Troubleshooting Avaya Ethernet Routing Switch 2500 Series

4.1
NN47215-700, 01.02
November 2010

Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer

Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of this documentation unless such modifications, additions, or deletions were performed by Avaya. End User agree to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked Web sites referenced within this site or documentation(s) provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Avaya provides a limited warranty on this product. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language, as well as information regarding support for this product, while under warranty, is available to Avaya customers and other parties through the Avaya Support Web site: http://www.avaya.com/support. Please note that if you acquired the product from an authorized Avaya reseller outside of the United States and Canada, the warranty is provided to you by said Avaya reseller and not by Avaya.

Licenses

Copyright

Third-party components

Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements (“Third Party Components”), which may contain terms that expand or limit rights to use certain portions of the Product (“Third Party Terms”). Information regarding distributed Linux OS source code (for those Products that have distributed the Linux OS source code), and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply to them is available on the Avaya Support Web site: http://www.avaya.com/support/Copyright/.

Trademarks

The trademarks, logos and service marks (“Marks”) displayed in this site, the documentation(s) and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the documentation(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya Inc.

All other trademarks are the property of their respective owners.

Downloading documents

For the most current versions of documentation, see the Avaya Support Web site: http://www.avaya.com/support

Contact Avaya Support

Avaya provides a telephone number for you to use to report problems or to ask questions about your product. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Web site: http://www.avaya.com/support

Contents

Chapter 1: New in this release

The following sections detail what's new in *Avaya Ethernet Routing Switch 2500 Series Troubleshooting, NN47215-700* for Release 4.3.

Stacking

The ERS 2500 Series software release v4.3 has the capability to stack up to eight units in a stack. Stacking functionality is available through two methods. First, by purchasing a stack enabled device. These devices have the rear ports set to stacking mode as default in the factory. These devices do not use or require a license for the feature. Second, a standalone unit can have the stacking feature enabled through the use of a Stacking License Kit that includes a license certificate and a License Authorization code (LAC) for use on the Avaya Licensing Portal. It is important to note that stack enabled switches can be stacked regardless of the method the stacking was enabled on them.

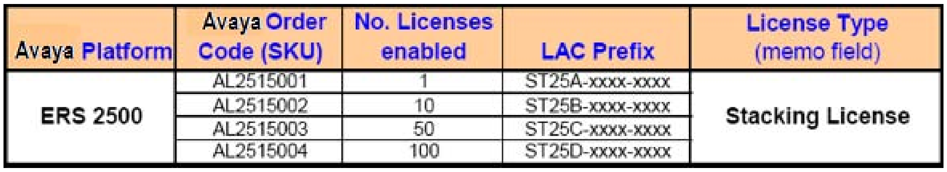
The stack enabled units are identifiable through CLI or JDM.

Stacking licensing

There are four variants of Stacking License Kits that are available for standalone switches. Each kit contains a license certificate and LAC. The license file management and generation is through the Avaya Licensing Portal. The license file is generated, downloaded and installed on each standalone ERS 2500 Series device that requires stacking functionality. The instructions are located on the license certificate.

The license file unlocks stacking functionality and allows the ports on the rear of the switch to be set to **Stacking Mode**. License files can be added and removed from the switch. Should you set a non stack enabled device to default, the license file is removed. There are two cases that may be encountered. First, when the stack is reset to default (#boot default) the switches continues to function in stack indefinitely. Second, when the licenses are removed (#clear license) the stack continues to work until the second reset.

Stack License Kits are available for 1, 10, 50, or 100 devices. The ERS 2500 Series licensing has a more intuitive LAC schema. The memo field in the license is also populated as part of the license file generation on the licensing portal.



Avaya Platform	Avaya Order Code (SKU)	No. Licenses enabled	LAC Prefix	License Type (memo field)
ERS 2500	AL2515001	1	ST25A-xxxx-xxxx	Stacking License
	AL2515002	10	ST25B-xxxx-xxxx	
	AL2515003	50	ST25C-xxxx-xxxx	
	AL2515004	100	ST25D-xxxx-xxxx	

Figure 1: License Schema

Stacking functionality and rear ports

Stacking mode must be configured on the rear ports before the switches are connected together. There is no auto-detection for the stacking function. The base unit must have the unit select switch set to on.

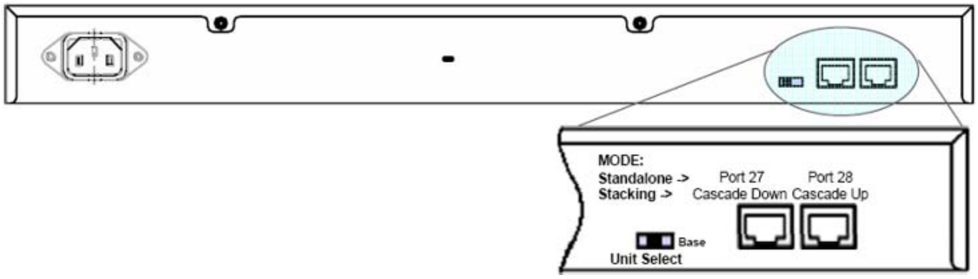


Figure 2: ERS 2500 rear ports

Each ERS 2500 Series device ships with a 46 cm (1.5 ft) stacking cable. The stacking cable is a black Cat5E cable. Spare stacking cables are available on the price list for additional purchase. Also available for purchase are additional cables of 1.5 m (5 ft) and 3 m (10 ft) and are similar to stack return cables,

You are permitted to use your own cables and longer lengths up to 100m. This is at your own risk and is not officially supported by GNTS.

Stack Licensing – rear port mode

The rear ports on the ERS 2500 series are configurable via ACLI and JDM in ‘config’ mode.

In ACLI, under PrivExec mode, you can use the following commands:

- `default rear-ports mode [unit <1-8>] {standalone | stacking}` to set the operating mode. The default is standalone.
- `show rear-ports mode` displays the operating mode of the rear ports.

Under JDM, the rear ports are be grayed out and not selectable in the switch view if the ports are in stacking mode.

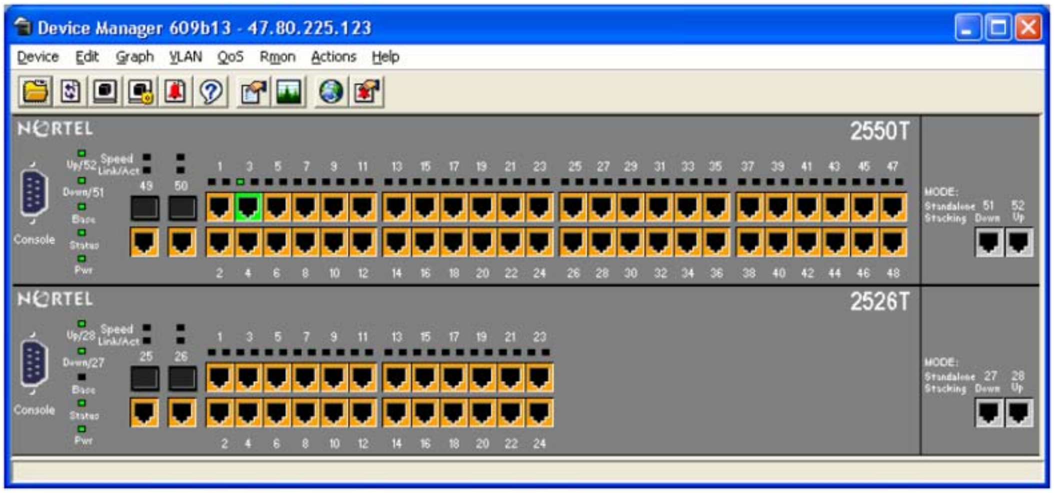


Figure 3: ERS 2500 JDM display

Power over Ethernet (POE) limitations

The status for the PoE port can appear incorrectly as InvalidPD rather than detecting. This occurs if the PD detect type on an ERS 2500-PWR is set to 802.3af and legacy while a PoE port on the switch is connected to a non-PoE device.

Be aware that this is a hardware limitation that is caused by the capacitive detection method used in the legacy mode (versus resistive/current based detection used in 802.3af compliant mode). Some devices are always errantly detected because they match the capacitive signature, dependent on the environment, cabling, etc.

Chapter 2: Introduction

Use this document to help you troubleshoot the Avaya Ethernet Routing Switch 2500 Series.

This document:

- Describes the diagnostic tools and utilities available for troubleshooting the Avaya Ethernet Routing Switch 2500 Series products using Avaya Command Line Interface (ACLI) and Device Manager (DM).
- 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 Avaya 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 Ethernet Routing Switch 2500 Series products support 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 Ethernet Routing Switch 2500 Series network topologies. Other tools are more general in their application and can be used to diagnose and monitor ingress and egress traffic.

Chapter 3: Troubleshooting planning

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

First, use the *Avaya Ethernet Routing Switch 2500 Series Documentation Roadmap* to familiarize yourself with the documentation set, so you know where to get information when 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 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.

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 fundamentals

This section describes available troubleshooting tools and their applications.

Port mirroring

Avaya Ethernet Routing Switch 2500 Series switches have a port mirroring feature that helps you to monitor and analyze network traffic. The port mirroring 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 Ethernet Routing Switch 2500 Series 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.

There are also limitations to the ingress and egress mode. First, the same limitation on the XTX portion also applies to the ingress and egress mode. Second, Avaya recommends that the monitor port and the mirror port be on the same unit in a stack.

Port mirroring commands

See *Avaya Ethernet Routing Switch 2500 Series Configuration — System Monitoring* (NN47215-502) for port mirroring command information.

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

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 *Avaya Ethernet Routing Switch 2500 Series Configuration — System Monitoring* (NN47215-502).

System logs

You can use the syslog messaging feature of the Ethernet Routing Switch 2500 Series products to manage event messages. The syslog software on the 2500 Series switch 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 an Ethernet Routing Switch 2500 Series device running in a network accessible to the workstation.

For more information about system logging, see *Avaya Ethernet Routing Switch 2500 Series Configuration — System Monitoring* (NN47215-502).

Auto Unit Replacement (AUR)

Enable 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.

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

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 is not replicated in the new unit.

AUR can be enabled or disabled from ACLI and DM. By default, AUR is enabled.

For more information about AUR, see *Avaya Ethernet Routing Switch 2500 Series Configuration — System* (NN47215-500).

Avaya knowledge and solution engine

The Knowledge and Solution Engine is a database of Avaya technical documents, troubleshooting solutions, software patches and releases, service cases, and technical bulletins. The Knowledge and Solution Engine is searchable by natural-language query.

Chapter 5: General diagnostic tools

The Avaya Ethernet Routing Switch 2500 Series device has diagnostic features available through DM and ACLI. 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 ACLI 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.

ACLI command modes

ACLI command modes provide different levels of authority for operation.

The ACLI has four major command modes, listed in order of increasing privileges:

- User EXEC
- Privileged EXEC
- Global configuration
- Interface configuration

Each mode provides a specific set of commands. The command set of a higher-privilege mode is a superset of a lower-privilege mode. That is, all lower-privilege mode commands are accessible when using a higher-privilege mode.

The command modes are as follows:

- `User EXEC mode:`

  The User EXEC mode (also referred to as exec mode) is the default ACLI command mode. User EXEC is the initial mode of access when the switch is first turned on and provides a limited subset of ACLI commands. This mode is the most restrictive ACLI mode and has few commands available.

- `Privileged EXEC mode:`

  The Privileged EXEC mode (also referred to as privExec mode) enables you to perform basic switch-level management tasks, such as downloading software images, setting passwords, and booting the switch. PrivExec is an unrestricted mode that allows you to view all settings on the switch, and if you are logged in with write access, you have access to all configuration modes and commands that affect operation of the switch (such as downloading images, rebooting, and so on).

- **`Global configuration mode:`** In the Global Configuration mode (also referred to as config mode), you can set and display general configurations for the switch such as IP address, SNMP parameters, Telnet access, and VLANs.
- **`Interface configuration mode:`**

  In the Interface Configuration mode (also referred to as config-if mode), you can configure parameters for each port or VLAN, such as speed, duplex mode, and rate-limiting.

It is possible to move between command modes on a limited basis. This is explained in the Common Procedures section of this document.

You can move between command modes on a limited basis. For more information about the ACLI command modes, see *Avaya Ethernet Routing Switch 2500 Series Fundamentals, NN47215-102*.

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 any failures before moving up to the network and application layers.

As part of your initial troubleshooting, Avaya recommends that you check the Knowledge and Solution Engine on the Avaya Web site for known issues and solutions related to the problem you are experiencing.

Gather information

Before contacting Avaya Technical Support, you must gather information that can help the Technical Support personnel. This includes 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 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

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.

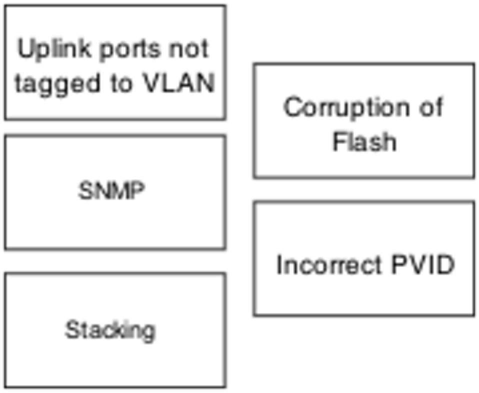


Figure 4: Emergency recovery trees

Navigation

- Corruption of flash on page 21
- Incorrect PVID on page 22
- Uplink ports not tagged to VLAN on page 23
- SNMP on page 25
- Stack on page 26

Corruption of flash

Corruption of the switch configuration file can sometimes occur due to power outage or environmental reasons makes 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).

