ExtremeSwitching

Troubleshooting Ethernet Routing Switch 3600 Series

Release 6.3
9035810 Rev AA
August 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 common problems and error messages and the techniques to resolve them.

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`.
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.

Table continues…

Convention	Description
	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/
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

There are no feature updates in this document.

Chapter 3: Troubleshooting tools

This document:

- describes the diagnostic tools and utilities available for troubleshooting using Command Line Interface (CLI) and Enterprise Device Manager (EDM)
- guides you through some common problems to achieve a first tier solution to these situations
- advises you what information to compile prior to troubleshooting or calling Extreme Networks for help

This documents assumes that you:

- have basic knowledge of networks, ethernet bridging, and IP routing
- are familiar with networking concepts and terminology
- have experience with Graphical User Interface (GUI)
- have basic knowledge of network topologies

Troubleshooting tools

The switch supports a range of protocols, utilities, and diagnostic tools that you can use to monitor and analyze traffic, monitor laser operating characteristics, capture and analyze data packets, trace data flows, view statistics, and manage event messages.

Certain protocols and tools are tailored for troubleshooting specific network topologies. Other tools are more general in their application and can be used to diagnose and monitor ingress and egress traffic.

Chapter 4: Troubleshooting planning

You can minimize the need for troubleshooting and to plan for doing it as effectively as possible.

1. Use the Documentation Reference for Ethernet Routing Switch 3600 Series to familiarize yourself with the documentation set, so you know where to get information when you need it.
2. Make sure the system is properly installed and maintained so that it operates as expected.
3. 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 onto a backup medium and store the backup offsite.
   - Store **passwords** in a safe place. It is a good practice 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 list 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.

4. 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 5: Troubleshooting fundamentals

This section describes available troubleshooting tools and their applications.

Port mirroring

The port mirroring feature helps you to monitor and analyze network traffic. This feature supports both ingress (incoming traffic) and egress (outgoing traffic) port mirroring. When 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.

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 limitations

The supports port mirroring in the following three modes:

- ingress mode (XRX or ->Port X)
- egress mode (XTX or Port X ->)
- ingress and egress mode (XRX or XTX or <->Port X)

There are limitations to the egress mode. As a standalone unit or in a stack, port-mirroring mode XTX mirrors egress traffic on the mirrored port, but does not mirror control packets generated by the switch. The monitor port does not receive copies of the generated control packets that egress from the mirrored port.

The following limitations apply to the ingress and egress mode:

- the same limitation on the XTX portion also applies to the ingress and egress mode
- the monitor port and the mirror port should be on the same unit in a stack.

Many to one Port mirroring

The Many to One Port Mirroring feature provides the ability of mirroring multiple ports to a single monitor port. With this feature, you can configure a single port to capture traffic from a set of selected ports. The captured traffic can be ingress or egress traffic.

Many to One Port Mirroring is supported in Stand-alone and stack configurations.

Many to One Port Mirroring modes

There are four modes of Many to One Port Mirroring. They are:

- ManyToOneRx. Monitors all traffic received on the mirrored ports.
- ManyToOneTx. Monitors all traffic transmitted by the mirrored ports.
- ManyToOneRxTx. Monitors all traffic received or transmitted by the mirror ports.
- XrxOrYtx. Monitors all traffic received by port X or transmitted by port Y.

Many to One Port Mirroring limitations

Following are the Many to One Port Mirroring limitations:

- Only ingress and egress port traffic mirroring is supported
- Can configure up to four mirror ports
- Mirror ports must continue to perform normal frame switching operation
- Cannot configure an MLT group as monitor port

Port mirroring commands

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

For more information, see Configuring System Monitoring on Ethernet Routing Switch 3600 Series.

Port statistics

Use port statistics commands to display information on received and transmitted packets at the ports. The ingress and egress counts occur at the MAC layer.

For more information regarding port statistics and commands, see Configuring System Monitoring on Ethernet Routing Switch 3600 Series.

System logs

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

The daemon syslogd 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 3600 Series.

Remote logging

As part of configuring system logging, you can specify remote logging parameters. This involves configuring a remote syslog address, enabling remote logging, and configuring the remote logging level.

For more information, see Configuring System Monitoring on Ethernet Routing Switch 3600 Series.

Software Exception Log

This feature allows an administrator to see the software exceptions generated in the switching system. The software exception log provides a method for capturing software faults in the SYSLOG application as critical customer messages. The CLI allows you to display and clear the last software exceptions generated in the system.

For more information, see Configuring System Monitoring on Ethernet Routing Switch 3600 Series.

Show environmental

This feature displays environmental information, such as power supply status, fan status, and switch system temperature.

For more information, see Configuring System Monitoring on Ethernet Routing Switch 3600 Series.

ASCII Configurator Generator

Use the ASCII Configurator Generator (ACG) tool to easily modify the configuration of a switch.

ACG generates an ASCII configuration file, which reproduces the behavior of the current binary configuration file. This function maintains backup configurations and provides a method to debug the current configuration of a switch.

For more information about configuration files, see Configuring Systems on Ethernet Routing Switch 3600 Series.

CPU and Memory Utilization

The CPU and Memory Utilization feature provides data for CPU and memory utilization. You can view CPU utilization information for the past 10 seconds (s), 1 minute (min), 10 minutes (min), 1 hour (hr), 24 hours (hr), or since system startup. The switch displays CPU utilization as a percentage. With CPU utilization information you can see how the CPU was used during a specific time interval.

The memory utilization provides information about the percentage of the dynamic memory currently used by the system. The switch displays memory utilization in terms of the lowest percentage of dynamic memory available since system startup.

No configuration is required for this display-only feature. For more information, see Configuring System Monitoring on Ethernet Routing Switch 3600 Series.

SNMP trap enhancements

With SNMP management, you can configure SNMP traps to automatically generate notifications globally, or on individual ports. These notifications can report conditions, such as an unauthorized access attempt or changes in port operating status. All notifications are enabled on individual interfaces by default.

The switch supports both industry-standard SNMP traps, as well as private Extreme Networks enterprise traps. SNMP trap notification-control provides a generic mechanism for the trap generation control that works with any trap type.

For more information, see Configuring System Monitoring on Ethernet Routing Switch 3600 Series.

SNMP Trap list web page in EDM

You can use Enterprise Device Manager (EDM) MIB Web page to query SNMP objects on the switch.

For more information, see Configuring System Monitoring on Ethernet Routing Switch 3600 Series.

Remote monitoring (RMON) (RFC1757) per port statistics, history, alarms, and events

Remote Monitoring (RMON) MIB is an interface between the RMON agent on a switch and an RMON management application, such as Enterprise Device Manager (EDM).

The RMON agent defines objects that are suitable for the management of any type of network, but some groups are targeted for Ethernet networks in particular. The RMON agent continuously collects statistics and monitors switch performance. This data can be viewed through CLI and EDM.

RMON has three major functions:

- creating and displaying alarms for user-defined events
- gathering cumulative statistics for Ethernet interfaces
- tracking a history of statistics for Ethernet interfaces

For more information on RMON per port statistics, history, alarms, and events, see Configuring System Monitoring on Ethernet Routing Switch 3600 Series.

Chapter 6: Troubleshooting Fabric Attach

This chapter contains details about how to troubleshoot common Fabric Attach (FA) problems you might 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 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

                              Service
Unit Port IfIndex Trunk Advertisement Authentication Keymode
____ ____ _______ _____ _____________ ______________ ________
1    1    1                Enabled        Enabled     Strict
1    2    2                Enabled        Enabled     Strict
1    3    3                Enabled        Enabled     Strict
1    4    4                Enabled        Enabled     Strict
1    5    5                Enabled        Enabled     Strict
1    6    6                Enabled        Enabled     Strict
1    7    7                Enabled        Enabled     Strict
1    8    8                Enabled        Enabled     Strict
1    9    9                Enabled        Enabled     Strict
1    10   10               Enabled        Enabled     Strict
```

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

================================================================================
                        Fabric Attach Discovered Elements
================================================================================
UNIT/                   MGMT                                          ELEM ASGN
PORT    TYPE            VLAN  STATE  SYSTEM ID                        AUTH AUTH
--------------------------------------------------------------------------------

================================================================================
                      Fabric Attach Authentication Detail
================================================================================
UNIT/                                 ELEM OPER           ASGN OPER
PORT   EXPANDED TYPE                  AUTH STATUS         AUTH STATUS
--------------------------------------------------------------------------------

State Legend: (Tagging/AutoConfig)
T=Tagged, U=UntaggedPvid, O=UntaggedOnly, D=Disabled, S=Spbm, V=Vlan, I=Invalid

Auth Legend:
AP=Authentication Pass, AF=Authentication Fail, NA=Not Authenticated, N=None

--------------------------------------------------------------------------------
```

Chapter 7: General diagnostic tools

You can use the diagnostic tools to help you troubleshoot operational and configuration issues using CLI or EDM. 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.

CLI Command Modes

Command Line Interface (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	Entrance commands	Exit commands

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

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

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

Interface Configuration
`Switch (config-if)#`
	From Global Configuration mode:
	To configure a port, enter
	`interface ethernet <port number>`
	To configure a VLAN, enter
	`interface vlan <vlan number>`
	To configure a loopback, enter
	`interface loopback <loopback number>`
		To return to Global Configuration mode, enter
		`exit`
		To return to Privileged Executive mode, enter
		`end`
		To exit CLI completely, enter
		`logout`

Router Configuration
`Switch (config-router)#`
	From Global Configuration mode:
	To configure RIP, enter `router rip`
		To return to Global Configuration mode, enter
		`exit`
		To return to Privileged Executive mode, enter
		`end`
		To exit CLI completely, enter
		`logout`

Table continues…

Command mode and sample prompt	Entrance commands	Exit commands

Application Configuration
`Switch (config-app)#`
	From Global, or Interface Configuration mode, enter
	`application`
		To return to Global Configuration mode, enter
		`exit`
		To return to Privileged Executive mode, enter
		`end`
		To exit CLI completely, enter
		`logout`

Chapter 8: 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.
- 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.
- **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.** When connectivity problems occur, get information on at least five working source and destination IP pairs and five IP pairs with connectivity issues. To obtain this information, use the following commands:

  - **`show tech`**

- **show running-config**
- **show port-statistics <port>**

Chapter 9: Emergency recovery trees

An Emergency Recovery Tree (ERT) is designed to quickly guide you through some common failures and solutions, by providing a quick reference for troubleshooting without procedural detail.

Emergency recovery trees

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.

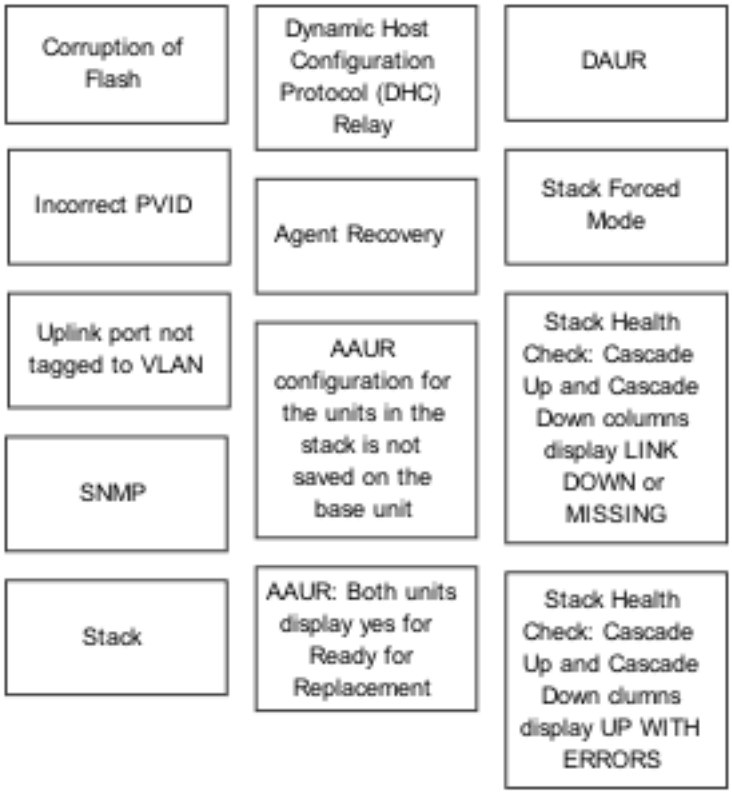


Figure 1: Emergency Recovery Trees

Corruption of flash

Corruption of the switch configuration file can sometimes occur due to power outage or environmental reasons, which 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 a Return Merchandise Authorization (RMA).

For assistance with tasks in the Corruption of Flash Emergency Recovery Tree, see Using the Diagnostics Menu on page 56.

Corruption of flash recovery tree

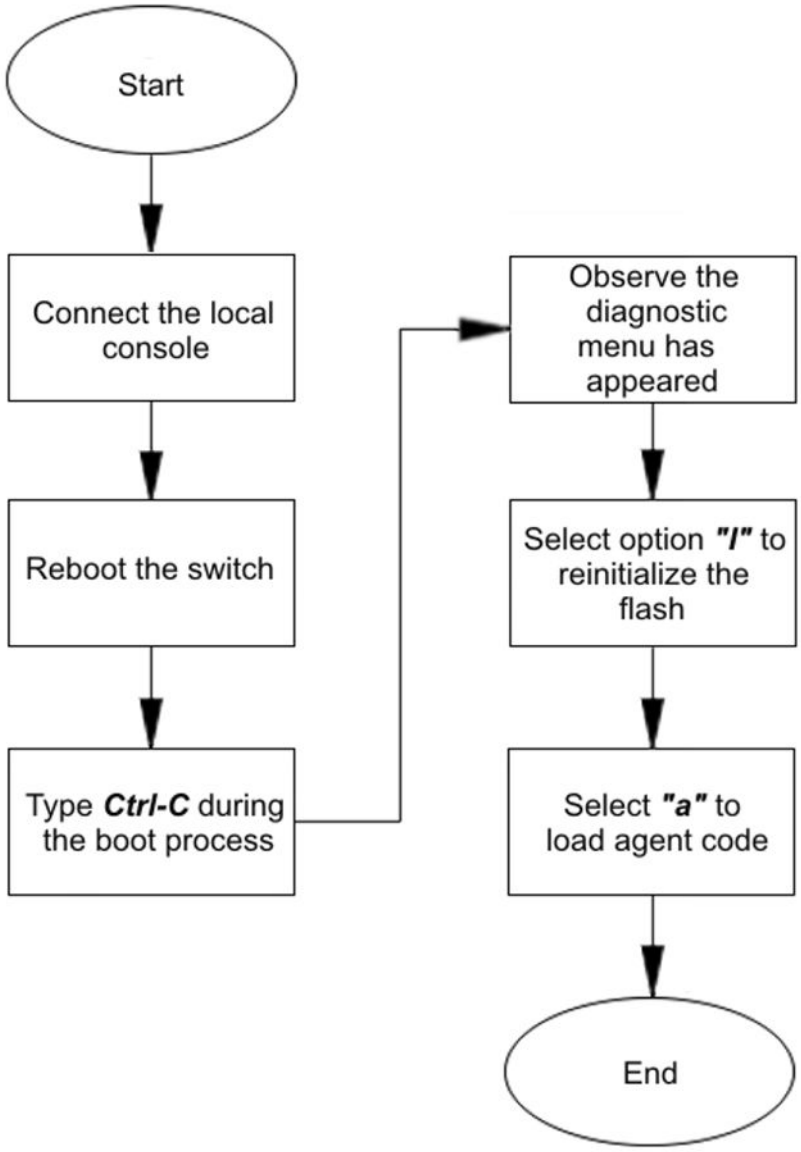


Figure 2: Corruption of flash recovery tree

Incorrect Port VLAN Identifier (PVID)

Port VLAN identifier (PVID) is a classification mechanism that associates a port with a specific VLAN. For example, a port with a PVID of 3 (PVID=3) assigns all untagged frames received on this port to VLAN 3.

An issue can occur where clients cannot communicate to critical servers when their ports are put in wrong VLAN. If the server 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**.

For examples that show how to check the PVID of ports, and how to make PVID corrections, see

- Example Checking PVID of ports on page 57
- Example VLAN Interface VLAN IDs on page 57

Incorrect PVID recovery tree

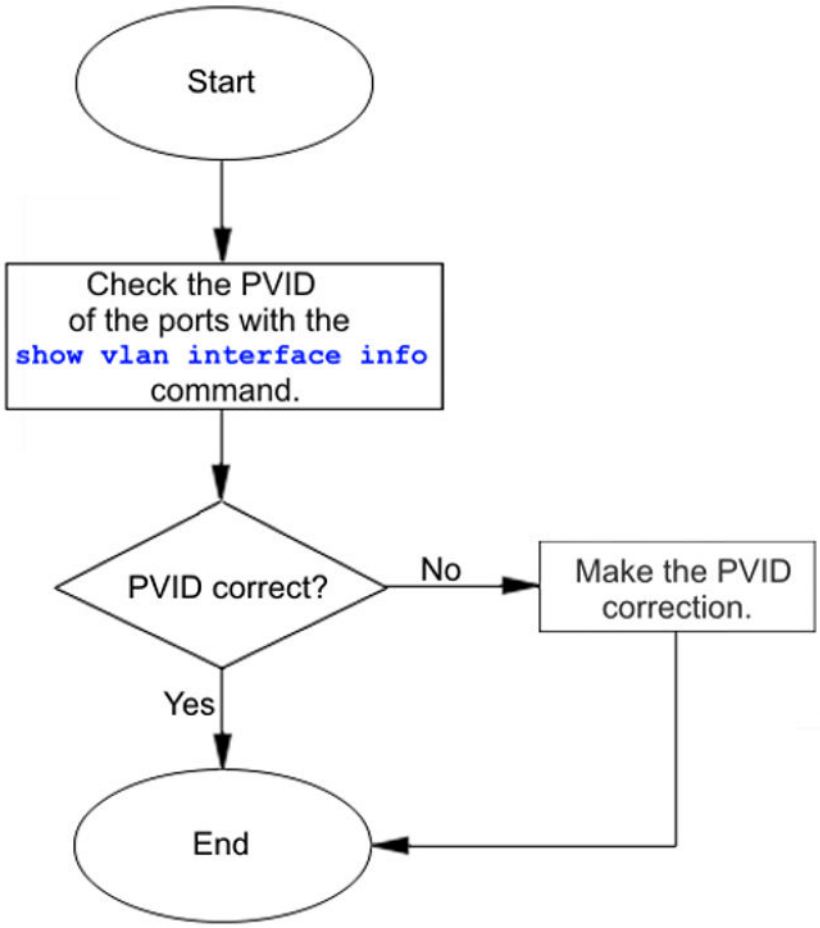


Figure 3: Incorrect PVID recovery tree

Uplink ports not tagged to VLAN

When an ERS 3600 Series switch is connected to an ERS 8600 Series switch or another switch, and devices in a VLAN on the ERS 8600 Series switch are not able to communicate with devices at the ERS 3600 Series switch in the same VLAN, then it is likely that the uplink ports are not tagged to the VLAN on the ERS 3600 Series switch.

