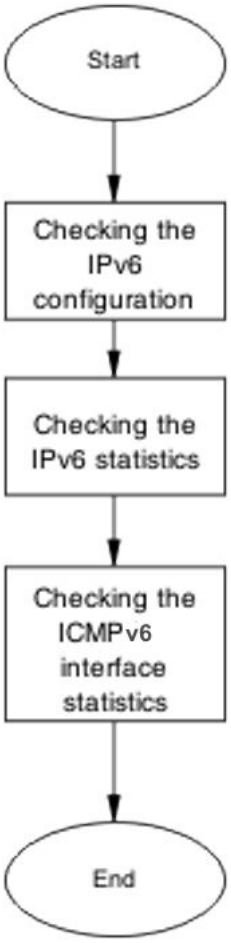


Figure 72: Task flow: IPV6 telnet/http/ssh to device does not work

Checking the IPv6 configuration

About this task

Use the procedure in this section to check the IPv6 configuration.

Procedure

Use the **show ipv6 default-gateway** command to display the status of the gateway.

Checking TCP statistics

About this task

Use the procedure in this section to view the TCP statistics.

Procedure

1. Use the **show ipv6 tcp** command to show the TCP statistics.
2. Use the **show ipv6 tcp connections** command to show the TCP connections.
3. Use the **show ipv6 tcp listener** command to show the TCP listeners.
4. Observe the command output.

UDPv6 communication does not work

This task flow assists you to correct UDPv6 connectivity issues.

UDPv6 communication does not work

About this task

Use this task flow to correct IPv6 connectivity issues for Telnet, Web, or SSH protocols.

Procedure

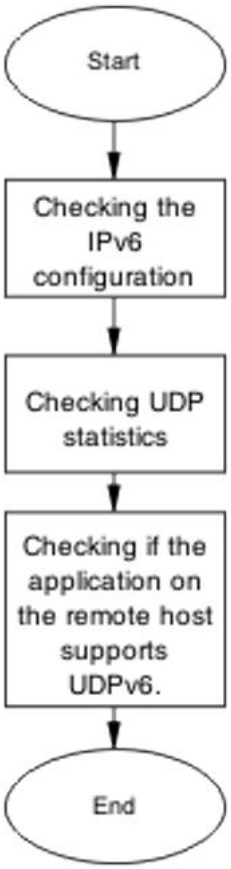


Figure 73: Task flow: UDPv6 communication does not work

Checking the IPv6 configuration

About this task

Use the procedure in this section to check the IPv6 configuration.

Procedure

Use the **`show ipv6 global`** command to display IPv6 configurations.

Checking UDP statistics

About this task

Use the procedure in this section to view the UDP statistics.

Procedure

1. Use the **`show ipv6 udp`** command to show the UDP statistics.

2. Use the **`show ipv6 udp endpoints`** command to show the UDP endpoints.
3. Observe the command output.

Checking if the application on the remote host supports UDPv6.

About this task

Use the client documentation to ensure UDPv6 is enabled on the remote host.

Cannot set IPv6 address

This taskflow assists you when you set an IPv6 address and it fails with the following reason: Max IPv6 addresses per interface exceeded.

Cannot set IPv6 address

About this task

This task flow assists you when you set an IPv6 address and it fails with the following reason: Max IPv6 addresses per interface exceeded.

Procedure

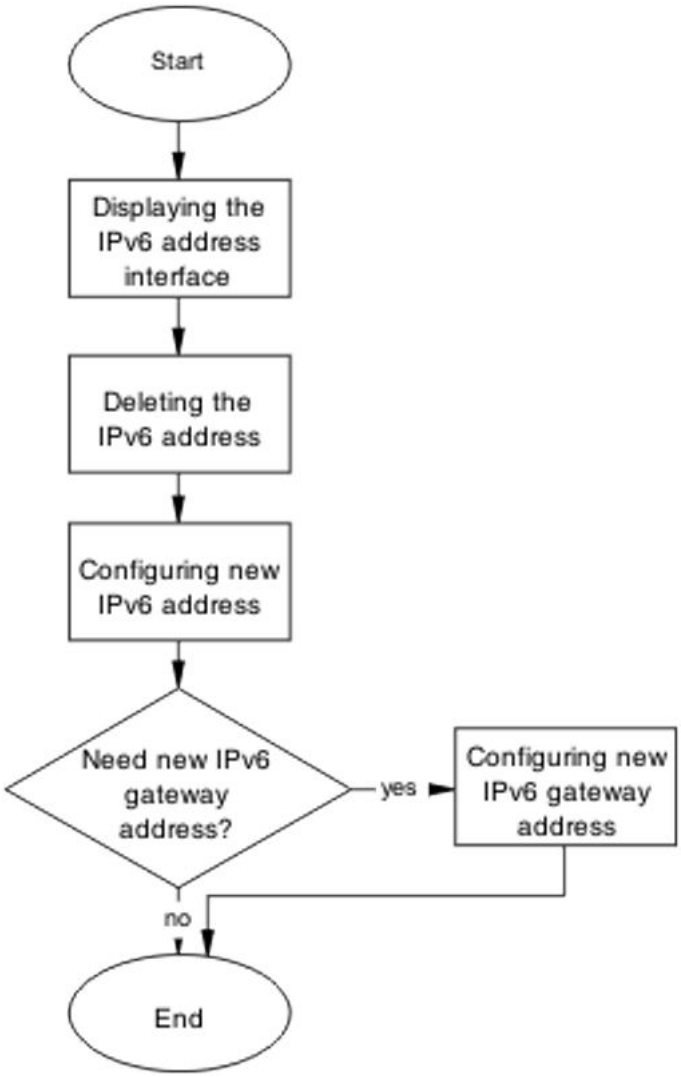


Figure 74: Task flow: Cannot set IPv6 address

Displaying the IPv6 address interface

About this task

Use the procedure in this section to display the IPv6 address interface information.

Procedure

Use the **`show ipv6 address interface`** command to display the IPv6 address interface information.

Deleting the IPv6 address

About this task

Use the procedure in this section to delete the IPv6 address.

Procedure

1. Use the **no ipv6 interface address <IPv6 address>** command to delete the IPv6 address.
2. Observe the command output.

Configuring new IPv6 address

About this task

Use the procedure in this section to configure a new IPv6 address.

Procedure

1. Use the **ipv6 address <IPv6 address>** command to configure the IPv6 address.
2. Observe the command output.

Configuring new IPv6 gateway address

About this task

Use the procedure in this section to configure a new gateway IPv6 address.

Procedure

1. Use the **ipv6 default-gateway <IPv6 address>** command to configure the gateway IPv6 address.
2. Observe the command output.

Chapter 12: Troubleshooting SFP and SFP+

This sections assists you to resolve a problem detecting supported SFP and SFP+ devices.

Troubleshooting SFP/SFP+ workflow

About this task

The following workflow assists you to resolve issues related to detecting SFPs or SFP+s.

Procedure

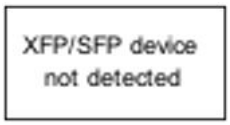


Figure 75: Work flow: Troubleshooting SFP/SFP+

XFP/SFP device not detected

This section describes how you can ensure an XFP or SFP device is connected.

XFP/SFP device not detected task flow

About this task

This following task flow steps you through the procedures to ensure an XFP or SFP device is connected.

Procedure

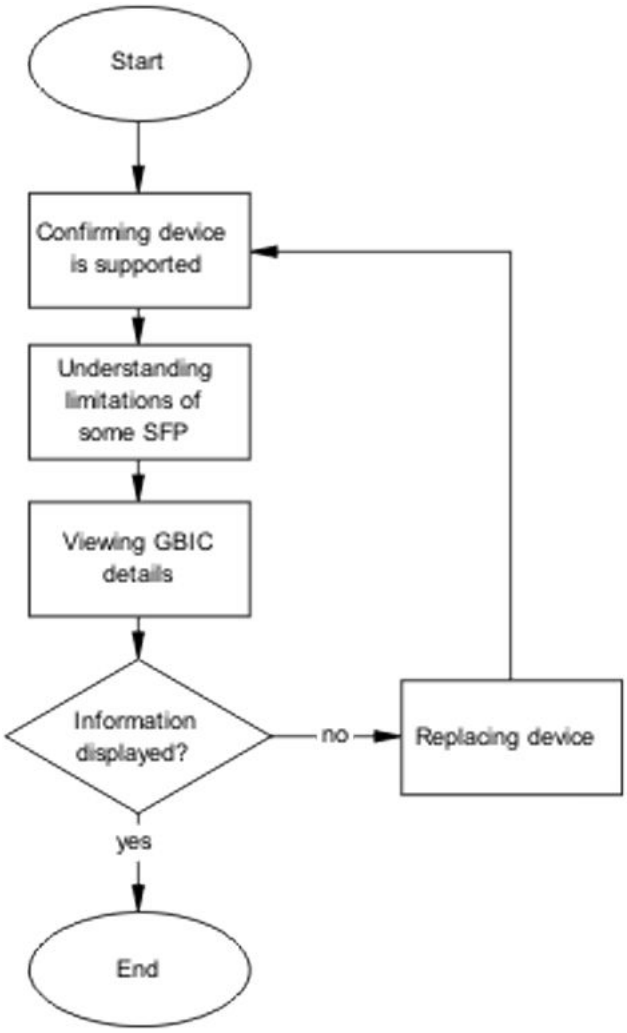


Figure 76: Task flow: XFP/SFP device not detected

Confirming Device is Supported

About this task

See the following XFP and SFP documentation to confirm that the device is supported on the switch:

- Release Notes for Ethernet Routing Switch 4900 and 5900 Series.
- Extreme Networks Pluggable Transceivers Installation Guide.

Enabling DDI logging

About this task

Enable DDI logging on ports.

Procedure

1. Enter Ethernet Interface Configuration mode:

   ```
   enable
   configure terminal
   interface Ethernet <port>
   ```

2. At the command prompt, enter the following command:

   ```
   ddi-logging enable [port <port>]
   ```

   Note:

   By default, logging is disabled for all ports.

Variable definitions

The following table describes the parameters for the **ddi-logging** command.

Variable	Value
port <port>	Specifies the port in one of the following formats: a single port (3), a range of ports (3-4), or a series of ports (3,5,6).

Viewing DDI logging status

About this task

Display DDI logging port status.

Procedure

1. Log on to CLI to enter User EXEC mode.
2. At the command prompt, enter the following command:

   ```
   show ddi-logging
   ```

Example

The following example shows sample output of the **show ddi-logging** command.

```
Switch>show ddi-logging
DDI Logging enabled on ports : 1
```

Viewing SFP DDI information

Use the following procedure to view SFP DDI information.

Procedure

1. Enter Global Configuration mode:

   ```
   enable

   configure terminal
   ```

2. At the command prompt, enter the following command:

   ```
   show interfaces gbic-info
   ```

Example

The following example displays sample output from the **`show interfaces gbic-info`** command.

```
Switch>show interfaces gbic-info
        Port  Number      3
        GBIC   Type       SX
        Wavelength        850 nm
        Vendor Name       EXTREME NETWORKS
        Vendor OUI        00176A
        Vendor Part #     AFBR-5715PZ-NT1
        Vendor Revision   N/A
        Vendor Serial     AVAGCNAS00FV1
        HW Options        TX_DISABLE TX_FAULT RX_LOSS
        Date Code         10/01/2011
        CLEI Code         IPUIAHCWAA
        Product Code      AA1419048-E6


Digital Diagnostic Interface supported

Calibration: Internal
Rx Power Measurement: Average

-------------------------------------------------------------------------------
        LOW_ALARM    LOW_WARN    ACTUAL    HIGH_WARN    HIGH_ALARM       STATUS
        THRESHOLD    THRESHOLD   VALUE     THRESHOLD    THRESHOLD
-------------------------------------------------------------------------------
Temp(C)        -5.000      0.000       29.468      90.000       95.000       NORMAL
Voltage(V)      2.9700     3.0200       3.2934      3.5800       3.6300      NORMAL
Bias(mA)        2.000      3.000        8.216      15.000       16.000       NORMAL
TxPower(dBm)   -9.5000    -8.9997     -5.2374     -1.9997      -1.0001      NORMAL
RxPower(dBm)   -13.0102   -11.9997    -7.3376     -1.0001       0.0000      NORMAL
```

Job aid

The following table describes output for the **`show interfaces gbic-info`** command.

Field	Description
Port Number	Indicates the active GBIC port.

Table continues…

Field	Description
GBIC Type	Indicates the type of SFP or SFP+ connector.
Wavelength	Indicates the wavelength in nm of the SFP or SFP+.
Vendor Name	Indicates the name of the SFP or SFP+ manufacturer.
Vendor OUI	Indicates the vendor ID of the SFP or SFP+ manufacturer.
Vendor Part #	Indicates the model of the SFP or SFP+.
Vendor Revision	Indicates the manufacturer revision level for the SFP or SFP+.
Vendor Serial	Indicates the manufacturer serial number for the SFP or SFP+.
HW Options	Indicates hardware options set for the SFP or SFP+.
Date Code	Indicates the manufacturer date code for the SFP or SFP+.
CLEI Code	Indicates the Telcordia register assignment CLEI code.
Product Code	Indicates the part number of the device.
Calibration	Indicates if the calibration is internal or external.
Rx Power Measurement	Indicates Rx power measurement as average or OMA.
Low_AlarmThreshold	Indicates the low alarm threshold
High_AlarmThreshold	Indicates the high alarm threshold.
High_WarnThreshold	Indicates the high warning threshold
Low_WarnThreshold	Indicates the low warning threshold.
Status	Indicates if any thresholds were exceeded.
Temp(C)	Indicates the current temperature in degrees Celsius of the SFP or SFP+.
Voltage(V)	Indicates the voltage of the SFP in volts.
Bias(mA)	Indicates the laser bias current in mA.
TxPower(dBm)	Indicates the transmit power of the SFP in dBm.
RxPower(dBm)	Indicates the receive power of the SFP in dBm.

Viewing GBIC details

About this task

Use this procedure to display the GBIC device details.

Procedure

1. Enter Global configuration mode.

2. Use the **show interfaces gbic-info** command to view device information.
3. Use the **show interfaces gbic-info port <port number>** command to view device information for a specific port.
4. Use Web-based management to view device information by navigating to Summary, Switch Information, Pluggable Port
5. Identify any unsupported devices.

Replacing device

About this task

Use this procedure to replace a device.

Procedure

1. See XFP and SFP documentation to familiarize yourself with the installation instructions.
2. Connect the SFP or XFP to a different SFP or XFP cage.

Chapter 13: Connectivity Fault Management

Use the information in this chapter to help you understand Connectivity Fault Management (CFM), and how to configure and use CFM using Command Line Interface (CLI) and Enterprise Device Manager (EDM).

