Troubleshooting
Avaya Ethernet Routing Switch 4500 Series

5.4
NN47205-700, 03.02
December 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

“Documentation” means information published by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya generally makes available to users of its products. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of documentation unless such modifications, additions, or deletions were performed by Avaya. End User agrees 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 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 its Hardware and Software (“Product(s)”). 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://support.avaya.com. Please note that if you acquired the Product(s) 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

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO/ ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AUTHORIZED AVAYA RESELLER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED AVAYA RESELLER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA AUTHORIZED RESELLER; AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE (“AVAYA”).

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, or Hardware provided by Avaya. All content on this site, the documentation and the Product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

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://support.avaya.com/Copyright.

Trademarks

The trademarks, logos and service marks (“Marks”) displayed in this site, the Documentation 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 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 non-Avaya trademarks are the property of their respective owners, and “Linux” is a registered trademark of Linus Torvalds.

Downloading Documentation

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

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://support.avaya.com.

Contents

Chapter 1: New in this release

The following sections detail what's new in *Avaya Ethernet Routing Switch 4500 Series Troubleshooting* (NN47205-700) for Release 5.3:

Features

See the following sections for information about features.

MAC Flush

Avaya Ethernet Routing Switch 4500 Series, Release 5.3, introduces MAC Flush. See MAC Flush on page 28.

MLT/DMLT trunk

Avaya Ethernet Routing Switch 4500 Series, Release 5.3, introduces MLT/DMLT trunk. See MLT/DMLT trunk on page 29.

ASCII download log enhancement

Avaya Ethernet Routing Switch 4500 Series, Release 5.3, introduces the ASCII download log feature to log failed commands. See ASCII download log enhancement on page 24.

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

Avaya Ethernet Routing Switch 4500 Series, Release 5.3, introduces SNMP traps for DHCP Snooping, Dynamic ARP Inspection, and IP Source Guard. See SNMP traps for DHCP Snooping, Dynamic ARP Inspection, and IP Source Guard on page 30.

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

Ethernet Routing Switch 4500 Series, Release 5.3, introduces SNMP traps for DHCP Snooping, Dynamic ARP Inspection, and IP Source Guard. See SNMP traps for DHCP Snooping, Dynamic ARP Inspection, and IP Source Guard on page 30.

Other changes

Stack loopback testing Updated the section Stack loopback testing with technical content. For more information about Stack loopback testing see Stack loopback testing on page 19.

Chapter 2: Introduction

This document is the first troubleshooting guide for the Avaya Ethernet Routing Switch 4500 Series software Release v5.1.

Use this document to help you troubleshoot the Avaya Ethernet Routing Switch 4500 Series software Release v5.2.

Use this document to help you troubleshoot the Avaya Ethernet Routing Switch 4500 Series software Release v5.3.

This document :

- Describes the diagnostic tools and utilities available for troubleshooting the Avaya Ethernet Routing Switch 4500 Series products using the Avaya Command Line Interface (ACLI).
- 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 Avaya Ethernet Routing Switch 4500 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 Avaya Ethernet Routing Switch 4500 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 some 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 4500 Series Documentation Roadmap* (NN47205-101) to familiarize yourself with the documentation set, so you know where to get information as you need it.

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

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

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

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

- Monitor your network over a period of time sufficient to allow you to obtain statistics and data to see patterns in the traffic flow, such as which devices are typically accessed or when peak usage times occur.
- Use a baseline analysis as an important indicator of overall network health. A baseline view of network traffic as it typically is during normal operation is a reference that you can compare to network

traffic data that you capture during troubleshooting. This speeds the process of isolating network problems.

Chapter 4: Troubleshooting tools

This section describes available troubleshooting tools and their applications.

Port mirroring

Avaya Ethernet Routing Switch 4500 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. After port mirroring is enabled, the ingress or egress packets of the mirrored (source) port are forwarded normally and a copy of the packets is sent from the mirrored port to the mirroring (destination) port. Although you can configure Avaya Ethernet Routing Switch 4500 Series to monitor both ingress and egress traffic, some restrictions apply:

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

You can also monitor traffic for specified MAC addresses.

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

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

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

Port mirroring commands

See *Avaya Ethernet Routing Switch 4500 Series Configuration — System Monitoring* (NN47205-502) 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 about received and transmitted packets at the ports. The ingress and egress counts occur at the MAC layer. Count updates occur once every second.

For more information regarding port statistics and commands, see *Avaya Ethernet Routing Switch 4500 Series Configuration — System Monitoring* (NN47205-502).

Stack loopback testing

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

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

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

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

For more detail regarding stack loopback testing, see *Avaya Ethernet Routing Switch 4500 Series Configuration — System Monitoring* (NN47205-502).

Stack health check

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

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

For detailed information about stack health check, see *Avaya Ethernet Routing Switch 4500 Series Configuration — System Monitoring* (NN47205-502).