Use the **`show vlan interface info`** command to see if ports are tagged or untagged:

- **Untagged frame**: a frame that carries no VLAN tagging information in the frame header.
- **Tagged frame:** a frame that contains the 32–bit 802.1q field (VLAN tag) and identifies the frame as belonging to a specific VLAN.
- **Untagged member:** a port configured as an untagged member of a specific VLAN. When an untagged frame exits the switch through an untagged member port, the frame header remains unchanged. When a tagged frame exits the switch through an untagged member port, the tag is stripped and the tagged frame is changed to an untagged frame.
- **Tagged member:** a port configured as a tagged member of a specific VLAN. When an untagged frame exits the switch through a tagged member port, the frame header changes to include the 32–bit tag associated with the ingress port PVID. When a tagged frame exits the switch through a tagged member port, the frame header remains unchanged. The original VLAN ID (VID) remains.

An example using the **`show vlan interface info`** command is provided in Example Checking PVID of ports on page 57.

To ensure that the uplink port(s) are tagged and a member of ALL of the configured VLANs, use the **`show vlan interface vids`** command. An example using the **`show vlan interface vids`** command is provided in Example VLAN Interface VLAN IDs on page 57.

Correct errors by adding missing VLANs to affected uplink ports. Refer to Tagging options on page 59.

Uplink ports not tagged to VLAN recovery tree

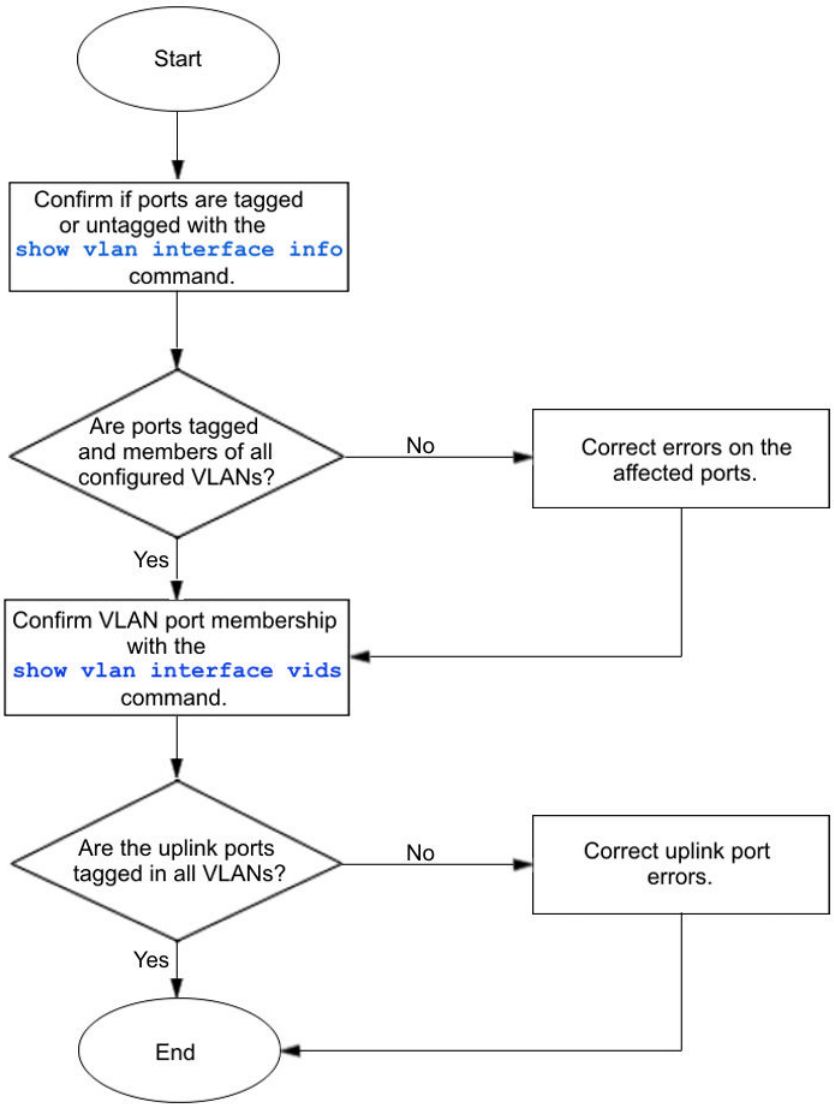


Figure 4: Uplink ports not tagged to VLAN recovery tree

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

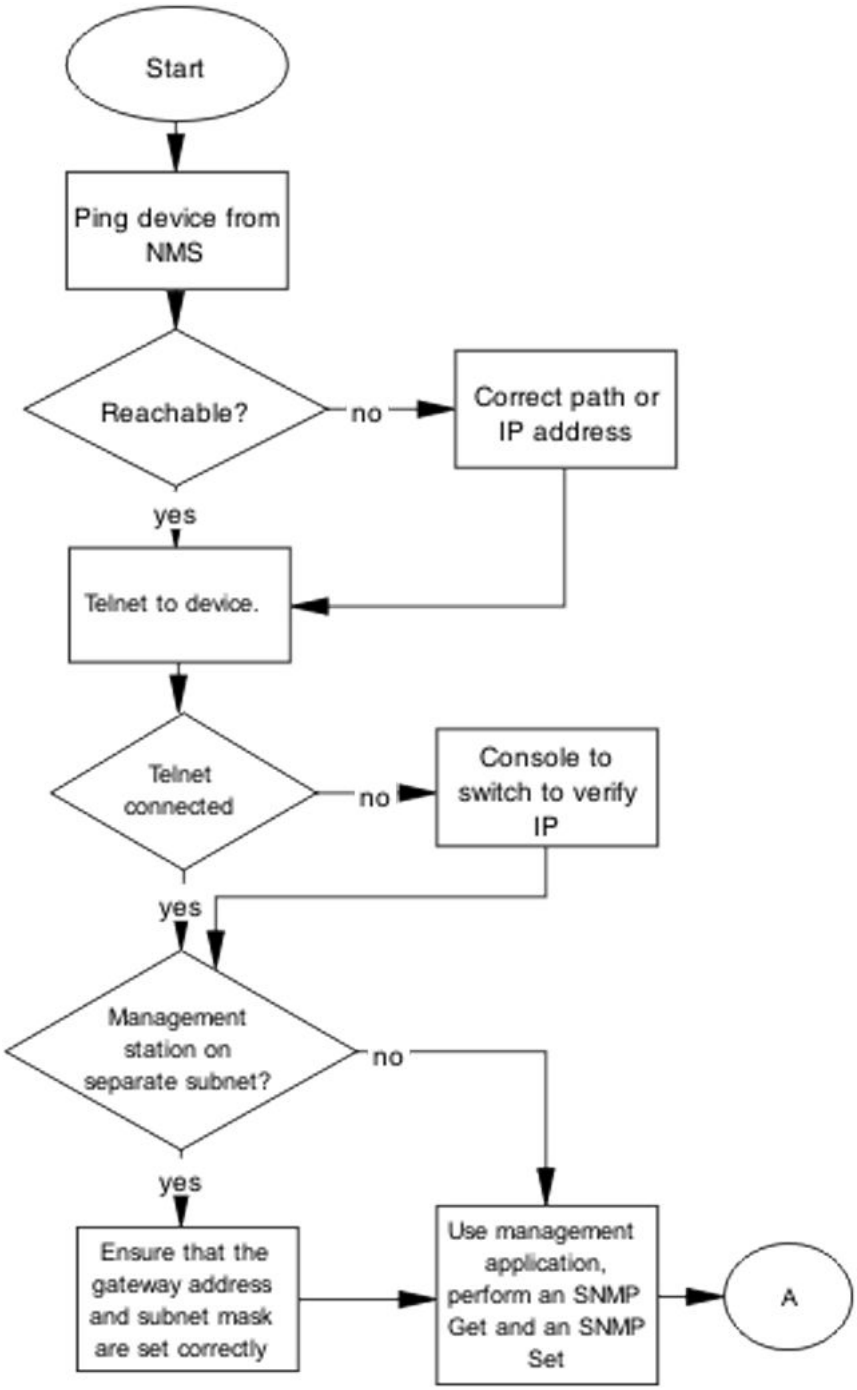


Figure 5: SNMP part 1

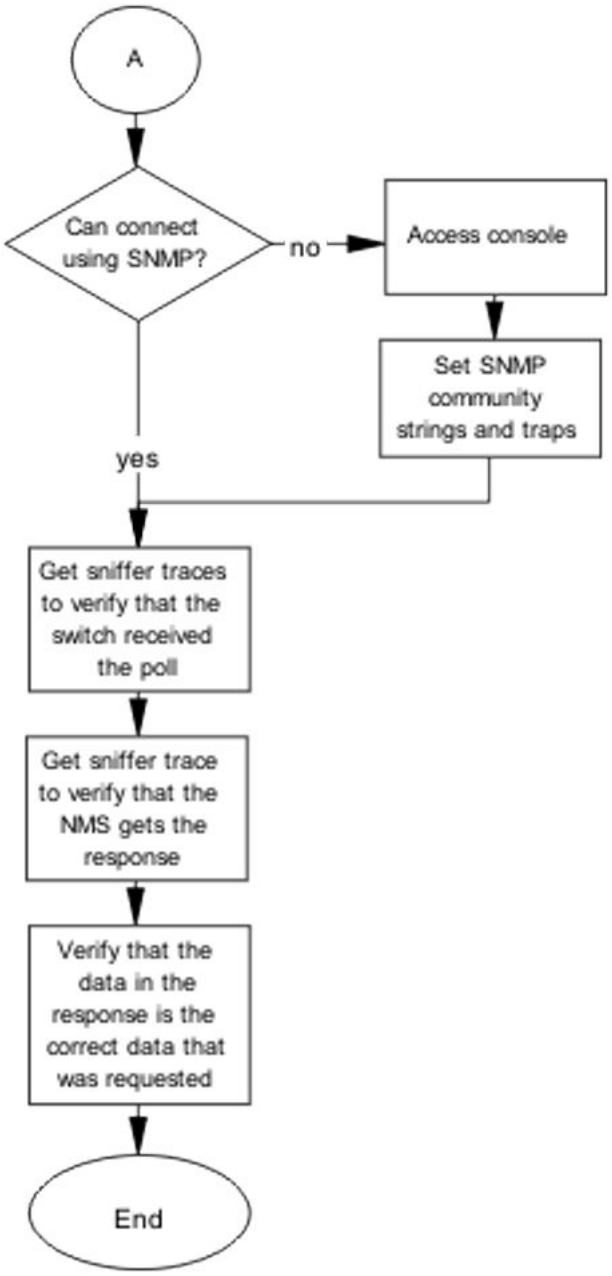


Figure 6: SNMP part 2

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 Select switch to the Base position. Only ONE switch in a stack configuration must have the Base Unit Select switch set to this position.
- Cable incorrectly inserted into the corresponding Cascade Up or Cascade Down port..

Stack recovery tree

About this task

The following figures show the stack recovery tree.