CFM fundamentals

The Shortest Path Bridging MAC (SPBM) network needs a mechanism to debug connectivity issues and to isolate faults. Connectivity Fault Management (CFM) operates at Layer 2 and provides an equivalent of ping and traceroute. To support troubleshooting of the SPBM cloud, the switch supports a subset of CFM functionality.

CFM is based on the IEEE 802.1ag standard.

IEEE 802.1ag Connectivity Fault Management (CFM) provides OAM tools for the service layer, which allows you to monitor and troubleshoot an end-to-end Ethernet service instance. CFM is the standard for Layer 2 ping, Layer 2 traceroute, and the end-to-end connectivity check of the Ethernet network.

The 802.1ag feature divides or separates a network into administrative domains called Maintenance Domains (MD). Each MD is further subdivided into logical groupings called Maintenance Associations (MA). A single MD can contain several MAs.

Each MA is defined by a set of Maintenance Points (MP). An MP is a demarcation point on an interface that participates in CFM within an MD. Two types of MP exist:

- Maintenance End Point (MEP)
- Maintenance Intermediate Point (MIP)

CFM supports three kinds of standard CFM messages: Continuity Check Message (CCM), Loopback Message (LBM), and Link Trace Message (LTM). Messages are sent between Maintenance Points (MP) in the system.

On the switch, CFM is implemented using the LBM and LTM features only to debug SPBM. CCM messages are not required or supported in the current release.

Maintenance Domain

A Maintenance Domain (MD) is the part of a network that is controlled by a single administrator. For example, a customer can engage the services of a service provider, who, in turn, can engage the

services of several operators. In this scenario, there can be one MD associated with the customer, one MD associated with the service provider, and one MD associated with each of the operators.

You assign one of the following eight levels to the MD:

- 0–2 (operator levels)
- 3–4 (provider levels)
- 5–7 (customer levels)

The levels separate MDs from each other and provide different areas of functionality to different devices using the network. An MD is characterized by a level and an MD name (optional).

A single MD can contain several Maintenance Associations (MA).

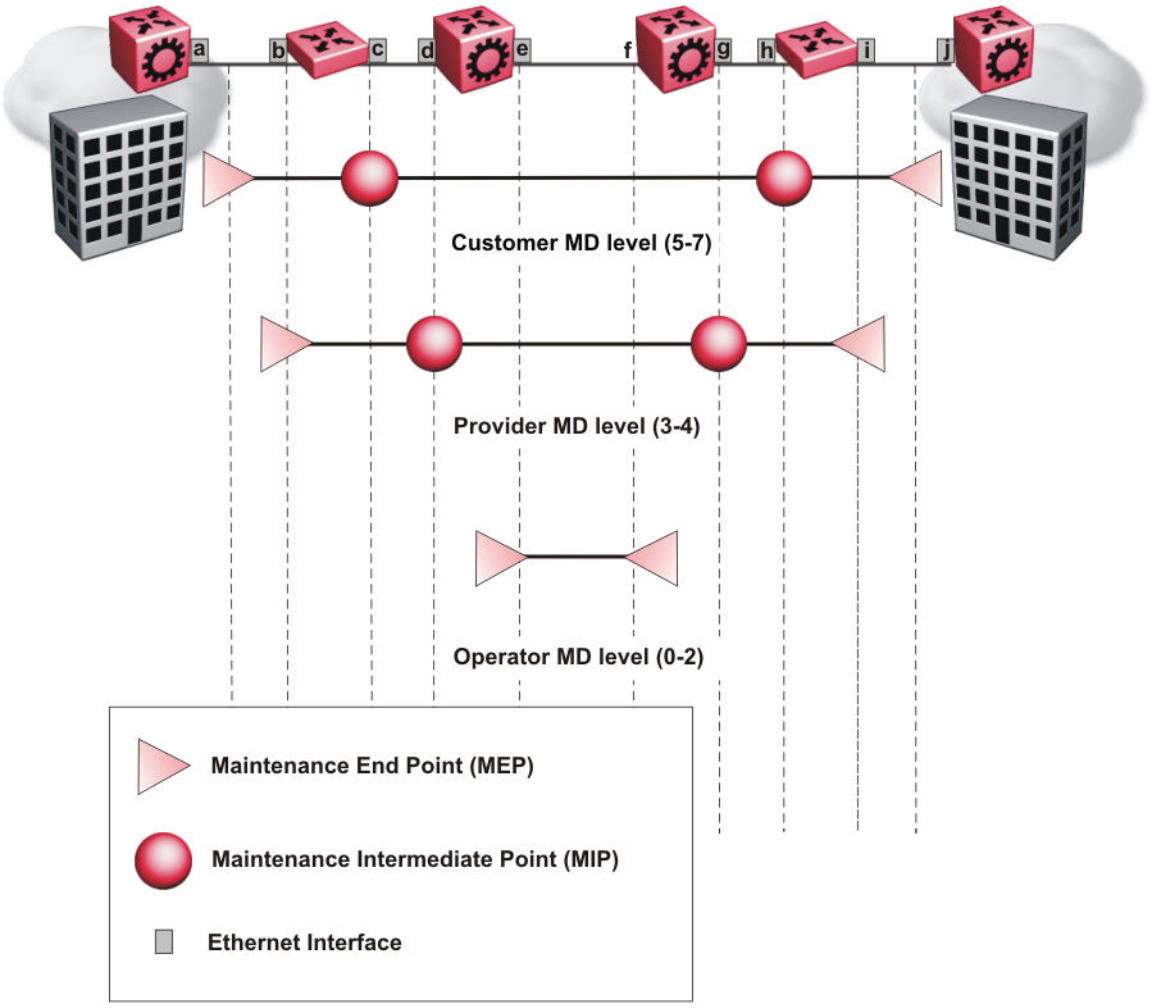
Note:

The switch supports one global MD, named spbm. The spbm MD has a default maintenance level of 4.

Maintenance Association

A Maintenance Association (MA) represents a logical grouping of monitored entities within its Domain. It can therefore represent a set of Maintenance association End Points (MEPs), each configured with the same Maintenance Association ID (MAID) and MD Level, established to verify the integrity of a single service instance.

The following figure shows MD level assignment in accordance with the 802.1ag standard. As shown in the figure, MIPs can be associated with MEPs. However, MIPs can also function independently of MEPs.



Maintenance Endpoint

A Maintenance Endpoint (MEP) represents a managed CFM entity, associated with a specific Domain Service Access Point (DoSAP) of a service instance, which can generate and receive CFM Protocol Data Units (PDU) and track any responses. A MEP is created by MEP ID under the context of an MA. MEP functionality can be divided into the following functions:

- Fault Detection
- Fault Verification
- Fault Isolation
- Fault Notification

Fault detection and notification are achieved through the use of Continuity Check Messages (CCM). CCM messages are not supported in the current release.

Fault verification

Fault verification is achieved through the use of Loopback Messages (LBM). An LBM is a unicast message triggered by the operator issuing an operational command. LBM can be addressed to either a MEP or Maintenance Intermediate Point (MIP) but only a MEP can initiate an LBM. The destination MP can be addressed by its MAC address. The receiving MP responds with a Loopback Response (LBR). LBM can contain an arbitrary amount of data that can be used to diagnose faults as well as performance measurements. The receiving MP copies the data to the LBR.

Loopback Message

The Loopback Message (LBM) packet is often compared to a ping. A MEP transmits the LBM packet. This packet can be addressed to another MEP or to the MAC address of the MP; in the case of SPBM, this is the SPBM system ID. Only the MP for which the packet is addressed responds with an LBR message. You can trigger an LBM with the `l2ping` command.

- Provides “ICMP ping like” functionality natively at Layer 2.
- DA is the MAC address of the target.
- Includes a transaction identifier that allows the corresponding LBR to be identified when more than one LBM request is waiting for a response.
- Only the target (MIP or MEP) responds.
- Initiator can choose the size and content of the data portion of the LBM frame.
- Can be used to check the ability of the network to forward different sized frames.

Layer 2 ping

The **`l2 ping`** command is a proprietary command that allows a user to trigger an LBM message.

For B-VLANs, specify either the destination MAC address or node name.

The **`l2 ping`** command provides a ping equivalent at Layer 2 for use with nodes on the SPBM B-VLAN in the customer domain.

For SPBM networks with IP Shortcut support enabled, the **`ip-address`** parameter is added to support the functionality.

Note:

Layer 2 ping supports B-VLANs only.

Fault isolation

Fault isolation is achieved through the use of Linktrace Messages (LTM). LTM is intercepted by all the MPs on the way to the destination MP. The switch supports two types of LTM.

The first type, the unicast LTM, can be addressed to either MEP or MIP MAC address. Each MP on the way decrements the TTL field in the LTM frame, sends Linktrace Reply (LTR), and forwards the original LTM to the destination. The LTM forwards until it reaches the destination or the TTL value is decremented to zero. LTR is a unicast message addressed to the originating MEP.

The second type, the proprietary LTM, is used to map the MAC addresses of the SPBM network; in this case the target MAC is a service instance identifier (I-SID), not an MP.

Linktrace Message

CFM offers Linktrace Message (LTM) for fault isolation. LTM allow operators, service providers and customers to verify the connectivity that they provide or use and to debug systems.

Link trace message — unicast

The LTM is often compared to traceroute. A MEP transmits the LTM packet. This packet specifies the target MAC address of an MP, which is the SPBM system ID. MPs on the path to the target address respond with an Linktrace reply (LTR). You can trigger an LTM with the `l2traceroute` command.

- LTM trace the path to any given MAC address or System Name.
- DA is unicast
- LTM contains:
  - Time to live (TTL)
  - Transaction Identifier
  - Originator MAC address
  - Target MAC address
- CFM forward the frame like any other data frame.
- MIP or MEP that is not on the path to the target discards the LTM and does not reply.
- MIP that is on the path to the target
  - Forwards the LTM after decrementing the TTL and replacing the SA with its own address.
  - Sends an LTR to the originator.
  - Identifies itself in the forwarded LTM and LTR by modifying TLV information.
- If the MIP or MEP is a target
  - Sends an LTR to the originator.
  - Identifies itself in the forwarded LTM and LTR by modifying TLV information.

- A MEP that is not the target but is on the path to the target
  - Generates a reply as described above.
  - It also sets one of the flags fields in the reply to indicate that it is the terminal MEP.

Link trace message — multicast

The multicast LTM can be used to trace the multicast tree from any node on any I- SID using the nickname MAC address and the I-SID multicast address.

Specifying a multicast target address for an LTM allows for the tracing of the multicast tree corresponding to that destination address (DA). With a multicast target every node that is in the active topology for that multicast address responds with a LTR and also forwards the LTM frame along the multicast path. Missing LTRs from the nodes in the path indicate the point of first failure.

This functionality allows you to better troubleshoot I-SID multicast paths in a SPBM network. You can use the command `l2tracetree` to trace the I-SID tree root.

Layer 2 traceroute

The **`l2traceroute`** command is a proprietary command that allows a user to trigger an LTM message.

For B-VLANs, specify either the destination MAC address or node name.

The **`l2 traceroute`** command provides a trace equivalent at Layer 2 for use with nodes on the SPBM B-VLAN in the customer domain.

For SPBM networks with IP Shortcut support enabled, the **`ip-address`** parameter is added to support the functionality.

Note:

Layer 2 traceroute supports B-VLANs only.

Layer 2 tracemroute

This command is used to verify IP Multicast SPBm routes. When the l2 tracemroute command is issued, all the nodes along the SPBM IP multicast route send a response if it is reachable.

Layer 2 tracetree

The **`l2tracetree`** command is a proprietary command that allows you to trigger a multicast LTM by specifying the B-VLAN and I-SID. Layer 2 tracetree allows you to view a multicast tree on the SPBM B-VLAN from the source node to the destination nodes for a particular I-SID.

Maintenance Domain Intermediate Points

Maintenance Domain Intermediate Points (MIPs) do not initialize any CFM messages. MIPs passively receive CFM messages, process the messages received and respond back to the originating MEP. By responding to received CFM messages, MIPs can support discovery of hop-by-hop path among MEPs, allow connection failures to be isolated to smaller segments of the network to help discover location of faults along the paths. MIP functionality can be summarized as:

- Respond to Loopback (ping) messages at the same level as itself and addressed to it.
- Respond to Linktrace (traceroute) messages.
- Forward Linktrace messages after decrementing the TTL.

Nodal MPs

Nodal MPs provide both MEP and MIP functionality for SPBM deployments. Nodal MPs are associated with a B-VLAN and are VLAN encapsulated packets. The Nodal MEP provides traceability and troubleshooting at the system level for a given B-VLAN. Each switch has a given MAC address and communicates with other switches. The SPBM instance MAC address is used as the MAC address of the Nodal MP. The Nodal B-VLAN MPs supports eight levels of CFM.

Configuration considerations

When you configure CFM, be aware of the following configuration considerations:

- The Maintenance level for MEPs and MIPs on a given B-VID (in a network) must be configured to the same level for them to respond to a given CFM command.
- CFM is supported only on B-VLANs.

CFM configuration using CLI

This section provides procedures to configure and use Connectivity Fault Management (CFM) using Command Line Interface (CLI). The Shortest Path Bridging MAC (SPBM) network needs a mechanism to debug connectivity issues and to isolate faults. This is performed at Layer 2, not Layer 3. To support troubleshooting of the SPBM cloud, the switch supports a subset of CFM functionality

Note:

When you enable CFM in an SBPM network, you should enable CFM on the Backbone Edge Bridges (BEB) and on all Backbone Core Bridges (BCB). If you do not enable CFM on a particular node, you cannot obtain CFM debug information from that node.

Configuring CFM

Use this procedure to configure auto-generated CFM Maintenance End Points (MEPs) and Maintenance Intermediate Point (MIP) level for every SPBM B-VLAN on the switch. This procedure automatically configures a Maintenance Domain (MD) , Maintenance Associations (MAs), MEP ID, and also associates the MEPs and MIP level to the SPBM VLANs.

About this task

When you enable CFM, you create a global MD (named spbm) for all the SPBM Nodal MEPs. The spbm MD has a default maintenance level of 4, which you can change with the level attribute. All the MEPs created use the MEP ID configured under the global context, which has a default value of 1. You can only modify the global context when CFM is disabled. The Nodal MEPs automatically associate with SPBM VLANs and associate to any SPBM VLAN added later. The MIP level maps to the global level. The MIP level automatically associates with the SPBM VLANs when CFM is enabled, and associate to any SPBM VLAN added later.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Configure the maintenance level for every CFM MEP and MIP level on all SPBM VLANs:

   Note:

   You can change the level before or after CFM is enabled. The default level is 4.