Corruption of flash recovery tree

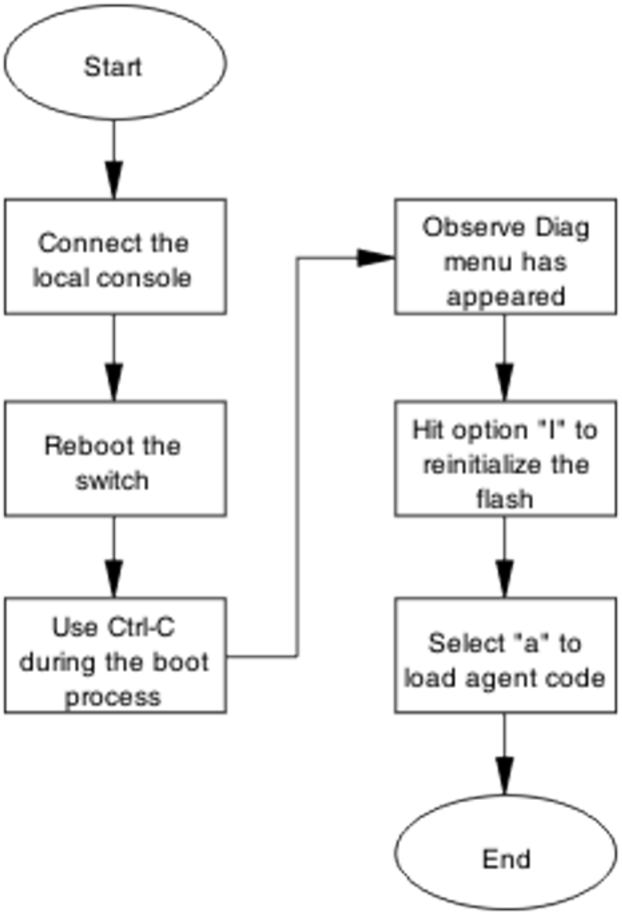

Start
Connect the local console
Reboot the switch
Use Ctrl-C during the boot process
Observe Diag menu has appeared
Hit option "I" to reinitialize the flash
Select "a" to load agent code
End

Figure 5: Corruption of flash

Incorrect PVID

An issue can occur where clients cannot communicate to critical servers when their ports are put in wrong VLAN. If the server is plugged in VLAN-3 and the PVID of the port is 2 then loss of communication can occur. This can be verified by checking the PVID of the ports.

Incorrect PVID Recovery Tree

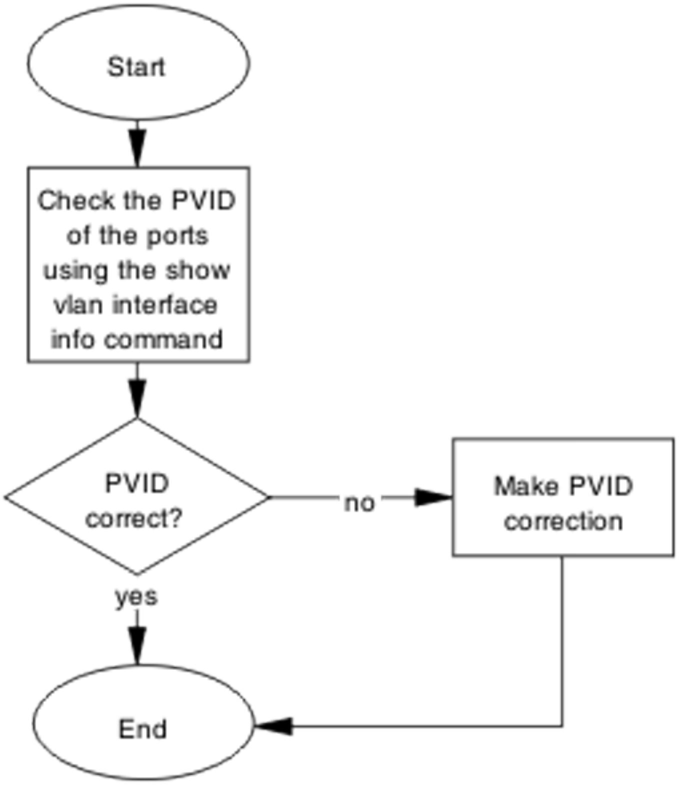

Start
Check the PVID of the ports using the show vlan interface info command
PVID correct?
no
Make PVID correction
yes
End

Figure 6: Incorrect PVID

Uplink ports not tagged to VLAN

When an ERS 2500 series switch is connected to an ERS 8600 series switch and devices in a VLAN on the ERS 8600 series switch are not able to communicate with devices at the ERS 2500 series switch in the same VLAN, then it is likely that the uplink ports are not tagged to the VLAN on the ERS 2500 series switch.

Uplink ports not tagged to VLAN recovery tree

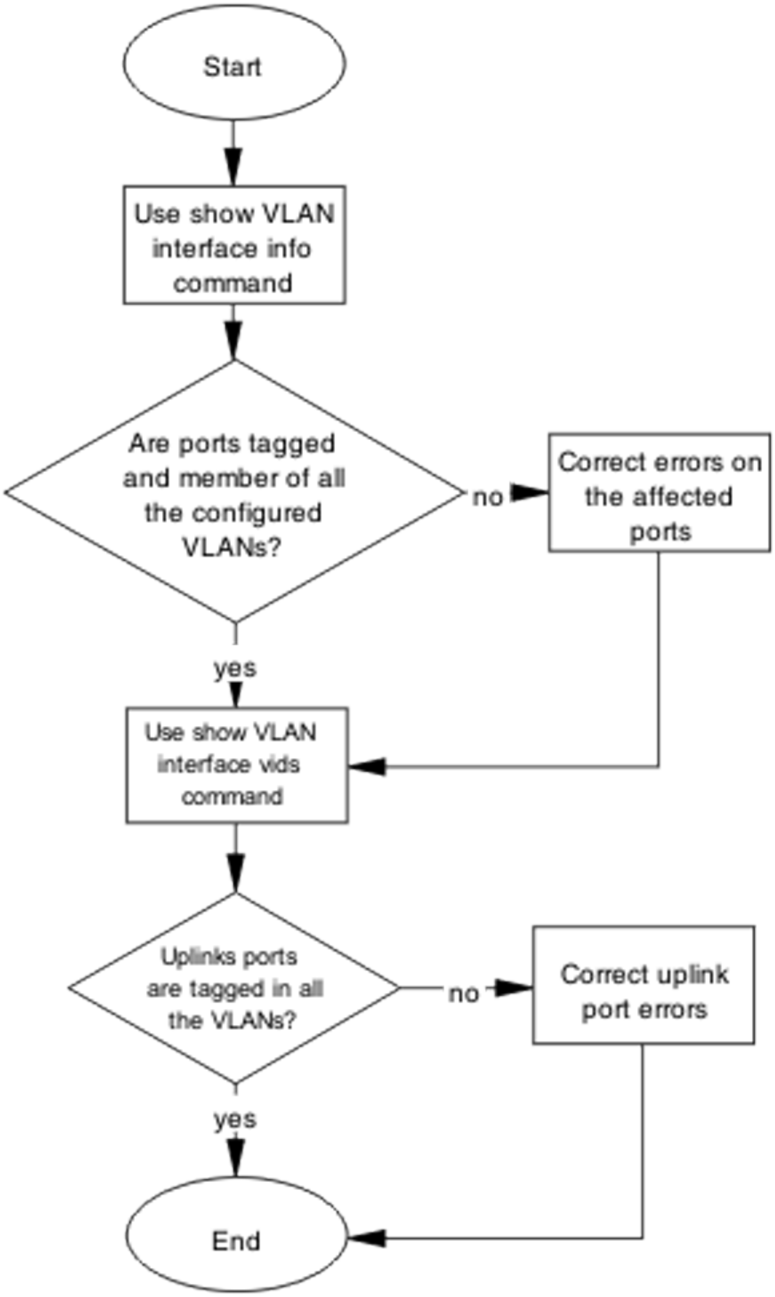

Start
Use show VLAN interface info command
Are ports tagged and member of all the configured VLANs?
no
Correct errors on the affected ports
yes
Use show VLAN interface vids command
Uplinks ports are tagged in all the VLANs?
no
Correct uplink port errors
yes
End

Figure 7: Uplink ports not tagged to VLAN

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, verify the trap configurations (the trap destination address and the traps configured to be sent).

SNMP recovery tree

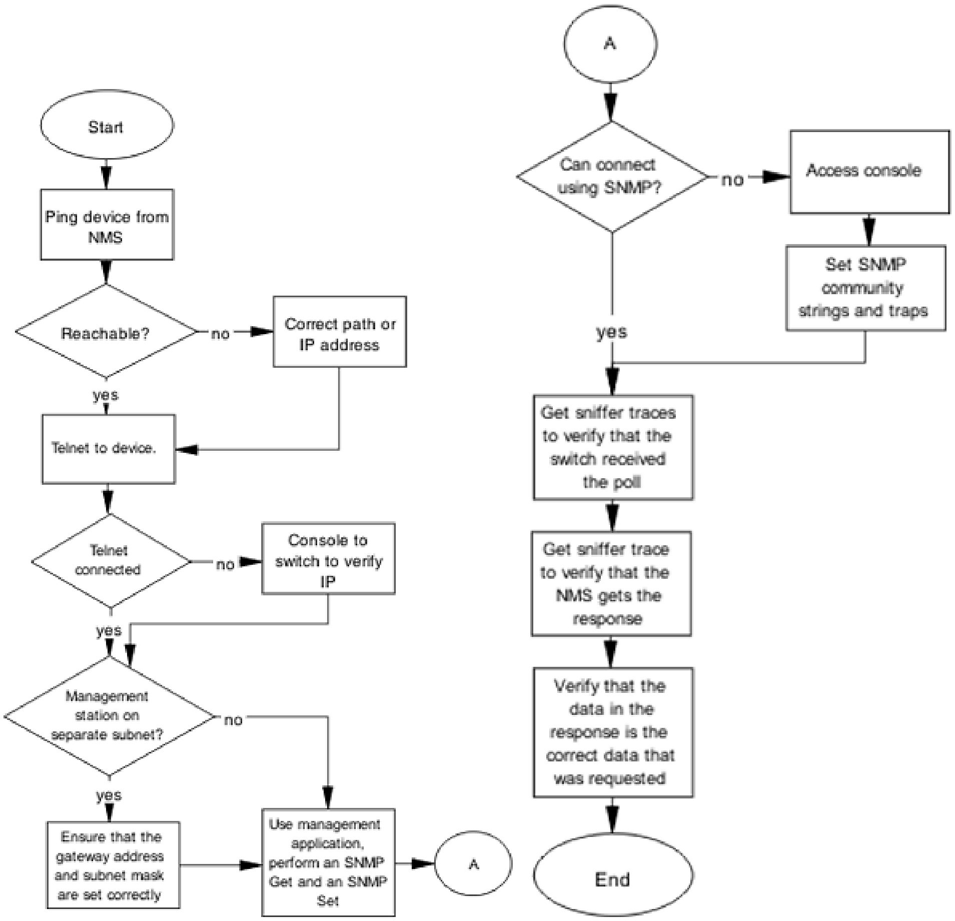

Start
Ping device from NMS
Reachable?
no
Correct path or IP address
yes
Telnet to device.
Telnet connected
no
Console to switch to verify IP
yes
Management station on separate subnet?
no
yes
Ensure that the gateway address and subnet mask are set correctly
Use management application, perform an SNMP Get and an SNMP Set
A
A
Can connect using SNMP?
no
Access console
Set SNMP community strings and traps
yes
Get sniffer traces to verify that the switch received the poll
Get sniffer trace to verify that the NMS gets the response
Verify that the data in the response is the correct data that was requested
End

Figure 8: SNMP

Stack

Stack failure can be the result of a communication error between the individual units due to configuration or cabling. Failures can also arise when there are multiple bases configured.