Procedure

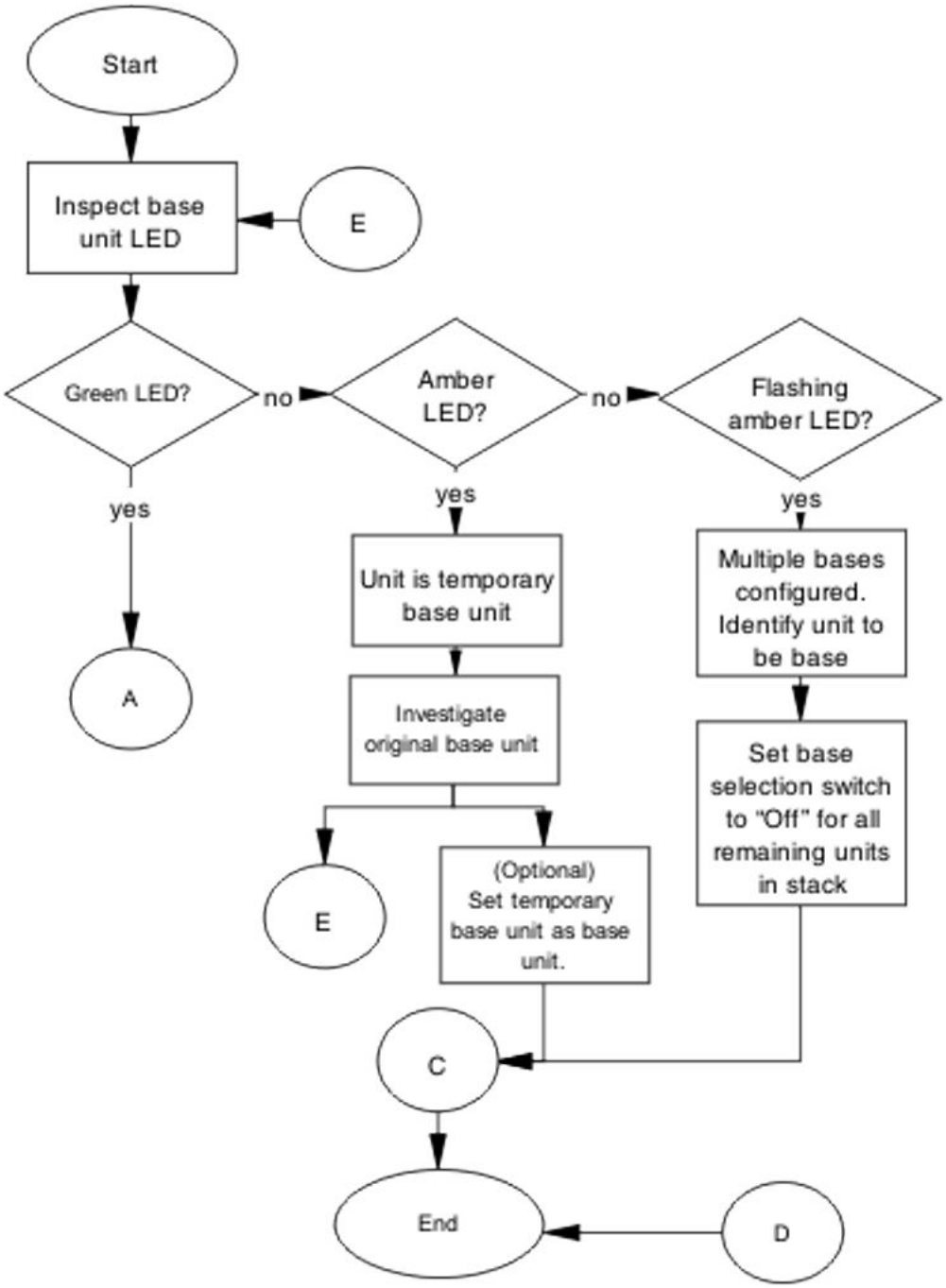


Figure 7: Stack part 1

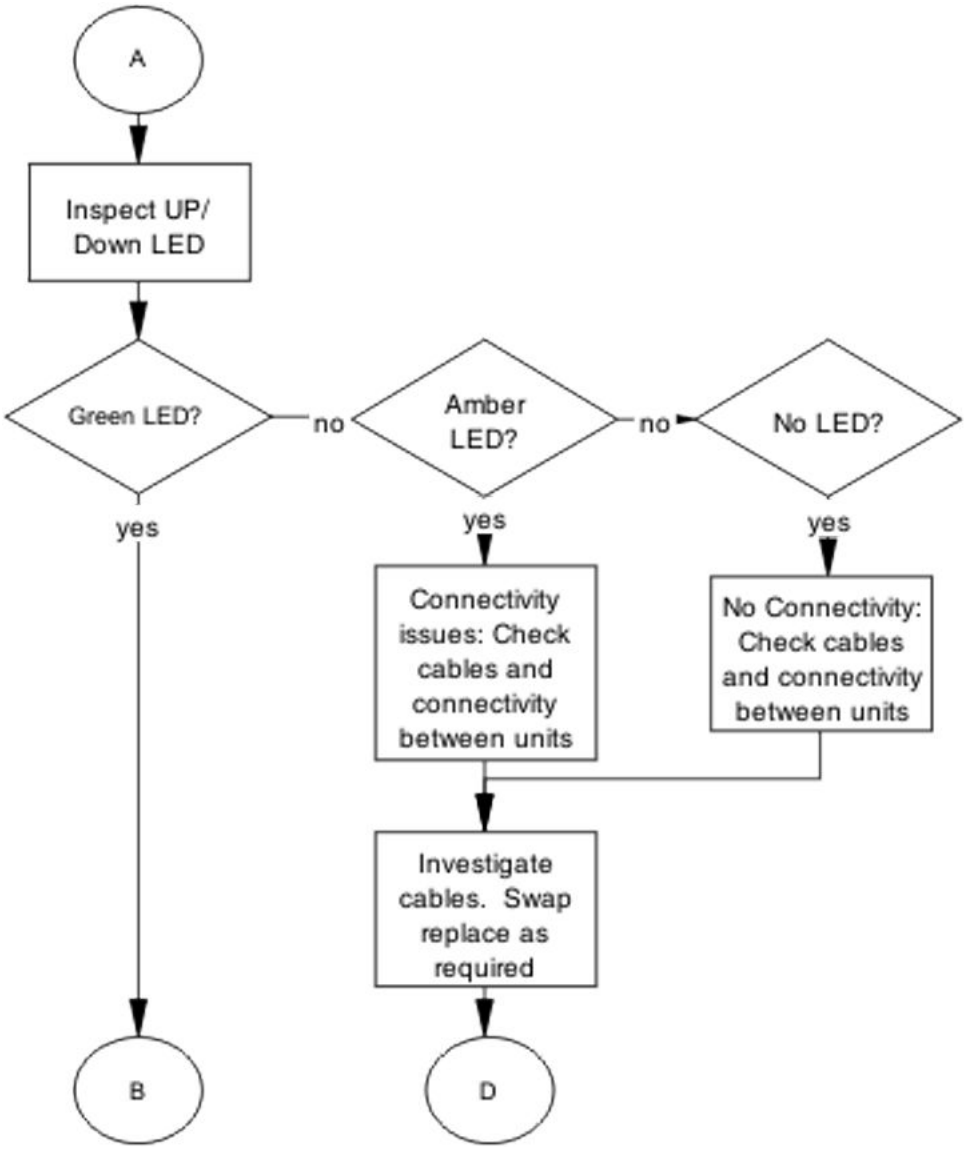


Figure 8: Stack part 2

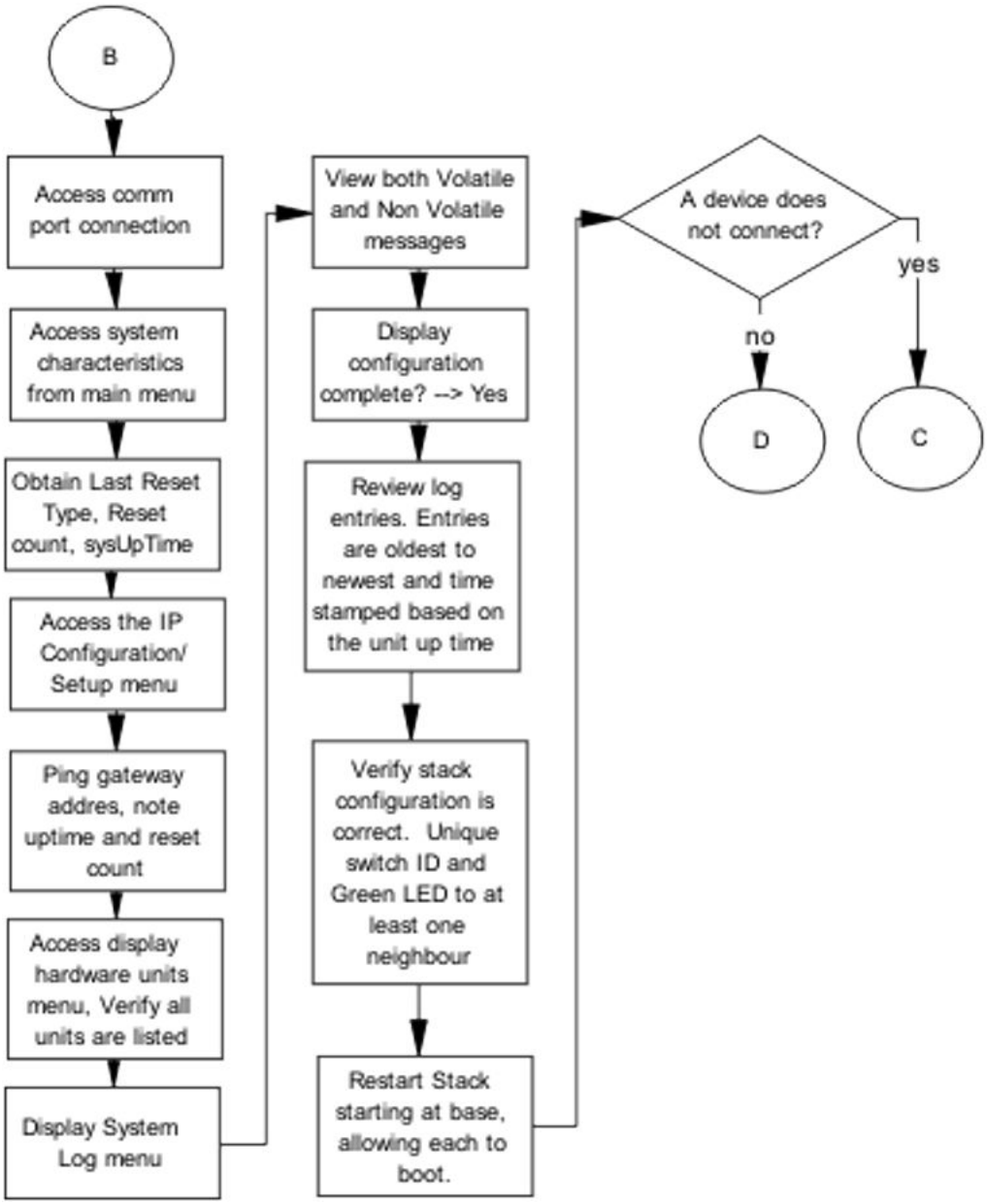


Figure 9: Stack part 3

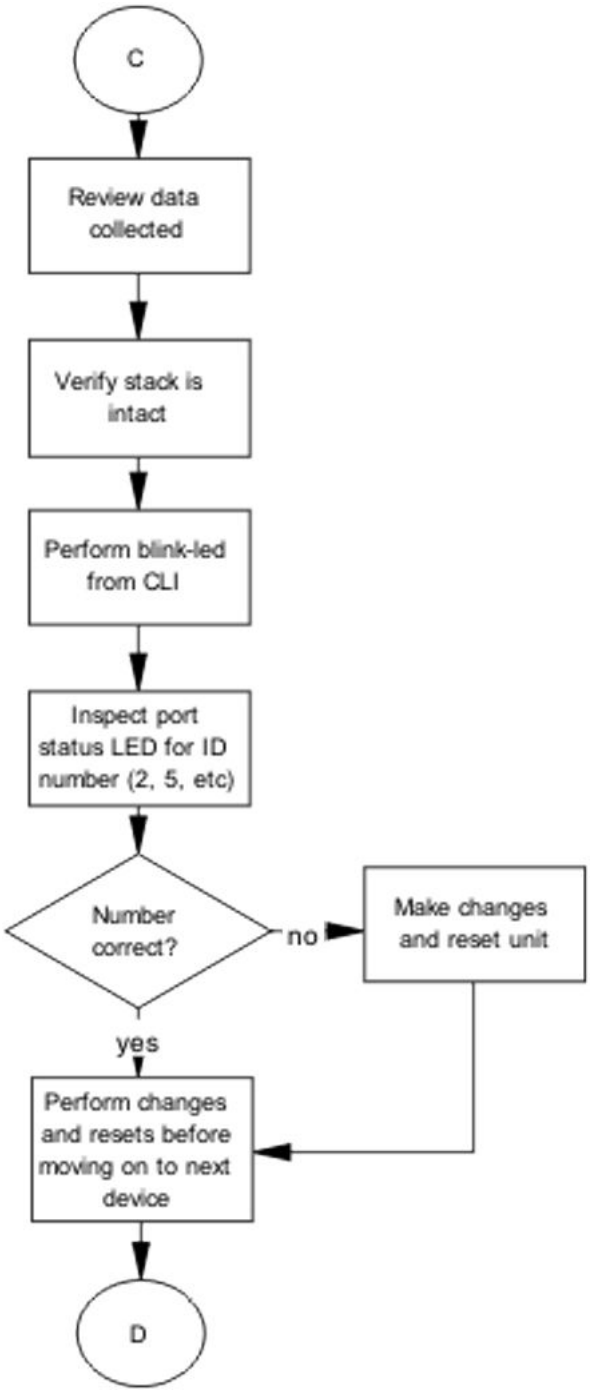


Figure 10: Stack part 4

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

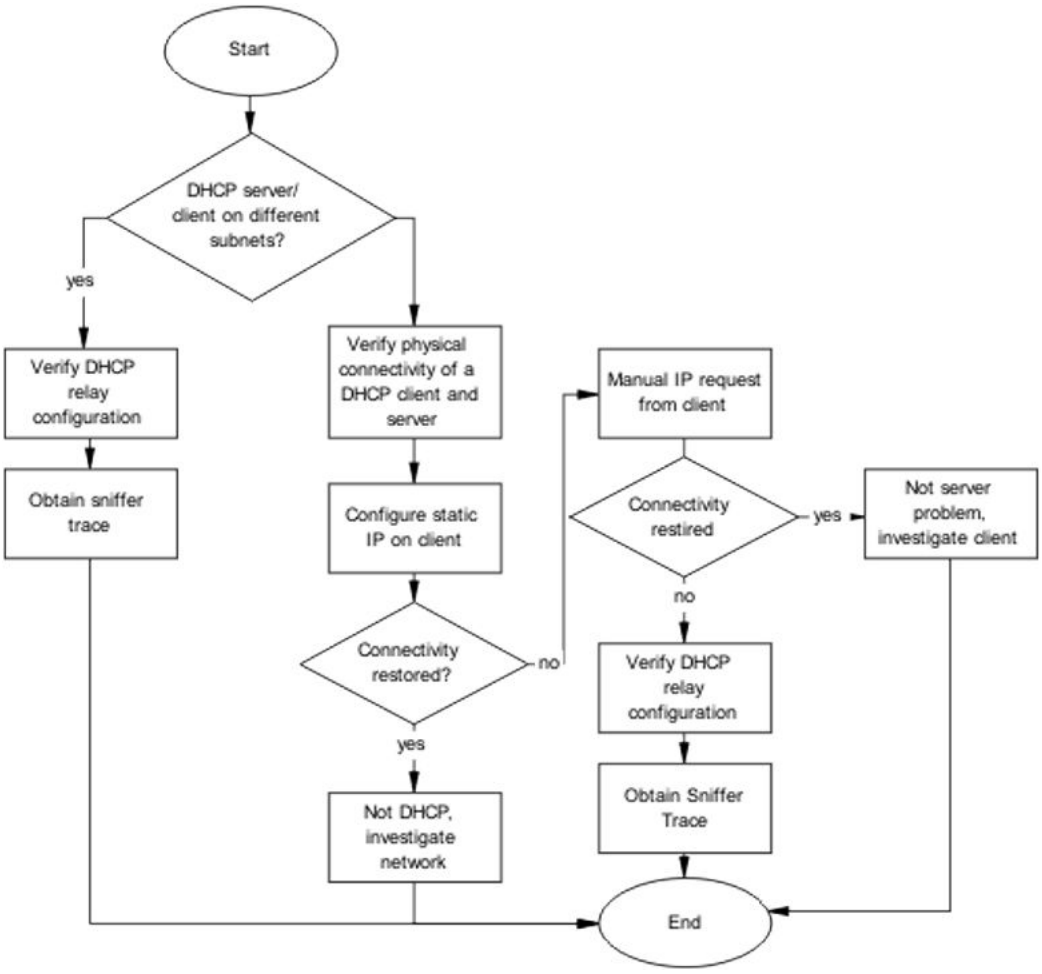


Figure 11: DHCP

Agent Recovery

In some cases during a software upgrade, the switch turns off before the software agent has been completely written to flash. This might be due to a power outage. In this case, the switch reports an error such as `Agent code verification fails!!`

Units exhibiting the symptoms should NOT be returned through the Return Merchandise Authorization (RMA). They should be corrected in the field.

For assistance with tasks shown in the Agent Recovery emergency recovery tree, see Using the Diagnostics Menu on page 56.

Agent Recovery Emergency Recovery Tree

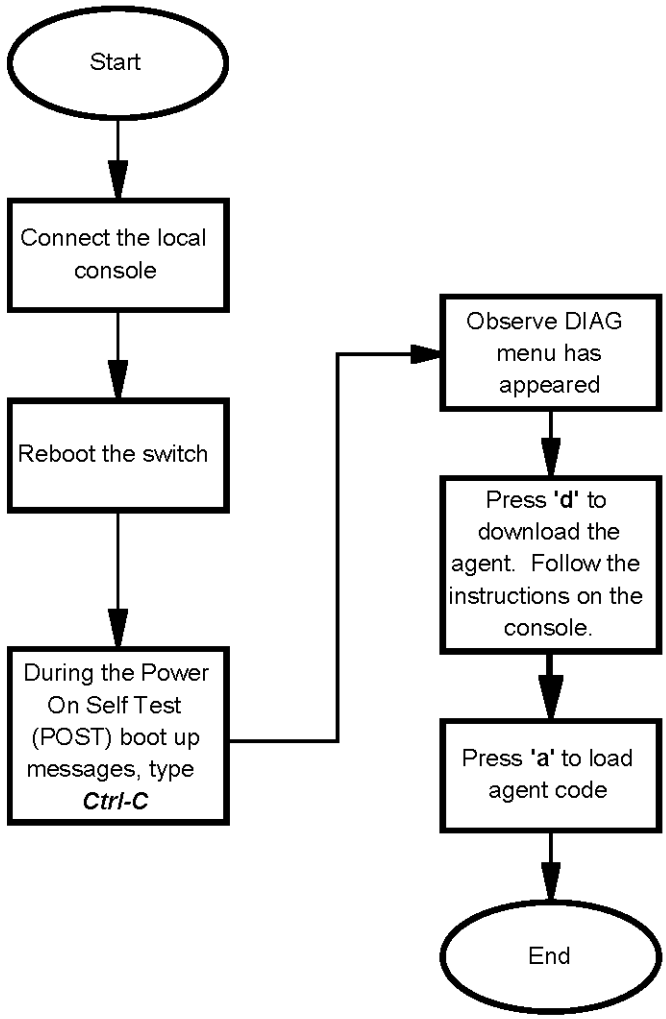


Figure 12: Agent Recovery Emergency Recovery Tree

AAUR: 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

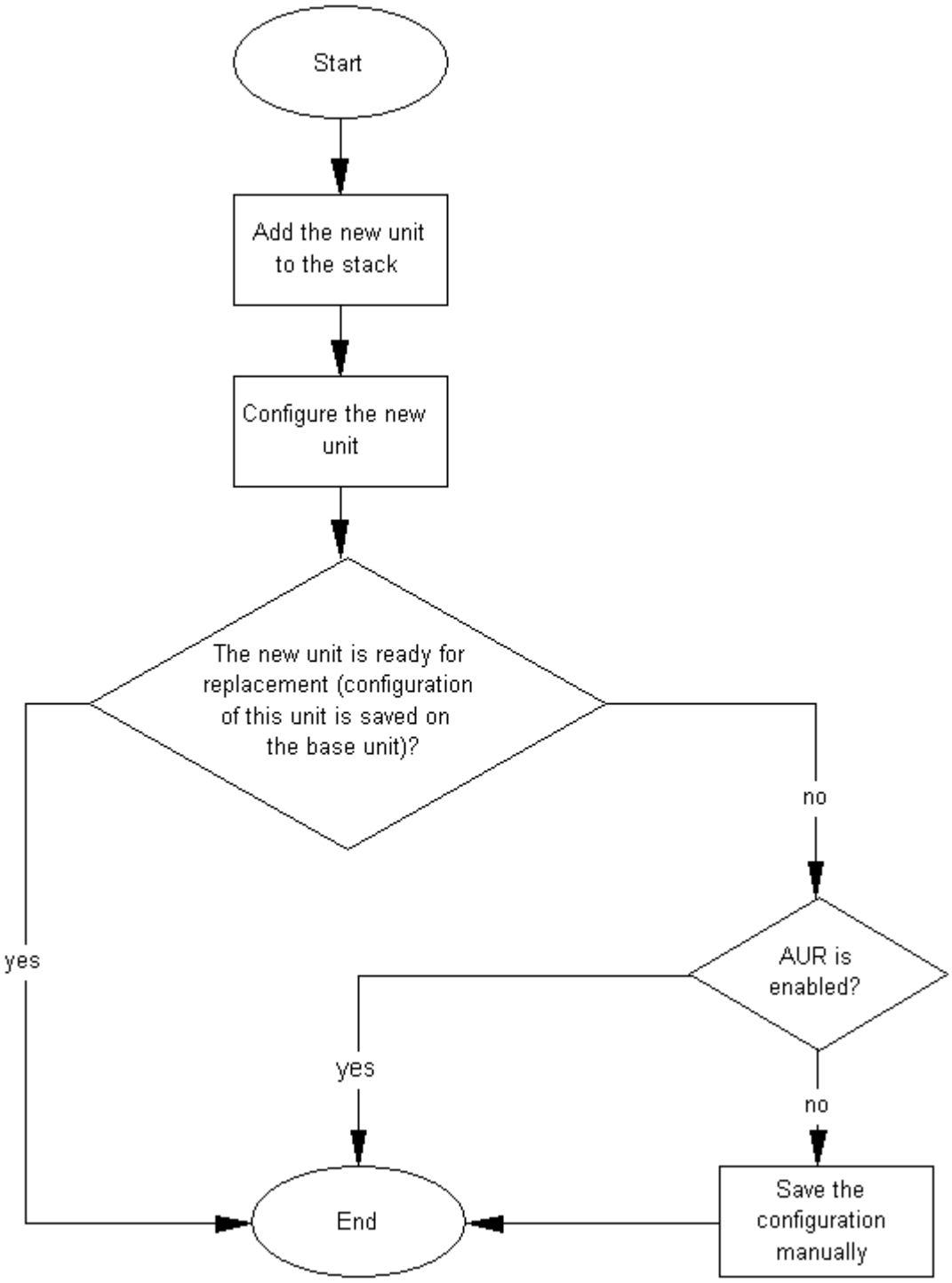


Figure 13: Configuration for the units in the stack is not saved on the base unit