Stack Forced Mode

The Avaya Ethernet Routing Switch 4500 Series may enter Stack Forced Mode (if configured as such) after a stack of two units breaks into one or two standalone switches. The Stack Forced Mode operation allows the standalone device that comes out of a broken stack of two to be managed using the previous stack IP address. After a stack of two fails, you have access to a device without the need of a standalone IP address.

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

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

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

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

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

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

. The

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

represents the device MAC address.

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

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

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

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

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

   ```
   Forced-Stack Mode: Disabled

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

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

```
Forced-Stack Mode: Enabled

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

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

```
Forced-Stack Mode: Enabled

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

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

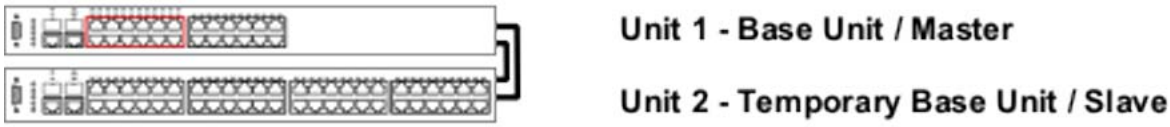


Figure 1: Forced stack mode example setup

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

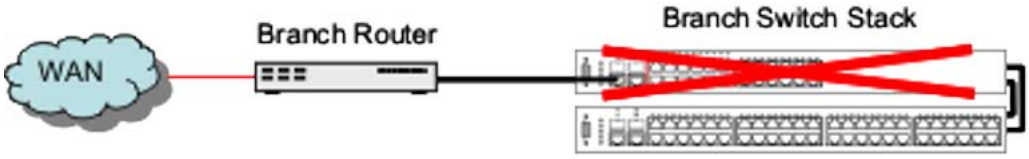


Figure 2: Remote Branch Office - Failure Scenario 1

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

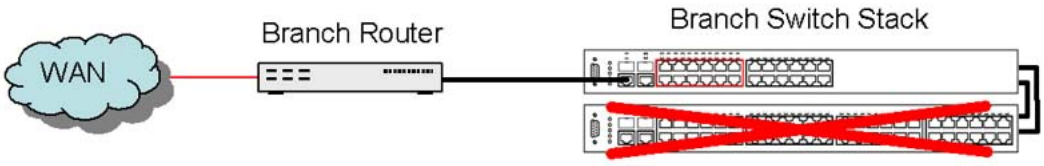


Figure 3: Remote Branch Office - Failure Scenario 2

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

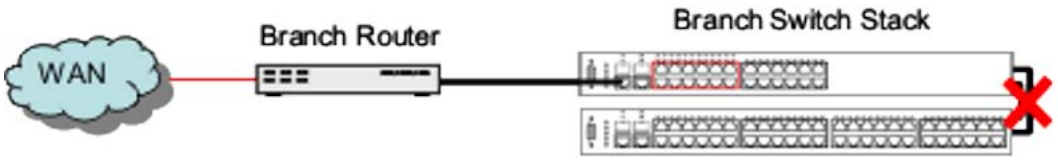


Figure 4: Remote Branch Office – Failure Scenario 3

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

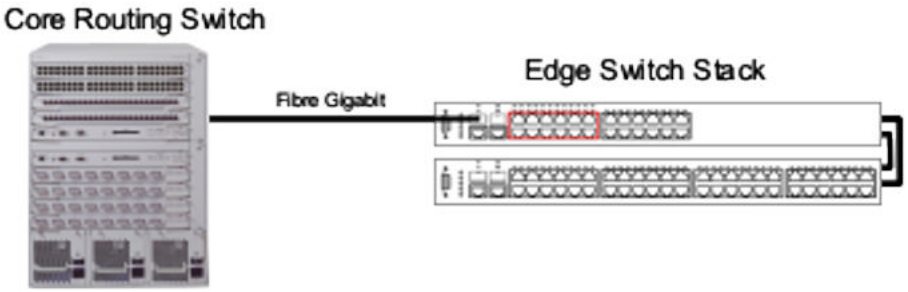


Figure 5: Wiring Closet Deployment 1

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

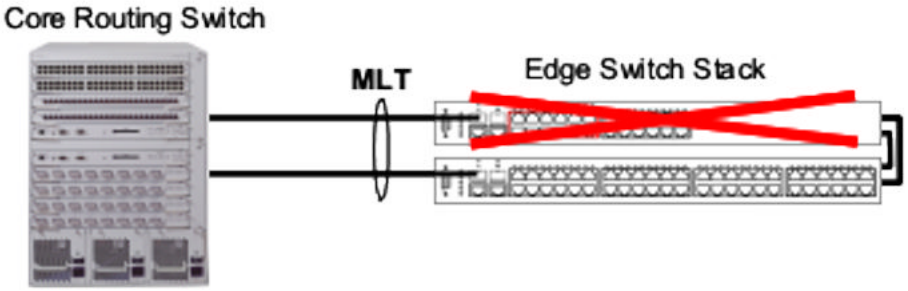


Figure 6: Wiring Closet Deployment 2 – Failure Scenario 1

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

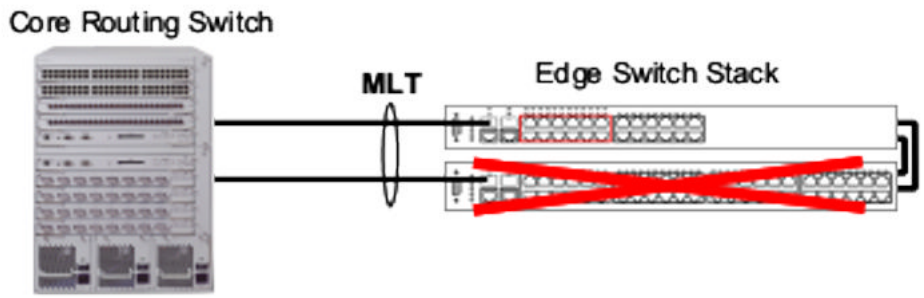


Figure 7: Wiring Closet Deployment 2 – Failure Scenario 2

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

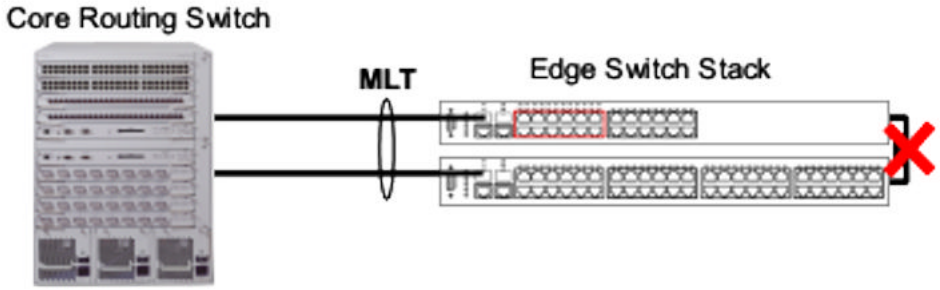


Figure 8: Wiring Closet Deployment 2 – Failure Scenario 3

System logs

You can use the syslog messaging feature of the Avaya Ethernet Routing Switch 4500 Series products to manage event messages. The Avaya Ethernet Routing Switch 4500 Series syslog software communicates with a server software component named 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 Avaya Ethernet Routing Switch 4500 Series device running in a network accessible to the workstation.

For more information about system logging, see *Avaya Ethernet Routing Switch 4500 Series Configuration — System Monitoring* (NN47205-502).

Backup config file

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

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

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

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

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

The following messages are loaded to the engineering log menu:

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

ASCII download log enhancement

The purpose of the ASCII Download Log feature is to log messages for describing the result of the ASCII Configuration File download, especially the failed commands, as informational customer messages.. You can log four hundred customer messages in Dynamic random access memory (DRAM).

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

- Connection error (ACG_DOWNLOAD_ERROR)—the connection failed and the ASCII configuration file can not be accessed or used. The message contains the cause of the error. The interface you use to start the ASCII file download does not matter. The logged message is the one from ACLI. The system logs an ACG_DOWNLOAD_ERROR error message for the following situations:

- Transfer Timed Out
- Invalid TFTP Server address
- Configuration failed
- Switch IP not set
- Stack IP not set
- TFTP Server address not set
- Mask not set
- File too large
- Invalid Configuration File
- Invalid Configuration File or File not found
- Error accessing ASCII file, file missing or can’t access USB device

- Connection error on load on boot (ACG_DOWNLOAD_ERROR_ ON_BOOT)—the connection failed at load on boot and the ASCII Configuration File can not be accessed. The IP and the filename is in the message if you use TFTP server, or the filename if you use USB .The message contains the cause of the error. If the IP number is unknown, the system uses the question mark character (?).
- Success (ACG_DOWNLOAD_OK)—the connection was successful. The ASCII Configuration File can be accessed and it can be used. The IP and the filename is in the message when you use TFTP server , or the filename when you use USB .
- Success on load on boot (ACG_DOWNLOAD_OK_ON_BOOT)—the connection was successful at load on boot. The ASCII Configuration File can be accessed and it can be used. The IP and the filename is in the message if you use a TFTP server usage, or the filename if you use USB .
- Failed command (ACG_CMD_ERR)—a command from the ASCII Configuration File failed. The failed command text line number is in the message. The cause is in the message with the following errors:
  - Invalid input detected
  - Ambiguous command
  - Incomplete command
  - Permission denied
  - Not allowed on slave

CPU and memory utilization

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

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

This feature is supported by both ACLI and Web-based management. For more information about the feature, see *Avaya Ethernet Routing Switch 4500 Series Configuration — System Monitoring* (NN47205-502).

Show commands

The **`show tech`** command has been enhanced to display more information. The show commands that are incorporated are as follows:

- show mac-address-table
- show ip route
- show ip arp
- show ip dhcp-relay
- show lacp aggr
- show lacp port
- show ipv address
- show ipv interface

Address Resolution Protocol

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

Caution:
Every time an IP interface or link goes up, the driver for that interface will typically send a gratuitous ARP to preload the ARP tables of all other local hosts. A gratuitous ARP will tell

us that host just has had a link up event, such as a link bounce, a machine just being rebooted or you are just configuring the interface up. If you see multiple gratuitous ARPs from the same host frequently, it can be an indication of bad Ethernet hardware or cabling resulting in frequent link bounces.

Dynamic ARP inspection

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

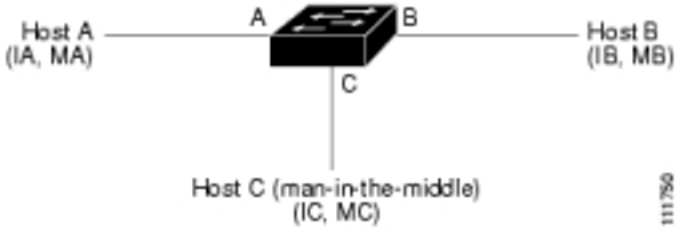


Figure 9: Dynamic ARP inspection

In the preceding figure, hosts A, B, and C are connected to the switch on interfaces A, B, and C, all of which are on the same subnet. Their IP and MAC addresses are shown in parentheses; for example, host A uses IP address IA and MAC address MA. After Host A needs to communicate to Host B at the IP layer, it broadcasts an ARP request for the MAC address associated with IP address IB. After the switch and Host B receive the ARP request, they populate their ARP caches with an ARP binding for a host with the IP address IA and a MAC address MA. After Host B responds, the switch and Host A populate their ARP caches with a binding for a host with the IP address IB and a MAC address MB.

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

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

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

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

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

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

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

The following ACLI commands are used for Dynamic ARP Inspection:

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