   ```
   cfm spbm [level <0-7>]
   ```

3. Assign a global CFM MEP ID for all CFM SPBM MEPs:

   Note:

   You can change the MEP ID only when CFM is disabled.

   ```
   cfm spbm mepid <1-8191>
   ```

4. Enable the CFM:

   ```
   cfm spbm enable
   ```

5. Display the global CFM SPBM configuration:

   ```
   show cfm spbm
   ```

6. If you want to default the CFM MD level, use the following command:

   ```
   default cfm spbm level
   ```

   Note:

   To enable fault verification between two CFM enabled devices, configure same level on both the devices.

7. If you want to default the MEP identifier, use the following command:

   ```
   default cfm spbm mepid
   ```

8. If you want to disable CFM, use one of the following commands:

   ```
   no cfm spbm enable
   ```

   ```
   default cfm spbm enable
   ```

Example

```
Switch> enable
Switch# configure terminal
Switch(config)# cfm spbm level 4
Switch(config)# cfm spbm mepid 200
Switch(config)# cfm spbm enable
Switch(config)# show cfm spbm
CFM Admin State:  Enabled
CFM Spbm Level:  4
CFM Mep Id:  200
```

Variable definitions

Use the data in the following table to use the **`cfm spbm`** commands.

Variable	Value
cfm spbm level *<0–7>*	Specifies the CFM MD level. The default is 4.
cfm spbm mepid *<1–8191>*	Specifies the MEP ID. The default is 1. **Note:** You can only modify the MEP ID when CFM is disabled.
cfm spbm *enable*	Enables CFM globally.
no cfm spbm *enable*	Disables CFM globally.
default cfm spbm level	Defaults the CFM MD level.
default cfm spbm mepid	Defaults the CFM MEP ID.
default cfm spbm enable	Defaults CFM. Default is globally disabled.
show cfm spbm	Displays the current CFM configuration.

Triggering an LBM Layer 2 ping

Use this procedure to trigger a Layer 2 ping, which acts like native ping. This feature enables CFM to debug Layer 2.

Before you begin

CFM SPBM must be enabled.

About this task

The LBM packet is often compared to ping. An MEP transmits the loopback message to an intermediate or endpoint within a domain for the purpose of fault verification. This can be used to check the ability of the network to forward different sized frames.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. Trigger a Layer 2 ping:

   ```
   l2ping {vlan <1-4094> routernodename WORD<0-255> | vlan <1-4094> mac
   <0x00:0x00:0x00:0x00:0x00:0x00> | ip-address <ip>} [burst-count <1-
   200>] [data-tlv-size <0-400>] [frame-size <64-1500>] [priority <0-
   7>] [testfill-pattern <all-zero|all-zero-crc|pseudo-random-bit-
   sequence|pseudo-random-bit-sequence-crc>] [time-out <1-10>]
   ```

Triggering an LTM Layer 2 traceroute

Use this procedure to trigger a Layer 2 traceroute, which acts like native traceroute. This feature enables CFM to debug Layer 2.

Note:

The MAC address must be learned before you can trace a route to a MAC address. For B-VLANs, IS-IS learns the MAC addresses and populates the FDB table.

`linktrace` traces the path up to the closest device to that MAC address that supports CFM.

Before you begin

CFM SPBM must be enabled.

About this task

The link trace message is often compared to traceroute. An MEP transmits the Linktrace Message packet to a maintenance endpoint with intermediate points responding to indicate the path of the traffic within a domain for the purpose of fault isolation. The packet specifies the target MAC address of an MP, which is the SPBM system ID. MPs on the path to the target address respond with an LTR.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. Trigger a Layer 2 traceroute:

   ```
   l2traceroute {<vlan <1-4094> routernodename WORD<0-255> | <vlan <1-4094> mac <0x00:0x00:0x00:0x00:0x00:0x00> | ip-address <ip>} [priority <0-7>] [ttl <1-255>]
   ```

Triggering an LTM Layer 2 tracetree

Use this procedure to trigger a Layer 2 tracetree. Layer 2 tracetree allows a user to trigger a multicast LTM message by specifying the B-VLAN and I-SID. The command allows the user to view a multicast tree on the SPBM B-VLAN from the source node to the destination nodes for a particular I-SID.

Before you begin

CFM SPBM must be enabled.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. Trigger a Layer 2 tracetree:

   ```
   l2tracetree vlan <1-4094> isid <1-16777215> [routernodename WORD<0-255> | mac <0x00:0x00:0x00:0x00:0x00:0x00>] [priority <0-7>] [ttl <1-255>]
   ```

Example

```
Switch# l2tracetree vlan 2 isid 1 mac 53:55:10:00:00:01

Please wait for l2tracetree to complete or press any key to abort


l2tracetree to 53:55:10:00:00:01, vlan 2 i-sid 1 nickname 5.55.10
hops 64
1   ERS-PETER4        00:15:9b:11:33:df -> ERS-MONTI0        00:14:0d:a2:b3:df
2   ERS-MONTI0        00:14:0d:a2:b3:df -> ERS-LEE2          00:15:e8:b8:a3:df
```

Variable definitions

Use the data in the following table to use the **`l2tracetree`** command.

Variable	Value
vlan <*1–4094*> isid <*1–16777215*>	• <1–4094> — Specifies the VLAN ID.

Table continues…

Variable	Value
	• <1–16777215> — Specifies the I-SID.
routernodename *WORD<0–255>*	WORD<0–255> — Specifies the Router Node Name.
mac *<0x00:0x00:0x00:0x00:0x00:0x00:0x00>*	<0x00:0x00:0x00:0x00:0x00:0x00:0x00> — Specifies the MAC address.
ttl *<1–255>*	Specifies the TTL value. The default is 64.
priority *<0–7>*	Specifies the priority value. The default is 7.

Triggering a Layer 2 tracemroute

Use the following procedure to verify IP Multicast over Fabric Connect routes. When the l2 tracemroute is command issued, all the nodes along the IP Multicast over Fabric Connect route send responses if the route is reachable.

Before you begin

- An I-SID must be specified.
- IGMP snooping must be enabled.
- CFM SPBM must be enabled.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Verify the IP Multicast over Fabric Connect routes:

   ```
   l2 tracemroute source <ip address> group <ip address> vlan <1-4094>
   [priority <0-7>|ttl-value <1-255>]
   ```

3. Verify IP Shortcut multicast over Fabric Connect routes:

   ```
   l2 tracemroute source <ip address> group <ip address> [priority <0-
   7>|ttl-value <1-255>]
   ```

Variable definitions

Use the data in the following table to use the **`l2 tracemroute source`** command.

Variable	Value
<A.B.C.D>	Specifies the source IP address.
group <A.B.C.D>	Specifies the IP Multicast over Fabric Connect group IP address.
vlan	Indicates the Vlan ID.

Table continues…

Variable	Value
priority <0–7>	Specifies the priority.
ttl <1–255>	Specifies the Time to Live value.

CFM configuration using EDM

This section provides procedures to configure Connectivity Fault management (CFM) using Enterprise Device Manager (EDM).

Note:

When you enable CFM in an SBPM network, you should enable CFM on the Backbone Edge Bridges (BEB) and on all Backbone Core Bridges (BCB). If you do not enable CFM on a particular node, you cannot obtain CFM debug information from that node.

Configuring CFM

Use this procedure to configure auto-generated CFM Maintenance End Points (MEPs) and Maintenance Intermediate Point (MIP) level for every SPBM B-VLAN on the switch. This procedure automatically configures a Maintenance Domain (MD), Maintenance Associations (MAs), MEP ID, and also associates the MEPs and MIP level to the SPBM VLANs.

About this task

When you enable CFM, you create a global MD (named spbm) for all the SPBM Nodal MEPs. The spbm MD has a default maintenance level of 4, which you can change with the level attribute. All the MEPs created use the MEP ID configured under the global context, which has a default value of 1. You can only modify the global context when CFM is disabled. The Nodal MEPs automatically associate with SPBM VLANs and associate to any SPBM VLAN added later. The MIP level maps to the global level. The MIP level automatically associates with the SPBM VLANs when CFM is enabled, and associate to any SPBM VLAN added later.

Procedure

1. From the navigation tree, expand the following folders: **Configuration** > **Edit** > **Diagnostics**.
2. Click **CFM**.
3. Click the **Globals** tab.
4. In the **SpbmAdminState** field, click a radio button to enable or disable CFM. specify an index value, name, and level for the MD.
5. In the **SpbmLevel** field, configure the maintenance level for every CFM MEP and MIP level on all the SPBM VLANs.
6. In the **SpbmMepId** field, assign a global CFM MEP ID for all CFM SPBM MEPs.
7. On the toolbar, click **Apply**.

Globals field descriptions

Use the data in the following table to use the **Globals** tab.

Name	Description
EtherType	Read only Ethernet type value. Value of 0x8902
SpbmAdminState	Enables or disables the SPBM CFM MD. Click the enable or disable radio button.
SpbmLevel	Specifies the MD level. Default is level 4.
SpbmMepId	Specifies the MEP identifier. Default is 1

Displaying CFM MD

Use this procedure to display the Connectivity Fault Management (CFM) Maintenance Domain (MD). An MD is the part of a network that is controlled by a single administrator. A single MD can contain several Maintenance Associations (MA).

Procedure

1. From the navigation tree, expand the following folders: **Configuration** > **Edit** > **Diagnostics**.
2. Click **CFM**.
3. Click the **MD** tab.
4. On the toolbar, click **Refresh** to display the current MD configuration.

MD field descriptions

Use the data in the following table to use the **MD** tab.

Name	Description
Index	Specifies a maintenance domain entry index.
Name	Specifies the MD name.
NumOfMa	Indicates the number of MAs that belong to this maintenance domain.
Level	Specifies the MD maintenance level. The default is 4.
NumOfMip	Indicates the number of MIPs that belong to this maintenance domain
Type	Indicates the type of domain.

Displaying CFM MA

Use this procedure to display a CFM Maintenance Association (MA). An MA represents a logical grouping of monitored entities within its Domain. It can therefore represent a set of Maintenance Endpoints (MEPs), each configured with the same Maintenance Association ID (MAID) and MD Level, established to verify the integrity of a single service instance.

Before you begin

You must configure a CFM MD.

Procedure

1. In the navigation tree, expand the following folders: **Configuration** > **Edit** > **Diagnostics**.
2. Click **CFM**.
3. Click the **MD** tab.
4. Select an existing MD.
5. On the toolbar, click **MaintenanceAssociation**.

MA field descriptions

Use the data in the following table to use the **MA** tab.

Name	Description
DomainIndex	Specifies the maintenance domain entry index.
AssociationIndex	Specifies a maintenance association entry index.
DomainName	Specifies the MD name.
AssociationName	Specifies the MA name.
NumOfMep	Indicates the number of MEPs that belong to this maintenance association.

Displaying CFM MEP

Use this procedure to display the CFM Maintenance Endpoint (MEP). A MEP represents a managed CFM entity, associated with a specific Domain Service Access Point (DoSAP) of a service instance, which can generate and receive CFM Protocol Data Units (PDU) and track any responses. A MEP is created by MEP ID under the context of an MA.

Procedure

1. In the navigation tree, expand the following folders: **Configuration** > **Edit** > **Diagnostics**.
2. Click **CFM**.
3. Click the **MD** tab.

4. Select an existing MD, and then click **MaintenanceAssociation**.
5. In the **MA** tab, select an existing MA, and then click **MaintenanceEndpoint**.

MEP field descriptions

Use the data in the following table to use the **MEP** tab.

Name	Description
DomainIndex	Specifies the MD index.
AssociationIndex	Specifies the MA index.
Id	Specifies the MEP ID.
DomainName	Specifies the MD name.
AssociationName	Specifies the MA name.
AdminState	Specifies the administrative state of the MEP. The default is disable.
MepType	Specifies the MEP type: • trunk • sg • endpt • vlan • port • endptClient • nodal • remotetrunk • remotesg • remoteendpt • remoteVlan • remotePort • remoteEndptClient
ServiceDescription	Specifies the service to which this MEP is assigned.

Configuring Layer 2 ping

Use this procedure to configure a Layer 2 ping. This feature enables CFM to debug Layer 2. It can also help you debug ARP problems by providing the ability to troubleshoot next hop ARP records.

Before you begin

CFM SPBM must be enabled.

Procedure

1. In the navigation tree, expand the following folders: **Configuration** > **Edit** > **Diagnostics**.
2. Click **L2Ping/L2Trace Route**.
3. From the **L2Ping** tab, configure the Layer 2 ping properties.
4. To initiate a Layer 2 ping, highlight an entry and click the **Start** button.
5. To update a Layer 2 ping, click the **Refresh** button.
6. To stop the Layer 2 ping, click the **Stop** button.

L2Ping field descriptions

Use the data in the following table to use the **L2Ping** tab.

Name	Description
VlanId	Identifies the backbone VLAN.
DestMacAddress	Specifies the target MAC address.
HostName	Specifies the target host name.
DestIsHostName	Indicates whether the host name is (true) or is not (false) used for L2Ping transmission.
Messages	Specifies the number of L2Ping messages to be transmitted. The default is 1.
Status	Specifies the status of the transmit loopback service: • ready: the service is available. • transmit: the service is transmitting, or about to transmit, the L2Ping messages. • abort: the service aborted or is about to abort the L2Ping messages. This field is also used to avoid concurrency or race condition problems that can occur if two or more management entities try to use the service at the same time. The default is ready.
ResultOk	Indicates the result of the operation: • true: the L2Ping Messages will be (or have been) sent. • false: the L2Ping Messages will not be sent. The default is true.
Priority	Specifies a 3–bit value to be used in the VLAN header, if present in the transmitted frame. The default is 7.

Table continues…

Name	Description
TimeoutInt	Specifies the interval to wait for an L2Ping time-out. The default value is 3 seconds.
TestPattern	Specifies the test pattern to use in the L2Ping PDU: • allZero: null signal without cyclic redundancy check • allZeroCrc: null signal with cyclic redundancy check with 32-bit polynomial • pseudoRandomBitSequence: pseudo-random-bit-sequence without cyclic redundancy check • pseudoRandomBitSequenceCrc: pseudo-random-bit-sequence with cyclic redundancy check with 32-bit polynomial. A cyclic redundancy check is a code that detects errors. The default value is allZero.
DataSize	Specifies an arbitrary amount of data to be included in the data TLV, if the data size is selected to be sent. The default is 0.
FrameSize	Specifies the frame size. If the frame size is specified then the data size is internally calculated and the calculated data size is included in the data TLV. The default is 0.
SourceMode	Specifies the source modes of the transmit loopback service: • nodal • smltVirtual The default is nodal.
SeqNumber	The transaction identifier/sequence number of the first loopback message (to be) sent. The default is 0.
Result	Displays the Layer 2 Ping result.