AAUR: 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

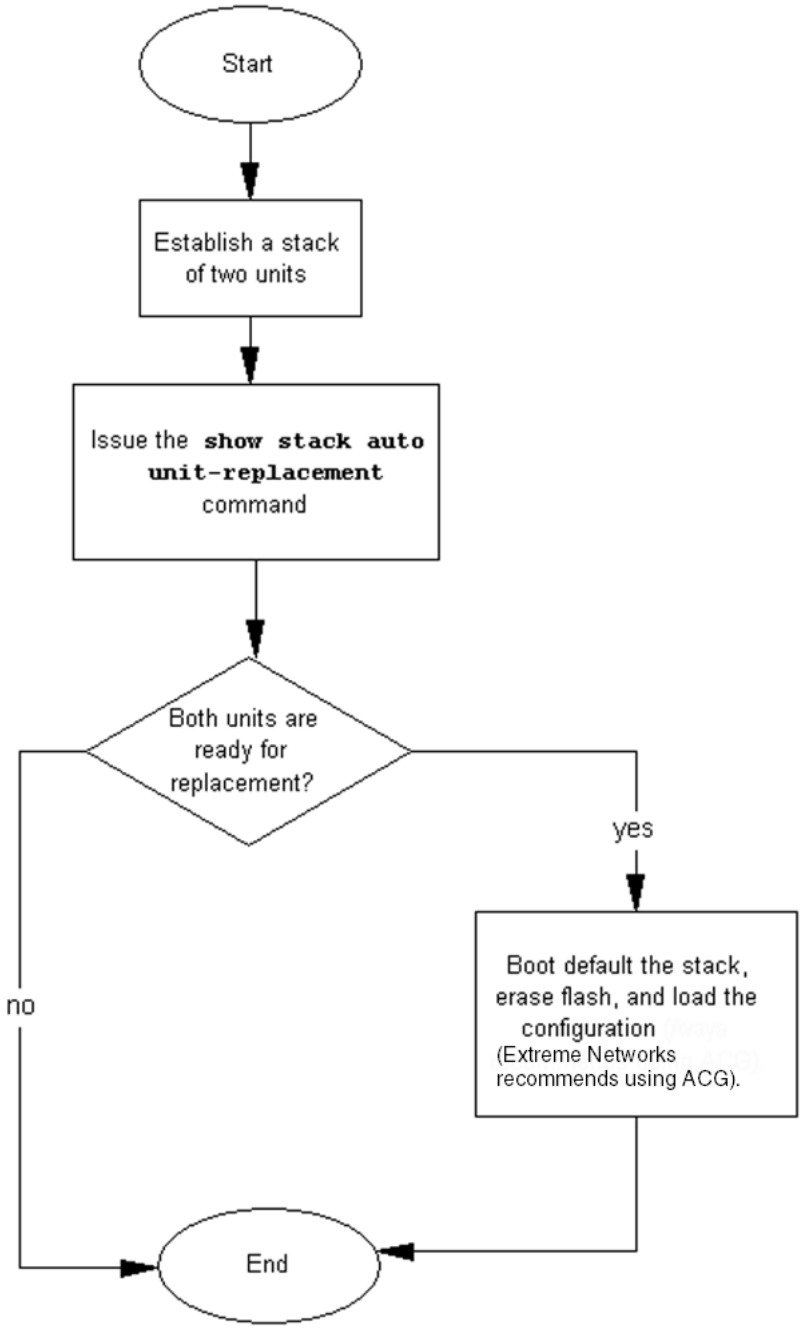


Figure 14: Both units display yes for Ready for Replacement

DAUR

If you add a new unit to a stack, and the units have different diagnostic images, the new unit should start to copy the diagnostic image from the existing stack. Use the recovery tree in this section if the new unit fails to copy the diagnostic image.

Diagnostic image transfer does not start recovery tree

About this task

The following figure shows the recovery tree to correct issues if a new unit fails to copy the diagnostic image from the stack.

Procedure

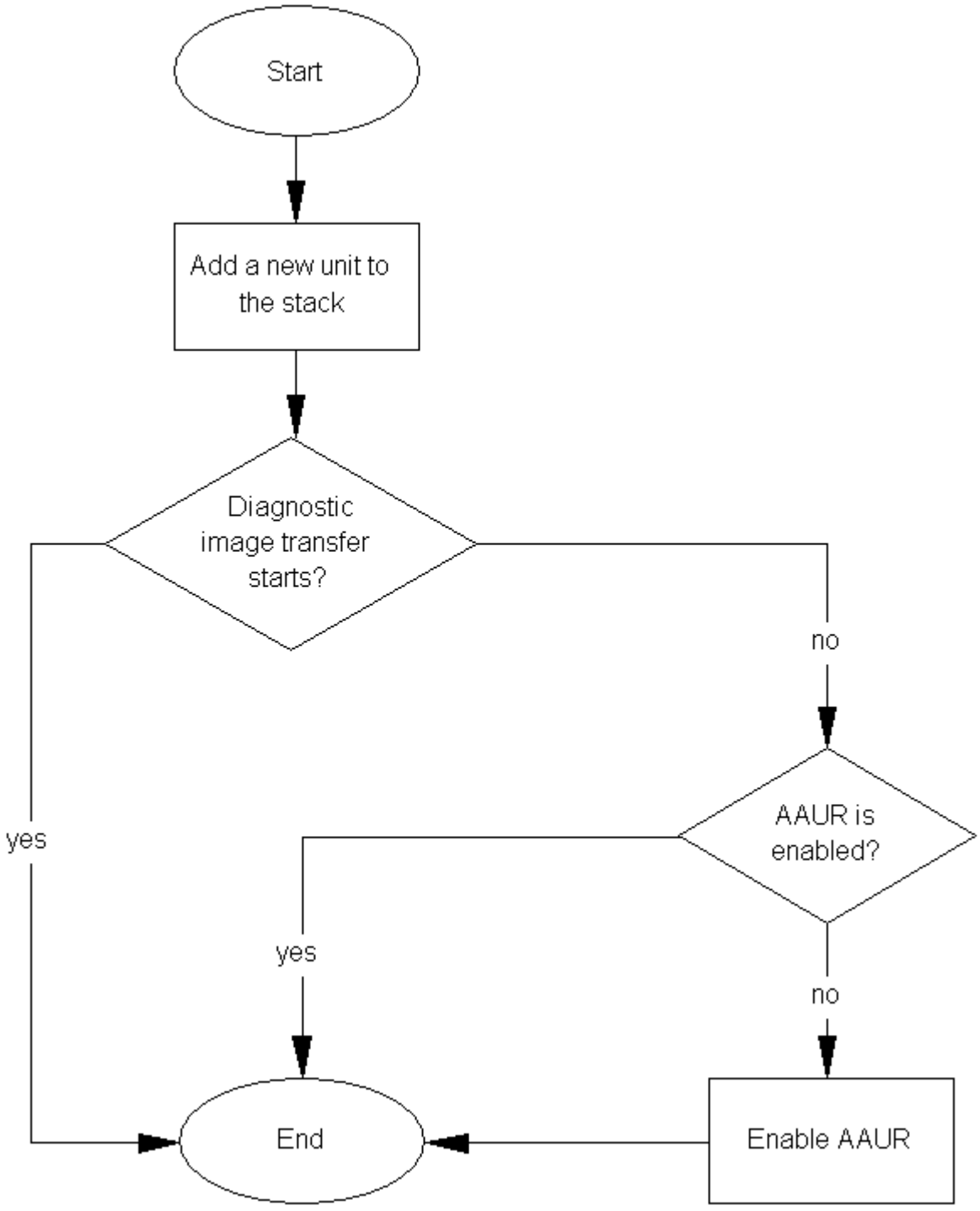


Figure 15: Diagnostic image transfer does not start

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 EDM 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.

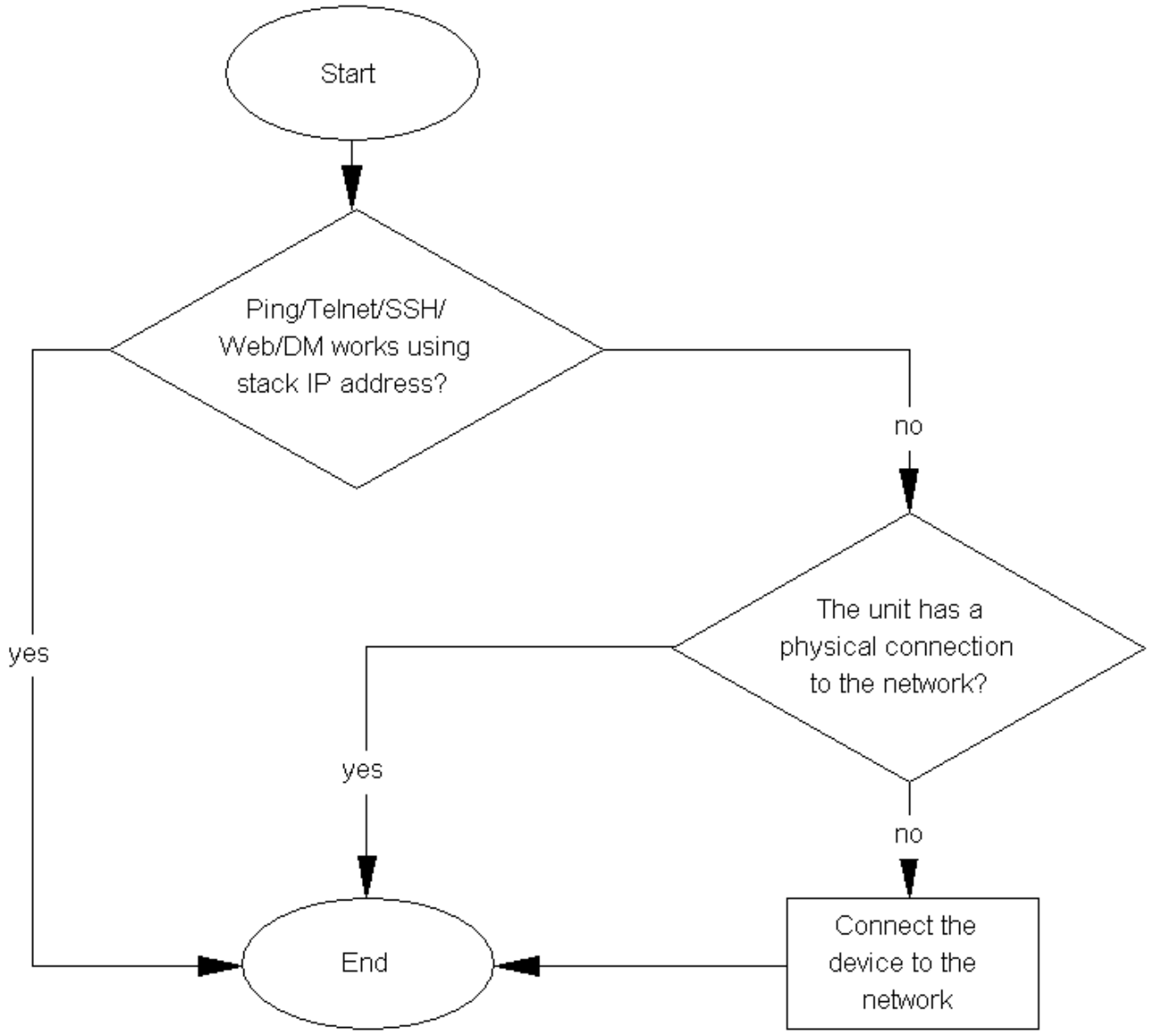


Figure 16: Ping/Telnet/SSH/Web/EDM do not work when you use the stack IP address

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.

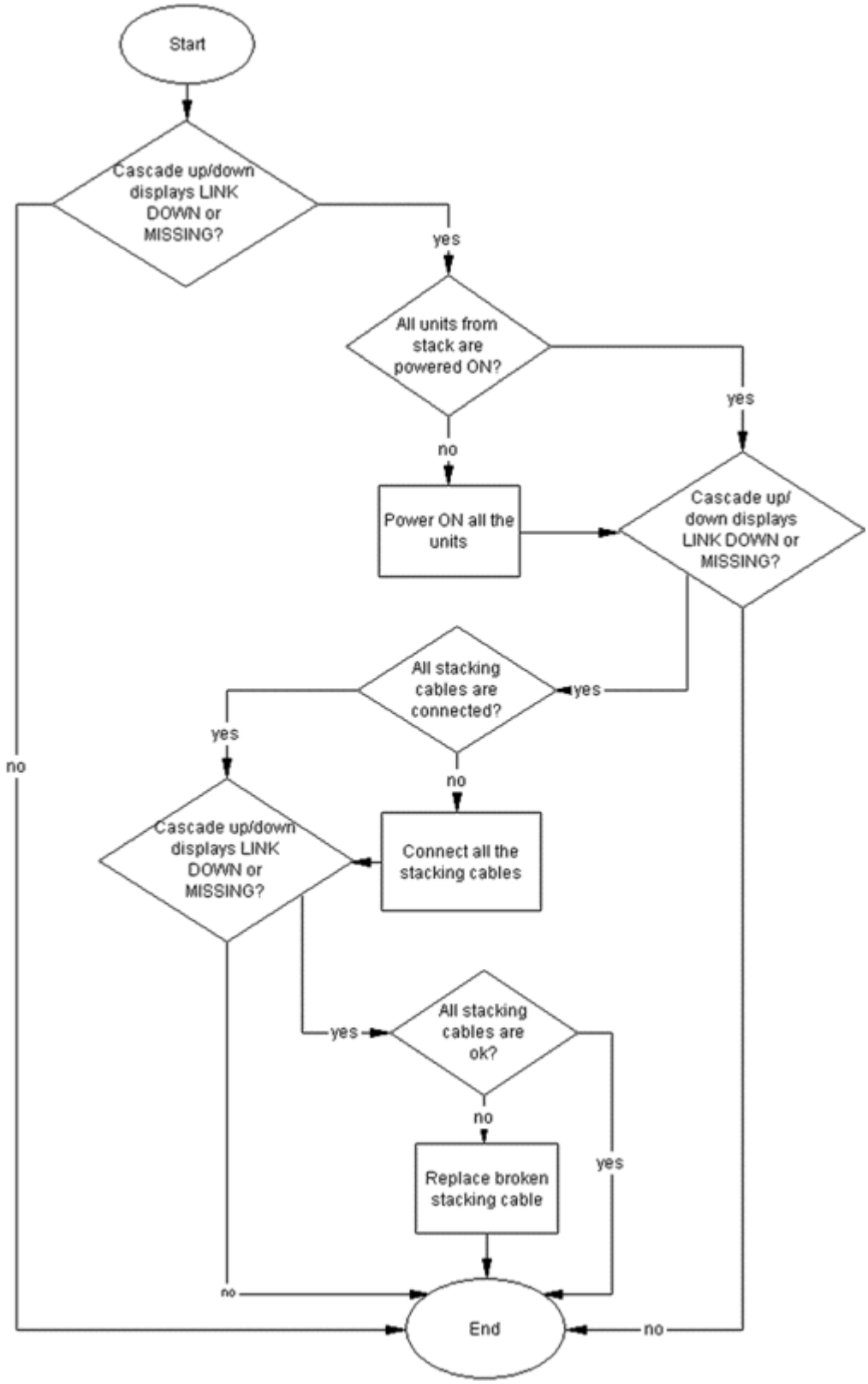


Figure 17: Stack Health Check: Cascade Up and Cascade Down columns display LINK DOWN or

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.

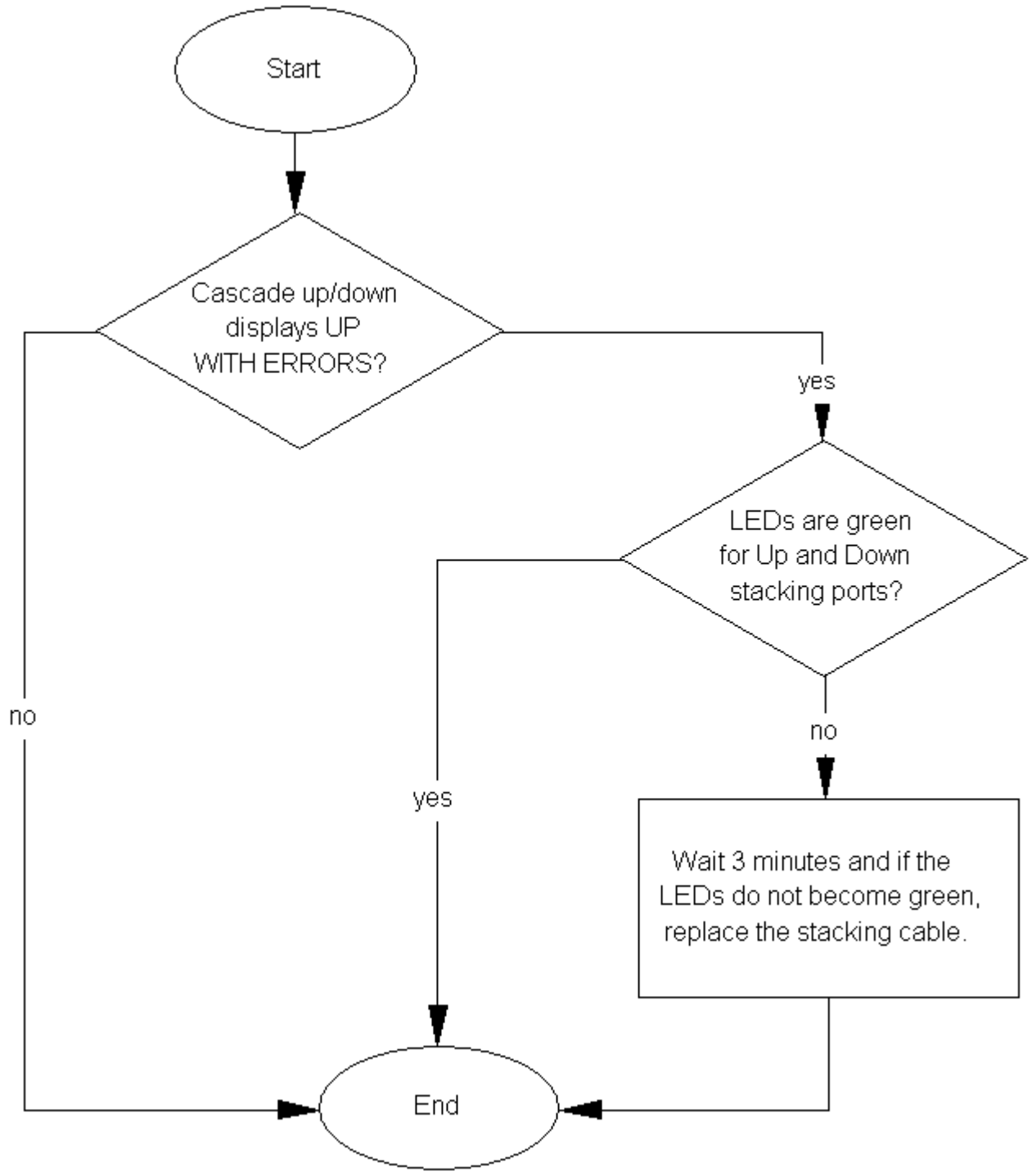


Figure 18: Stack Health Check: Cascade Up and Cascade Down columns display UP WITH ERRORS

Using the Diagnostics Menu

On power up, the Power-On Self Tests (POST) are executed and the following is displayed:

```
Test 111     DDRAM Walking 1/0s           -PASSED
Test 112     DDRAM Byte/Word/Long         -PASSED
Test 113     DDRAM Power-of-2             -PASSED
Test 121     ROM Config                   -PASSED
Test 151     FANs Status                  -PASSED
Test 207     XGS SWITCH Registers         -PASSED
Test 221     PHYs Register                -PASSED
Test 271     Ports Internal Loopback      -PASSED
```

If an error is found, the test reports FAILED and an error message is displayed and stored in the Error Log. The Error Log may contain up to 10 POST (or Burn-In) errors. Use the 'e' — **`show errors`** command in the Press menu or the Manufacturing **`SHOWLOG`** command to display errors. Clear errors using the **`INITLOG`** command.