MAC Flush

The Avaya Ethernet Routing Switch 4500 Series Release 5.3 supports MAC Flush. MAC Flush is a direct way to flush out MAC addresses from the MAC table. If the Layer 2 Forwarding Database (FDB) appears corrupted, you can:

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

- per VLAN
- across the whole switch

The following ACLI commands are used for MAC Flush:

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

MLT/DMLT trunk

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

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

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

From Release 5.3 onward, the switch generates SNMP traps for the following:

- DHCP Snooping
- IP Source Guard
- Dynamic ARP Inspection

From Release 5.3 onward, the switch generates the following additional trap notifications:

- `send_bsaiArpPacketDroppedOnUntrustedPort_trap`

  - generated when there is an invalid IP/MAC binding

- `send_bsSourceGuardReachedMaxIpEntries_trap`

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

- `send_bsSourceGuardCannotEnablePort_trap`

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

- `send_bsDhcpSnoopingBindingTableFull_trap`

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

- `send_bsDhcpSnoopingTrap_trap`

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

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

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

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

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

- bsDhcpSnoopingBindingTableFull
- bsDhcpSnoopingTrap
- bsaiArpPacketDroppedOnUntrustedPort
- bsSourceGuardReachedMaxIpEntries
- bsSourceGuardCannotEnablePort

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

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

Dynamic Host Configuration Protocol Relay (DHCP) relay

The Avaya Ethernet Routing Switch 4500 Series Release 5.2 supports static routes. In order for DHCP servers to talk to clients on different VLANs or subnets, the feature relays client requests to DHCP servers on different Layer 3 VLANs and a relay server replies back to the clients.

The maximum number of client/server pairs that Release 5.2 supports is 256, which is the maximum number of VLANs.

For more information about ACLI and Web-based management of DHCP relay, see *Avaya Ethernet Routing Switch 4500 Series Configuration — IP Routing and Multicast* (NN47205-506).

Auto Unit Replacement

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

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

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

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

For more information about AUR, see *Avaya Ethernet Routing Switch 4500 Series Configuration — System* (NN47205-500).

Diagnostic Auto Unit Replacement (DAUR)

DAUR provides the capability of updating the diagnostic image of the non-base unit with the diagnostic image in the base unit of a stack. This happens if the AAUR feature is enabled in the stack.

DAUR performs an upgrade of the diagnostic image on inserted units in the same way that AAUR performs this function for agent code when AAUR is enabled.

After you enable the AAUR feature, it triggers a DAUR process if a stand-alone unit (with a different version diagnostic image) is connected to the stack.

There are no commands specifically for DAUR; after AAUR is enabled or disabled, DAUR is enabled or disabled.

After you enable AAUR on a stack, and you add another unit with a different software image, the new unit fails to join the stack and enters in stand-alone mode. The new unit sends an AAUR request to its UP-stream port neighbor. If it does not receive an answer, it sends the request on its DOWN-stream port. The switch reboots after the image is properly transferred.

Important:

If the unit is powered off while the diagnostic image is being programmed to the flash, the diagnostic image is corrupted. The only way to recover is to download the diagnostic image using the console serial port. At boot time, press “Shift + 3” to accede to the downloading menu.

If you add a unit that has its base switch set to off to a unit that has the base switch set, the non-base unit retrieves the image from the other unit.