Stack Recovery Tree

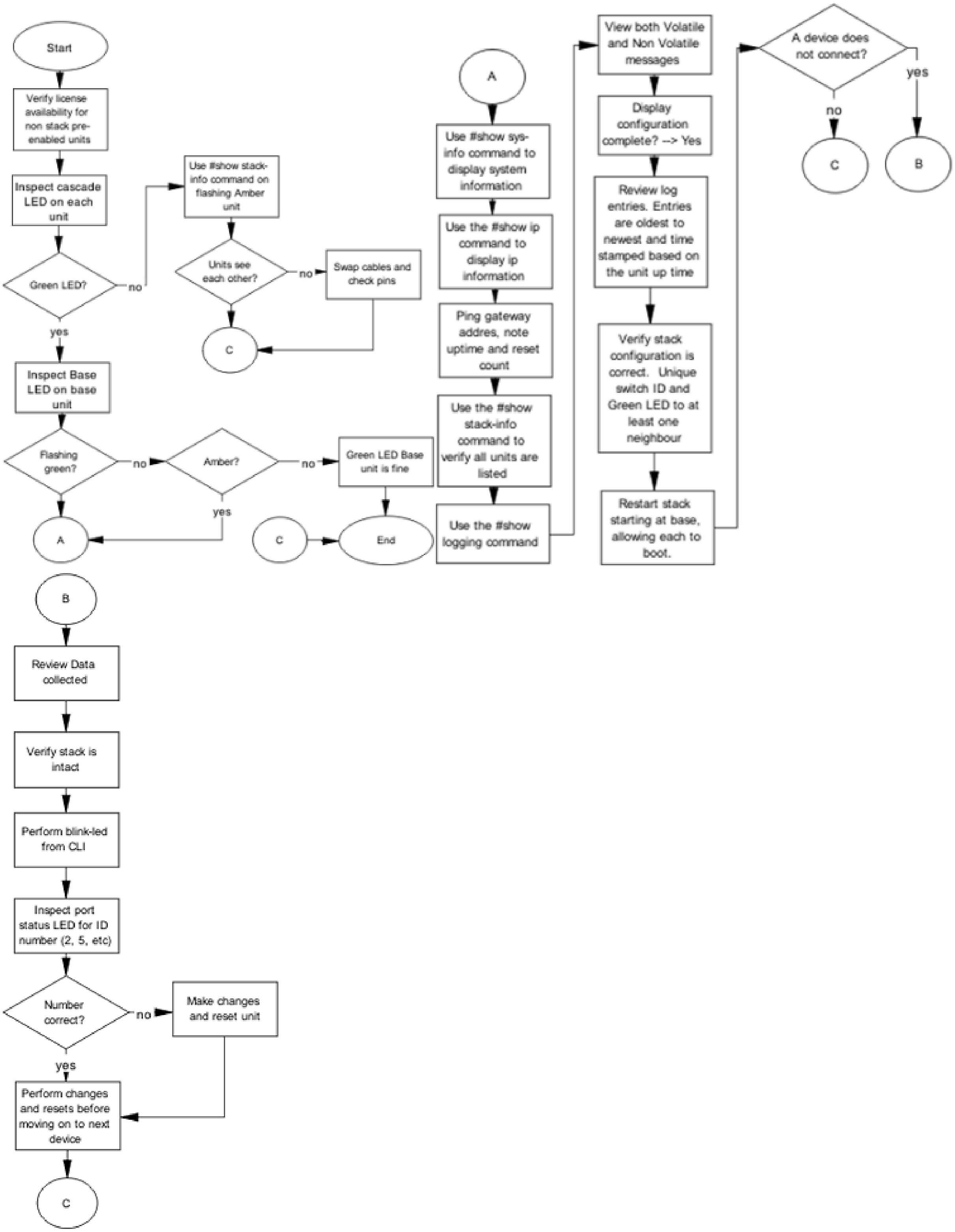

Start
Verify license availability for non stack pre-enabled units
Inspect cascade LED on each unit
Green LED?
no
yes
Use #show stack-info command on flashing Amber unit
Units see each other?
no
Swap cables and check pins
C
Inspect Base LED on base unit
Flashing green?
no
Amber?
no
yes
Green LED Base unit is fine
A
C
End
B
Review Data collected
Verify stack is intact
Perform blink-led from CLI
Inspect port status LED for ID number (2, 5, etc)
Number correct?
no
Make changes and reset unit
yes
Perform changes and resets before moving on to next device
C
A
Use #show sys-info command to display system information
Use the #show ip command to display ip information
Ping gateway addres, note uptime and reset count
Use the #show stack-info command to verify all units are listed
Use the #show logging command
View both Volatile and Non Volatile messages
Display configuration complete? --> Yes
Review log entries. Entries are oldest to newest and time stamped based on the unit up time
Verify stack configuration is correct. Unique switch ID and Green LED to at least one neighbour
Restart stack starting at base, allowing each to boot.
A device does not connect?
no
yes
C
B

Figure 9: Stack

Chapter 8: Troubleshooting hardware

Use this section for hardware troubleshooting specific to the Ethernet Routing Switch 2500 Series.

Work flow: Troubleshooting hardware

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

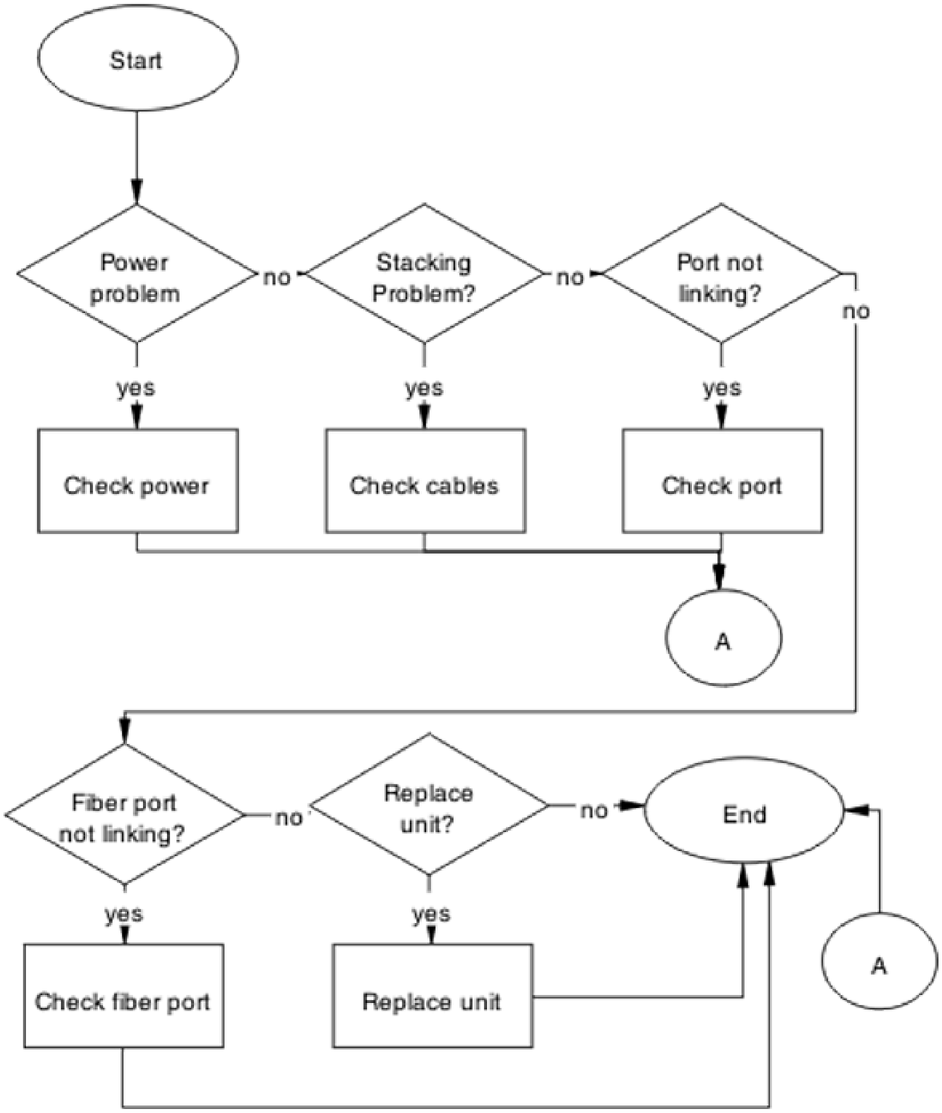


Figure 10: Troubleshooting hardware

Navigation

- Check power on page 31
- Check cables on page 33
- Check port on page 34
- Check fiber port on page 36
- Replace unit on page 38

Check power

Confirm power is being delivered to the device.

Task flow: Check power

The following task flow assists you to confirm that the Ethernet Routing Switch 2500 Series device is powered correctly.

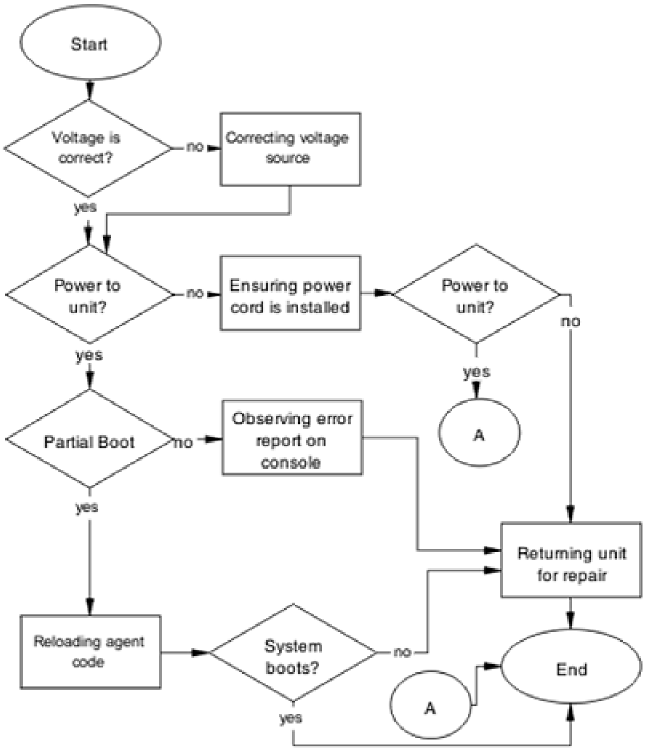


Figure 11: Check power

Navigation

- Correcting voltage source on page 32
- Ensuring power cord is installed on page 32
- Observing error report on console on page 32
- Reloading agent code on page 32
- Returning unit for repair on page 33

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 Ethernet Routing Switch 2500 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 may cause further complications.

1. Use the `show sys-info` command to view the software version.
2. See *Avaya Ethernet Routing Switch 2500 Series Release 4.3 Release Notes* (NN47215-400) for information about software installation.

Returning unit for repair

Return unit to Avaya for repair.

Contact Avaya for return instructions and RMA information.

Check cables

Confirm the stacking cables are correctly connected.

Task flow: Check cables

The following task flow assists you to confirm the stacking cables on the Ethernet Routing Switch 2500 Series device are installed correctly.

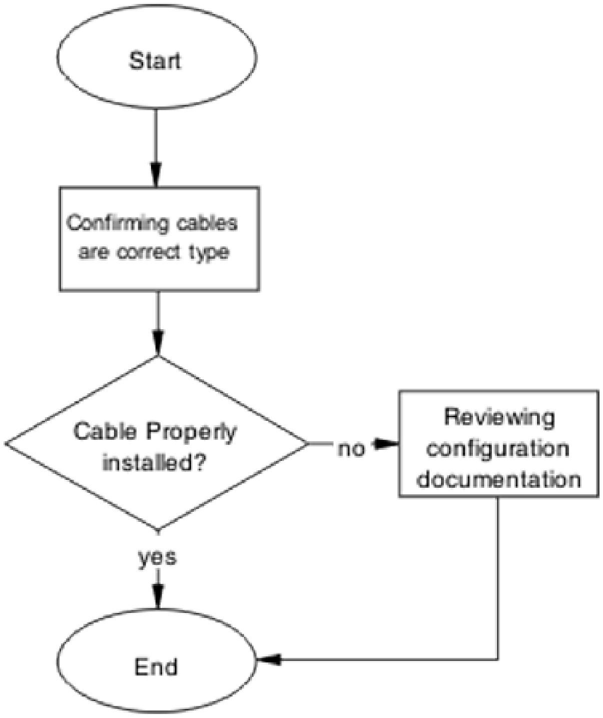

Start
Confirming cables are correct type
Cable Properly installed?
no
Reviewing configuration documentation
yes
End

Figure 12: Check cables

Navigation

- Confirming cables are the correct type on page 34
- Reviewing configuration documentation on page 34

Confirming cables are the correct type

Ensure the cables use RJ45 connectors. The 2500 Series software Release v4.3 supports the use of both straight and crossover Cat5e cabling.

Reviewing configuration documentation

Review the stacking procedures in *Avaya Ethernet Routing Switch 2500 Series Configuration — System* (NN47215-500).

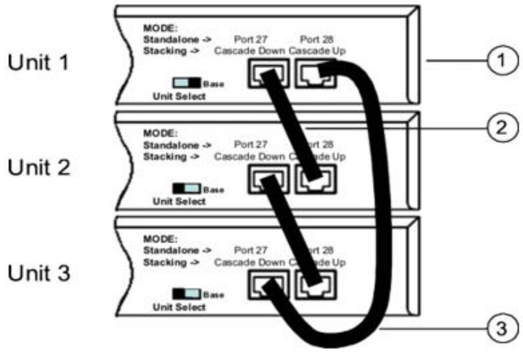


Figure 13: Stack configuration

1. Base unit
2. Cascade cable
3. Cascade cable (used for return)

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.