If you type `CTRL-C` on the console during the power-up or reset sequence, the Diagnostics display the following break message:

```
       >>Break Recognized - Wait . .
```

After Diagnostics finish initializing, the “Press” menu is displayed:

```
Press 'a'   to run Agent Code
Press 'd'   to download agent/diag/bootloader code
Press 'e'   to display Errors
Press 'i'   to initialize config flash
Press 'p'   to run POST tests
Press 'r'   to reset the box.
```

If you press . . .	Result

a	Diagnostics executes the Agent code (if present):
	`Starting Agent Version:   5.0.0.xxx`
	`Decompressing the image     done,`
	`Initializing . . . .`

d	The following information is required:
	`Enter Port Number                          [ <all> ]:`
	`Enter Speed:   10, 100 or 1G              [ 100 ]:`
	`Enter Local IP Address                  [ 0.0.0.0 ]:`
	`Enter Server IP Address                 [ 0.0.0.0 ]:`
	`Enter Subnet Mask                       [ 255.255.255.0 ]:`
	`Enter Filename:`

e	The POST test errors are re-displayed:
	`System Resets   =        1.`
	`Burn-In Loops   =        0.`
	`Burn-In Errors  = DISABLED`
	`Default Baud    =     9600`
	
	`Error Log:`
	`Bad Port Mask   = 00000000`
	`Loop Test Error Description:`
	`<errors>`

i	The flash config/log area is initialized. This area is used by the Agent code.

Table continues…

If you press . . .	Result
p	The POST tests are executed again.
r	Resets the switch

Example Checking PVID of ports

The following figure shows output from the **show vlan interface info** command.

```
3526T#show vlan interface info
      Filter     Filter
     Untagged Unregistered
Port  Frames     Frames     PVID PRI    Tagging     Name
---- -------- ------------ ---- --- ------------- ---------
1    No       Yes          1    0   UntagAll      Port 1
2    No       Yes          1    0   UntagAll      Port 2
3    No       Yes          1    0   UntagAll      Port 3
4    No       Yes          1    0   UntagAll      Port 4
5    No       Yes          1    0   UntagAll      Port 5
6    No       Yes          1    0   UntagAll      Port 6
7    No       Yes          1    0   UntagAll      Port 7
8    No       Yes          1    0   UntagAll      Port 8
9    No       Yes          1    0   UntagAll      Port 9
10   No       Yes          1    0   UntagAll      Port 10
11   No       Yes          1    0   UntagAll      Port 11
12   No       Yes          1    0   UntagAll      Port 12
13   No       Yes          1    0   UntagAll      Port 13
14   No       Yes          1    0   UntagAll      Port 14
15   No       Yes          1    0   UntagAll      Port 15
16   No       Yes          1    0   UntagAll      Port 16
17   No       Yes          1    0   UntagAll      Port 17
18   No       Yes          1    0   UntagAll      Port 18
```

Example VLAN Interface VLAN IDs

The following figure provides example output from the **show vlan interface vids** command.

```
3526T#show vlan interface vids
Port VLAN VLAN Name          VLAN VLAN Name          VLAN VLAN Name
---- ---- ----------------  ---- ----------------  ---- ----------------
1    1    VLAN #1
---- ---- ----------------  ---- ----------------  ---- ----------------
2    1    VLAN #1
---- ---- ----------------  ---- ----------------  ---- ----------------
3    1    VLAN #1
---- ---- ----------------  ---- ----------------  ---- ----------------
4    1    VLAN #1
---- ---- ----------------  ---- ----------------  ---- ----------------
5    1    VLAN #1
---- ---- ----------------  ---- ----------------  ---- ----------------
6    1    VLAN #1
---- ---- ----------------  ---- ----------------  ---- ----------------
7    1    VLAN #1
---- ---- ----------------  ---- ----------------  ---- ----------------
8    1    VLAN #1
---- ---- ----------------  ---- ----------------  ---- ----------------
9    1    VLAN #1
---- ---- ----------------  ---- ----------------  ---- ----------------
10   1    VLAN #1
---- ---- ----------------  ---- ----------------  ---- ----------------
```

Tagging options

Use the commands and outputs in this example to assist in adding missing VLANs to affected uplink ports.

```
3526T(config)#vlan ports 1 tagging ?
  disable         Disable tagging on this port
  enable          Enable tagging on this port
  tagAll          Enable tagging on this port
  tagPvidOnly     Enable tagging of packets matching the Pvid on this port
  untagAll        Disable tagging on this port
  untagPvidOnly   Disable tagging of packets matching the Pvid on this port

3526T(config)#show vlan interface info
      Filter     Filter
     Untagged Unregistered
Port  Frames     Frames     PVID PRI    Tagging     Name
---- -------- ------------ ---- --- ------------- ----------------
1     No       Yes          1    0   UntagAll      Port 1
2     No       Yes          1    0   UntagAll      Port 2
3     No       Yes          1    0   UntagAll      Port 3
4     No       Yes          1    0   UntagAll      Port 4
5     No       Yes          1    0   UntagAll      Port 5

3526T(config)#vlan ports 1 tagging enable

3526T(config)#show vlan interface info
      Filter     Filter
     Untagged Unregistered
Port  Frames     Frames     PVID PRI    Tagging     Name
---- -------- ------------ ---- --- ------------- ----------------
1     No       Yes          1    0   TagAll        Port 1
2     No       Yes          1    0   UntagAll      Port 2
3     No       Yes          1    0   UntagAll      Port 3
4     No       Yes          1    0   UntagAll      Port 4
5     No       Yes          1    0   UntagAll      Port 5
```

Chapter 10: Troubleshooting hardware

Use this section for hardware troubleshooting.

Work flow Troubleshooting hardware

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

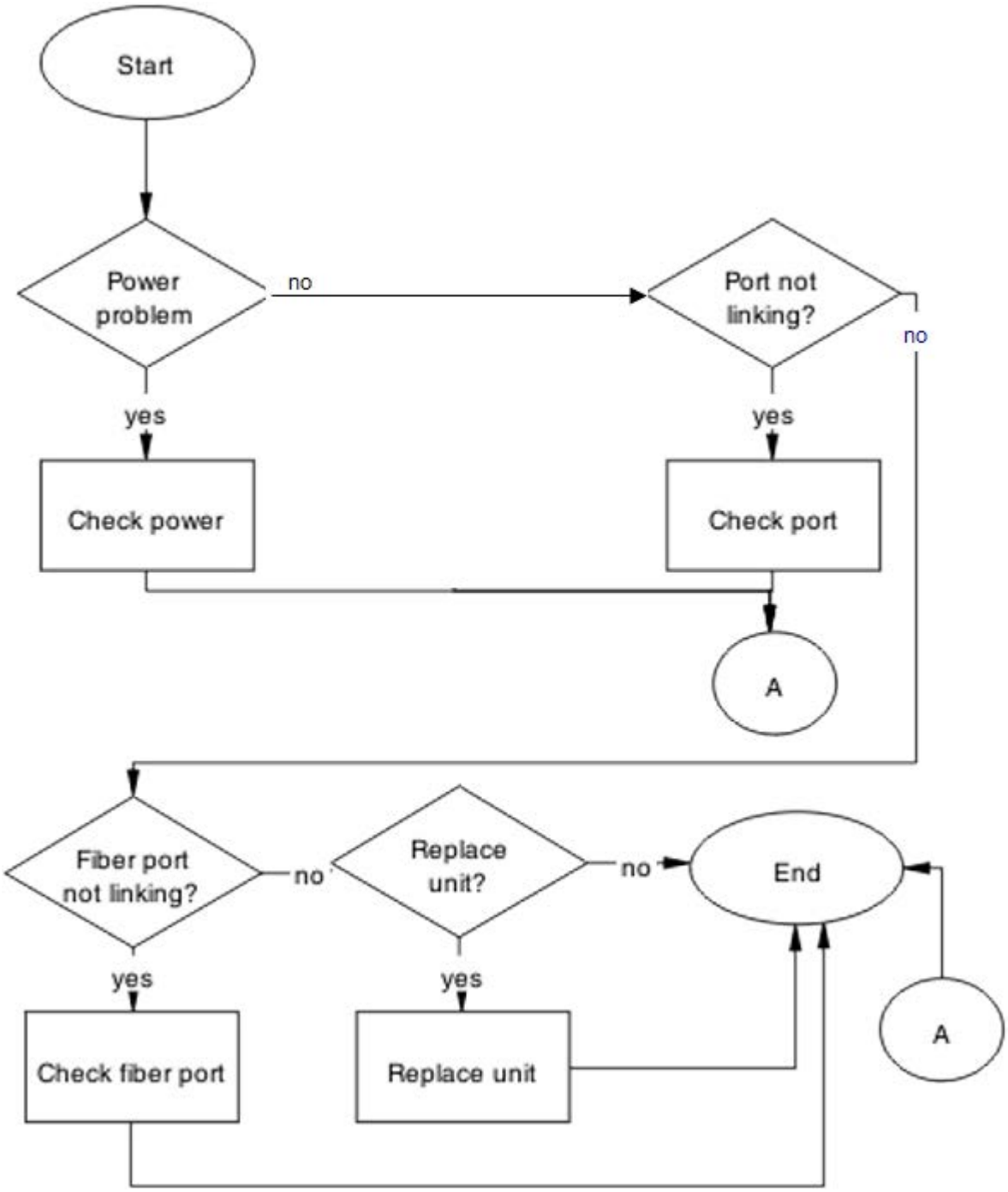


Figure 19: Troubleshooting hardware

Check power

Confirm power is being delivered to the device.

Task flow Check power

The following task flow assists you to confirm that the ERS 3600 Series device is powered correctly.

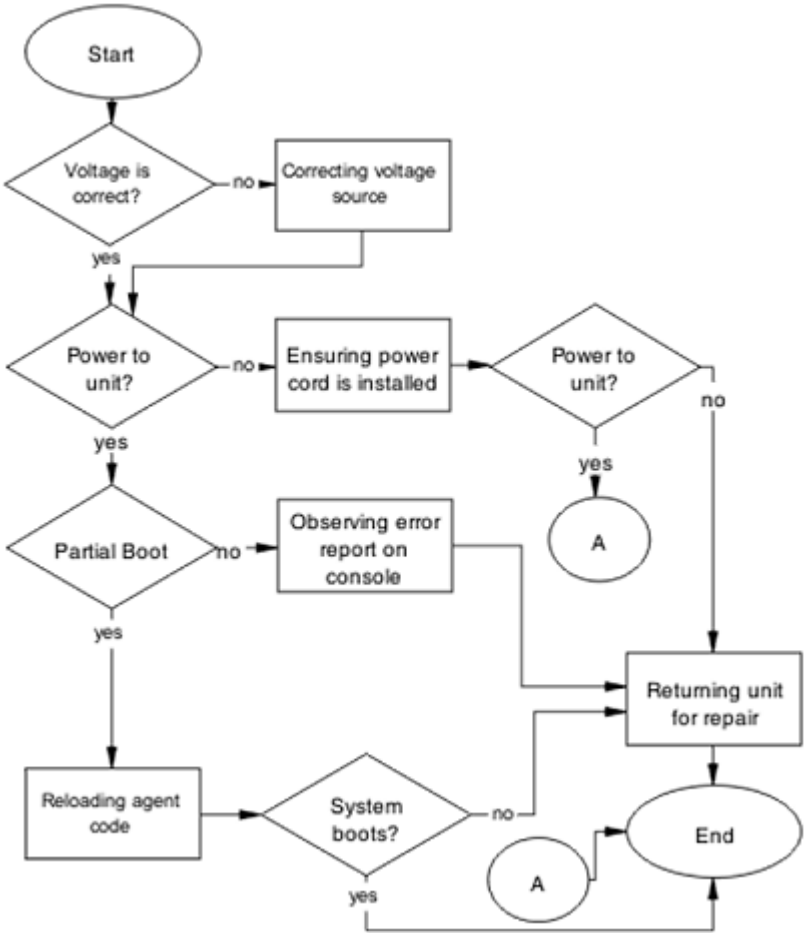


Figure 20: Check power

Correcting voltage source

Confirm the power cord is connected to the appropriate voltage source.

Ensuring power cord is installed

Confirm the power cord is properly installed for the device. All power cords are to be firmly seated.

Observing error report on console

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

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 agent code

Reload the agent code on the ERS 3600 Series device 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 might cause further complications.

1. Use the show sys-info command to view the software version.

   For information about software installation, see .

Returning unit for repair

Return unit to Extreme Networks for repair.

Contact Extreme Networks for return instructions and RMA information.

Check port

Confirm the port and ethernet cable connecting the port are in proper configuration.

Task flow Check port

The following task flow assists you to check the port and ethernet cables:

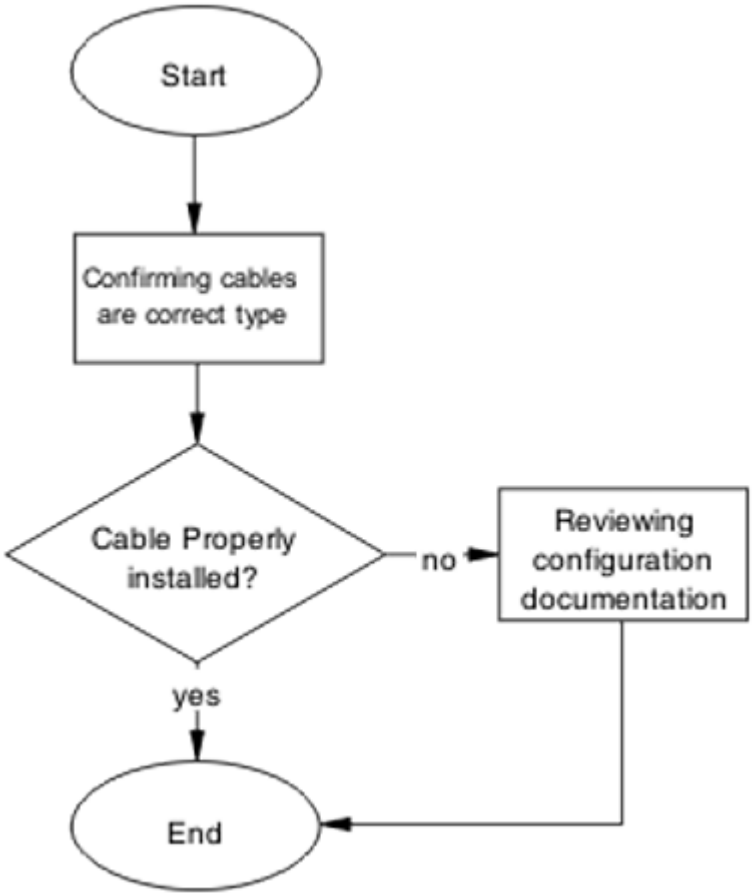


Figure 21: Check port

Viewing port information

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

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

Enabling the port

Enable the port.

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

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

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

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

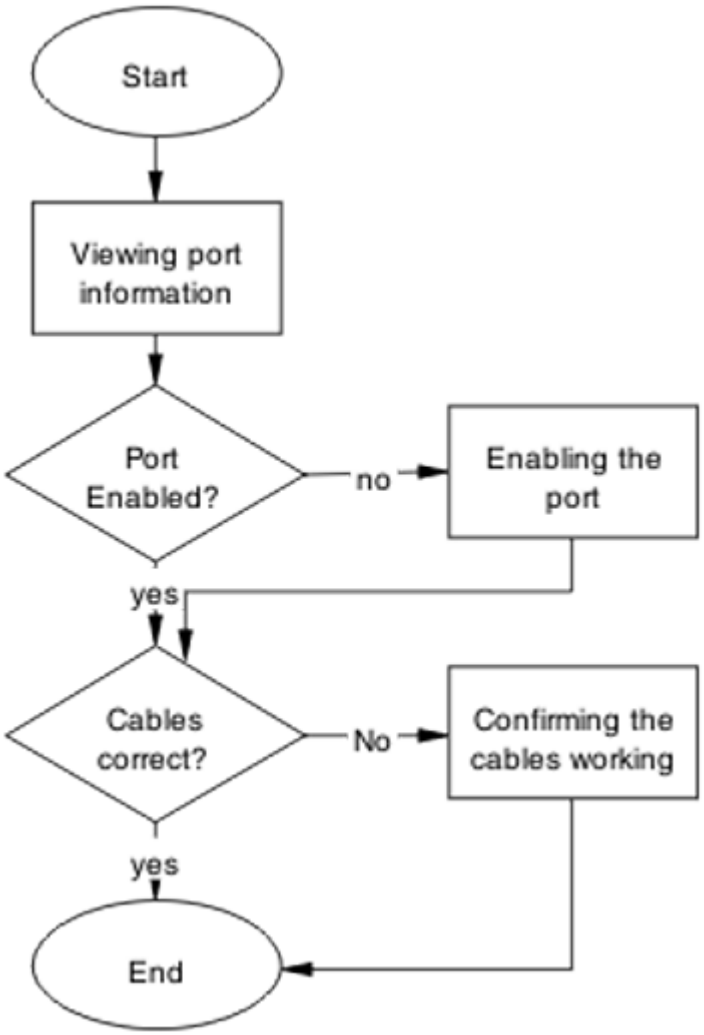


Figure 22: Check fiber port

Viewing fiber port information

Review the port information to ensure the port is enabled.