Initiating a Layer 2 traceroute

Use this procedure to trigger a Layer 2 traceroute. This feature enables CFM to debug Layer 2.

If you configure **IsTraceTree** to false then EDM performs Traceroute on the unicast path. If you configure **IsTraceTree** to true then EDM performs TraceTree on the multicast tree.

Important:

The MAC address must be learned before you can trace a route to a MAC address.

For B-VLANs, IS-IS learns the MAC address and populates the FDB table.

Linktrace traces the path up to the closest device to that MAC address that supports CFM.

Before you begin

CFM SPBM must be enabled.

Procedure

1. In the navigation tree, expand the following folders: **Configuration** > **Edit** > **Diagnostics**.
2. Click **L2Ping/L2Trace Route**.
3. Click the **L2 Traceroute/TraceTree** tab.
4. To configure the traceroute or tracetree, highlight an entry and populate the required column fields.
5. To start the traceroute, click the **Start** button.
6. To update the traceroute, click the **Refresh** button.
7. To stop the traceroute, click the **Stop** button.

L2Traceroute/TraceTree field descriptions

Use the data in the following table to use the **L2Traceroute/TraceTree** tab.

Name	Description
VlanId	Specifies a value that uniquely identifies the Backbone VLAN (B-VLAN).
Priority	Specifies a 3–bit value to be used in the VLAN header, if present in the transmitted frame. The default is 7.
DestMacAddress	Specifies the target MAC address.
HostName	Specifies the target host name.
DestIsHostName	Specifies whether the host name is (true) or is not (false) used for the L2Trace transmission.
Isid	Specifies the Service Instance Identifier (I-SID).
NickName	Specifies the nickname of the destination SPBM device.
IsTraceTree	Specifies whether the multicast tree or unicast path is traced. If you configure **IsTraceTree** to false then EDM performs Traceroute on the unicast path. If you configure **IsTraceTree** to true then EDM performs TraceTree on the multicast tree.
Status	Indicates the status of the transmit loopback service: • ready: the service is available. • transmit: the service is transmitting, or about to transmit, the L2Trace messages. • abort: the service aborted or is about to abort the L2Trace messages.

Table continues…

Name	Description
	This field is also used to avoid concurrency or race condition problems that can occur if two or more management entities try to use the service at the same time. The default is ready.
ResultOk	Indicates the result of the operation: • true: the L2Trace messages will be (or have been) sent. • false: the L2Trace messages will not be sent. The default is true.
Ttl	Specifies the number of hops remaining to this L2Trace. This value is decremented by 1 by each Bridge that handles the L2Trace. The decremented value is returned in the L2Trace. If 0 on output, the L2Trace is not transmitted to the next hop. The value of the time-to-live (TTL) field in the L2Trace is defined by the originating MEP. The default value is 64.
SourceMode	Specifies the source mode of the transmit loopback service. The default is nodal.
SeqNumber	Specifies the transaction identifier/sequence number of the first loopback message (to be) sent. The default is 0.
Flag	L2Trace result flag indicating L2Trace status or error code: • none (1): No error • internalError (2): L2Trace internal error • invalidMac (3): Invalid MAC address • mepDisabled (4): MEP must be enabled in order to perform L2Trace • noL2TraceResponse (5): No L2Trace response received • l2TraceToOwnMepMac (6): L2Trace to own MEP MAC is not sent • l2TraceComplete (7): L2Trace completed • l2TraceLookupFailure (8): Lookup failure for L2Trace

Table continues…

Name	Description
	• l2TraceLeafNode (9): On a leaf node in the I-SID tree • l2TraceNotInTree (10): Not in the I-SID tree

Initiating a Layer 2 tracemroute

Before you begin

CFM SPBM must be enabled.

About this task

Use this procedure to trigger a Layer 2 tracemroute.

Procedure

1. In the navigation tree, expand the following folders: **Configuration** > **Edit** > **Diagnostics**.
2. Click **L2Ping/L2Trace Route**.
3. Click **L2 TraceMroute**.
4. Click **Insert**.
5. In the **SrcIpAddrType** field, enter the source IP address.
6. In the **GroupIpAddr** field, enter the group IP address.
7. In the **VlanId** field, enter the VLAN id.
8. In the **Priority** field, enter the priority.
9. In the **Ttl** field, enter the Time to Live value.
10. Click **Insert**.

L2 Tracemroute field descriptions

Use the data in the following table to use the **L2 TraceMroute** tab.

Name	Description
SrcIPAddrType	Specifies the ipv4 address type.
SrcIpAddr	Specifies the source IP address.
GroupIpAddrType	Specifies the SPBM multicast group ipv4 address type.
GroupIpAddr	Specifies the SPBM multicast group IP address.
ServiceType	Indicates value maps to VLAN. ServiceType can be vlan or vrfid.
VlanId	Indicates the Vlan ID.

Table continues…

Name	Description
Priority	Specifies a 3–bit value to be used in the VLAN header, if present in the transmitted frame. The default is 7.
Ttl	Specifies the Time to Live value.
SeqNumber	Specifies the transaction identifier or sequence number of the first message sent or to be sent.
Status	Specifies the status of the transmit loopback service: • ready: the service is available. • transmit: the service is transmitting, or about to transmit the trace messages. • abort: the service is aborted or about to abort the trace messages. This field is also used to avoid concurrency or race condition problems that could occur if two or more management entities try to use the service at the same time.
ResultOk	Indicates the result of the operation: • true: the Trace Message(s) will, or have been sent. • false: the Trace Message(s) will not be sent.
Flag	L2Tracemroute result flag indicating L2Tracemroute status or error code. Each of the following values represents a status or error case: • 1 - No error • 2 - Internal Error • 3 - Mep must be enabled in order to perform trace • 4 - No response received • 5 - Trace completed • 6 - On a leaf node in the I-SID tree • 7 - No Data Isid was found for S,G

Viewing Layer 2 traceroute results

Use this procedure to view Layer 2 traceroute results. This feature enables CFM to debug Layer 2. You can use Layer 2 traceroute to debug ARP problems by troubleshooting next hop ARP records.

About this task

You can display Layer 2 tracetree results to view a multicast tree on the SPBM B-VLAN from the source node to the destination nodes for a particular I-SID.

Procedure

1. In the navigation tree, expand the following folders: **Configuration** > **Edit** > **Diagnostics**.
2. Click **L2Ping/L2Trace Route**.
3. Click the **L2Traceroute/TraceTree** tab.
4. Click the **Refresh** button to update the results.
5. To view the traceroute results, highlight an entry, and then click **Result**.

L2 Tracerout/TraceTree Result field descriptions

Use the data in the following table to use the **L2 Tracerout/TraceTree Result** tab.

Name	Description
VlanId	A value that uniquely identifies the Backbone VLAN (B-VLAN).
SeqNumber	The transaction identifier/sequence number of the first loopback message (to be) sent. The default is 0.
Hop	The number of hops away from L2Trace initiator.
ReceiveOrder	An index to distinguish among multiple L2Trace responses with the same Transaction Identifier field value. This value is assigned sequentially from 1, inthe order that the Linktrace Initiator received the responses.
Ttl	Time-to-Live (TTL) field value for a returned L2Trace response.
SrcMac	MAC address of the MP that responds to the L2Trace request for this L2TraceReply.
HostName	The host name of the replying node.
LastSrcMac	The MAC address of the node that forwarded the L2Trace to the responding node.
LastHostName	The host name of the node that forwarded the L2Trace to the responding node.
Ttl	Time-to-Live (TTL) field value for a returned L2Trace response.

Viewing Layer 2 tracemroute results

About this task

Use this procedure to view Layer 2 tracemoute results.

Procedure

1. In the navigation tree, expand the following folders: **Configuration** > **Edit** > **Diagnostics**.
2. Click **L2Ping/L2Trace Route**.
3. Click the **L2 TraceMroute** tab.
4. Click the **Refresh** button to update the results.
5. To view the tracemroute results, highlight an entry, and then click **Result**.

L2 Tracemroute Result field descriptions

Use the data in the following table to use the **L2 TraceMroute Result** tab.

Name	Description
SrcIPAddrType	Specifies the ipv4 address type.
SrcIpAddr	Specifies the source IP address.
GroupIpAddrType	Specifies the IP Multicast over Fabric Connect group ipv4 address type.
GroupIpAddr	Specifies the IP Multicast over Fabric Connect group IP address.
ServiceType	Indicates value maps to VLAN. ServiceType can be vlan or vrfid.
ServiceId	Specifies the value of VLAN. Range is from 1 to 4094.
Hop	The number of hops away from trace initiator.
ReceiveOrder	An index to distinguish among multiple responses with the same Transaction Identifier field value. This value is assigned sequentially from 1, in the order that the Linktrace Initiator received the responses.
Ttl	Specifies the Time to Live value.
SrcMac	MAC address of the MP that responds to the L2TraceMroute request for this L2TraceReply.
HostName	The host name of the replying node.
LastSrcMac	The MAC address of the node that forwarded the L2TraceMroute to the responding node.
LastHostName	The host name of the node that forwarded the L2TraceMroute to the responding node.
SpbmVlanId	Specifies the SPBM VLAN ID used for the trace.
Bmac	Specifies the multicast MAC address for the group.
Isid	Specifies the Service Instance Identifier (I-SID).

Chapter 14: Troubleshooting IGMP

This sections assists you to resolve multicast flooding issues.

Multicast packets not flooding network

This section describes how you can enable multicast flooding on a network.

Multicast packets not flooding network task flow

About this task

The following task flow steps you through the procedures to enable multicast flooding on the network.

Procedure

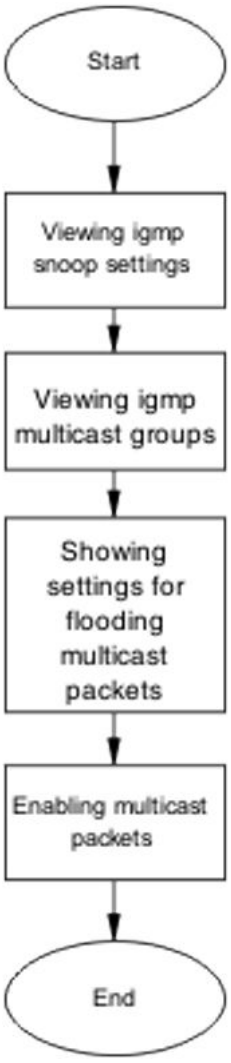


Figure 77: Task flow: Multicast packets not flooding network

Result

Navigation

- Viewing IGMP Snoop Settings on page 194
- Viewing IGMP multicast groups on page 197

Viewing IGMP Snoop Settings

About this task

Use this procedure to display general information about IGMP snooping in a specific VLAN.

Note:

To ensure all fields are displayed in the command output, increase the terminal width using the `terminal width 132` command.

Procedure

1. Enter Interface Configuration mode:

   enable

   configure terminal

   interface vlan <vid>

2. Use the **`show ip igmp interface`** command to display IGMP interface information.
3. Use the **`show ip igmp snooping`** command to display information about the IGMP snooping configuration.
4. Observe the displayed information.

Example

The following is an example of verifying the IGMP snooping configuration.

```
Switch(config)#show ip igmp interface vlan 101
     Query      Oper                 Query   Wrong              LastMbr Send
VLAN Intvl Vers Vers Querier         MaxRspT Query Joins Robust Query   Query Mode
---- ----- ---- ---- --------------- ------- ----- ----- ------ ------- ----- ----------

101  125   2    2    0.0.0.0         100     0     0     2      10      Yes   routed-spb

Switch(config)#show ip igmp interface vlan 201
     Query      Oper                 Query   Wrong              LastMbr Send
VLAN Intvl Vers Vers Querier         MaxRspT Query Joins Robust Query   Query Mode
---- ----- ---- ---- --------------- ------- ----- ----- ------ ------- ----- ----------

201  125   2    2    0.0.0.0         100     0     0     2      10      Yes   snoop-spb
```

Variable Definitions

Variable	Definition
<vid>	Specifies the VLAN ID between 1 and 4094.

Job aid

The following table describes the output of the command **`show ip igmp interface`**.

Field	Description
VLAN	Indicates the VLAN on which IGMP is configured.
Query Intvl	Specifies the frequency (in seconds) at which host query packets are transmitted on the interface.
Vers	Specifies the version of IGMP configured on this interface.

Table continues…

Field	Description
Oper Vers	Specifies the version of IGMP running on this interface.
Querier	Specifies the IP address of the IGMP querier on the IP subnet to which this interface is attached.
Query MaxRspT	Indicates the maximum query response time (in tenths of a second) advertised in IGMPv2 queries on this interface.
Wrong Query	Indicates the number of queries received whose IGMP version does not match the Interface version. You must configure all routers on a LAN to run the same version of IGMP. Thus, if queries are received with the wrong version, a configuration error occurs.
Joins	Indicates the number of times a group membership was added on this interface.
Robust	Specifies the robust value configured for expected packet loss on the interface.
LastMbr Query	Indicates the maximum response time (in tenths of a second) inserted into group-specific queries sent in response to leave group messages, and is also the amount of time between group specific query messages. Use this value to modify the leave latency of the network. A reduced value results in reduced time to detect the loss of the last member of a group. This does not apply if the interface is configured for IGMPv1.
Send Query	Indicates whether the ip igmp send-query feature is enabled or disabled. Values are YES or NO. Default is disabled.
MODE	Indicates the protocol configured on the VLAN added. If routed-spb displays in the MODE column, then IP Multicast over Fabric Connect is enabled on the Layer 3 VSN or for IP shortcuts. If snoop-spb displays in the MODE column, then IGMP is enabled on a VLAN with an associated I-SID (Layer 2 VSN).

The following table describes the output of the command **`show ip igmp snooping`**.

Field	Description
Vlan	Indicates the VLAN ID.
Snoop Enable	Indicates whether snoop is enabled (true) or disabled (false).
Proxy Snoop Enable	Indicates whether IGMP proxy is enabled (true) or disabled (false).

Table continues…

Field	Description
Static Mrouter Ports	Indicates the static mrouter ports in this VLAN that provide connectivity to an IP multicast router.
Active Mrouter Ports	Displays all dynamic (querier port) and static mrouter ports that are active on the interface.
Mrouter Expiration Time	Specifies the time remaining before the multicast router is aged out on this interface. If the switch does not receive queries before this time expires, it flushes out all group memberships known to the VLAN. The Query Max Response Interval (obtained from the queries received) is used as the timer resolution.

Viewing IGMP multicast groups

About this task

Use this procedure to display general information about IGMP snooping in a specific VLAN.