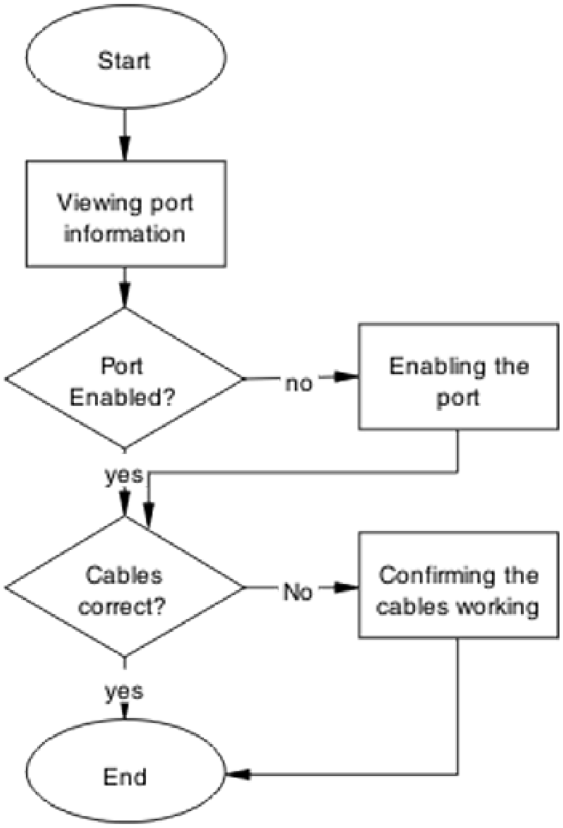


Figure 14: Check port

Navigation

- Viewing port information on page 35
- Enabling the port on page 36
- Confirming the cables are working on page 36
- Confirming the cables are working on page 36

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 fastethernet <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 fastethernet <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.

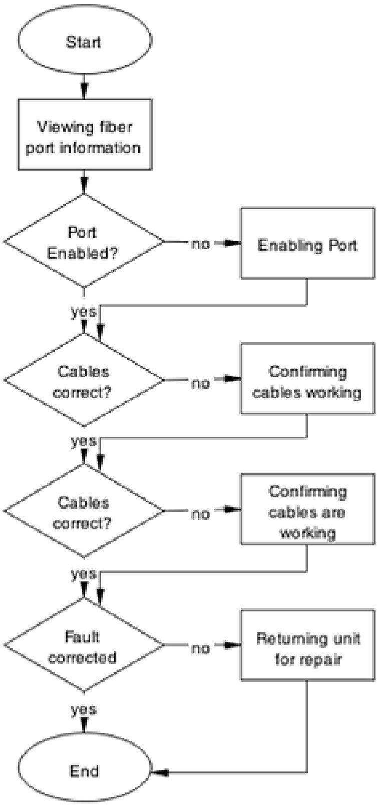

Start
Viewing fiber port information
Port Enabled?
no
Enabling Port
yes
Cables correct?
no
Confirming cables working
yes
Cables correct?
no
Confirming cables are working
yes
Fault corrected
no
Returning unit for repair
yes
End

Figure 15: Check fiber port

Navigation

- Viewing fiber port information on page 37
- Enabling the port on page 38
- Confirming cables are working on page 38
- Returning unit for repair on page 38

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 Ethernet Routing Switch 2500 series 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 Avaya for repair

Contact Avaya 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 and in *Avaya Ethernet Routing Switch 2500 Series — Regulatory Information* (NN47215-100).

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.

In order for AUR to function properly, the new unit and the existing units in the stack must all be running the same version of software (Release 4.1 software or later).

AUR is not designed for the situation of removing and reinserting the same switch (with the same MAC address).

For detailed information about AUR, see *Avaya Ethernet Routing Switch 2500 Series Configuration — System* (NN47215-500).

Task flow: Replace a unit in a stack

The following task flow assists you to replace one of the 2500 Series devices in a stack. This in 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 verify software procedures are not required.

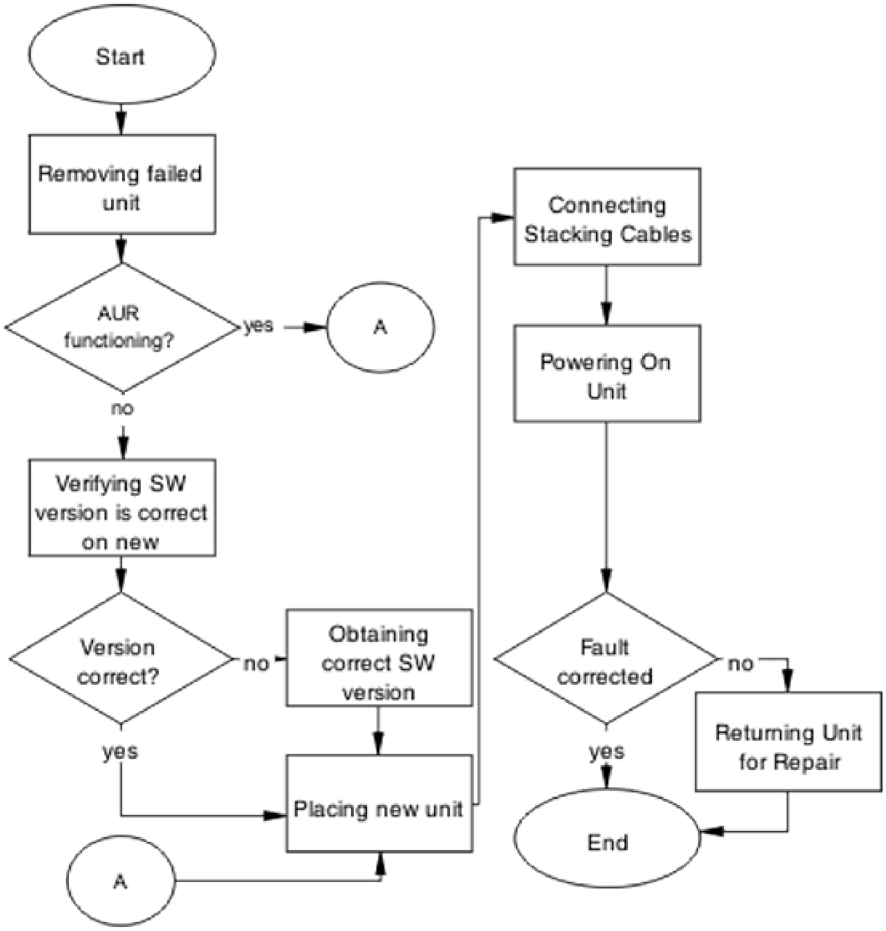


Figure 16: Replace unit

Navigation

- Removing failed unit on page 40
- Verifying software version is correct on new device on page 41
- Obtaining the correct software version on page 41
- Placing a new unit on page 41
- Connecting stacking cables on page 41
- Powering on the unit on page 42
- Returning unit for repair on page 42

Removing failed unit

Remove the failed unit from the stack.

1. Maintain power to the stack. Do not power down the stack.
2. Remove the failed device.

Verifying software version is correct on new device

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

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

Obtaining the correct software version

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.

See *Avaya Ethernet Routing Switch 2500 Series Release 4.3 Release Notes* (NN47215-400) for software installation.

Placing a new unit

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

Connecting stacking cables

Reconnect the stacking cables to correctly stack the device.

1. Review the stacking section in *Avaya Ethernet Routing Switch 2500 Series Configuration — System* (NN47215-500) for cabling details.
2. Connect the cables in accordance with physical stack requirements.

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 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 unit for repair

Return the unit to Avaya for repair.

Contact Avaya for return instructions and RMA information.

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**. 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.

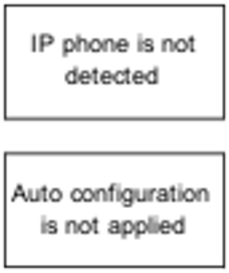


Figure 17: Troubleshooting ADAC

Navigation

- IP phone is not detected on page 44
- Auto configuration is not applied on page 49

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.

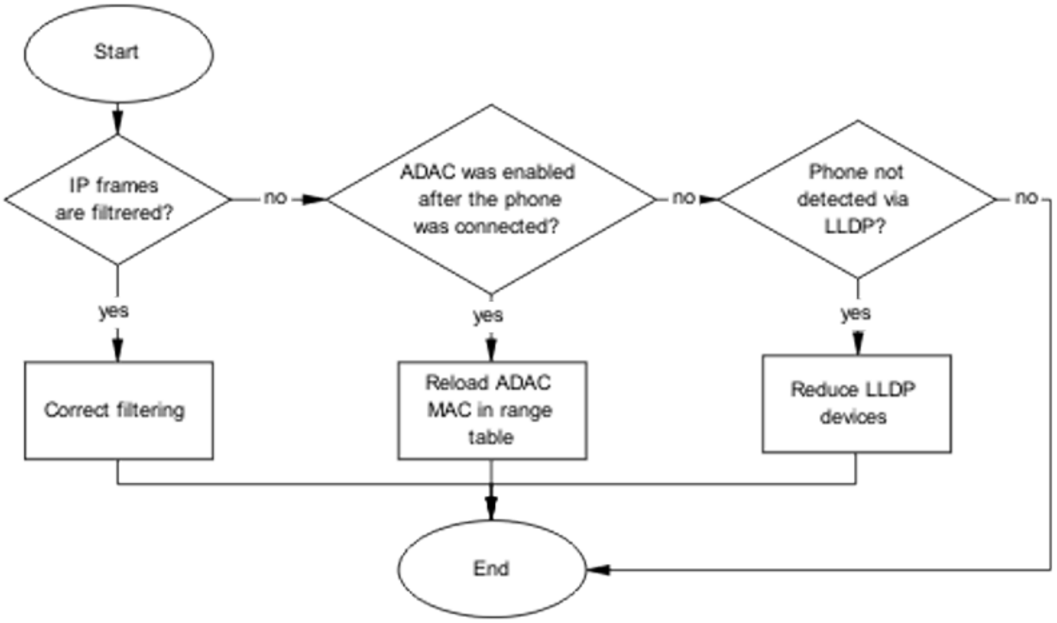

Start
IP frames are filtrered?
no
ADAC was enabled after the phone was connected?
no
Phone not detected via LLDP?
no
yes
yes
yes
Correct filtering
Reload ADAC MAC in range table
Reduce LLDP devices
End

Figure 18: IP phone not detected

Navigation

- Correct filtering on page 44
- Reload ADAC MAC in range table on page 46
- Reduce LLDP devices on page 47

Correct filtering

Configure the VLAN filtering to allow ADAC.

Task flow: Correct filtering

The following task flow assists you to correct the filtering.

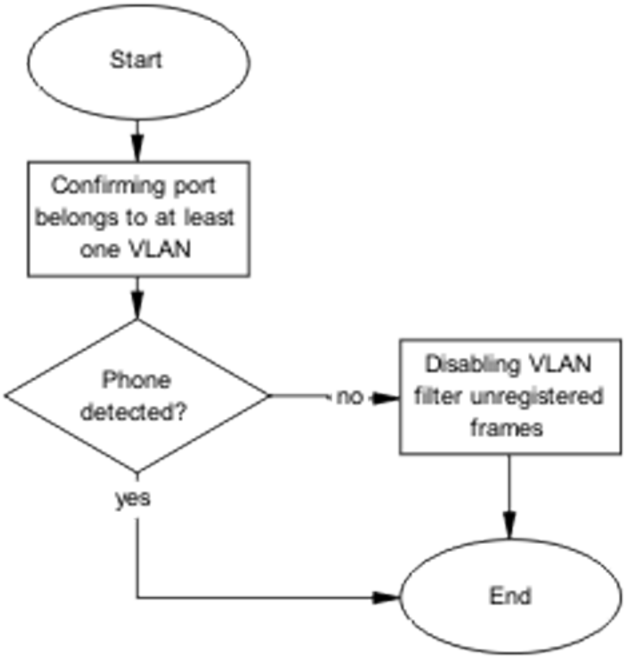

Start
Confirming port belongs to at least one VLAN
Phone detected?
no
Disabling VLAN filter unregistered frames
yes
End

Figure 19: Correct filtering

Navigation

- Confirming port belongs to at least one VLAN on page 45
- Disabling the VLAN filtering of unregistered frames on page 45

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.

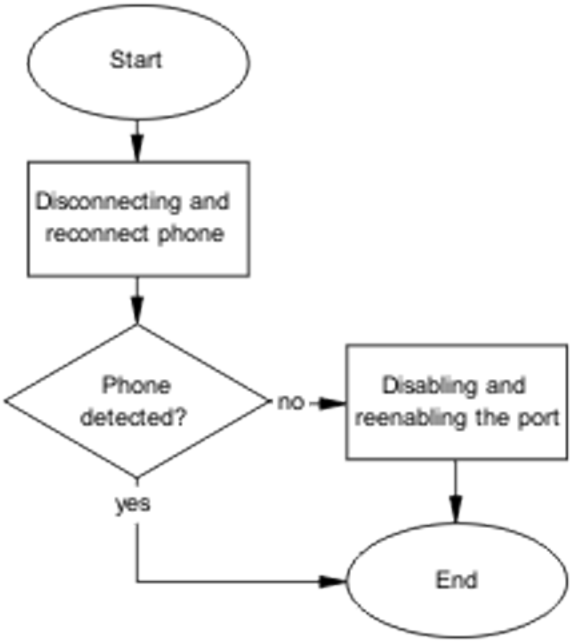

Start
Disconnecting and reconnect phone
Phone detected?
no
Disabling and reenabling the port
yes
End

Figure 20: Reload ADAC MAC in range table

Navigation

- Disconnecting and reconnecting phone on page 46
- Disabling and enabling the port on page 47

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 re-enable 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.