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

Enabling the port

Ensure the port on the switch device is enabled.

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 cables are working

Confirm that the cables are working on the port.

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.

Returning unit for repair

Return unit to Extreme Networks for repair.

Contact Extreme Networks for return instructions and RMA information.

Replace unit

Remove 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 device.

Verifying software version is correct on new device

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

1. Connect the new device to the console.
2. Use the `show sys-info` command to view the software version.

Powering on the unit

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

Prerequisites

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.

1. Connect the power to the unit.
2. Allow time 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 unit for repair

Return unit to Extreme Networks for repair.

Contact Extreme Networks for return instructions and RMA information.

Chapter 11: 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**. When ADAC is enabled, all VLAN settings that you manually made on ADAC uplink or telephony ports are dynamic and are not saved to non-volatile memory. When the unit is reset, these settings are lost. ADAC detects the ports again and re-applies the default settings for them.

You do not manually create a VLAN to be used as the voice VLAN and then try to set this VLAN as the ADAC voice VLAN using the command `adac voice-vlan x`. ADAC automatically creates the voice VLAN when needed. You only have to reserve or set the VLAN number used by ADAC with the `adac voice-vlan x` command.

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 does not detect phones.

Work flow Troubleshooting ADAC

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

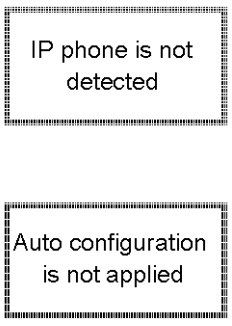


Figure 23: Troubleshooting ADAC

IP phone is not detected

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

Work flow IP phone not detected

The following work flow assists you to resolve detection issues.

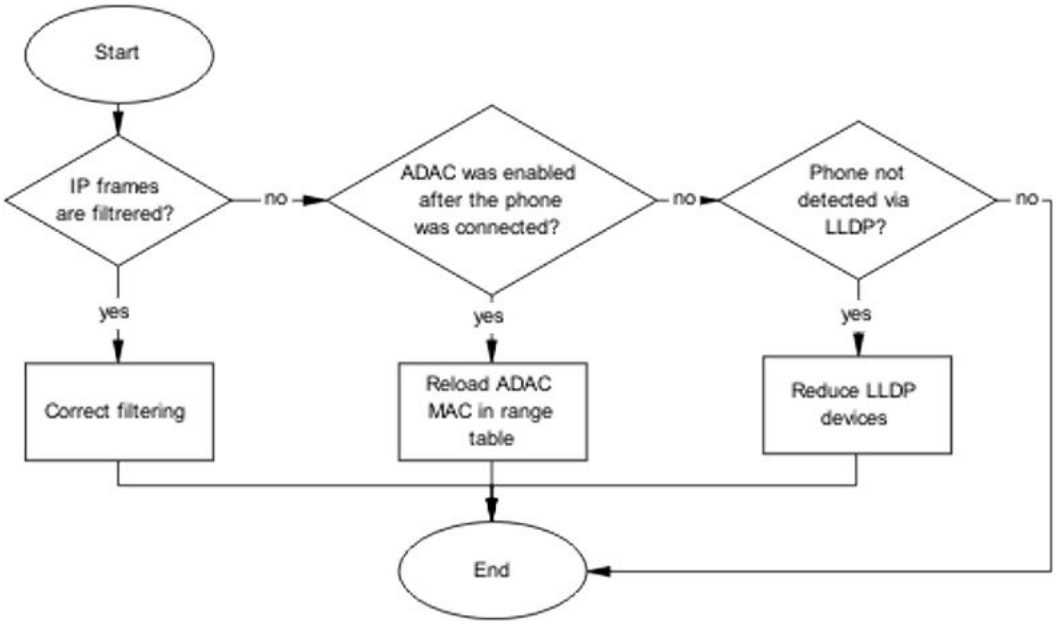


Figure 24: IP phone not detected

Correct filtering

Configure the VLAN filtering to allow ADAC.

Task flow Correct filtering

The following task flow assists you to correct the filtering.

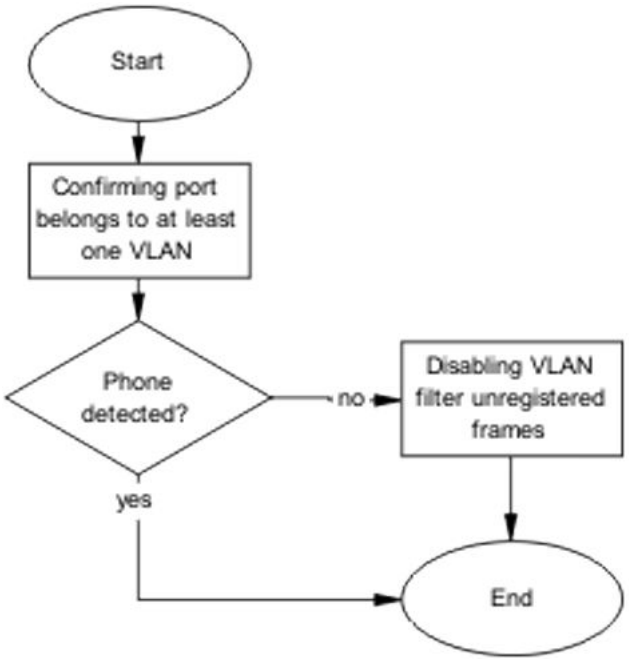


Figure 25: Correct filtering

Confirming port belongs to at least one VLAN

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

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

Change the unregistered frames filtering of the VLAN.

1. Use the `vlan ports <port> filter-unregistered-frames enable` 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

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

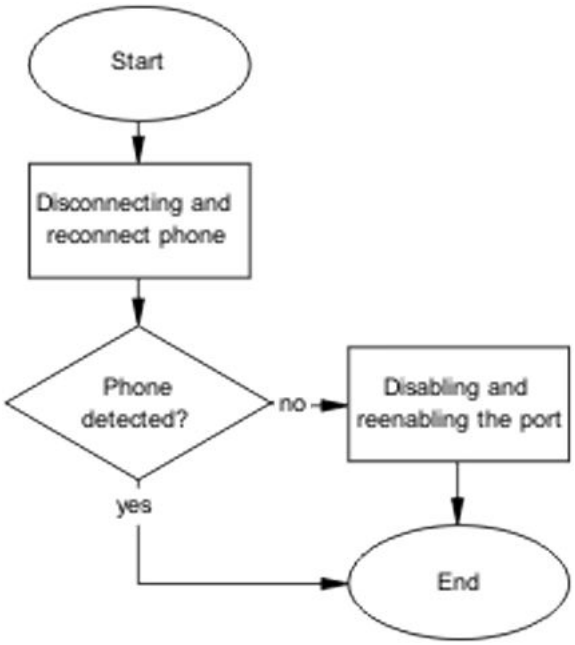


Figure 26: Reload ADAC MAC in range table

Disconnecting and reconnecting phone

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

1. Follow local procedures to disconnect the phone.
2. Follow local procedures to reconnect the phone.

Disabling and enabling the port

Disable ADAC on the port and then enable it to detect the phone. When disable and reenable the port administratively, the MAC addresses already learned on the respective port are aged out.

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

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

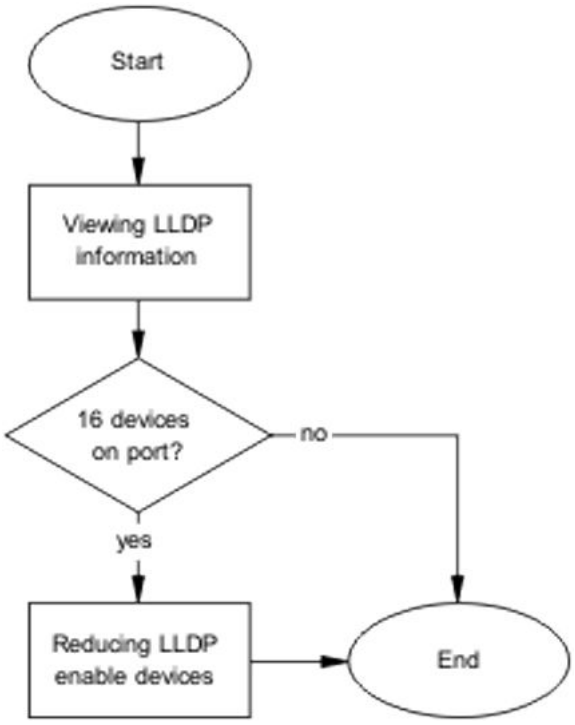


Figure 27: Reduce LLDP devices

Viewing LLDP information

Display the LLDP devices that are connected to a port.

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

Reduce the number of LLDP devices on the system.

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

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

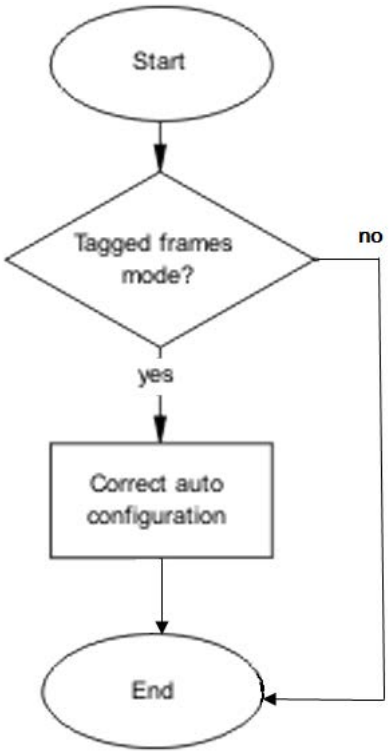


Figure 28: Auto configuration is not applied

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

The following task flow assists you to correct auto configuration.

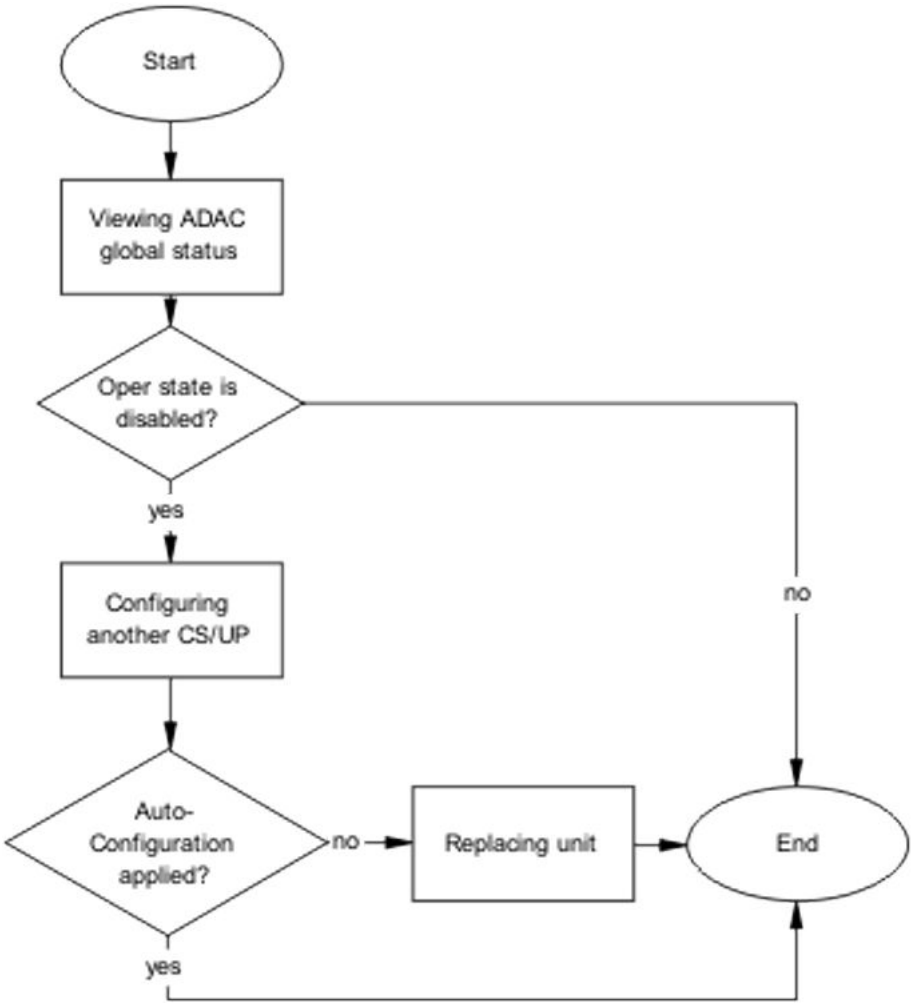


Figure 29: Correct auto configuration

Viewing ADAC global status

Display the global status of ADAC.

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

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

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.

Chapter 12: Troubleshooting authentication

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

Work flow Troubleshooting authentication

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

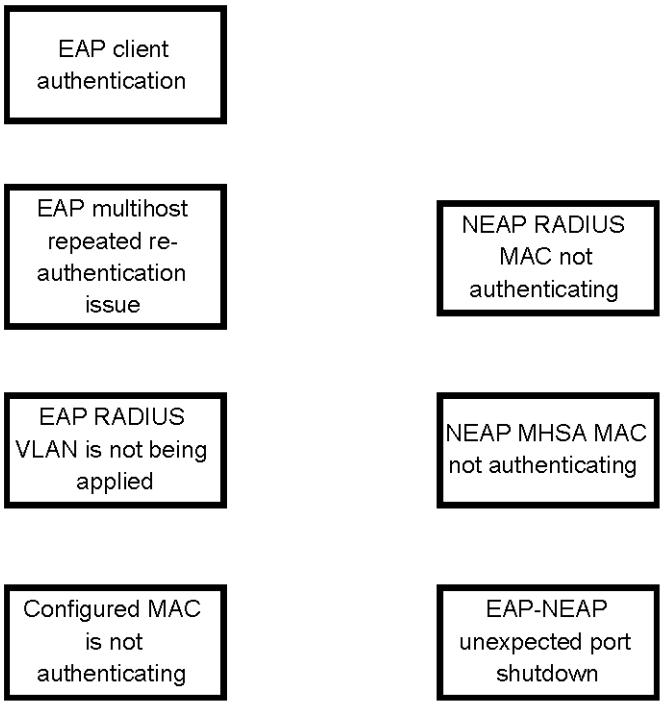


Figure 30: Troubleshooting authentication

EAP client authentication

This section provides troubleshooting guidelines for the EAP and non-EAP features.

Work flow EAP client is not authenticating

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

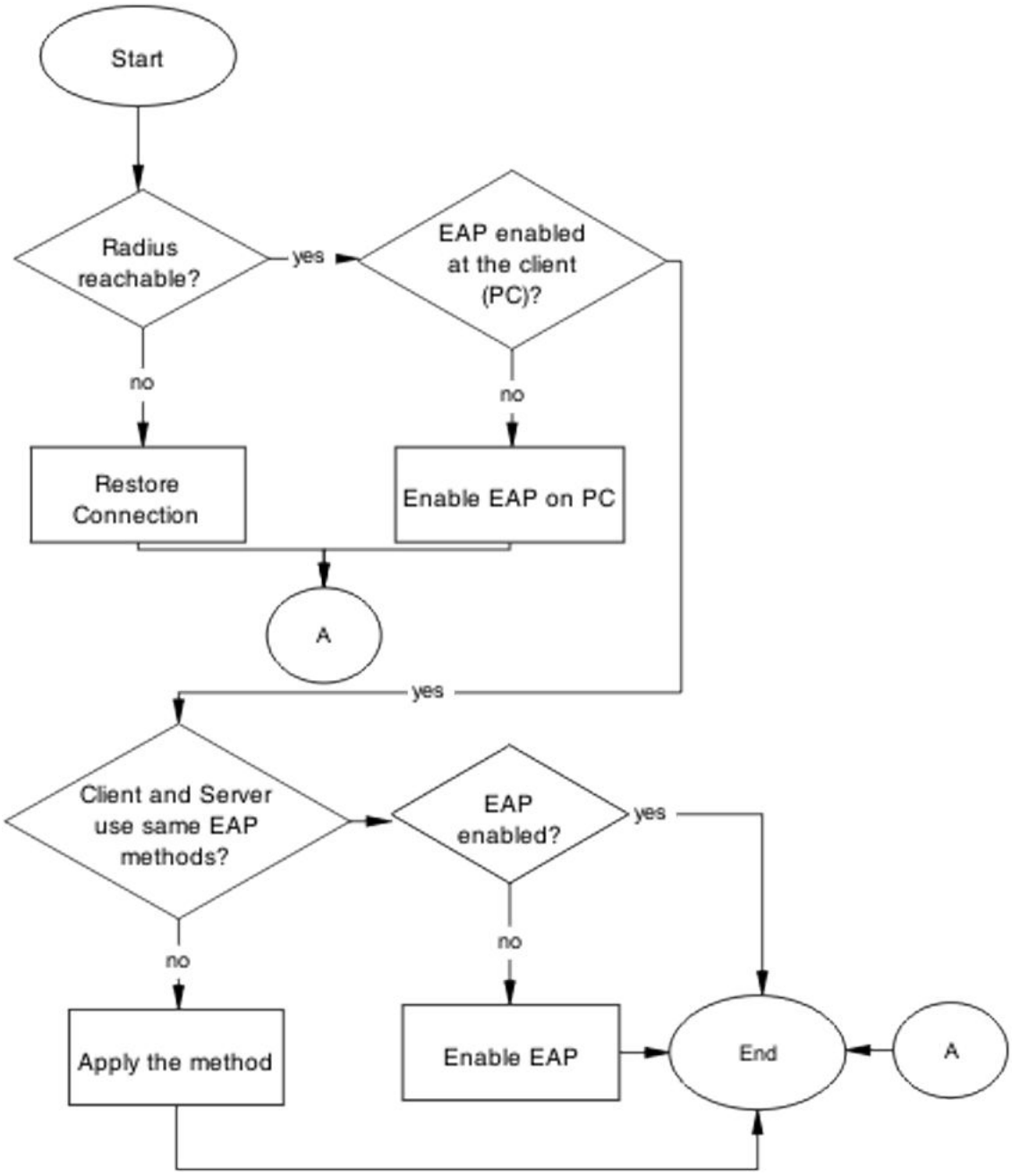


Figure 31: EAP client is not authenticating

Restore RADIUS connection

Ensure that the RADIUS server has connectivity to the device.