The AAUR enabled/disabled state is ignored for the unit that is added to the stack under the following conditions:

- If a unit with AAUR disabled is added to a stack that has AAUR enabled, then the image transfer process starts.
- If a unit with AAUR enabled is added to a stack that has AAUR disabled, then there is no image transfer.

After the diagnostic image version is updated, an AAUR check is performed. If the added unit has the same agent image as the stack, the unit reboots. Otherwise, an AAUR is performed.

In the case where a unit with Release 5.0 or Release 5.1 software is added to a stack having an agent image that exceeds 6M, the agent transfer is stopped.

You may encounter the following situations:

- A stack is running the Release 5.2 non_ssh software and 5.2 diagnostic image:
  - If the agent image on the added unit is Release 5.0 or 5.1 and the diagnostic version is also Release 5.0 or 5.1, then, because the Release 5.2 image size is less than 6M, AAUR starts the agent image transfer and then the unit reboots. After the reboot, the unit has the new Release 5.2 image that supports DAUR and the 5.2 diagnostic image is transferred. The unit reboots again and joins the stack.
  - If the agent image on the added unit is Release 5.2_ssh software with the Release 5.2.0.1 diagnostic image, then, because both images support DAUR, the new added unit does not join the stack . A diagnostic update is performed and, because the agent images are different, an agent update is also performed, after which the switch reboots. The switch joins the stack after reboot.
- A stack with Release 5.3 or newer and Release 5.3 diagnostic image:
  - If the agent image on the added unit is Release 5.1 or 5.0 and the Release 5.1 or 5.0 diagnostic, then, because the 5.3 image size is greater than 6M, the AAUR transfer is stopped and a serious error message is logged on the Release 5.3 master unit. A manual download must be performed for both the diagnostic and agent images.
  - If the agent image on the added unit is Release 5.2 with the Release 5.2.0.1 diagnostic, then both images support DAUR and the Release 5.2 diagnostic supports images greater than 6M. The new added unit does not join the stack. A diagnostic update is first performed and then, because the agent images are different, an agent update is performed and the switch reboots. The switch joins the stack after reboot .

Note that an agent or diagnostic image update can be an upgrade or a downgrade. There is no DAUR downgrade if the stack image is Release 5.0 or 5.1 (these images do not support DAUR), but AAUR is performed.

A stack with Release 5.1 or 5.0 software and the Release 5.1 or 5.0 diagnostic image

If the agent image on the added unit is Release 5.2 with the Release 5.2.0.1 diagnostic image, the new added unit does not join stack because the stack does not support DAUR. A diagnostic upgrade or downgrade is not performed and, because agent images are

different, an agent downgrade is performed and the switch reboots. The switch joins the stack after reboot .

The following table shows the expected behavior for various combinations of agent and diagnostic images.

Stack master image and diagnostic version	Slave image diagnostic version	Expected behavior
Software 5.0/5.1 Diagnostic 5.0/5.1	Software 5.0/5.1 Diagnostic 5.0/5.1	Same image. Unit joins stack.
	Software 5.0/5.1 Diagnostic 5.2	Same image. Unit joins stack.
Software 5.0/5.1 Diagnostic 5.2	Software 5.2 Diagnostic 5.0/5.1	AAUR is performed. AAUR downgrades the unit image, and then reboots the unit. The unit joins the stack after the reboot. No DAUR performed as DAUR is unavailable on 5.0/5.1
	Software 5.2 Diagnostic 5.2	
Software 5.2_SSH/ non SSH Diagnostic 5.2	Software 5.0/5.1 Diagnostic 5.0/5.1	AAUR is performed. AAUR upgrades the unit image, and then reboots the stack. DAUR upgrades the diagnostic image then reboots the unit. The unit joins the stack after the reboot.
	Software 5.0/5.1 Diagnostic 5.2	AAUR is performed. AAUR upgrades the unit image, and then reboots the unit. The unit joins the stack because the diagnostic images are the same.