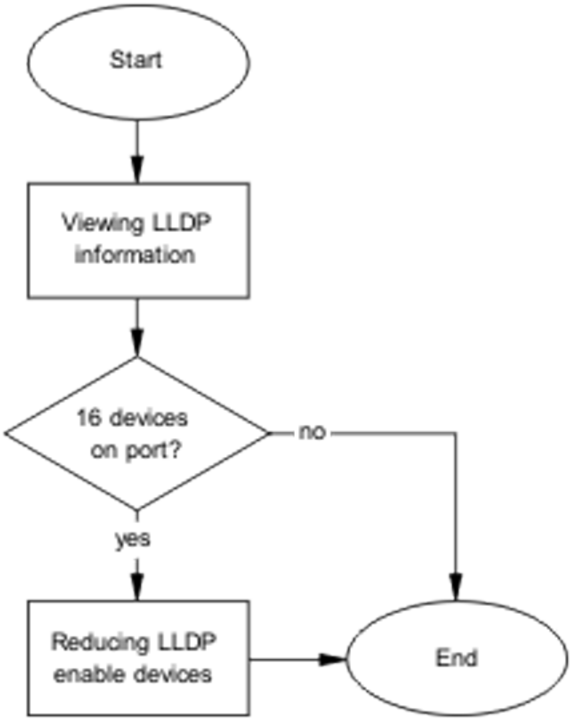


Figure 21: Reduce LLDP devices

Navigation

- Viewing LLDP information on page 48
- Reducing LLDP enabled devices on page 48

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.

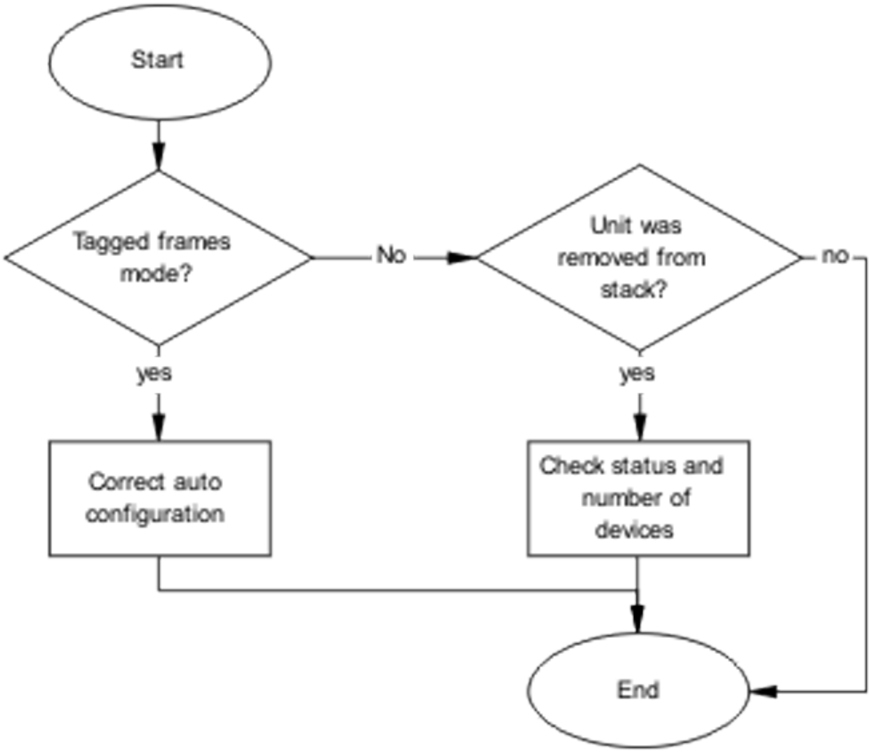

Start
Tagged frames mode?
No
Unit was removed from stack?
no
yes
yes
Correct auto configuration
Check status and number of devices
End

Figure 22: Auto configuration is not applied

Navigation

- Correct auto configuration on page 50
- Check the status and number of devices on page 52

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.

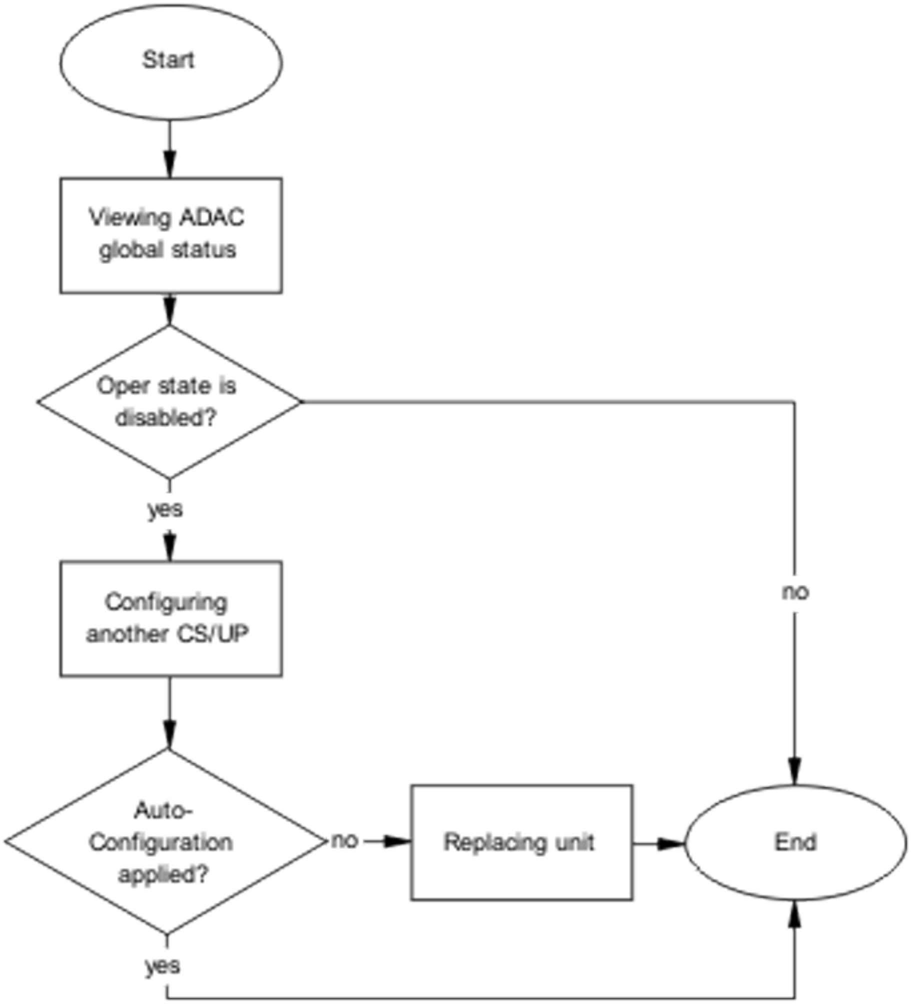

Start
Viewing ADAC global status
Oper state is disabled?
yes
no
Configuring another CS/UP
Auto-Configuration applied?
no
Replacing unit
End
yes

Figure 23: Correct auto configuration

Navigation

- Viewing ADAC global status on page 51
- Configuring another call server and uplink port on page 52
- Replacing Unit on page 52

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.

Replacing Unit

Replace unit to replicate configuration if AUR is enabled.

1. Follow the replacement guidelines in *Avaya Ethernet Routing Switch 2500 Series — System Configuration* (NN47215-500).
2. Refer to the unit replacement section in the Troubleshooting Hardware section of this document.

Check the 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

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

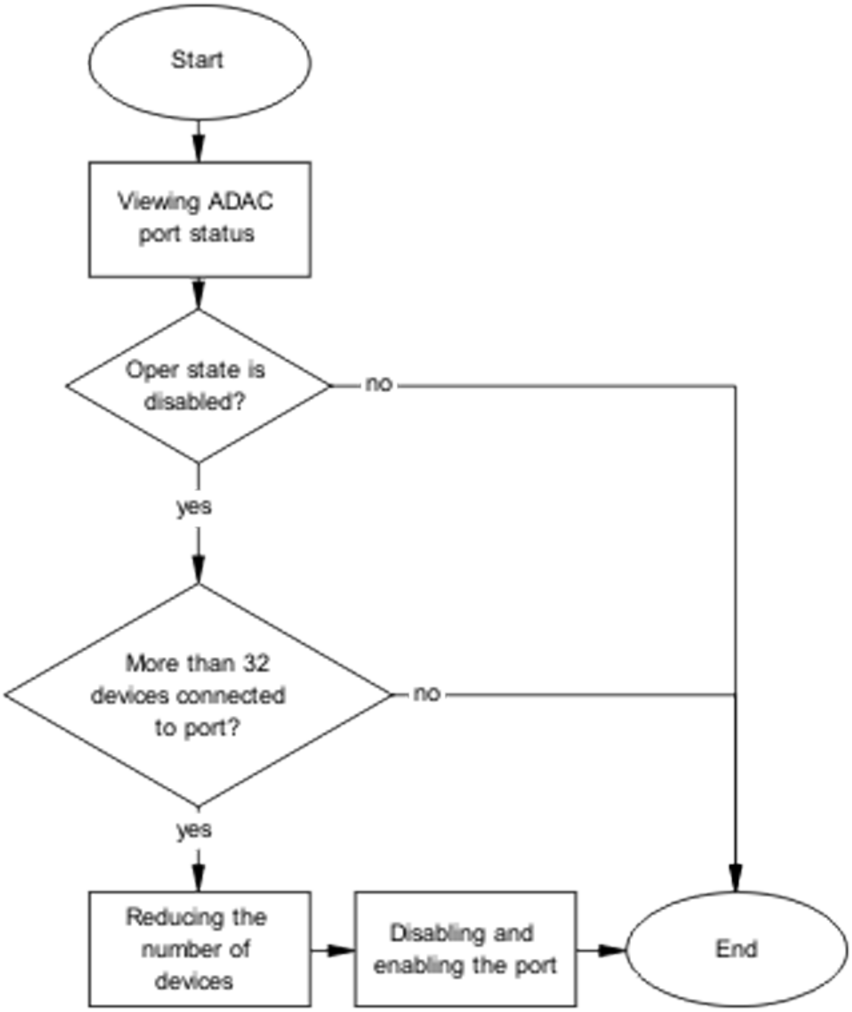

Start
Viewing ADAC port status
Oper state is disabled?
no
yes
More than 32 devices connected to port?
no
yes
Reducing the number of devices
Disabling and enabling the port
End

Figure 24: Check status and number of devices

Navigation

- Viewing ADAC port status on page 53
- Reducing the number of devices on page 54
- Disabling and enabling the port on page 54

Viewing ADAC port status

Display the status of ADAC on the port.

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

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 32 devices connected.

Disabling and enabling the port

Administratively disable and enable to port to initialize configuration.

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

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

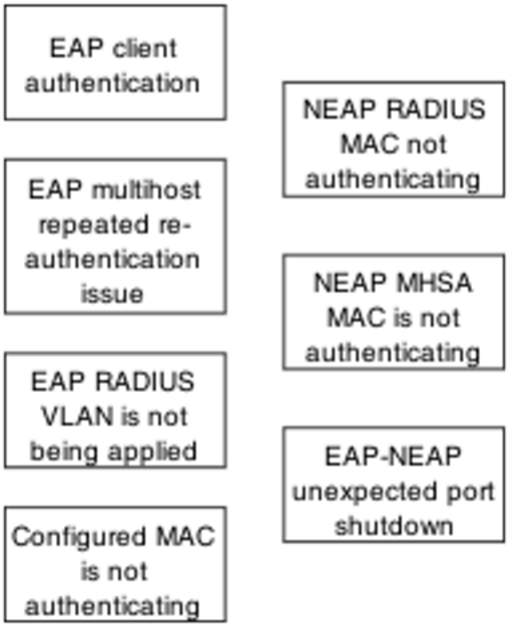

EAP client authentication
EAP multihost repeated re-authentication issue
EAP RADIUS VLAN is not being applied
Configured MAC is not authenticating
NEAP RADIUS MAC not authenticating
NEAP MHSA MAC is not authenticating
EAP-NEAP unexpected port shutdown

Figure 25: Troubleshooting authentication

Navigation

- EAP client authentication on page 56
- EAP multihost repeated re-authentication issue on page 64
- EAP RADIUS VLAN is not being applied on page 68
- Configured MAC is not authenticating on page 74
- Non-EAP RADIUS MAC not authenticating on page 79

- Non-EAP MHSA MAC is not authenticating on page 83
- EAP–non-EAP unexpected port shutdown on page 87

EAP client authentication

This section provides troubleshooting guidelines for the EAP and non-EAP features on the Ethernet Routing Switch 2500 Series devices.

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.