Task flow Restore RADIUS connection

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

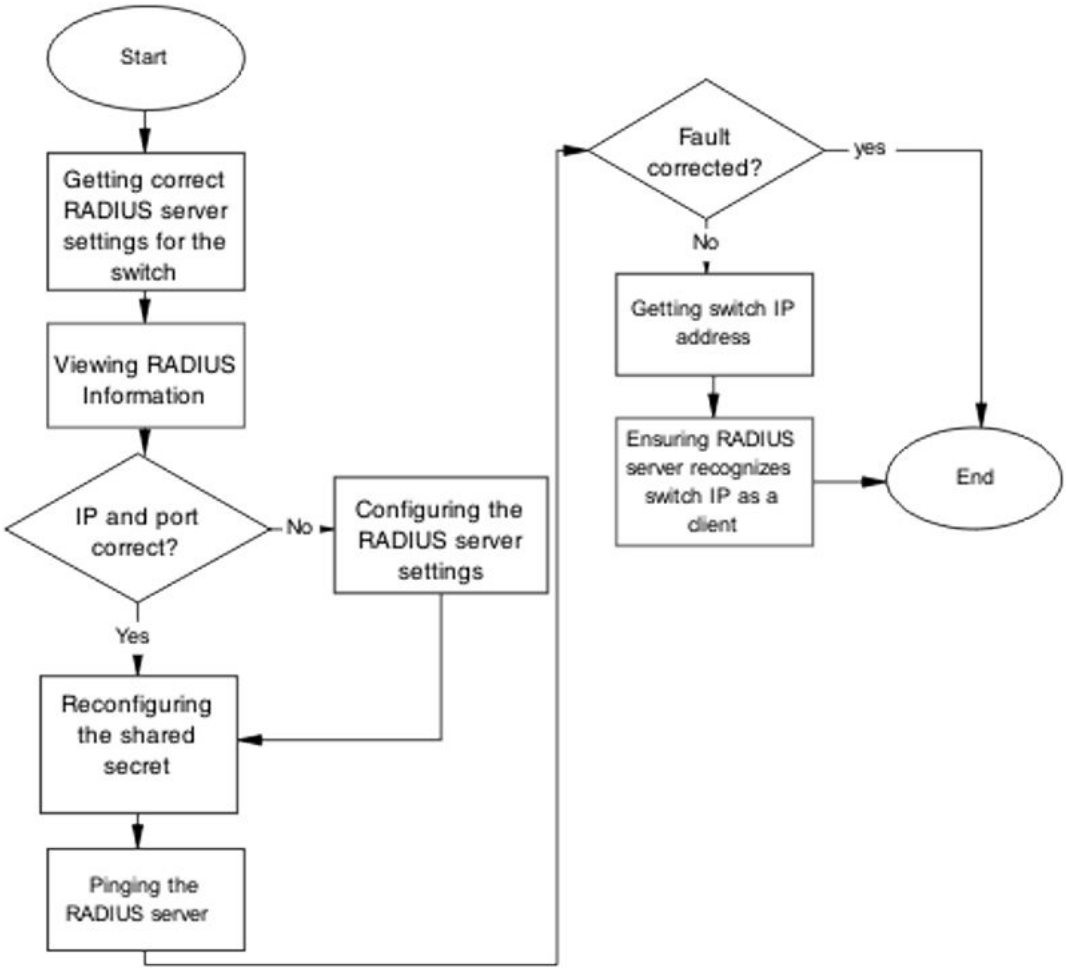


Figure 32: Restore RADIUS connection

Getting correct RADIUS server settings for the switch

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

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

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.

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

The RADIUS server settings must be correct for the network.

Follow vendor documentation to set the RADIUS server settings.

Reconfiguring the shared secret

Reset the shared secret in case there was any corruption.

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

Pinging the RADIUS server

Ping the RADIUS server to ensure connection exists.

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

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

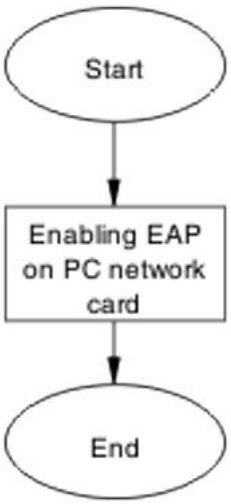


Figure 33: Enable EAP on the PC

Enabling EAP on PC network card

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

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

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

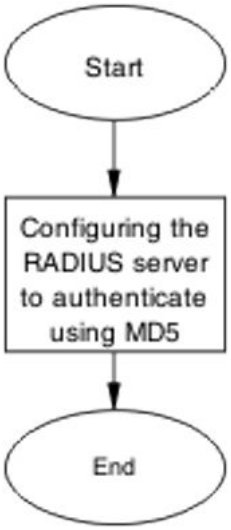


Figure 34: Apply the method

Configuring the RADIUS server

Configure the RADIUS server to authenticate using MD5.

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

Enable EAP globally

Task flow Enable EAP globally

The following task flow assists you to enable EAP globally.

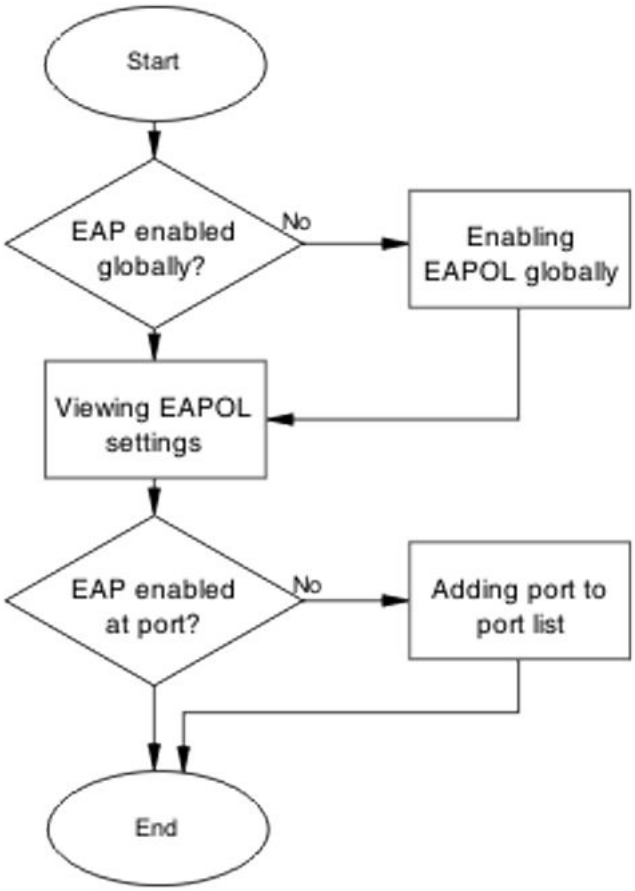


Figure 35: Enable EAP globally

Enabling EAP globally

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

Viewing EAPOL settings

Review the EAPOL settings to ensure EAP is enabled.

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

Setting EAPOL port administrative status to auto

Set the EAPOL port administrative status to auto.

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.

EAP multihost repeated re-authentication issue

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

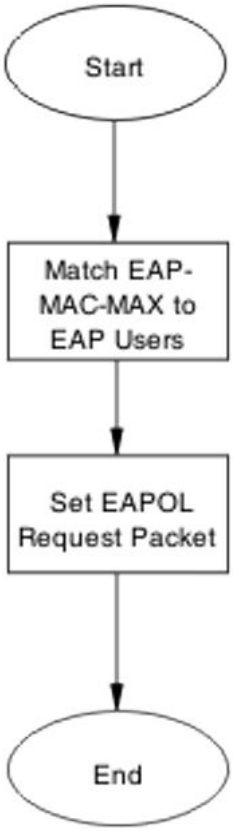


Figure 36: EAP multihost repeated re-authentication issue

Match EAP-MAC-MAX to EAP users

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

Identifying number of users at allowed max

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

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

Task flow Match EAP-MAC-MAX to EAP users

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

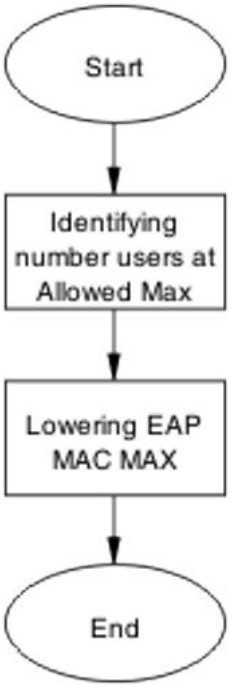


Figure 37: Match EAP-MAC-MAX to EAP users

Lowering EAP max MAC

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

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

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

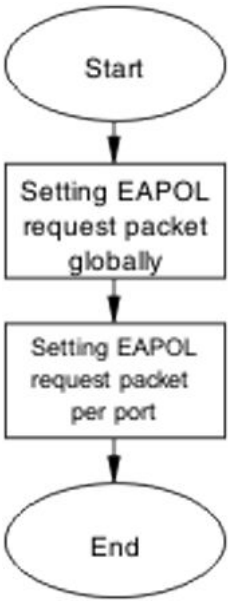


Figure 38: Set EAPOL request packet

Setting EAPOL request packet globally

Globally change the EAPOL request packet from multicast to unicast.

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

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

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

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

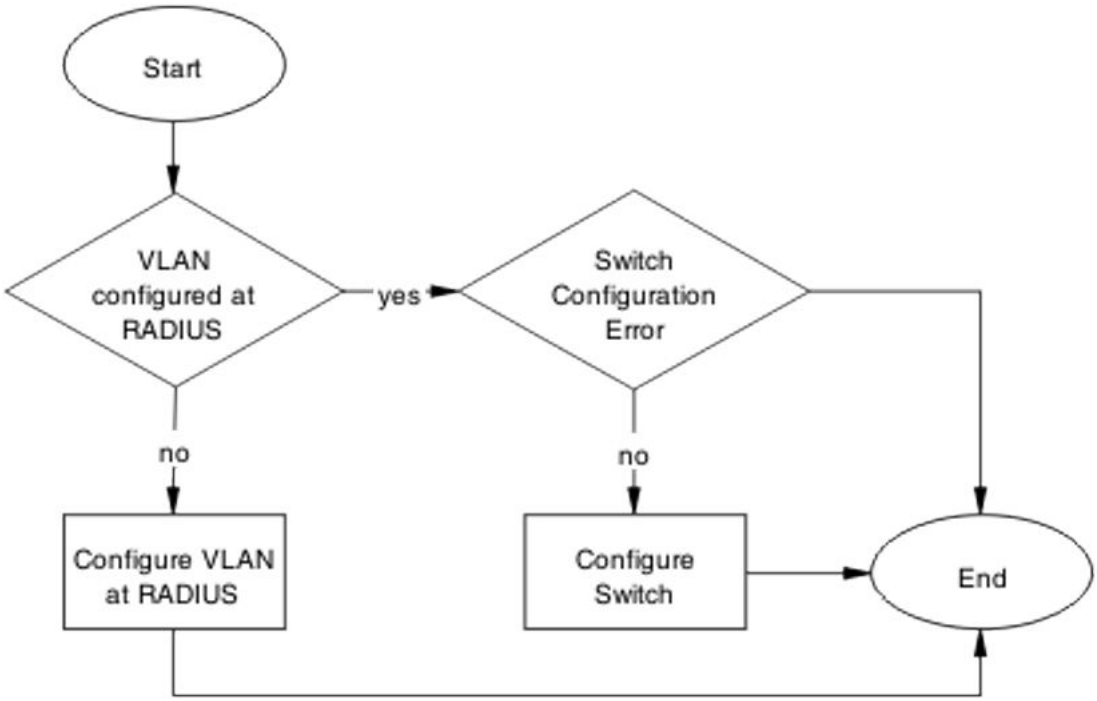


Figure 39: EAP RADIUS VLAN is not being applied

Configure VLAN at RADIUS

Correct any discrepancies in VLAN information at the RADIUS server.

Task flow Configure VLAN at RADIUS

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

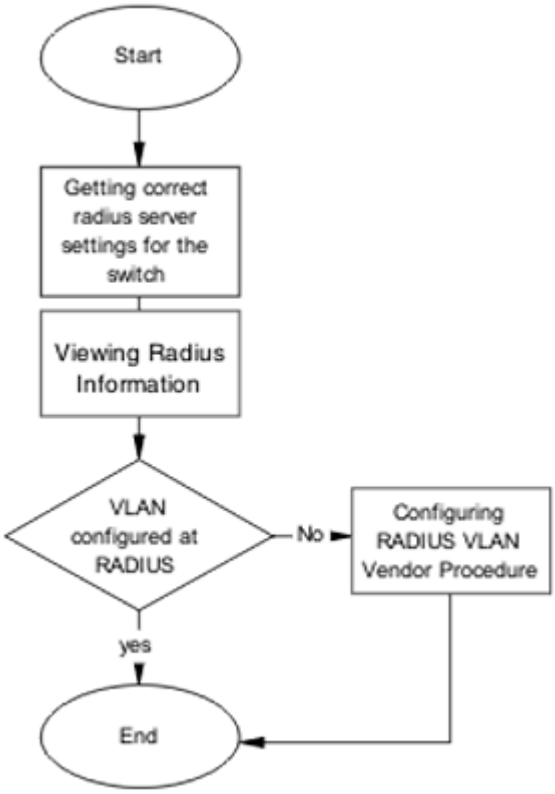


Figure 40: Configure VLAN at RADIUS

Getting correct RADIUS server settings

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

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

Viewing RADIUS information

Obtain the radius information to identify its settings.

Use vendor documentation to obtain settings display.

Configuring RADIUS

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 RADIUSassigned 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 switch

The VLAN must be configured correctly on the switch.

Task flow Configure switch

The following task flow assists you to configure the VLAN on the device.

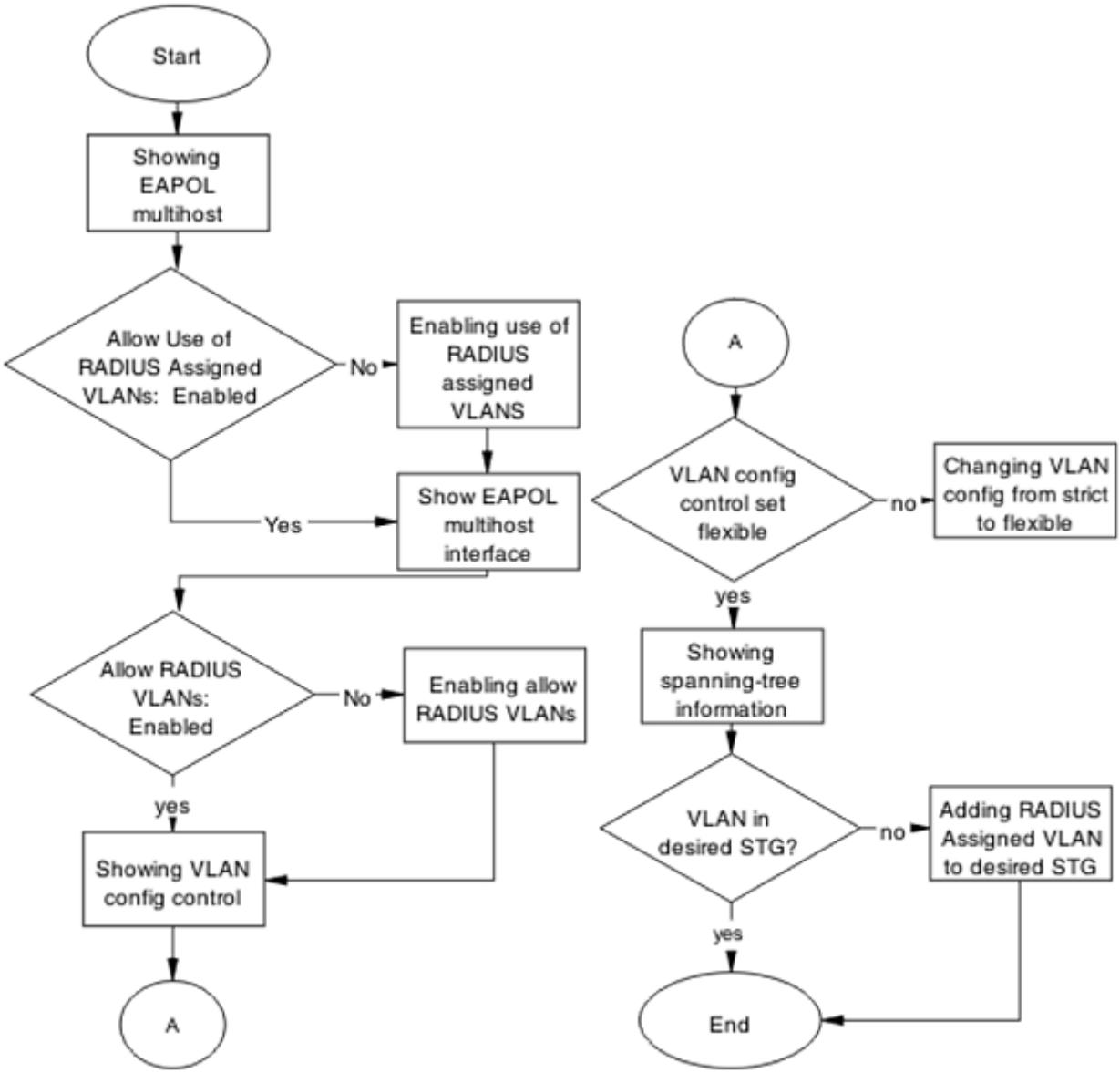


Figure 41: Configure switch task

Showing EAPOL multihost

Identify the EAPOL multihost information.

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

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

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

Display the EAPOL interface information.

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

Display the VLAN config control information.

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

Changing VLAN config from strict to flexible

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

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.

Configured MAC is not authenticating

Correct a MAC to allow authentication.