	Software 5.2_non SSH/SSH Diagnostic 5.1	Because the diagnostic and agent images are different, DAUR upgrades the diagnostic image, and then AAUR transfers the agent. AAUR and DAUR reboot the unit. The unit joins the stack after the reboot.
	Software 5.2_non SSH/SSH Diagnostic 5.2	AAUR performs the agent image transfer and reboots the unit. The unit joins the stack after the reboot.

The following logs are provided on the unit transferring the image:

- `Informational: DAUR - Info: Send request for new diag image`

  – message logged after a stand-alone unit sends a DAUR request

- `Informational: DAUR - Info: Start receive image`

  – message logged after the unit starts to receive an image

- `Serious: DAUR - Warning: Diag image check sum ERROR`

– message logged after the checksum for the receive image is not the same as the master’s checksum

- `Informational: DAUR - Info: Diag transfer finished`

  – message logged after the image is properly transferred and programmed to flash.

- `Serious: AAUR - Warning: unsupported image size. Please update image manually`

  – message logged after the slave AAUR could not support images greater than 6M.

The following logs are provided on the unit receiving the image:

- `Informational: DAUR - Info: Receive request for diag image. Unable to start transfer`

  – message logged after a unit receives a request for DAUR transfer and it does not start transfer. The possible causes are that the AAUR feature is disabled, that the diagnostic image of the receiving unit is different from the diagnostic image of this unit, or the message was received by a stand-alone unit (which does not have the base unit switch selected).

- `Informational: DAUR - Info: Receive request for diag image, start transfer`

  – message logged after a unit receives a request for DAUR transfer and it starts transfer.

- `Informational: DAUR - Info: Diag transfer finished`

  – message logged after the image is properly transferred.

- `Informational: DAUR - Info: Slave refuse transfer`

  – message logged when a slave unit refuses diagnostic transfer.

- `Serious: DAUR - Warning: Slave diag image check sum ERROR`

  – message logged when the slave announces that the checksum was wrong.

Multicast behavior

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

After the switch learns that a client wants a particular stream, it stops flooding the stream to all ports, and sends only to the client that requested it.

However, if no clients request the stream, and the switch has not learned the multicast address for the stream, the stream has an unknown multicast address. The switch broadcasts the traffic to all ports.

This is normal behavior. You can disable multicast flooding using the **`unknown-mcast-no-flood enable`** command.

IPv6

IPv6 provides dual-stack configuration that allows both IPv4 and IPv6 protocol stacks to run simultaneously. Release 5.2 supports IPv6 for management purposes only.

Running IPv6 is optional. Release 5.2 provides a maximum of one IPv6 interface for the management VLAN only. The IPv6 interface must be enabled on the management VLAN and IPv6 globally enabled on the IPv6 stack.

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

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

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

For detailed information about IPv6, see *Avaya Ethernet Routing Switch 4500 Series Configuration — System* (NN47205-500).

Light Emitting Diode (LED) display

The Avaya Ethernet Routing Switch 4500 Series displays diagnostic and operation information through the LEDs on the unit. Familiarize yourself with the interpretation of the LEDs on the 4500 series device. See the technical document *Avaya Ethernet Routing Switch 4500 Series — Installation* (NN47205-300) for detailed information regarding the interpretation of the LEDs.

NSNA passive device behavior

If you remove a PC or passive device from behind a phone and plug that PC or passive device behind another phone, the **`show nsna client`** command displays the PC or passive device MAC address twice until you plug another device into the first phone.

This is normal behavior and does not indicate a problem.

The following example shows an output from the command that demonstrates the behavior.