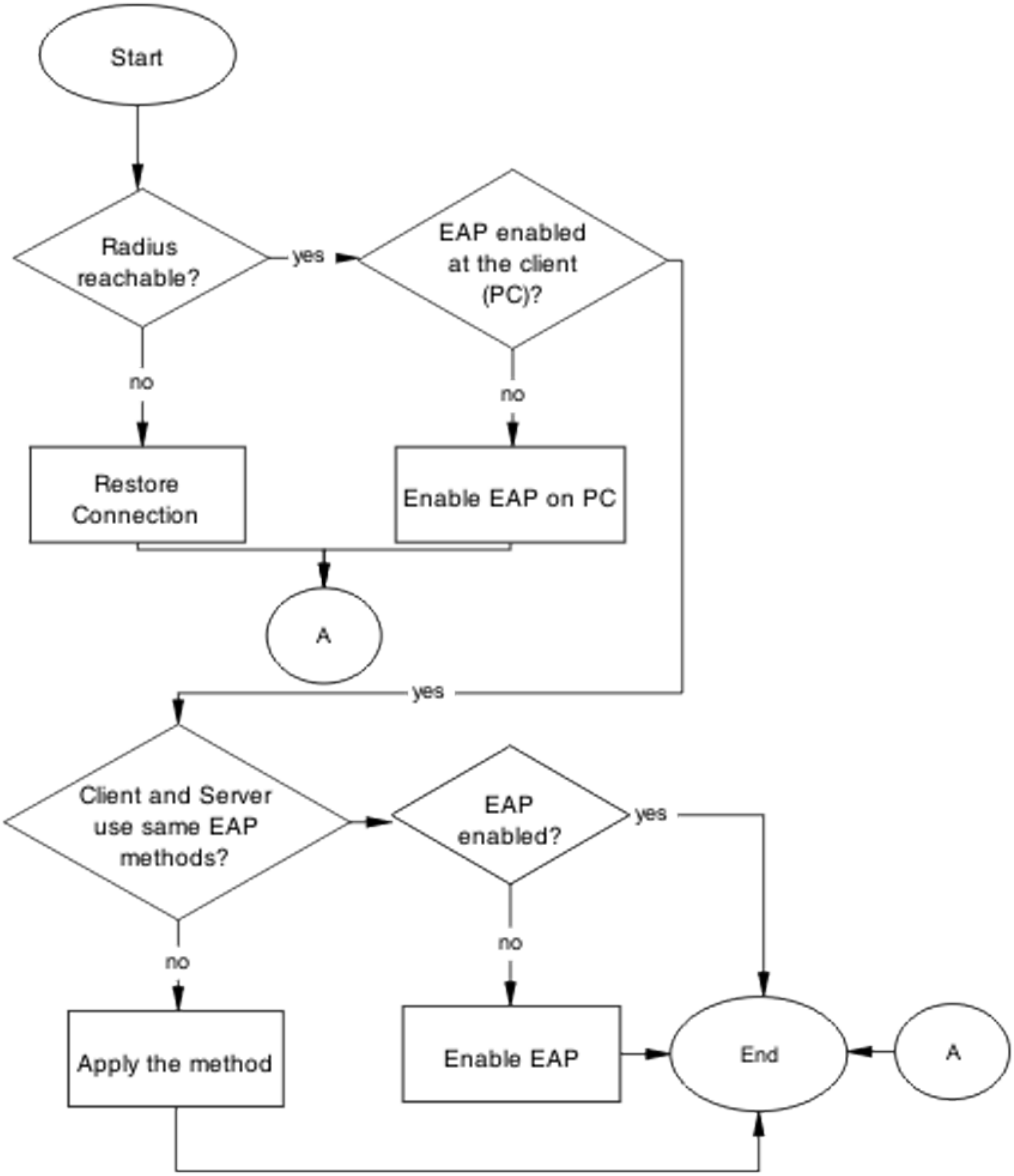


Figure 26: EAP client is not authenticating

Navigation

- Restore RADIUS connection on page 58
- Enable EAP on the PC on page 60
- Apply the method on page 61
- Enable EAP globally on page 62

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.

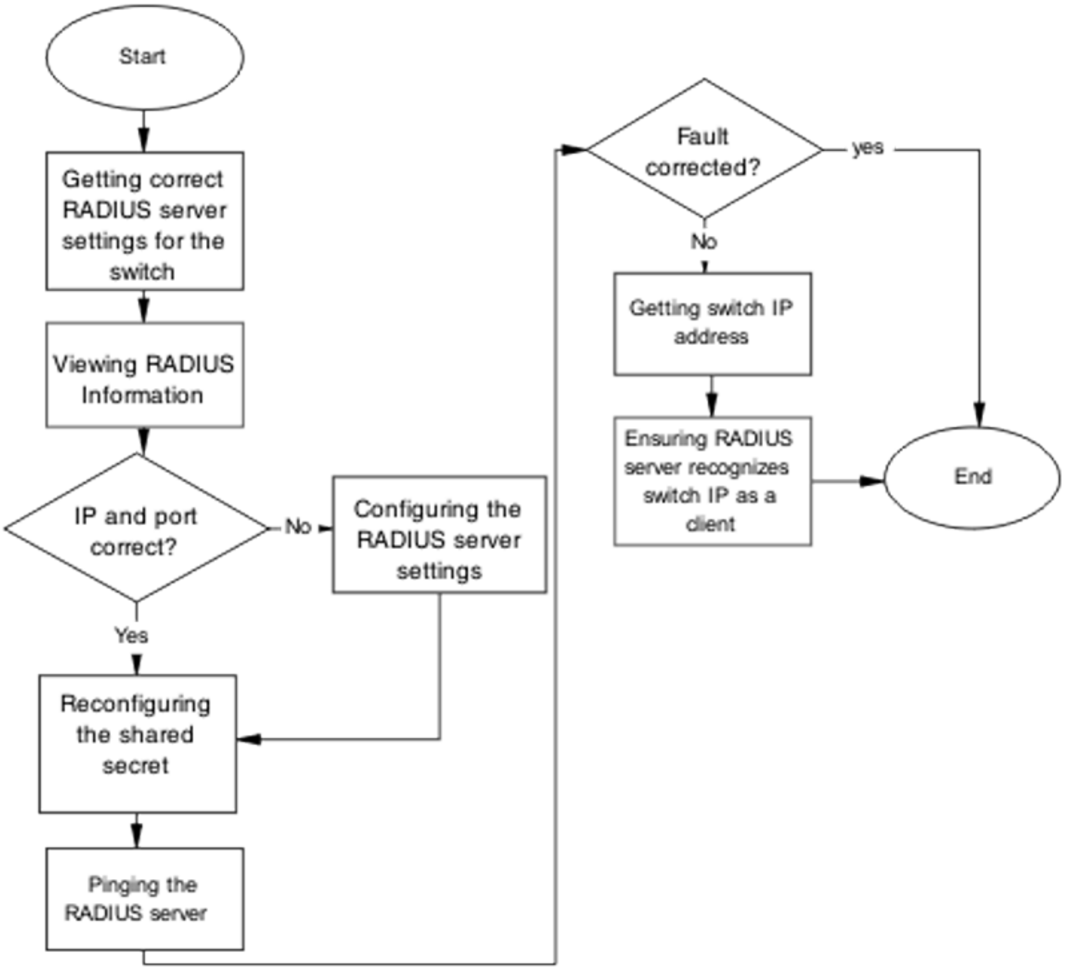

Start
Getting correct RADIUS server settings for the switch
Viewing RADIUS Information
IP and port correct?
No
Configuring the RADIUS server settings
Yes
Reconfiguring the shared secret
Pinging the RADIUS server
Fault corrected?
yes
No
Getting switch IP address
Ensuring RADIUS server recognizes switch IP as a client
End

Figure 27: Restore RADIUS connection

Navigation

- Getting correct RADIUS server settings for the switch on page 59
- Viewing RADIUS information on page 59
- Configuring the RADIUS server settings on page 59
- Pinging the RADIUS server on page 59

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.

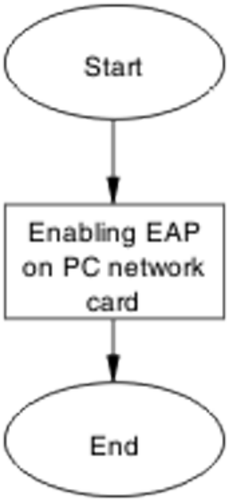


Figure 28: Enable EAP on the PC

Navigation

- Enabling EAP on PC network card on page 60

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.

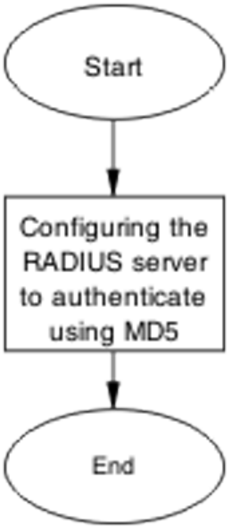


Figure 29: Apply the method

Navigation

Configuring the RADIUS server on page 61

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

Enable EAP globally on the 2500 Series device.

Task flow: Enable EAP globally

The following task flow assists you to enable EAP globally on the 2500 Series device.

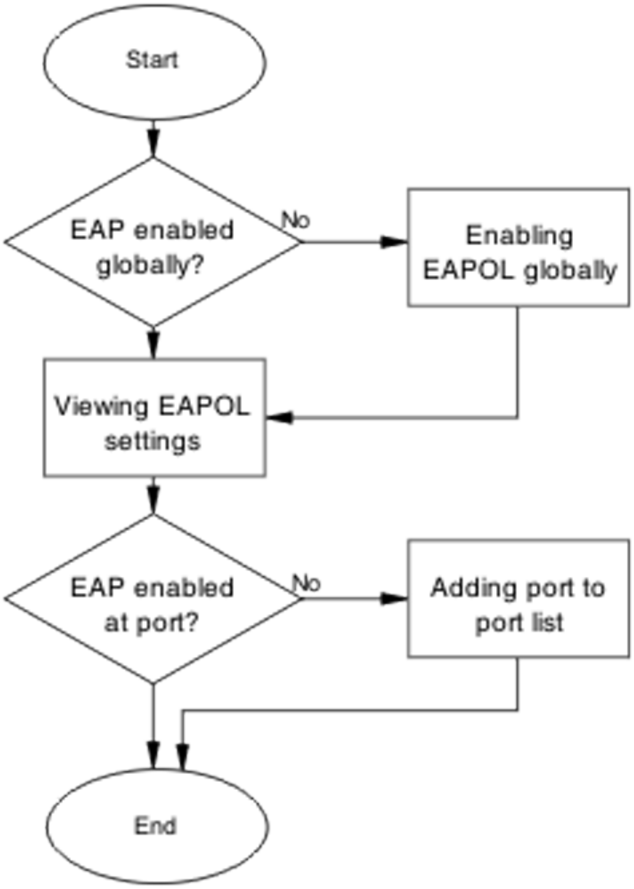


Figure 30: Enable EAP globally

Navigation

- Enabling EAP globally on page 63
- Viewing EAPOL settings on page 64
- Setting EAPOL port administrative status to auto on page 64

Enabling EAP globally

Enable EAP globally on the Ethernet Routing Switch 2500 Series device.

1. Use the `eapol enable` command to enable EAP globally on the 2500 Series device.
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.

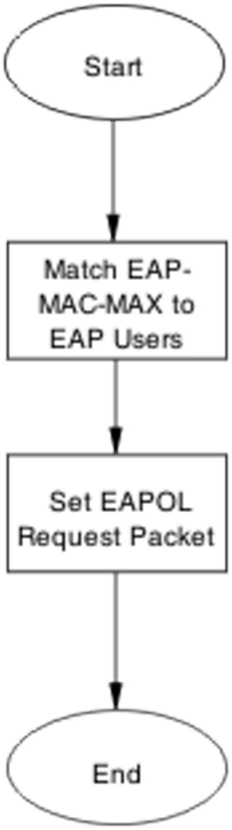


Figure 31: EAP multihost repeated re-authentication issue

Navigation

- Match EAP-MAC-MAX to EAP users on page 65
- Set EAPOL request packet on page 67

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

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

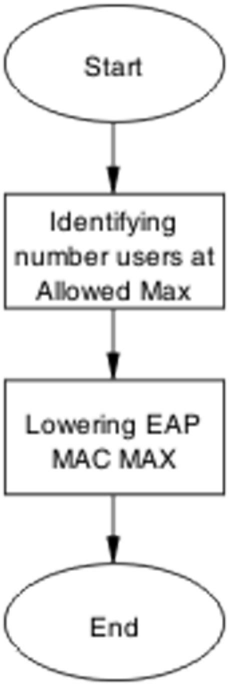


Figure 32: Match EAP-MAC-MAX to EAP users

Navigation

- Identifying number of users at allowed max on page 66
- Lowering EAP max MAC on page 66

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.

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.

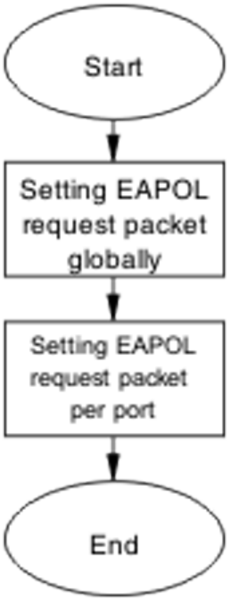

Start
Setting EAPOL request packet globally
Setting EAPOL request packet per port
End

Figure 33: Set EAPOL request packet

Navigation

- Setting EAPOL request packet globally on page 67
- Setting EAPOL request packet for a port on page 68

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.