Work flow Configured MAC is not authenticating

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

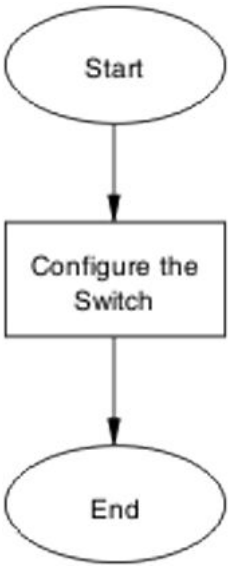


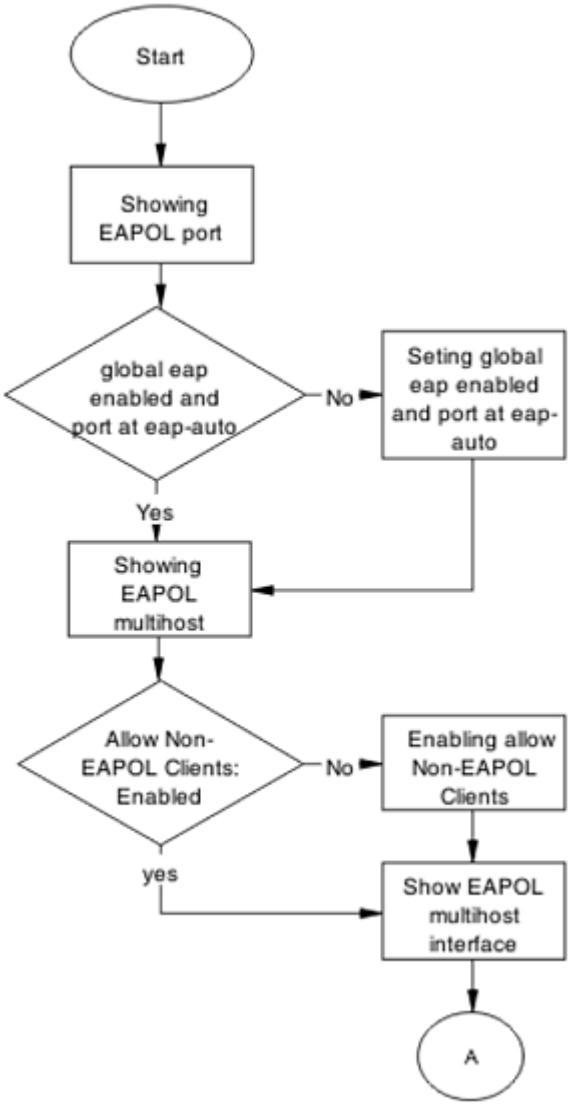
Figure 42: Configured MAC is not authenticating

Configure the switch

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

Task flow Configure the switch

The following task flow assists you to ensure the MAC is authenticating on the switch.


Start
Showing EAPOL port
global eap enabled and port at eap-auto
No
Seting global eap enabled and port at eap-auto
Yes
Showing EAPOL multihost
Allow Non-EAPOL Clients: Enabled
No
Enabling allow Non-EAPOL Clients
yes
Show EAPOL multihost interface
A

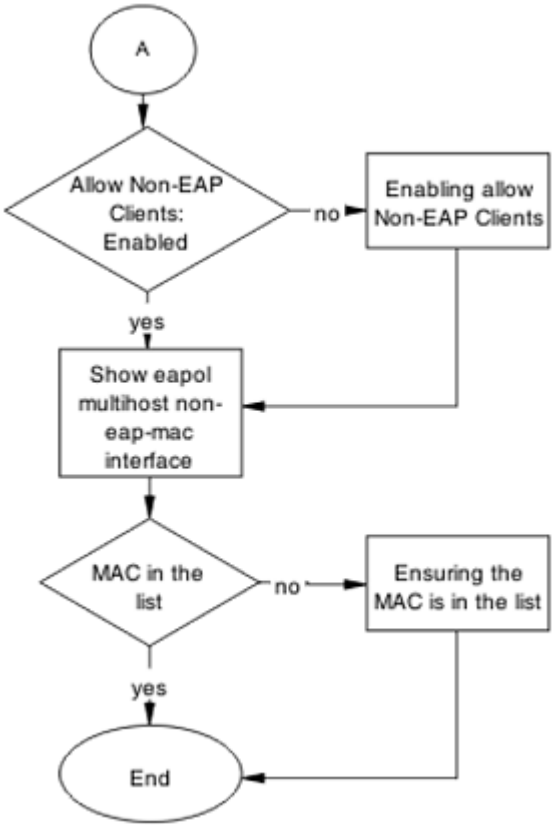


Figure 43: Configure the switch

Showing EAPOL port

Display the EAPOL port information

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

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

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

Display the EAPOL multihost information.

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

Correct the non-EAPOL client attribute.

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

Display the EAPOL multihost interface information.

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.

Enabling multihost status and allow non-EAPOL clients

Correct the non-EAP client attribute.

1. Use the `eapol multihost allow-non-eap-enable` command to allow non- EAPOL clients.
2. Use the `eapol multihost enable` command to enable multihost status.

Showing EAPOL multihost non-eap-mac interface

Display the EAPOL multihost interface information.

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 in the list

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

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

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

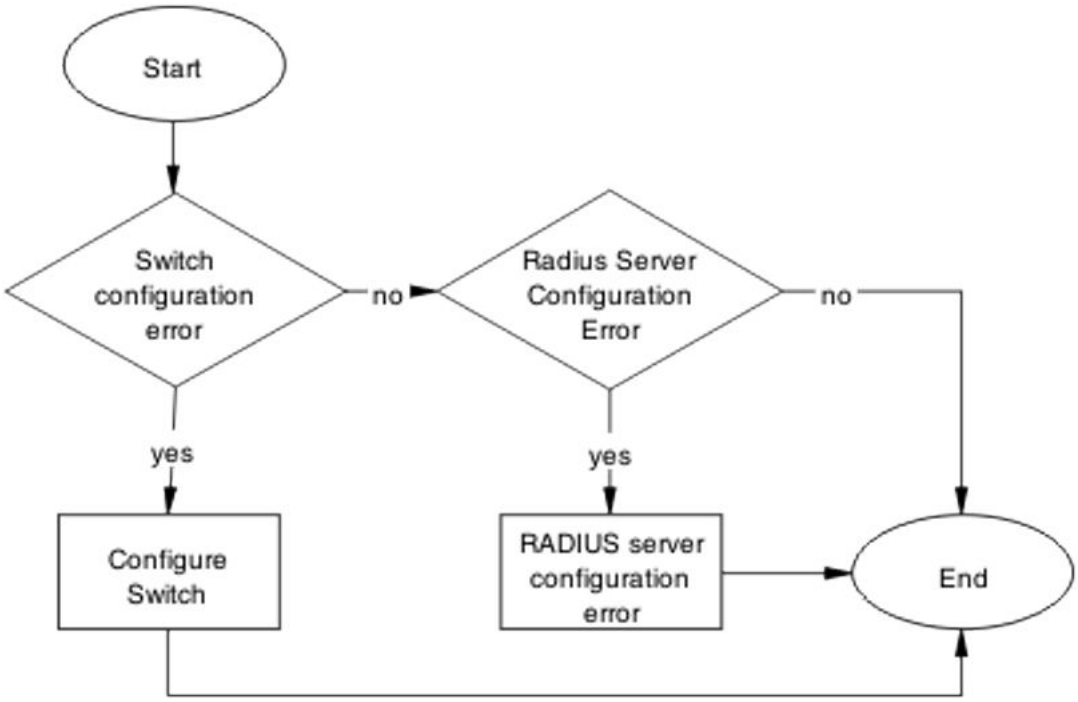


Figure 44: Non-EAP RADIUS MAC not authenticating

Configure switch

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

Task flow Configure switch

The following task flow assists you to configure the switch to correct the RADIUS MAC issue.

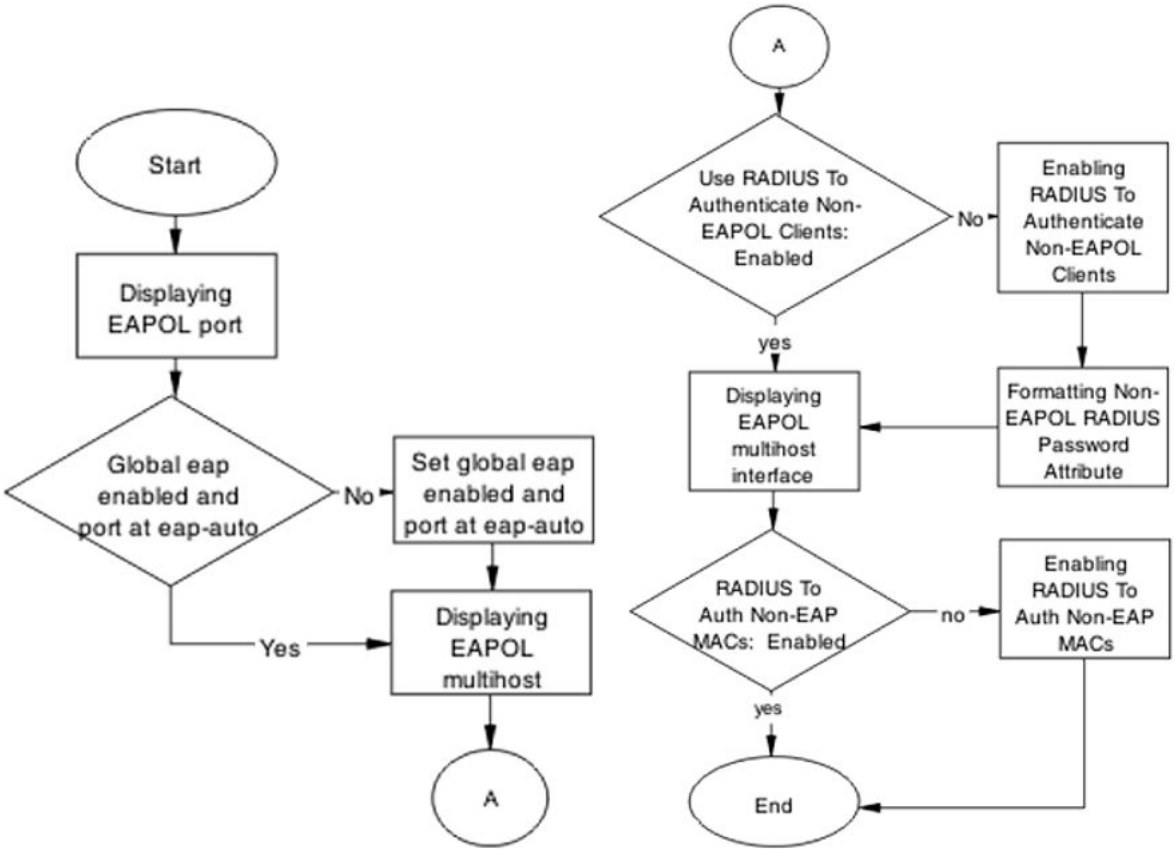


Figure 45: Configure switch

Displaying EAPOL port

Review the EAPOL port information.

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

Setting global EAP enabled and port at eap-auto

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

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

Review the EAPOL multihost information.

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

- Non-EAPOL RADIUS Password Attribute Format:

  `MACAddr`

Enabling RADIUS to authenticate non-EAPOL clients

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

Apply changes to the RADIUS server using vendor documentation.

Formatting non-EAPOL RADIUS password attribute

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

RADIUS server is to have the format changed to `MACAddr`.

Displaying EAPOL multihost interface

Review the EAPOL multihost information.

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

Make the required changes on the RADIUS server to authenticate non-EAP clients. Apply changes to RADIUS server using vendor documentation.

RADIUS server configuration error

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

Task flow RADIUS server configuration error

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

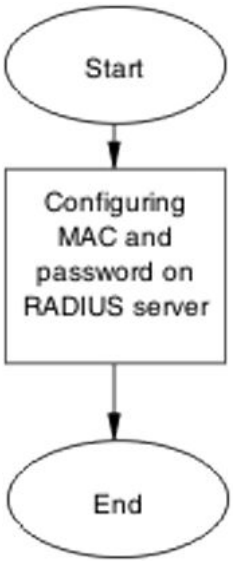


Figure 46: RADIUS server configuration error

Configuring MAC and password on RADIUS server

The RADIUS server requires that the MAC address and password for the switch is correct. If it is incorrect, the switch might 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

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

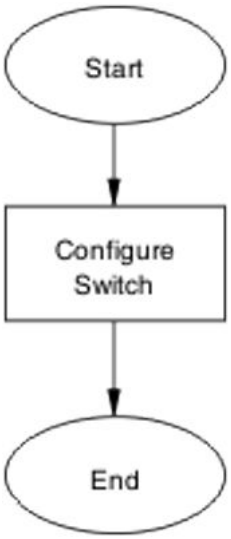


Figure 47: Non-EAP MHSA MAC is not authenticating

Configure switch

Configure the switch to enable MHSA.

Task flow Configure switch

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

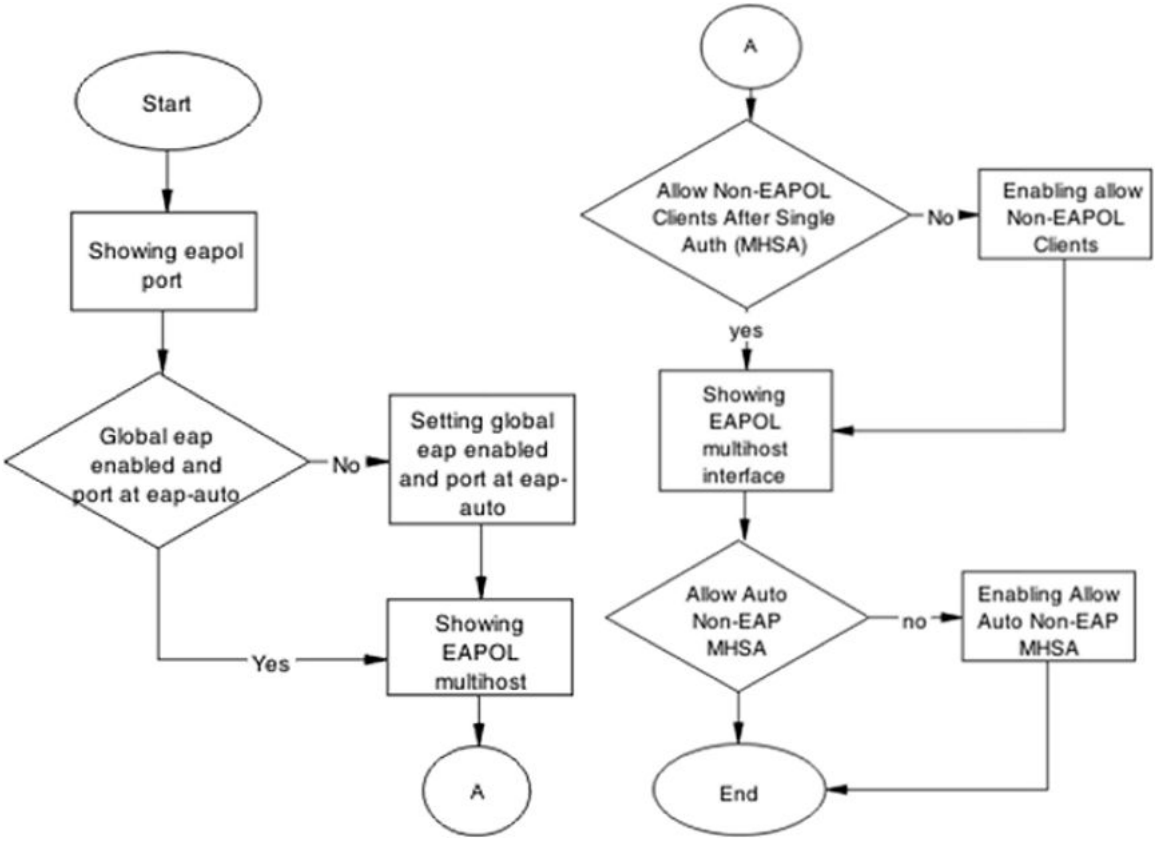


Figure 48: Configure switch

Showing EAPOL port

Review the EAPOL port information.

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.

Showing EAPOL multihost

Review the EAPOL multihost information.

1. Enter the `show eapol port multihost` command to display the information.
2. Note the following:

   Use RADIUS To Authenticate NonEAPOL Clients is enabled

Formatting non-EAPOL RADIUS password attribute

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 `MACAddr`.

Enabling RADIUS to authenticate non-EAPOL clients

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

Apply changes to RADIUS server using vendor documentation.

Showing EAPOL multihost interface

Review the EAPOL multihost information.

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

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

Apply changes to 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

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

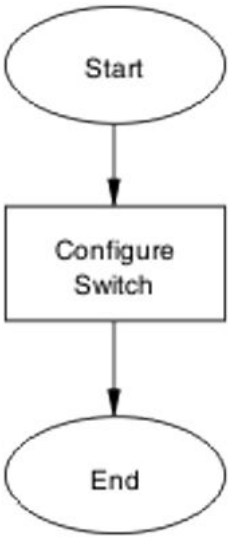


Figure 49: EAP — non-EAP unexpected port shutdown

Configure switch

Configure ports to allow more unauthorized clients.

Task flow Configure switch

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

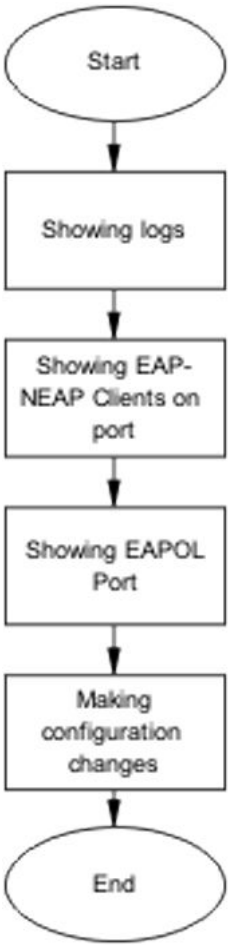


Figure 50: Configure switch

Showing Logs

Display log information to provide additional information.

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

Showing EAP–non-EAP clients on port

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

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

Showing EAPOL port information

Display EAPOL port information for additional information.

1. Use the `show eapol port <port#>` command to display the port information.

2. Observe the log output and note any anomalies.

Making changes

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

1. Use the `eapol status auto`command to change to eap-auto.
2. In the Interface Configuration Mode, use the `shut/no shut` commands.

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.