Procedure

1. Use the **`show ip igmp group`** command to display the information.
2. Observe the displayed information.

Job aid

The following table describes the output of the command.

Field	Description
Group Address	Indicates the multicast group address
VLAN	Indicates the VLAN interface on which the group exists.
Member Address	Indicates the IP address of the IGMP receiver (host or IGMP reporter). The IP address is 0.0.0.0 if the type is static.
Expiration	Indicates the time left before the group report expires. This variable is updated upon receiving a group report.
Type	Specifies the type of membership: static or dynamic
In Port	Identifies the member port for the group. This is the port on which group traffic is forwarded and in those case where the type is dynamic, it is the port on which the IGMP join was received.

Flushing the IGMP router table

About this task

Use this procedure to flush the IGMP router table.

If multicast traffic does not reach a client port, flush the port in order to re-learn the client on the port. If a group is not learned, flush IGMP group members in order to re-learn the group.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. Flush entries from the IGMP router table:

   ```
   ip igmp flush {all {grp-member | mrouter | stream} | ethernet
   <portlist>}
   ```

Variable definitions

Use the data in the following table to use the **`ip igmp flush`** command.

Variable	Description
all	Flushes all entries of the selected type.
grp-member	Flushes the learned IGMP group members.
mrouter	Flushes the IGMP Mrouters.
stream	Flushes the received IGMP streams.
ethernet <portlist>	Specifies the port or list of ports to flush.
vlan <1-4094>	Specifies the VLAN interface for which to flush selected type entries.

Viewing MVR information

This section describes how you can view MVR information on a network.

Configuring MVR globally

Before you begin

Disable Protocol Independent Multicast (PIM).

Procedure

1. Enter Global Configuration mode:

```
enable
configure terminal
```

2. Configure MVR on the switch:

```
[no] mvr enable
```

Variable definitions

Variable	Value
no	Disables MVR on the switch.

Viewing MVR VLAN configuration

Before you begin

Enable MVR globally.

Procedure

1. Enter Privileged EXEC mode:

```
enable
```

2. Enter the following command to display the MVR VLAN configuration:

```
show mvr vlan
```

Example

```
Switch(config)#show mvr vlan
VLAN  Type
----  --------
100   Source
200   Receiver
300
400   Receiver
```

Viewing MVR global information

Procedure

1. Enter Privileged EXEC mode:

```
enable
```

2. Display MVR global information:

```
show mvr
```

Example

```
Switch(config)#show mvr
MVR Admin Status: Enabled
MVR Multicast Source VLAN: 100
```

Viewing configured MVR IP Multicast address ranges

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. Display the configured MVR IP Multicast address ranges:

   ```
   show mvr group-range
   ```

Example

```
Switch#show mvr group
Switch#show mvr group-range
Group             Mask
---------------  ---------------
233.252.0.1         255.255.255.0
233.252.0.2         255.255.255.0
Number of Entries: 2
```

Chapter 15: Troubleshooting RSTP SNMP traps

The Rapid Spanning Tree Protocol (RSTP) SNMP traps feature provides the ability to receive SNMP notification about the RSTP protocol. These events are also logged to syslog.

Troubleshooting RSTP SNMP traps workflow

About this task

The following workflow assists you to resolve RSTP trap issues.

Procedure

Figure 78: Work flow: Troubleshooting RSTP SNMP traps

No RSTP SNMP traps are received

Use this task flow to help you ensure that RSTP SNMP traps are received.

No RSTP SNMP traps are received task flow

About this task

The following task flow helps you to ensure that RSTP SNMP traps are received.

Procedure

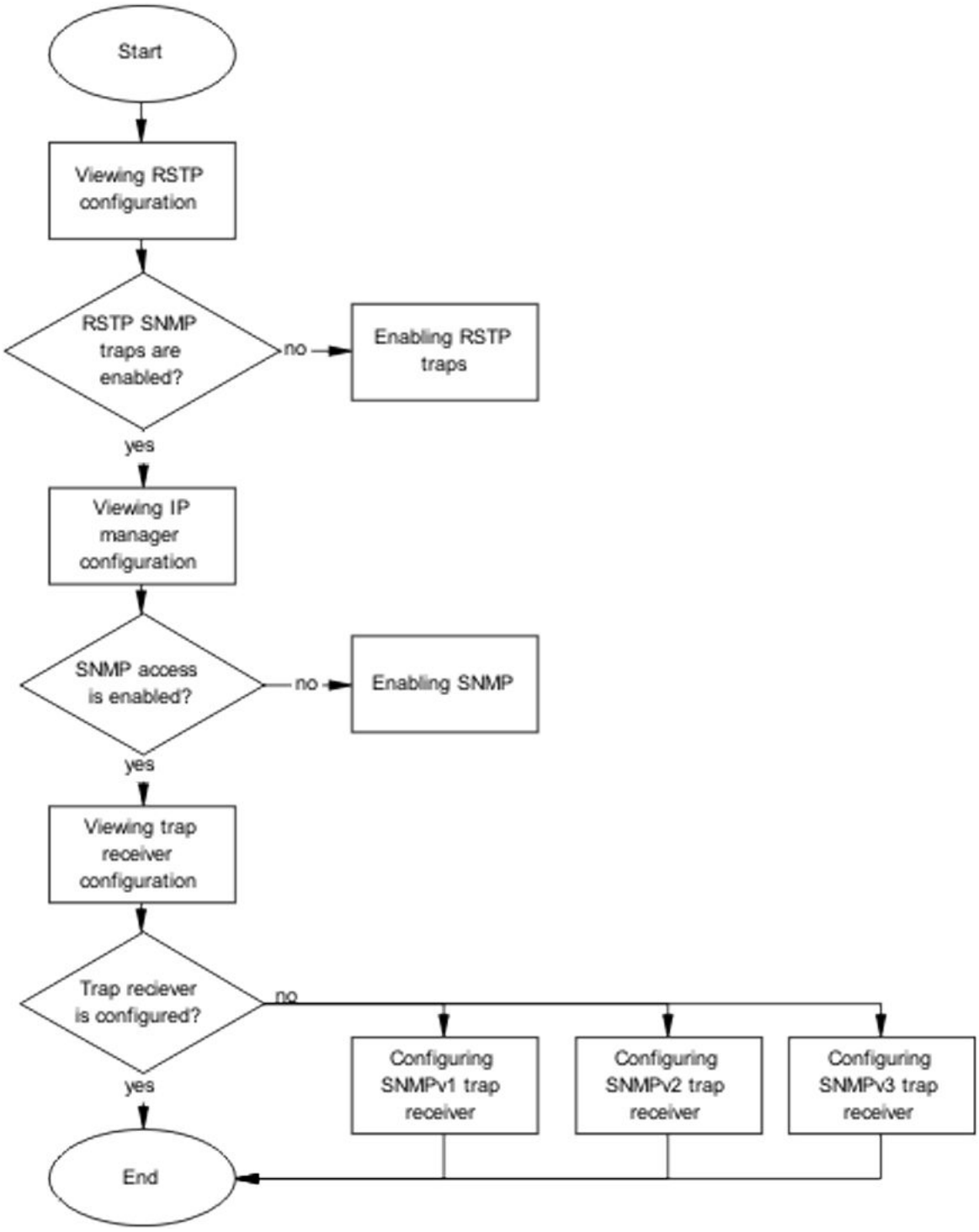


Figure 79: Task flow: No RSTP SNMP traps are received

Viewing RSTP configuration

About this task

Use the procedure in this section to view the existing RSTP configuration.

Procedure

1. Use the **`show spanning-tree rstp config`** command to display the RSTP configuration.
2. Observe the command output.

Job aid

The following is an example of output from the command.

```
Priority (hex):                 8000
Stp Version:                    Rstp Mode
Bridge Max Age Time:            20 seconds
Bridge Hello Time:              2 seconds
Bridge Forward Delay Time:      15 seconds
Tx Hold Count:                  3
Path Cost Default Type:         32-bit
STP Traps:                      Disabled
```

Enabling RSTP traps

About this task

Use the procedure in this section to enable RSTP traps.

Procedure

1. Use the **`spanning-tree rstp traps`** command to enable RSTP traps.
2. Observe the command output.

Viewing IP manager configuration

About this task

Use the procedure in this section to display the IP manager configuration.

Procedure

1. Use the **show ipmgr** command to view the IP manager configuration.
2. Observe the command output.

Job aid

The following is an example of output from the command.

```
TELNET Access:                                  Enabled

SNMP Access:                                    Disabled

WEB Access:                                     Enabled

SSH Access:                                     Enabled
```

Enabling SNMP

About this task

Use the procedure in this section to enable SNMP.

Procedure

1. Use the **snmp-server enable** command to enable SNMP.
2. Observe the command output.

Viewing trap receiver configuration

About this task

Use the procedure in this section to display the trap receiver configuration.

Procedure

1. Use the **show snmp-server host** command to view the trap receiver configuration.
2. Observe the command output.

Configuring SNMPv1 trap receiver

About this task

Use the procedure in this section to configure an SNMPv1 trap receiver.

Procedure

1. Use the **`snmp-server host <IP Address> public`** command to configure the SNMPv1 trap receiver.
2. Observe the command output.

Variable Definitions

Variable	Definition
IP address	IPv4 address of the server host

Configuring SNMPv2 trap receiver

About this task

Use the procedure in this section to configure an SNMPv2 trap receiver.

Procedure

1. Use the **`snmp-server community notify-view`** command to configure the community string.
2. When prompted, enter and confirm the community string.
3. Use the **`snmp-server host <IP address> v2c <string>`** command to configure the community string.

Variable Definitions

Variable	Definition
IP address	IPv4 address of the server host
string	The community string that has been defined for sending SNMPv2c traps

Configuring SNMPv3 trap receiver

About this task

Use the procedure in this section to configure an SNMPv3 trap receiver.

Procedure

1. Use the **`snmp-server user trapuser notify-view`** command to configure the trap user.
2. Use the **`snmp-server host <IP address> v3 no-auth <user>`** command to configure the community string.

Variable Definitions

Variable	Definition
IP address	IPv4 address of the server host
user	The user that has been defined for sending SNMPv3 traps

Chapter 16: Troubleshooting SPBM

You can only configure Shortest Path Bridging MAC (SPBM) when the stack operation mode is pure.

Displaying IS-IS configuration

About this task

Display the IS-IS configuration.

Procedure

1. Display global IS-IS information:

   ```
   show isis
   ```

2. Verify the ISIS interfaces administration and operations status are `UP`:

   ```
   show isis interface
   ```

3. Display IS-IS adjacencies:

   ```
   show isis adjacencies
   ```

4. Display IS-IS configuration components:

   ```
   show isis system-id
   ```

   ```
   show isis int-auth
   ```

   ```
   show isis int-ckt-level
   ```

Example

```
ERS-1# show isis

=========================================
              ISIS General Info
=========================================
            AdminState : enabled
            RouterType : Level 1
             System ID : 00aa.bbcc.0001
  Max LSP Gen Interval : 900
  Min LSP Gen Interval : 30
                Metric : wide

              Overload : true
```

```
         Csnp Interval : 10
         PSNP Interval : 2
     Rxmt LSP Interval : 5
             spf-delay : 100
           Router Name : ERS-1
     Num of Interfaces : 1
 Num of Area Addresses : 1
```

```
ERS-1# show isis interface
================================================================================
                                ISIS Interfaces
================================================================================
IFIDX      TYPE    LEVEL     OP-STATE  ADM-STATE  ADJ    UP-ADJ  SPBM-L1-METRIC
--------------------------------------------------------------------------------
Port1/20   pt-pt   Level 1   UP        UP         1      1       10
```

```
ERS-1# show isis adjacencies
================================================================================
 ISIS Adjacencies
================================================================================
INTERFACE L STATE        UPTIME PRI HOLDTIME SYSID             HOST-NAME
--------------------------------------------------------------------------------
Port1/20  1 UP         01:49:31 127       18 00dd.eeff.0008    ERS-8
```

```
ERS-1# show isis system-id
================================================================================
                                ISIS System-Id
================================================================================
SYSTEM-ID
--------------------------------------------------------------------------------
00aa.bbcc.0001

ERS-1# show isis int-auth
================================================================================
                              ISIS Interface Auth
================================================================================
IFIDX        AUTH-TYPE       AUTH-KEYID      AUTH-KEY
--------------------------------------------------------------------------------

Port1/20     none            0

ERS-1# show isis int-ckt-level
================================================================================
                          ISIS Circuit Level Parameters
================================================================================
IFIDX           LEVEL                DIS                  CKTID
--------------------------------------------------------------------------------

Port1/20        Level 1                                   1
```

Displaying SPBM configuration

About this task

Use the following procedure to display the SPBM IS-IS configuration.

Procedure

1. Display SPBM configuration:

```
show isis spbm
```

2. Display SPBM Unicast FIB information:

```
show isis spbm unicast-fib
```

3. Display SPBM unicast tree information:

```
show isis spbm unicast-tree
```

4. Display SPBM multicast FIB information:

```
show isis spbm multicast-fib
```

5. Display SPBM nick-name:

```
show isis spbm nick-name
```

Example

```
ERS-1# show isis spbm
=====================================================
                    ISIS SPBM Info
=====================================================
SPBM           B-VID      PRIMARY    NICK         LSDB
INSTANCE                  VLAN       NAME         TRAP
-----------------------------------------------------
1              40,41      40             0.10.01      disable
```

```
ERS-1# show isis spbm-fib

================================================================================
                          SPBM UNICAST FIB ENTRY INFO
================================================================================
DESTINATION        BVLAN  SYSID            HOST-NAME         OUTGOING     COST
ADDRESS                                                      INTERFACE
--------------------------------------------------------------------------------
00:aa:bb:cc:00:02  40     00aa.bbcc.0002   ERS-2             1/20         20
00:dd:ee:ff:00:08  40     00dd.eeff.0008   ERS-8             1/20         10
00:aa:bb:cc:00:02  41     00aa.bbcc.0002   ERS-2             1/20         20
00:dd:ee:ff:00:08  41     00dd.eeff.0008   ERS-8             1/20         10
```

```
ERS-1# show isis spbm multicast-fib
================================================================================
                         SPBM MULTICAST FIB ENTRY INFO
================================================================================
MCAST DA           ISID   BVLAN  SYSID                HOST-NAME         OUTGOING
                                                                        INTERFACES
--------------------------------------------------------------------------------
03:10:01:00:03:e8  1000   40     00aa.bbcc.0001       ERS-1             3/5,1/20
03:10:02:00:03:e8  1000   40     00aa.bbcc.0002       VSP-2             3/5
03:10:01:00:03:e8  1000   41     00aa.bbcc.0001       ERS-1             3/5,1/20
03:10:02:00:03:e8  1000   41     00aa.bbcc.0002       VSP-2             3/5
03:10:01:00:03:e9  1001   40     00aa.bbcc.0001       ERS-1             3/6,1/20
03:10:02:00:03:e9  1001   40     00aa.bbcc.0002       VSP-2             3/6
03:10:01:00:03:e9  1001   41     00aa.bbcc.0001       ERS-1             3/6,1/20
03:10:02:00:03:e9  1001   41     00aa.bbcc.0002       VSP-2             3/6
```

```
ERS-1# show isis spbm nick-name

=====================================================
                          ISIS SPBM NICK-NAME
=====================================================
 ================================================================================
 LSP ID               LIFETIME    NICK-NAME    VIRTUAL-BMAC    HOST-NAME
```

```
================================================================================
00aa.bbcc.0001.00-00   334        5.10.01    0000.0000.0000    ERS-1
00aa.bbcc.0002.00-00   576        5.01.01    0000.0000.0000    ERS-2
00aa.bbcc.0008.00-00   828        5.01.10    0000.0000.0000    ERS-8
```

Displaying VLAN to ISID associations

About this task

Display VLAN to ISID associations.