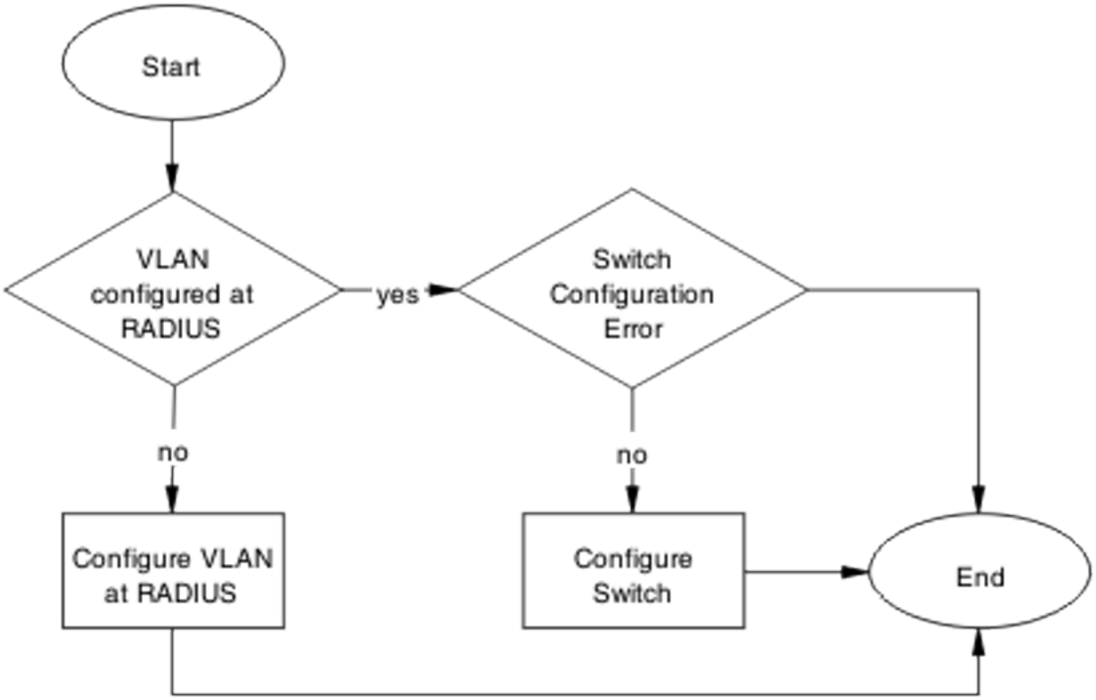


Figure 34: EAP Radius VLAN is not being applied

Navigation

- Configure VLAN at RADIUS on page 69
- Configure switch on page 71

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.

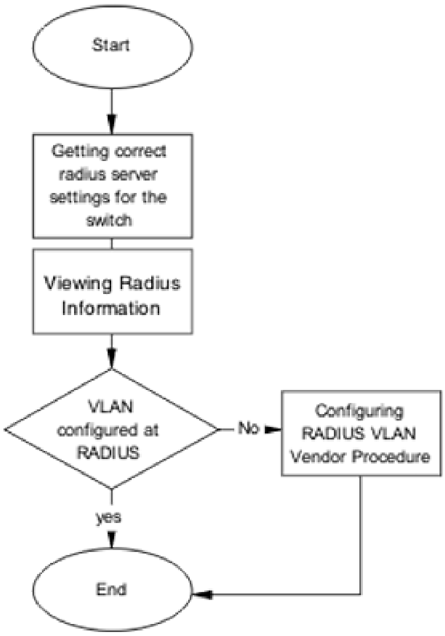

Start
Getting correct radius server settings for the switch
Viewing Radius Information
VLAN configured at RADIUS
No
Configuring RADIUS VLAN Vendor Procedure
yes
End

Figure 35: Configure VLAN at RADIUS

Navigation

- Getting correct RADIUS server settings on page 70
- Viewing RADIUS information on page 70
- Configuring RADIUS on page 71

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 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 switch

The VLAN must be configured correctly on the Ethernet Routing Switch 2500 Series device.

Task flow: Configure switch

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

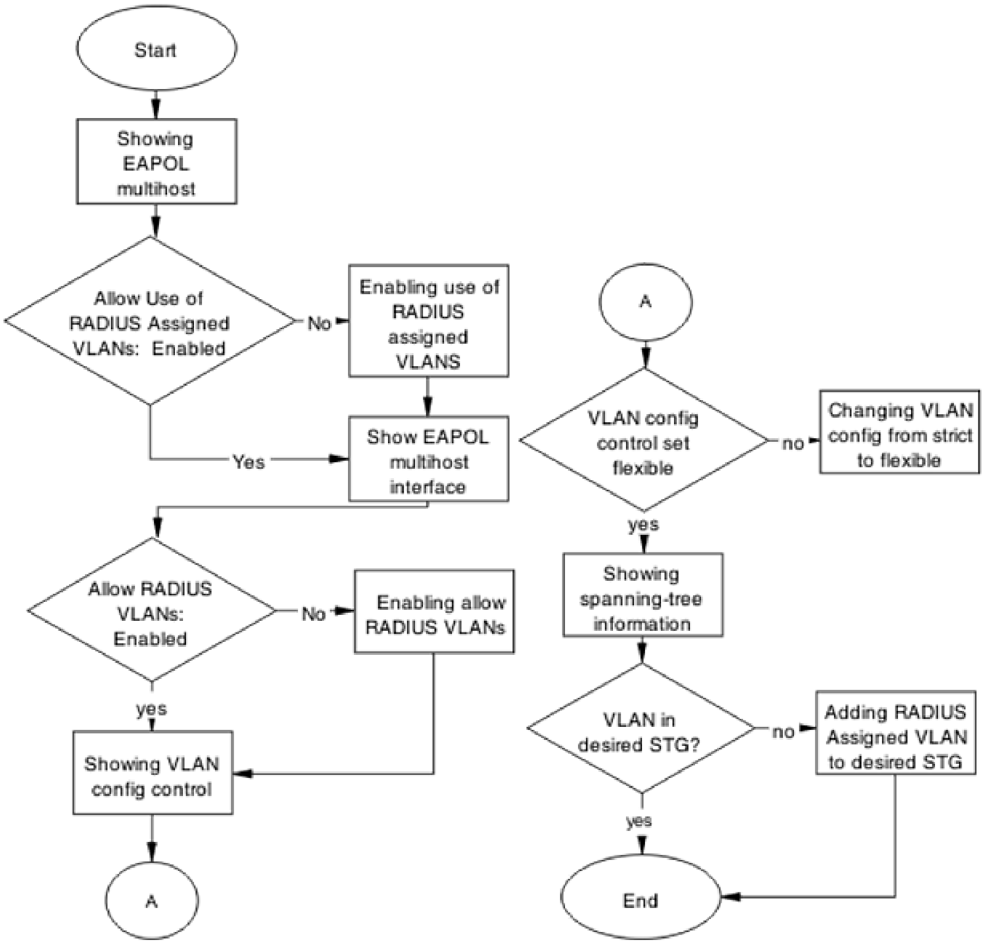

Start
Showing EAPOL multihost
Allow Use of RADIUS Assigned VLANs: Enabled
No
Enabling use of RADIUS assigned VLANS
Yes
Show EAPOL multihost interface
Allow RADIUS VLANs: Enabled
No
Enabling allow RADIUS VLANs
yes
Showing VLAN config control
A
A
VLAN config control set flexible
no
Changing VLAN config from strict to flexible
yes
Showing spanning-tree information
VLAN in desired STG?
no
Adding RADIUS Assigned VLAN to desired STG
yes
End

Figure 36: Configure switch task

Navigation

- Showing EAPOL multihost on page 72
- Enabling use of RADIUS assigned VLANs on page 73
- Showing EAPOL multihost interface on page 73
- Showing VLAN config control on page 73
- Changing VLAN config from strict to flexible on page 73
- Showing spanning tree on page 74
- Adding RADIUS assigned VLAN to desired STG on page 74

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.

Showing spanning tree

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 RADIUS assigned VLAN after EAP authentication succeeds.

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

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

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

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

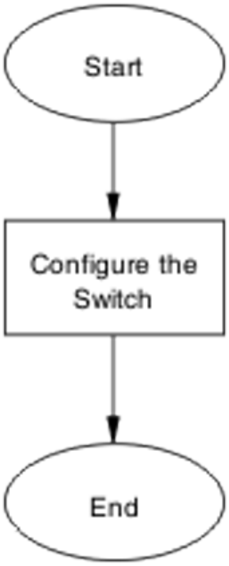


Figure 37: Configured MAC is not authenticating

Navigation

- Configure the switch on page 75

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 2500 Series device.

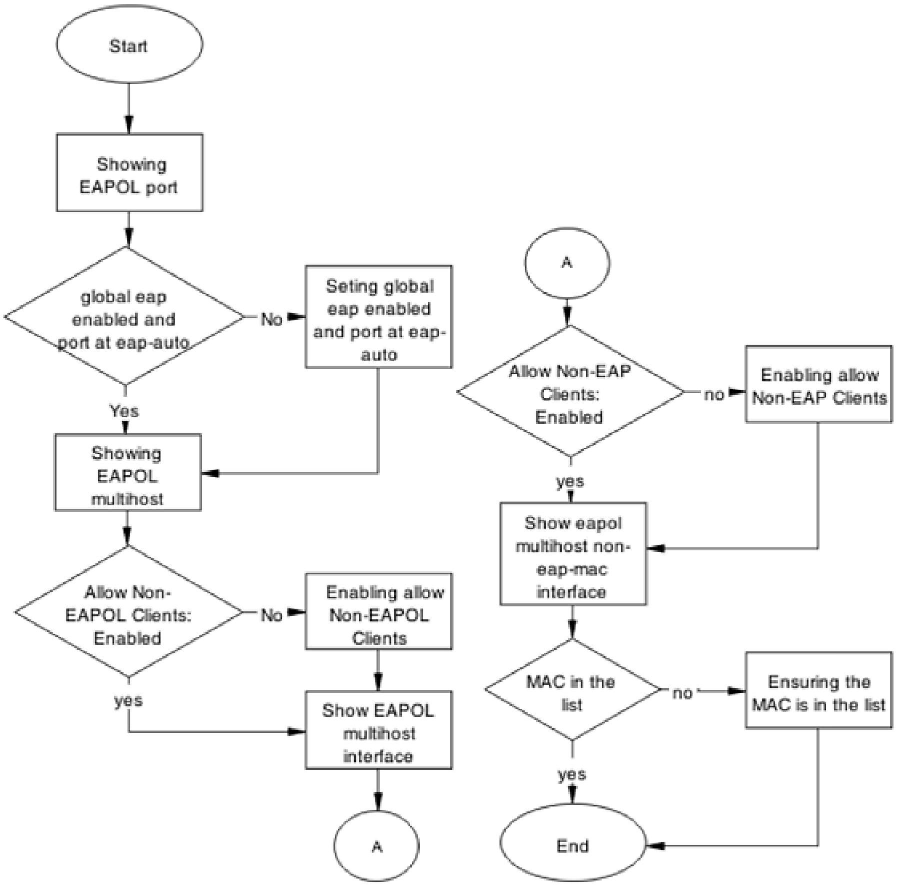

Start
Showing EAPOL port
global eap enabled and port at eap-auto
No
Seting global eap enabled and port at eap-auto
Yes
Showing EAPOL multihost
Allow Non-EAPOL Clients: Enabled
No
Enabling allow Non-EAPOL Clients
yes
Show EAPOL multihost interface
A
A
Allow Non-EAP Clients: Enabled
no
Enabling allow Non-EAP Clients
yes
Show eapol multihost non-eap-mac interface
MAC in the list
no
Ensuring the MAC is in the list
yes
End

Figure 38: Configure the switch

Navigation

- Showing EAPOL port on page 76
- Setting global EAP enabled and port at eap-auto on page 77
- Showing EAPOL multihost on page 77
- Enabling allow non-EAPOL clients on page 77
- Showing EAPOL multihost interface on page 77
- Enabling multihost status and allow non-EAPOL clients on page 78
- Showing EAPOL multihost non-eap-mac interface on page 78
- Ensuring MAC in the list on page 78

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 <port>` 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.