```
4526GTX-PWR(config)#show nsna client
Total Number of Clients:  5

Unit/Port  Device Client MAC     Filter Type  Vlan ID    Vlan ID    IP Address      Exp
---------------------------------------------------------------------------------------
1/9        00:0f:ea:ef:33:68     Passive      210 (R)    210 (R)    10.100.210.117  Yes
1/9        00:19:e1:e3:a4:51     IP Phone     240 (V)    210 (R)    10.100.240.10   No
3/16       00:0a:e4:0b:47:44     IP Phone     240 (V)    230 (G)    10.100.240.12   No
3/16       00:0f:ea:ef:33:68     Passive      210 (R)    230 (G)    10.100.210.117  No
```

Figure 10: Command output example

The device with MAC address 00:0f:ea:ef:33:68 was removed from the IP phone on unit one, port nine. The device was then connected to the IP phone on unit three, port sixteen. The MAC address of the device remains visible on unit one, port nine until a new device is connected to that port, after which the display shows the new MAC address.

NSNA and filter use

Avaya recommends that you carefully manage the number of applications that require filters and that run on the switch simultaneously. For example, Avaya recommends that applications such as IP Source Guard be applied to a small number of ports when used along with the NSNA solution because both applications rely on filters to function correctly.

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 4500 Series device has diagnostic features available through DM, ACLI, and Web-based Management. You can use these diagnostic tools to help you troubleshoot operational and configuration issues. You can configure and display files, view and monitor port statistics, trace a route, run loopback and ping tests, test the switch fabric, and view the address resolution table.

This document focuses on using 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.

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

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.

You can move between command modes on a limited basis. For more information about the ACLI command modes, see *Avaya Ethernet Routing Switch 4500 Series Fundamentals* (NN47205-102).

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 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 that is running on all devices.