Tip:

Other useful commands include:

```
show vlan
show vlan interface info
show vlan interface vids
```

Procedure

Display VLAN to ISID associations:

```
show vlan i-sid
```

Example

```
ERS-1# show vlan i-sid
================================================
                                  Vlan I-SID
================================================
VLAN_ID    I-SID
--------------------------------------------------------------------------------
1
23         1000
111        1001

ERS-2# show vlan i-sid
================================================
                                  Vlan I-SID
================================================
VLAN_ID    I-SID
--------------------------------------------------------------------------------
1
23         1000
111        1001
```

Verifying Forwarding Database information

About this task

Verify the forwarding database (FDB) information.

Procedure

Display the FDB information:

```
show mac-address vid <1-
```

```
show vlan remote-mac-table <1-
```

Example

```
ERS-1# show mac-address vid 23
   MAC Address    Vid       Source            MAC Address    Vid       Source
----------------- ---- ---------------     ----------------- ---- ---------------
00-91-00-23-00-03   23 Unit:3 Port: 5      00-81-00-23-00-01   23 I-SID-1000
00-81-00-23-00-02   23 I-SID-1000
```

```
ERS-1# show vlan  remote-mac-table 23
================================================================================
                              Vlan Remote Mac Table
================================================================================
VLAN STATUS  MAC-ADDRESS        DEST-MAC           BVLAN DEST-SYSNAME      PORTS
--------------------------------------------------------------------------------
23   learned 00:81:00:23:00:01  00:aa:bb:cc:00:02  40    ERS-2             1/20
23   learned 00:81:00:23:00:02  00:aa:bb:cc:00:02  40    ERS-2             1/20
```

Verifying ISIS interfaces and receive protocol control packets

About this task

Verify ISIS interfaces and receive protocol control packets.

Procedure

Display ISIS interfaces and receive protocol control packets:

```
show isis int-l1-cntl-pkts
```

Example

```
ERS-1# show isis int-l1-cntl-pkts
================================================================================
                        ISIS L1 Control Packet Counters
================================================================================
IFIDX         DIRECTION     HELLO        LSP          CSNP         PSNP
================================================================================
Unit/Port: 1/15 Transmitted   236383       2005         2            4939

Unit/Port: 1/15 Received      239601       4613         126          2338

Unit/Port: 1/23 Transmitted   0            0            0            0

Unit/Port: 1/23 Received      0            0            0            0
```

Verifying UNI configuration

About this task

Verify UNI configuration.

Procedure

Display UNI information:

```
show i-sid
```

```
show vlan interface info <port>
```

Example

```
ERS-1# show i-sid
I-SID     Vid  UNI-type    Ports
--------- ---- ----------- ------------
11        11   C-VLAN      1/5, 2/7
1001      1001 C-VLAN      NONE
```

```
ERS-1# show vlan interface info 1/5
      Filter     Filter
     Untagged Unregistered
Port  Frames     Frames     PVID PRI    Tagging     Name
---- -------- ------------ ---- --- ------------ --------------
1/5  No       Yes          11   0   TagAll       Unit 1, Port 5
```

Verifying SPBM Unicast FIB entries

About this task

Verify SPBM Unicast FIB entries for nodes in the SPBM cloud.

Procedure

Display the SPBM FIB entry information:

```
show isis spbm unicast-fib
```

Example

```
ERS-1# show isis spbm unicast-fib
================================================================================
                           SPBM UNICAST FIB ENTRY INFO
================================================================================
DESTINATION        BVLAN  SYSID          HOST-NAME       OUTGOING   COST
ADDRESS                                                  INTERFACE
================================================================================
00:1a:8f:10:53:df  100    001a.8f10.53df  MERS2-8606      Port: 1/15 30
00:1a:8f:10:53:e0  100    001a.8f10.53df  MERS2-8606      Port: 1/15 30
00:1a:8f:10:53:df  101    001a.8f10.53df  MERS2-8606      Port: 1/15 30
00:1a:8f:10:53:e0  101    001a.8f10.53df  MERS2-8606      Port: 1/15 30
00:1a:8f:10:53:e0  100    001a.8f10.b3df  MERS4-8606      Port: 1/15 10
00:1a:8f:10:b3:df  100    001a.8f10.b3df  MERS4-8606      Port: 1/15 10
00:1a:8f:10:53:e0  101    001a.8f10.b3df  MERS4-8606      Port: 1/15 10
00:1a:8f:10:b3:df  101    001a.8f10.b3df  MERS4-8606      Port: 1/15 10
fc:a8:41:f3:11:11  100    fca8.41f3.1111  stack-gicu      Port: 1/15 20
```

```
fc:a8:41:f3:11:11  101    fca8.41f3.1111  stack-gicu      Port: 1/15 20
fc:a8:41:f3:9f:df  100    fca8.41f3.9fdf  apancu          Port: 1/15 20
fc:a8:41:f3:9f:df  101    fca8.41f3.9fdf  apancu          Port: 1/15 20
fc:a8:41:f5:04:00  100    fca8.41f5.0400  VSP7000                    0
fc:a8:41:f5:04:00  101    fca8.41f5.0400  VSP7000                    0
```

Verifying SPBM network topology

About this task

Verify SPBM network topology.

Procedure

Verify the SPBM network topology:

```
show isis spbm unicast-tree <1-
```

Example

```
ERS-1# show isis spbm unicast-tree 100
Node:fca8.41fd.0400.00 (marius11) -> Node:001a.8f10.53df.00 (MERS2-8606) ->
    Node:fca8.41f3.1111.00 (stack-gicu) ->
    Node:001a.8f10.b3df.00 (MERS4-8606) -> ROOT

Node:fca8.41f3.9fdf.00 (apancu) -> Node:001a.8f10.b3df.00 (MERS4-8606) -> ROOT

Node:fca8.41f3.1111.00 (stack-gicu) -> Node:001a.8f10.b3df.00 (MERS4-8606) ->
    ROOT

Node:001a.8f10.b3df.00 (MERS4-8606) -> ROOT

Node:001a.8f10.53df.00 (MERS2-8606) -> Node:fca8.41f3.1111.00 (stack-gicu) ->
    Node:001a.8f10.b3df.00 (MERS4-8606) -> ROOT
```

Verify SPBM Multicast FIB entries

About this task

Verify SPBM Multicast FIB entries (carry b-cast and m-cast traffic).

Procedure

Verify SPBM Multicast FIB entries:

```
show isis spbm unicast-fib
```

Example

```
ERS-1# show isis spbm unicast-fib
================================================================================
                          SPBM UNICAST FIB ENTRY INFO
================================================================================
DESTINATION        BVLAN  SYSID          HOST-NAME       OUTGOING   COST
ADDRESS                                                  INTERFACE
```

```
================================================================================
00:1a:8f:10:53:df  1000   001a.8f10.53df  MERS2-8606      Port: 1/15 10
00:1a:8f:10:53:e0  1000   001a.8f10.53df  MERS2-8606      Port: 1/15 10
00:1a:8f:10:53:df  1001   001a.8f10.53df  MERS2-8606      Port: 1/15 10
00:1a:8f:10:53:e0  1001   001a.8f10.53df  MERS2-8606      Port: 1/15 10
fc:a8:41:f5:07:df  1000   fca8.41f5.07df  puiub-stack               0
fc:a8:41:f5:07:df  1001   fca8.41f5.07df  puiub-stack               0
--------------------------------------------------------------------------------
  Total number of SPBM UNICAST FIB entries 6
--------------------------------------------------------------------------------
```

Verifying LSDB information

About this task

Verify LSDB information.

Procedure

Verify LSDB information:

```
show isis lsdb
```

Example

```
ERS-1# show isis lsdb
================================================================================
                                ISIS LSDB
================================================================================
LSP ID                    LEVEL     LIFETIME  SEQNUM     CHKSUM    HOST-NAME

================================================================================
001a.8f10.53df.00-00      1         1134      0x2095     0x9288    MERS2-8606

001a.8f10.b3df.00-00      1         1140      0x1923     0x130b    MERS4-8606

fca8.41f3.1111.00-00      1         630       0x248      0x4a67    stack-gicu

fca8.41f3.9fdf.00-00      1         364       0x264      0x5526    apancu

fca8.41f5.0400.00-00      1         777       0x6        0xc0e0    puiub-stack

fca8.41fd.0400.00-00      1         624       0x4e5      0x3a78    marius11

================================================================================
Level-1 : 6 out of 6 Total Num of LSP Entries
Level-2 : 0 out of 6 Total Num of LSP Entries
================================================================================

puiub-stack(config)#show isis lsdb detail
================================================================================
                              ISIS LSDB (DETAIL)
================================================================================


Level-1 LspID: 001a.8f10.53df.00-00     SeqNum: 0x00000469      Lifetime:  8341
        Chksum: 0x9288  PDU Length: 419
        Host_name: MERS2-8606
        Attributes:     IS-Type 1
```

```
TLV:1   Area Addresses: 1
        Area Address:01

TLV:22  Extended IS reachability:
        Adjacencies: 2
                 fca8.41fd.0400.00(marius11)      Metric:10
                                port id: 155 num_port 1
                                Metric: 10
                 fca8.41f3.1111.00(stack-gicu)    Metric:10
                                port id: 138 num_port 1
                                Metric: 10
```

Using CFM

About this task

Use CFM to diagnose the network.

Procedure

Use CFM to diagnose the network:

```
cfm spbm enable
```

```
show cfm
```

```
l2ping
```

```
l2traceroute
```

```
l2tracetree
```

Troubleshooting Fabric Attach

This chapter contains details about how to troubleshoot common Fabric Attach (FA) problems you may encounter.

Verifying FA settings

Use this procedure to verify the FA settings.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. Verify the FA settings:

   ```
   show fa agent
   ```

Example

The following example displays output sample for the `show fa agent` command in FA Server mode.

```
Switch(config)#show fa agent

Fabric Attach Service Status: Enabled
Fabric Attach Element Type: Server
Fabric Attach Zero Touch Status: Enabled
Fabric Attach Auto Provision Setting: Server
Fabric Attach Provision Mode: SPBM
Fabric Attach Agent Timeout: 240 seconds
Fabric Attach Extended Logging Status: Disabled
```

The following example displays output sample for the `show fa agent` command in FA Proxy mode.

```
Switch(config)#show fa agent

Fabric Attach Service Status: Enabled
Fabric Attach Element Type: Proxy
Fabric Attach Zero Touch Status: Enabled
Fabric Attach Auto Provision Setting: Proxy
Fabric Attach Provision Mode: Legacy
Fabric Attach Client Proxy Status: Enabled
Fabric Attach Standalone Proxy Status: Disabled
Fabric Attach Agent Timeout: 240 seconds
Fabric Attach Extended Logging Status: Disabled
Fabric Attach Primary Server Id: <none>
Fabric Attach Primary Server Descr: <none>
```

Verifying FA message authentication status

Use this procedure to verify whether both FA Proxy and FA Server have the same authentication settings (enabled on both, or disabled on both).

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Use the `show fa port-enable` command to check message authentication status.
3. If message authentication settings are different on FA Proxy and FA Server, use the `[no] [default] fa message-authentication` command to change message authentication settings.

Example

The following example displays sample output for the `show fa port-enable` command.

```
Switch(config)#show fa port-enable

Unit Port IfIndex Service Advertisement Authentication
---- ---- ------- -------------------- --------------
```

```
1     1     1             Enabled             Enabled
1     2     2             Enabled             Enabled
1     3     3             Enabled             Enabled
1     4     4             Enabled             Enabled
1     5     5             Enabled             Enabled
1     6     6             Enabled             Enabled
```

Verifying FA per-port settings

Use this procedure to check FA per-port settings that may prohibit message exchange.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Use the `show fa port-enable` command to check FA per-port settings.
3. If FA per-port settings prohibit message exchange, use the `fa port-enable` command to enable FA on required ports.
4. You can repeat step 2 to confirm settings.

Verifying discovered FA elements

Use this procedure to check the discovered FA elements.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. Verify the discovered FA elements:

   ```
   show fa elements
   ```

Example

The following example displays sample output for the `show fa elements` command.

```
Switch(config)#show fa elements

Unit/ Element    Element           Element
Port   Type      Subtype            VLAN   Auth    System ID
----- ------- -------------------- ------- ---- ------------------------------
1/10  Client  Wireless AP (Type 1)  1       AP  00:22:67:00:58:00:00:00:01:0a
MLT2  Server  Server (Auth)         1234    AP  fc:a8:41:fa:f8:00:20:00:00:02
2/10  Client  Wireless AP (Type 1)  0       NA  64:a7:dd:03:38:29:00:00:00:01
3/12  Client  Wireless AP (Type 1)  0       AF  64:07:34:03:12:ac:00:00:00:08
```

Chapter 17: Troubleshooting SLA Monitor Agent

Use SLAMon Agent to detect, identify, and isolate issues which impact end-to-end network performance.

Architecture

The architecture supports the ability to perform QoS and DSCP tests through CLI between any two Networking devices with SLAMon Agents without need for an SLAMon server. In addition, it supports secure agent-server communication through certificate-based authentication and encrypted agent-server communication secure communications. Diagnostic Server provides network-wide QoS and DSCP monitoring, along with graphical display, alarms and alerts, trend analysis, and logging.

Supporting NTR and RTP

Note:

Server control over agent may impact NTR and RTP results.

NTR

The target device does not need to support SLAMon. If standard Traceroute works, NTR traces are available. Server control over agent may impact the NTR results.