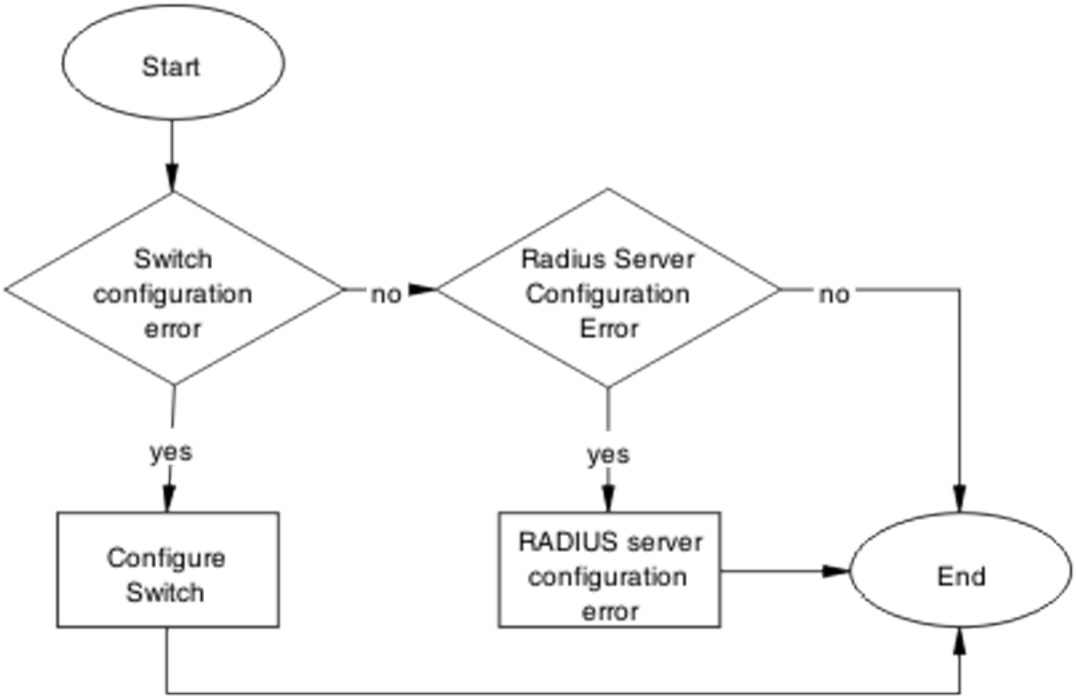

Start
Switch configuration error
no
Radius Server Configuration Error
no
yes
yes
Configure Switch
RADIUS server configuration error
End

Figure 39: Non-EAP RADIUS MAC not authenticating

Navigation

- Configure switch on page 79
- RADIUS server configuration error on page 82

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 2500 Series device to correct the RADIUS MAC issue.

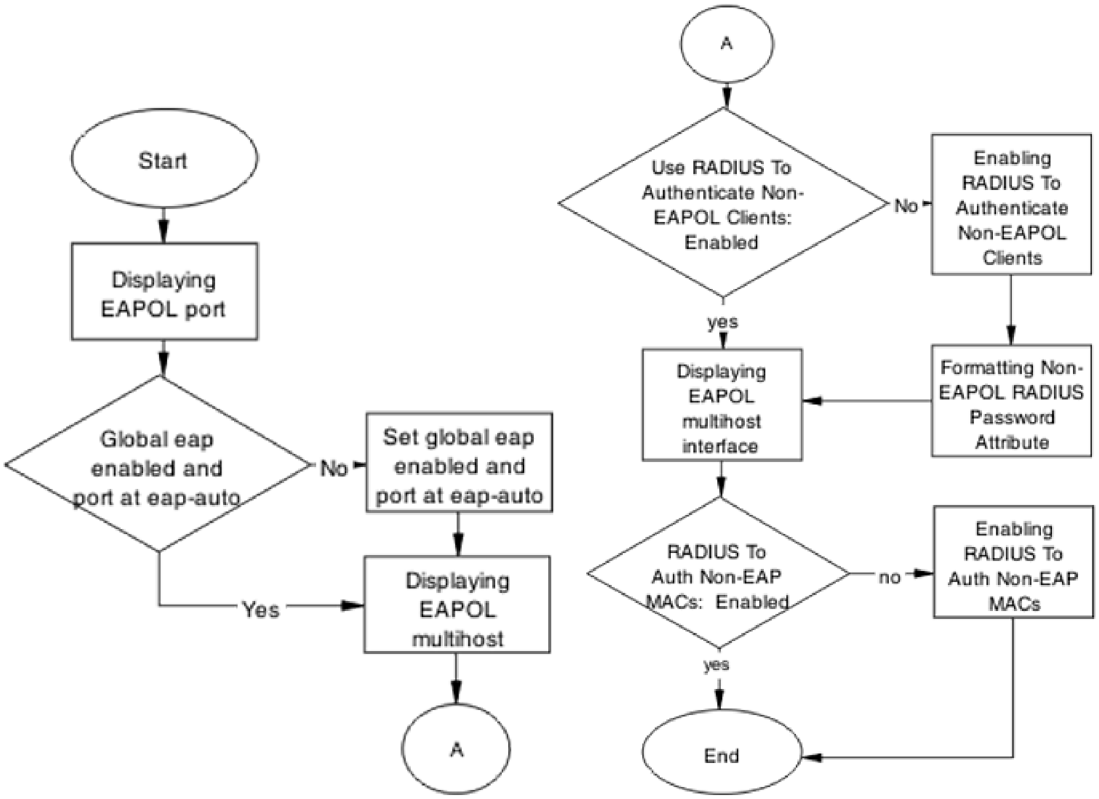

A
Start
Use RADIUS To Authenticate Non-EAPOL Clients: Enabled
No
Enabling RADIUS To Authenticate Non-EAPOL Clients
Displaying EAPOL port
yes
Displaying EAPOL multihost interface
Formatting Non-EAPOL RADIUS Password Attribute
Global eap enabled and port at eap-auto
No
Set global eap enabled and port at eap-auto
RADIUS To Auth Non-EAP MACs: Enabled
no
Enabling RADIUS To Auth Non-EAP MACs
Yes
Displaying EAPOL multihost
yes
A
End

Figure 40: Configure switch

Navigation

- Displaying EAPOL port on page 80
- Setting global eap enabled and port at eap-auto on page 81
- Displaying EAPOL multihost on page 81
- Enabling RADIUS to authenticate non-EAPOL clients on page 81
- Formatting non-EAPOL RADIUS password attribute on page 81
- Displaying EAPOL multihost interface on page 82
- Enabling RADIUS To Auth non-EAP MACs on page 82

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 required changes to enable EAP globally and to set the port status 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: `IpAddr.MACAddr.PortNumber`

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 `IpAddr.MACAddr.PortNumber`.

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 2500 Series device be configured.

Task flow: RADIUS server configuration error

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

Start
Configuring MAC and password on RADIUS server
End

Figure 41: RADIUS server configuration error

Navigation

- Configuring MAC and password on RADIUS server on page 83

Configuring MAC and password on RADIUS server

The RADIUS server requires that the MAC address and password for the 2500 Series device be correct. If it is incorrect, the 2500 Series device 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

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

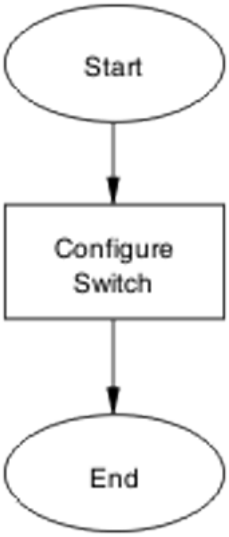


Figure 42: Non-EAP MHSA MAC is not authenticating

Navigation

Configure switch on page 84

Configure switch

Configure the switch to enable MHSA.

Task flow: Configure switch

The following task flow assists you to enable MHSA on the 2500 Series device.

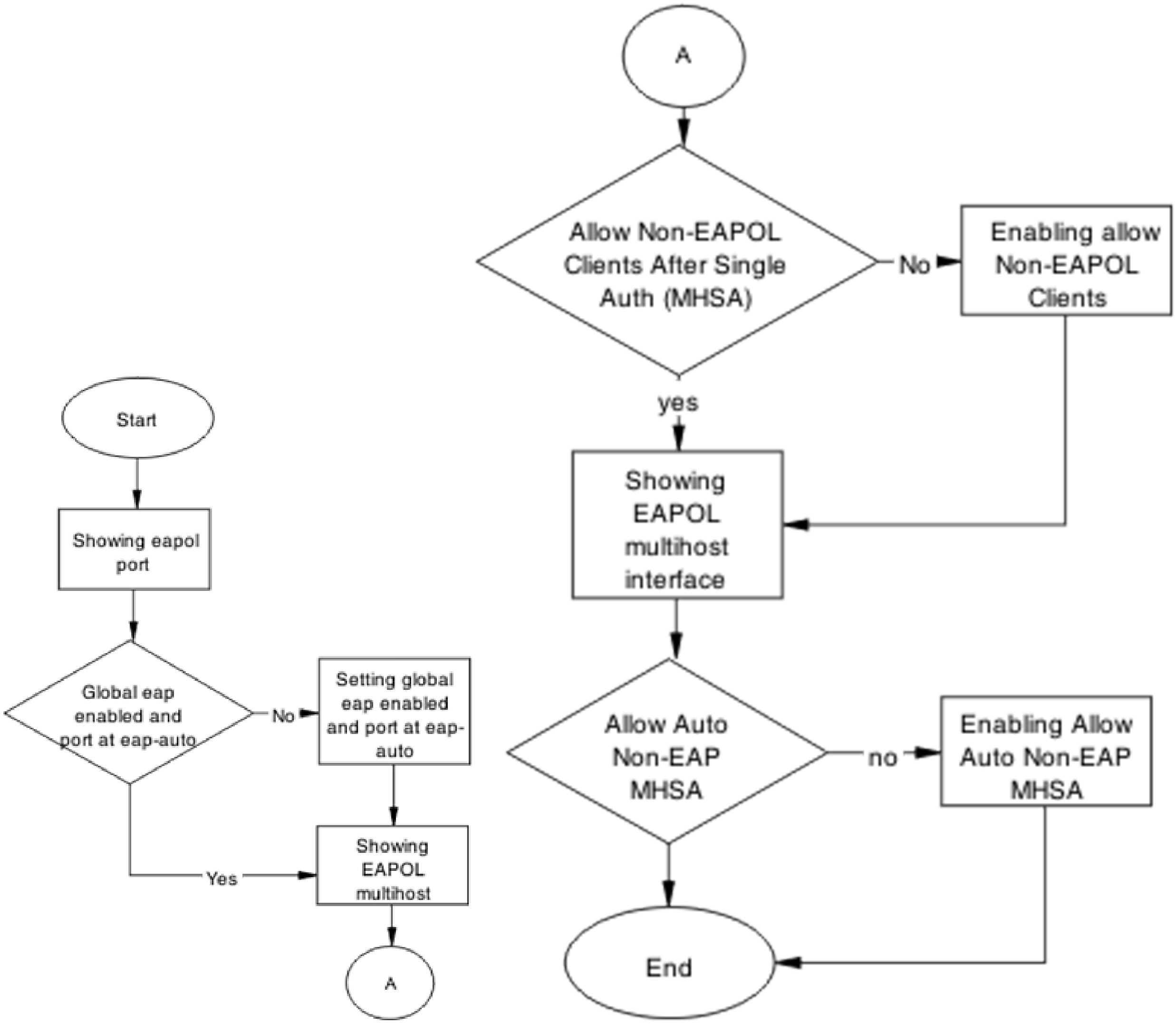

A
Allow Non-EAPOL Clients After Single Auth (MHSA)
No
Enabling allow Non-EAPOL Clients
yes
Start
Showing EAPOL multihost interface
Showing eapol port
Global eap enabled and port at eap-auto
No
Setting global eap enabled and port at eap-auto
Allow Auto Non-EAP MHSA
no
Enabling Allow Auto Non-EAP MHSA
Yes
Showing EAPOL multihost
End
A

Figure 43: Configure switch

Navigation

- Showing EAPOL port on page 85
- Setting global EAP enabled and port at eap-auto on page 86
- Showing EAPOL multihost on page 86
- Formatting non-EAPOL RADIUS password attribute on page 86
- Showing EAPOL multihost interface on page 87
- Enabling RADIUS to auth non-EAP MACs on page 87

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.

Setting global EAP enabled and port at eap-auto

Make the required changes to ensure that EAP is enabled globally and that the port 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

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 `IpAddr.MACAddr.PortNumber`.

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.

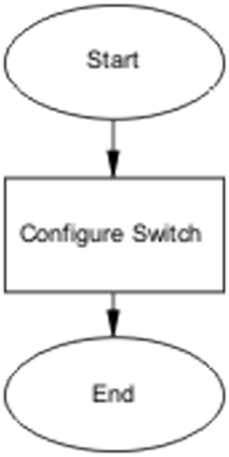


Figure 44: EAP–non-EAP unexpected port shutdown

Navigation

- Configure switch on page 88

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.

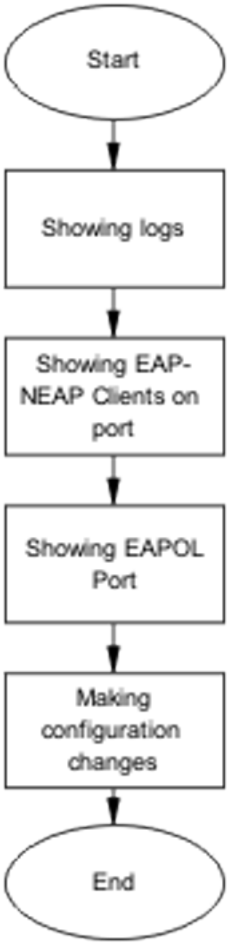

Start
Showing logs
Showing EAP-NEAP Clients on port
Showing EAPOL Port
Making configuration changes
End

Figure 45: Configure switch

Navigation

- Showing Logs on page 89
- Showing EAP–non-EAP clients on port on page 90
- Showing EAPOL port information on page 90
- Making changes on page 90

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 `eap-force-unauthorised` 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.