When programming in CLI, agents registered with a server should refuse server tests while manual NTR tests are being performed.

RTP

The target device must support SLAMon and SLAMon must be enabled.

When programming in CLI, “Server bypass” is required if agent not registered. Agents that are registered with a server must refuse server tests while manual RTP tests are performed.

Chapter 18: Troubleshooting DHCP/BootP relay

Bootp/DHCP Relay serves the purpose of IP configuration for Bootp/DHCP clients that do not have a BootP/DHCP Server configured in the same subnet.

Troubleshooting DHCP/BootP relay work flow

About this task

The following workflow helps you to identify some common issues.

Procedure

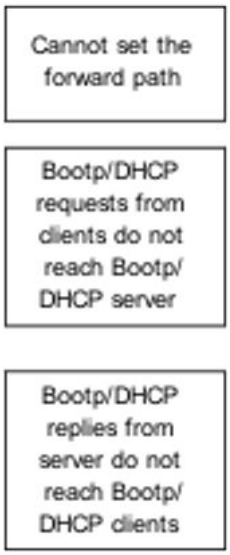


Figure 80: Work flow: Troubleshooting DHCP/BootP relay

Cannot set the forward path

This task flow assists you to resolve the following error message if it appears:

- ```
  % Cannot modify settings
  % Error agent/server does not exist
  ```

Cannot set the forward path task flow

About this task

The following task flow helps you to verify that the relay agent IP address is the same as the one configured on the VLAN where relay is performed.

Procedure

Figure 81: Task flow: Cannot set the forward path

Viewing VLAN IP information

About this task

Use this procedure to verify that the relay agent IP address from the forward path command is the same as the one on the VLAN where relay is to be performed.

Procedure

1. Use the **`show vlan ip`** command to display the information.
2. Verify that the relay agent IP address from the forward path command is the same as the one on the VLAN where relay is to be performed.
  ```

Bootp/DHCP requests from clients do not reach Bootp/DHCP server

This section assists you to identify and correct connectivity issues between a client and the DHCP or BootP server.

Bootp/DHCP requests from clients do not reach Bootp/DHCP server task flow

About this task

The following task flows identify the procedures to identify and correct connectivity issues between a client and the DHCP or BootP server.

Procedure

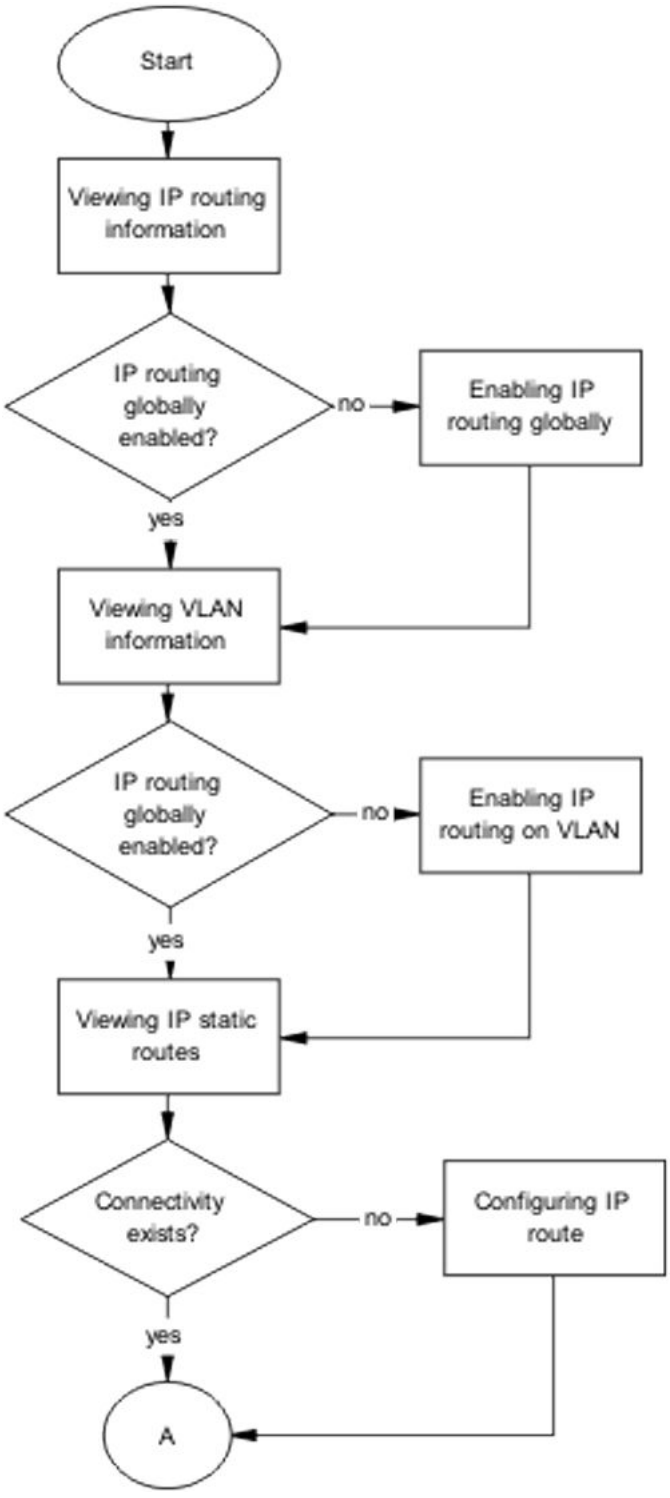


Figure 82: Task flow: Bootp/DHCP requests from clients do not reach Bootp/DHCP server part 1

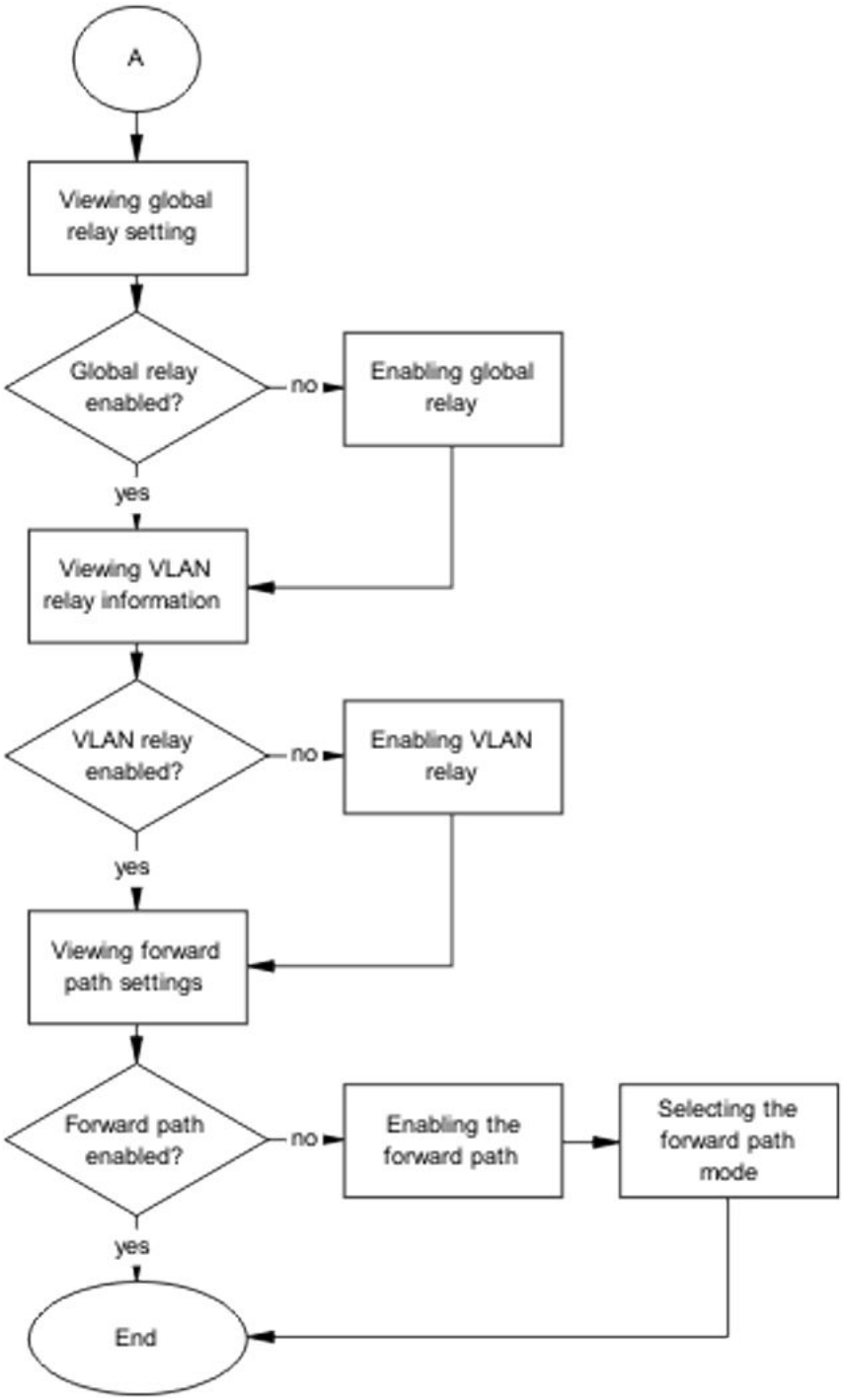


Figure 83: Task flow: Bootp/DHCP requests from clients do not reach Bootp/DHCP server part 2

Viewing IP routing information

About this task

Use the procedure in this section to view IP routing information.

Procedure

1. Enter the **`show ip routing`** command to view IP routing information.
2. Identify that IP routing is enabled.

Enabling IP routing globally

About this task

Use the procedure in this section to enable IP routing globally.

Procedure

1. Enter the **`ip routing`** command to enable IP routing globally.
2. Enter the **`show ip routing`** command to confirm that global IP routing is now enabled.

Viewing VLAN information

About this task

Use the procedure in this section to view VLAN information.

Procedure

1. Enter the **`show vlan ip`** command to view VLAN information.
2. Verify that the interfaces are enabled under the Offset Routing column.

Enabling IP routing on VLAN

About this task

Use the procedure in this section to enable IP routing on a VLAN.

Procedure

1. Enter the **`interface vlan <VLANID>`** command to select the VLAN interface to be modified.
2. Enter the **`ip routing`** command to enable IP routing on the interface.

Variable Definitions

Variable	Definition
VLANID	Unique ID of the VLAN

Viewing IP static routes

About this task

Use the procedure in this section when the server is not connected to the same Ethernet Routing Switch and configure a client with static IP for connectivity purposes. From that client, ping the server. If the ICMP echo requests do not reach the server, verify that a route is configured on the switch for the server.

Procedure

1. Enter the **`show ip route static`** command to display the IP static route information.
2. Observe the command output.

Configuring IP route

About this task

Use the procedure in this section to configure the IP route.

Procedure

1. Enter the **`ip route <server.ip.address.class> <netmask> <next.hop.ip.address> <cost>`** command to configure the IP route.
2. Observe the command output.

Viewing global relay setting

About this task

Use the procedure in this section to view the global relay configuration.

Procedure

1. Enter the **`show ip dhcp-relay`** command to display the global relay configuration.
2. Observe the command output and confirm DHCP relay is enabled.

Enabling global relay

About this task

Use the procedure in this section to enable DHCP relay globally.

Procedure

1. Enter the **`ip dhcp-relay`** command to enable DHCP relay globally.
2. Observe the command output.

Viewing VLAN relay information

About this task

Use the procedure in this section to display the VLAN relay configuration.

Procedure

1. Enter the **`show vlan dhcp-relay`** command to display the VLAN relay configuration.
2. Observe the command output.

Enabling VLAN relay

About this task

Use the procedure in this section to enable VLAN relay.

Procedure

1. Enter the **`interface vlan <VLANID>`** command to select the VLAN interface to be modified.
2. Enter the **`ip dhcp-relay`** command to enable DHCP relay on the interface.

Variable Definitions

Variable	Definition
VLANID	Unique ID of the VLAN

Viewing forward path settings

About this task

Use the procedure in this section to display the forward path settings.

Procedure

1. Enter the **`show ip dhcp-relay fwd-path`** command to display the forward path configuration.
2. Ensure that the interface is enabled.

Enabling the forward path

About this task

Use the procedure in this section to enable the forward path.

Procedure

1. Enter the **`ip dhcp-relay fwd-path <interface address> <server address> enable`** command to enable the forward path.
2. Ensure that the command completes.

Variable Definitions

Variable	Definition
interface address	IPv4 address of the interface
server address	IPv4 address of the server

Selecting the forward path mode

About this task

Use the procedure in this section to configure the forward path mode.

Procedure

1. Enter the **`ip dhcp-relay fwd-path <interface address> <server address> mode [boot | dhcp | boot-dhcp]`** command to configure the forward path mode.
2. Ensure that the command completes.

Variable Definitions

Variable	Definition
interface address	IPv4 address of the interface
server address	IPv4 address of the server

Bootp/DHCP replies from server do not reach Bootp/DHCP clients

This section helps you to resolve issues related to Bootp/DHCP replies from the server that do not reach Bootp/DHCP clients.

Bootp/DHCP replies from server do not reach Bootp/DHCP clients task flow

About this task

The following task flow identifies the procedure to resolve issues related to Bootp/DHCP replies from the server that do not reach Bootp/DHCP clients.

Procedure

Figure 84: Task flow: Bootp/DHCP replies from server do not reach Bootp/DHCP clients

Verifying IP connectivity between server and client

Before you begin

- The server is not connected to the same Ethernet Routing Switch.

About this task

Use the procedure in this section to verify the connectivity between the DHCP server and its client.

Procedure

1. Use the **`show ip route static`** command to ensure ICMP requests from the client reach the server.
2. From the server, ping the client configured with a static IP address.
3. Verify that a route is configured on the server and the route points to the subnet of the client.
4. Using the server documentation, configure the route if it does not exist.

Glossary

Address Resolution Protocol (ARP)	Maps an IP address to a physical machine address, for example, maps an IP address to an Ethernet media access control (MAC) address.
Agent Auto Unit Replacement (AAUR)	Enabled by default, AAUR inspects all units in a stack and downloads the stack software image to any joining unit with a dissimilar image.
American Standard Code for Information Interchange (ASCII)	A code to represent characters in computers. ASCII uses uppercase and lowercase alphabetic letters, numeric digits, and special symbols.
Authentication, Authorization, and Accounting (AAA)	Authentication, Authorization, and Accounting (AAA) is a framework used to control access to a network, limit network services to certain users, and track what users do. Authentication determines who a user is before allowing the user to access the network and network services. Authorization allows you to determine what you allow a user to do. Accounting records what a user is doing or has done.
Auto MDIX	The automatic detection of transmit and received twisted pairs. When Auto MDIX is active, you can use any straight or crossover category 5 cable to provide connection to a port. You must enable Autonegotiation to activate Auto MDIX.
Auto polarity	Compensates for reversal of positive and negative signals on the receive cables. When you enable autonegotiation, auto polarity can reverse the polarity of a pair of pins to correct polarity of received data.
Auto Unit Replacement (AUR)	Allows users to replace a unit from a stack while retaining the configuration of the unit. Stack power must remain on during the unit replacement. AUR does not work in a stack of two units only.
Auto-Detection and Auto-Configuration (ADAC)	Provides automatic switch configuration for IP phone traffic support and prioritization. ADAC can configure the switch whether it is directly connected to the Call Server or uses a network uplink.
Automatic PVID	Automatically sets the port-based VLAN ID when you add the port to the VLAN. The PVID value is the same value as the last port-based VLAN ID associated with the port.

Autonegotiation	Allows the switch to select the best speed and duplex modes for communication between two IEEE-capable devices.
Autosensing	Determines the speed of the attached device if it is incapable of autonegotiation or if it uses an incompatible form of autonegotiation.
Autotopology	An Enterprise Network Management System (ENMS) protocol that automates and simplifies discovery and collection of network topology information, presented in a table.
base unit (BU)	When you connect multiple switches into a stack, one unit, and only one unit, must be designated as a base unit to perform stack configuration tasks. The position of the unit select switch, on the back of the switch, determines base unit designation.
Bootstrap Protocol (BootP)	A User Datagram Protocol (UDP)/Internet Protocol (IP)-based protocol that a booting host uses to configure itself dynamically and without user supervision.
Bridge Protocol Data Unit (BPDU)	A data frame used to exchange information among the bridges in local or wide area networks for network topology maintenance.
Bridging	A forwarding process, used on Local Area Networks (LAN) and confined to network bridges, that works on Layer 2 and depends on the Spanning Tree Protocol (STP) or Rapid Spanning Tree Protocol (RSTP). Bridging is also known as MAC forwarding.
CLI	Command Line Interface (CLI) is a text-based, common command line interface used for device configuration and management across Extreme Networks products.
CLI modes	Differing command modes are available within the text-based interface, dependant on the level of user permissions determined by logon password. Each successive mode level provides access to more complex command sets, from the most restrictive—show level only, to the highest configuration levels for routing parameters, interface configuration, and security.
Custom AutoNegotiation Advertisement (CANA)	An enhancement of the IEEE 802.3 autonegotiation process on the 10/100/1000 copper ports. Custom AutoNegotiation Advertisement offers improved control over the autonegotiation process. The system advertises all port capabilities that include, for tri-speed ports, 10 Mb/s, 100 Mb/s, 1000 Mb/s speeds, and duplex and half-duplex modes of operation. This advertisement results in autonegotiation between the local and remote end that settles on the highest common denominator. Custom AutoNegotiation Advertisement can advertise a user-defined subset of the capabilities that settle on a lower or particular capability.

daemon	A program that services network requests for authentication and authorization. A daemon verifies, identifies, grants or denies authorizations, and logs accounting records.
Differentiated Services (DiffServ)	A network architecture enabling service providers and enterprise network environments to offer varied levels of service for different traffic types.
Differentiated Services Code Point (DSCP)	The first six bits of the DS field. The DSCP uses packet marking to guarantee a fixed percentage of total bandwidth to each of several applications (guarantees quality of service).
Differentiated Services Quality of Service (DiffServ QoS)	Allows specific level of performance designation, on a packet-by-packet basis, for high performance and reliable service for voice or video over IP, or for preferential treatment of data over other traffic.
Domain Name System (DNS)	A system that maps and converts domain and host names to IP addresses.
Duplicate Address Detection (DAD)	A method used to discover duplicate addresses in an IPv6 network.
Dynamic Host Configuration Protocol (DHCP)	A standard Internet protocol that dynamically configures hosts on an Internet Protocol (IP) network for either IPv4 or IPv6. DHCP extends the Bootstrap Protocol (BOOTP).
equal cost multipath (ECMP)	Distributes routing traffic among multiple equal-cost routes.
Extensible Authentication Protocol over LAN (EAPoL)	A port-based network access control protocol. EAPoL provides security in that it prevents users from accessing network resources before they are authenticated.
Fabric Attach (FA)	A feature used to extend the fabric edge to devices that do not have full SPBM support. Fabric Attach also decreases the configuration requirements on the SPBM devices by off-loading some configuration to the attached non-SPBM devices and by automating certain configuration steps that occur most often.
flash memory	All switch configuration parameters are stored in flash memory. If you store switch software images in flash memory, you can update switch software images without changing switch hardware.
Gigabit Ethernet (GbE)	Ethernet technology with speeds up to 100 Gbps.

Gigabit Interface Converter (GBIC)	A hotswappable input and output enhancement component, designed for use with Extreme Networks products, that allows Gigabit Ethernet ports to link with other Gigabit Ethernet ports over various media types.
Internet Control Message Protocol (ICMP)	A collection of error conditions and control messages exchanged by IP modules in both hosts and gateways.
Internet Group Management Protocol (IGMP)	IGMP is a host membership protocol used to arbitrate membership in multicast services. IP multicast routers use IGMP to learn the existence of host group members on their directly attached subnets.
Internet Protocol Flow Information eXport (IPFIX)	An IETF standard that improves the Netflow V9 protocol. IPFIX monitors IP flows.
Internet Protocol Manager (IP Manager)	Used to limit access to switch management features by defining IP addresses allowed access to the switch.
Internet Protocol Security (IPsec)	Internet Protocol security (IPsec) is a set of security protocols and cryptographic algorithms that protect communication in a network. Use IPsec in scenarios where you need to encrypt packets between two hosts, two routers, or a router and a host.
Internet Protocol version 4 (IPv4)	The protocol used to format packets for the Internet and many enterprise networks. IPv4 provides packet routing and reassembly.
Internet Protocol version 6 (IPv6)	An improved version of the IP protocol, IPv6 improves the IPv4 limitations of security and user address numbers.
Layer 2	Layer 2 is the Data Link Layer of the OSI model. Examples of Layer 2 protocols are Ethernet and Frame Relay.
Layer 3	Layer 3 is the Network Layer of the OSI model. An example of a Layer 3 protocol is Internet Protocol (IP).
light emitting diode (LED)	A semiconductor diode that emits light when a current passes through it.
Link Aggregation	Provides the mechanism to create and manage trunk groups automatically using Link Aggregation Control Protocol (LACP).
Link Aggregation Control Protocol (LACP)	A network handshaking protocol that provides a means to aggregate multiple links between appropriately configured devices.
Link Layer Discovery Protocol (LLDP)	Link Layer Discovery Protocol is used by network devices to advertise their identities. Devices send LLDP information at fixed intervals in the form of

	Ethernet frames, with each frame having one Link Layer Discovery Protocol Data Unit.
Local Area Network (LAN)	A data communications system that lies within a limited spatial area, uses a specific user group and topology, and can connect to a public switched telecommunications network (but is not one).
management information base (MIB)	The MIB defines system operations and parameters used for the Simple Network Management Protocol (SNMP).
mask	A bit string that the device uses along with an IP address to indicate the number of leading bits in the address that correspond with the network part.
maximum transmission unit (MTU)	The largest number of bytes in a packet—the maximum transmission unit of the port.
media	A substance that transmits data between ports; usually fiber optic cables or category 5 unshielded twisted pair (UTP) copper wires.
Media Access Control (MAC)	Arbitrates access to and from a shared medium.
media access unit (MAU)	The equipment in a communications system that adapts or formats signals, such as optical signals, for transmission over the propagation medium.
Message Digest 5 (MD5)	A one-way hash function that creates a message digest for digital signatures.
MultiLink Trunking (MLT)	A method of link aggregation that uses multiple Ethernet trunks aggregated to provide a single logical trunk. A multilink trunk provides the combined bandwidth of multiple links and the physical layer protection against the failure of a single link.
Multiple Spanning Tree Protocol (MSTP)	Configures multiple instances of the Rapid Spanning Tree Protocol (RSTP) on the switch.
Network Time Protocol (NTP)	A protocol that works with TCP that assures accurate local time keeping with reference to radio and atomic clocks located on the Internet. NTP synchronizes distributed clocks within milliseconds over long time periods.
nonbase unit (NBU)	A nonbase unit is any unit in a stack except the base unit.
NonVolatile Random Access Memory (NVRAM)	Random Access Memory that retains its contents after electrical power turns off.

Open Shortest Path First (OSPF)	A link-state routing protocol used as an Interior Gateway Protocol (IGP).
policy-enabled networking	User-defined characteristics that can be set in policies used to control and monitor traffic.
port	A physical interface that transmits and receives data.
port mirroring	A feature that sends received or transmitted traffic to a second destination.
port VLAN ID	Used to coordinate VLANs across multiple switches. When you create a port-based VLAN on a switch, assign a VLAN identification number (VLAN ID) and specify the ports that belong to the VLAN.
Power over Ethernet (PoE)	The capacity of a switch to power network devices, according to the 802.3af standard, over an Ethernet cable. Devices include IP phones, Wireless LAN Access Points (WLAN AP), security cameras, and access control points.
prefix	A group of contiguous bits, from 0 to 32 bits in length, that defines a set of addresses.
Protocol Data Units (PDUs)	A unit of data that is specified in a protocol of a specific layer and that consists of protocol-control information of the specific layer and possibly user data of that layer.
Proxy Address Resolution Protocol (Proxy ARP)	Allows the switch to respond to an Address Resolution Protocol (ARP) request from a locally attached host (or end station) for a remote destination.
quality of service (QoS)	QoS features reserve resources in a congested network, allowing you to configure a higher priority for certain devices. For example, you can configure a higher priority for IP deskphones, which need a fixed bit rate and split the remaining bandwidth between data connections if calls in the network are more important than the file transfers.
Rapid Spanning Tree Protocol (RSTP)	Reduces the recovery time after a network breakdown. RSTP enhances switch-generated Topology Change Notification (TCN) packets to reduce network flooding.
rate limiting	Rate limiting sets the percentage of traffic that is multicast, broadcast, or both, on specified ports.
real time clock	Provides the switch with time information if Simple Network Time Protocol (SNTP) time is unavailable.
redundant power supply unit (RPSU)	Provides alternate backup power over a DC cable connection into an Extreme Networks Ethernet Routing Switch.

Remote Authentication Dial-in User Service (RADIUS)	A protocol that authenticates, authorizes, and accounts for remote access connections that use dial-up networking and Virtual Private Network (VPN) functionality.
request for comments (RFC)	A document series published by the Internet Engineering Task Force (IETF) that describe Internet standards.
routing switch	Virtualizes the physical router interfaces to switches. A virtual router port, or interface, acts as a router port to consolidate switching and routing functions in the broadcast domain, or between broadcast domains, and enable IP routing for higher traffic volumes.
Secure Shell (SSH)	SSH uses encryption to provide security for remote logons and data transfer over the Internet.
SFP	A hot pluggable, small form-factor pluggable (SFP) transceiver, which is used in Ethernet applications up to 1 Gbps.
shortest path first (SPF)	A class of routing protocols that use Djikstra's algorithm to compute the shortest path through a network, according to specified metrics, for efficient transmission of packet data.
Simple Network Time Protocol (SNTP)	Provides a simple mechanism for time synchronization of the switch to any RFC 2030-compliant Network Time Protocol (NTP) or SNTP server.
spanning tree	A simple, fully-connected active topology formed from the arbitrary physical topology of connected bridged Local Area Network components by relaying frames through selected bridge ports. The protocol parameters and states that are used and exchanged to facilitate the calculation of the active topology and to control the bridge relay function.
Spanning Tree Group (STG)	A collection of ports in one spanning-tree instance.
Spanning Tree Protocol (STP)	MAC bridges use the STP to exchange information across Local Area Networks to compute the active topology of a bridged Local Area Network in accordance with the Spanning Tree Protocol algorithm.
stack	Stackable Extreme Networks Ethernet Routing Switch can be connected in a stack configuration of two or more units, up to eight units maximum. A switch stack operates and is managed as a single virtual switch.
stack IP address	An IP address must be assigned to a stack so that all units can operate as a single entity.
stack unit	Any switch within a stack.

stand-alone	Refers to a single Extreme Networks Ethernet Routing Switch operating outside a stack.
Terminal Access Controller Access Control System plus	Terminal Access Controller Access Control System plus (TACACS+) is a security protocol that provides centralized validation of users who attempt to gain access to a router or network access server. TACACS+ uses Transmission Control Protocol (TCP) for its transport to ensure reliable delivery and encrypts the entire body of the packet. TACACS+ provides separate authentication, authorization, and accounting services. TACACS+ is not compatible with previous versions of TACACS.
Time Domain Reflectometer (TDR)	Provides diagnostic capability on Ethernet copper ports to test connected cables for defects. The TDR interrupts 10/100 MB/s links but does not affect 1 GB/s links.
time-to-live (TTL)	The field in a packet used to determine the valid duration for the packet. The TTL determines the packet lifetime. The system discards a packet with a TTL of zero.
Transmission Control Protocol (TCP)	Provides flow control and sequencing for transmitted data over an end-to-end connection.
Trivial File Transfer Protocol (TFTP)	A protocol that governs transferring files between nodes without protection against packet loss.
trunk	A logical group of ports that behaves like a single large port.
type of service (TOS)	A field in the IPv4 header that determines the Class of Service prior to the standardization of Differentiated Services.
unit select switch	Use the unit select switch on the back of a unit in the stack to designate the unit as the base or nonbase unit.
unshielded twisted pair (UTP)	A cable with one or more pairs of twisted insulated copper conductors bound in a single plastic sheath.
User Datagram Protocol (UDP)	In TCP/IP, a packet-level protocol built directly on the Internet Protocol layer. TCP/IP host systems use UDP for application-to-application programs.
Virtual Local Area Network (VLAN)	A Virtual Local Area Network is a group of hosts that communicate as if they are attached to the same broadcast domain regardless of their physical location. VLANs are layer 2 constructs.
Virtual Router Redundancy Protocol (VRRP)	A protocol used in static routing configurations, typically at the edge of the network. This protocol operates on multiple routers on an IP subnet and elects a primary gateway router. When the primary router fails, a backup router is quickly available to take its place.

Voice over IP (VOIP) The technology that delivers voice information in digital form in discrete packets using the Internet Protocol (IP) rather than the traditional circuit-committed protocols of the public switched telephone network (PSTN).

XFP A pluggable 10 gigabit transceiver capable of providing different optical media for a switch. The XFP is similar to an SFP transceiver but is larger in size.