- A **`network topology diagram`**: Get an accurate and detailed topology diagram of your network that shows the nodes and connections. Your planning and engineering function should have this diagram.
- **`Recent changes`**: Find out about recent changes or upgrades to your system, your network, or custom applications (for example, has configuration or code been changed). Get the date and time of the changes, and the names of the persons who made them. Get a list of events that occurred prior to the trouble, such as an upgrade, a LAN change, increased traffic, or installation of new hardware.
- **`Connectivity information`**: To help troubleshoot connectivity problems, you should always provide source and destination IP pairs to facilitate in troubleshooting. Ten pairs

is a good rule of thumb (five working pairs and five pairs with connectivity issues). Use the following commands to get connectivity information:

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

Chapter 7: Emergency recovery trees

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

Emergency recovery trees

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.

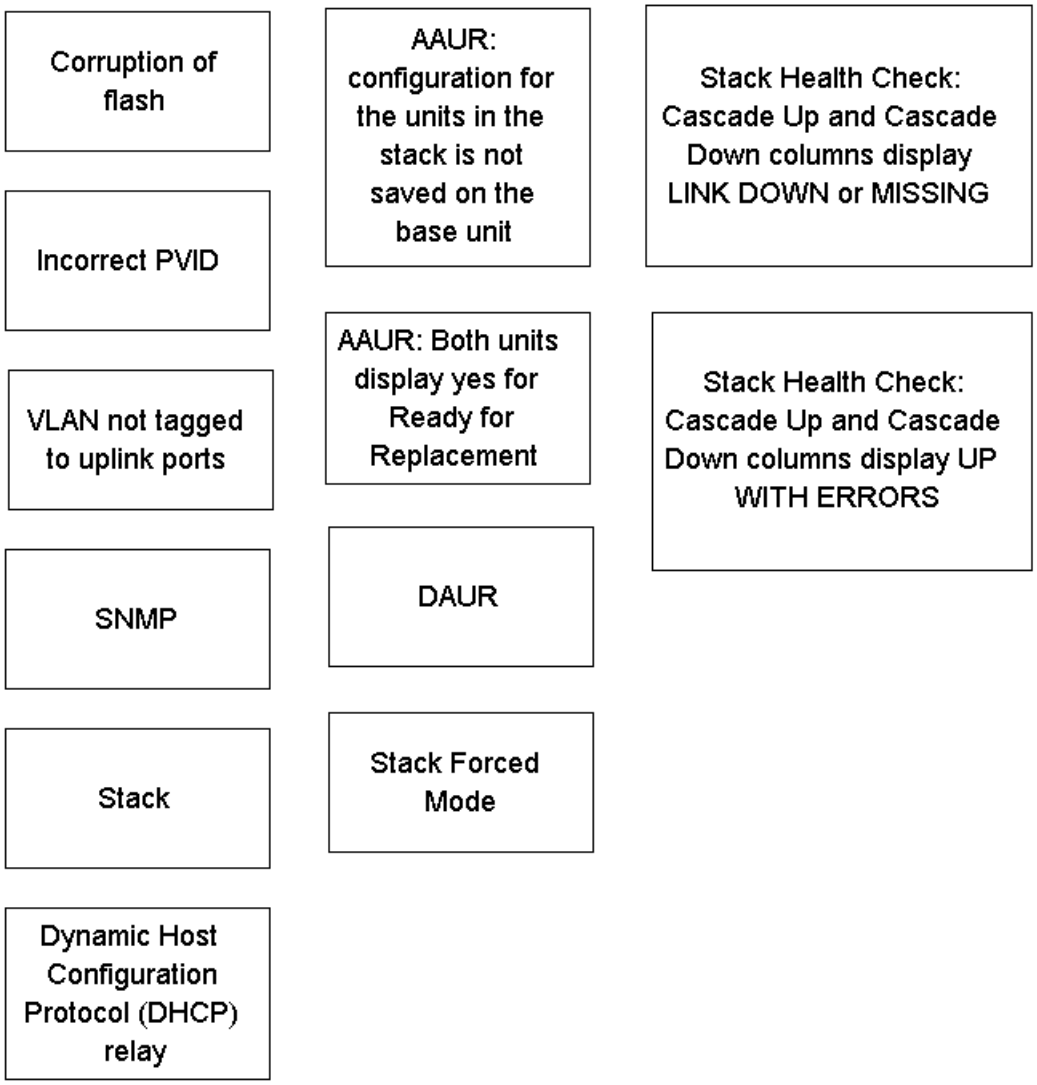


Figure 11: Emergency recovery trees

Navigation

- Corruption of flash on page 45
- Incorrect PVID on page 46
- VLAN not tagged to uplink ports on page 47

Corruption of flash

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

Corruption of flash recovery tree

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

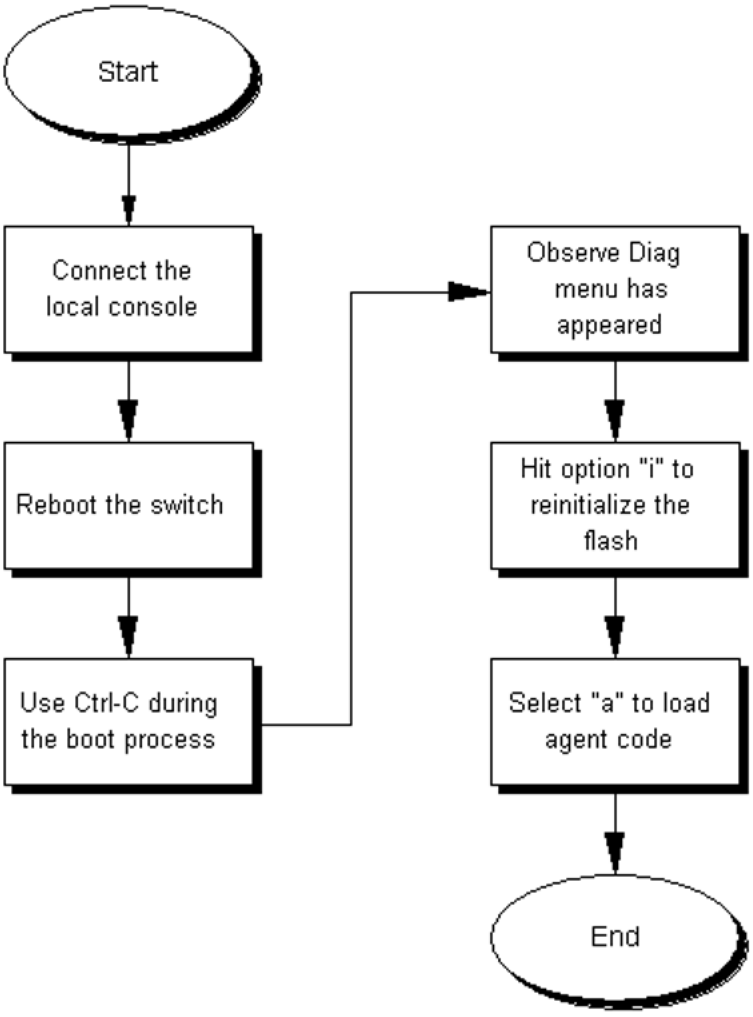


Figure 12: Corruption of flash

Incorrect PVID

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

Incorrect PVID recovery tree

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

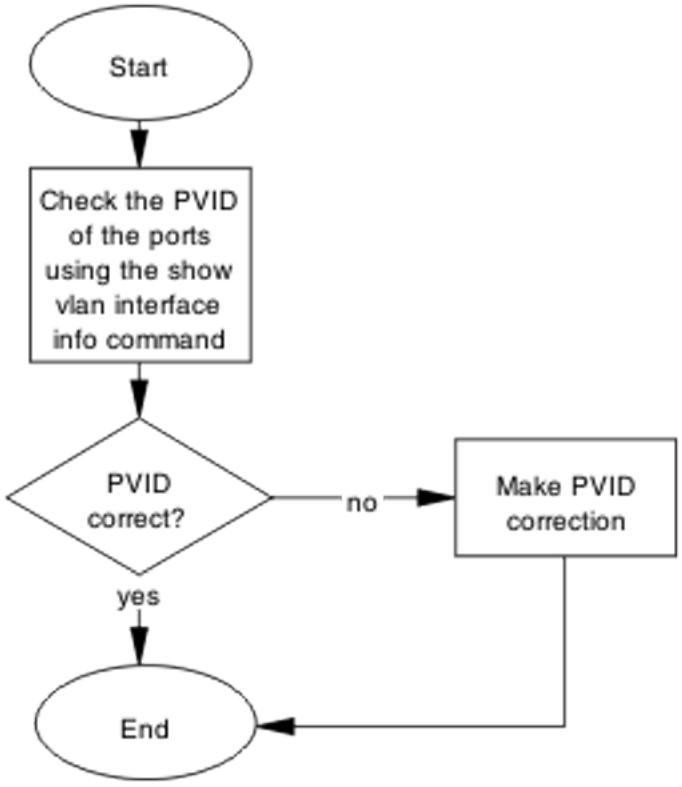


Figure 13: Incorrect PVID

VLAN not tagged to uplink ports

After a 4500 Series switch is connected to an 8600 Series switch and devices in a VLAN on the 8600 Series switch are unable to communicate with devices at the 4500 Series switch in the same VLAN, then it is likely that the uplink ports are not tagged to the VLAN on the 4500 Series switch.

VLAN not tagged to uplink ports recovery tree

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

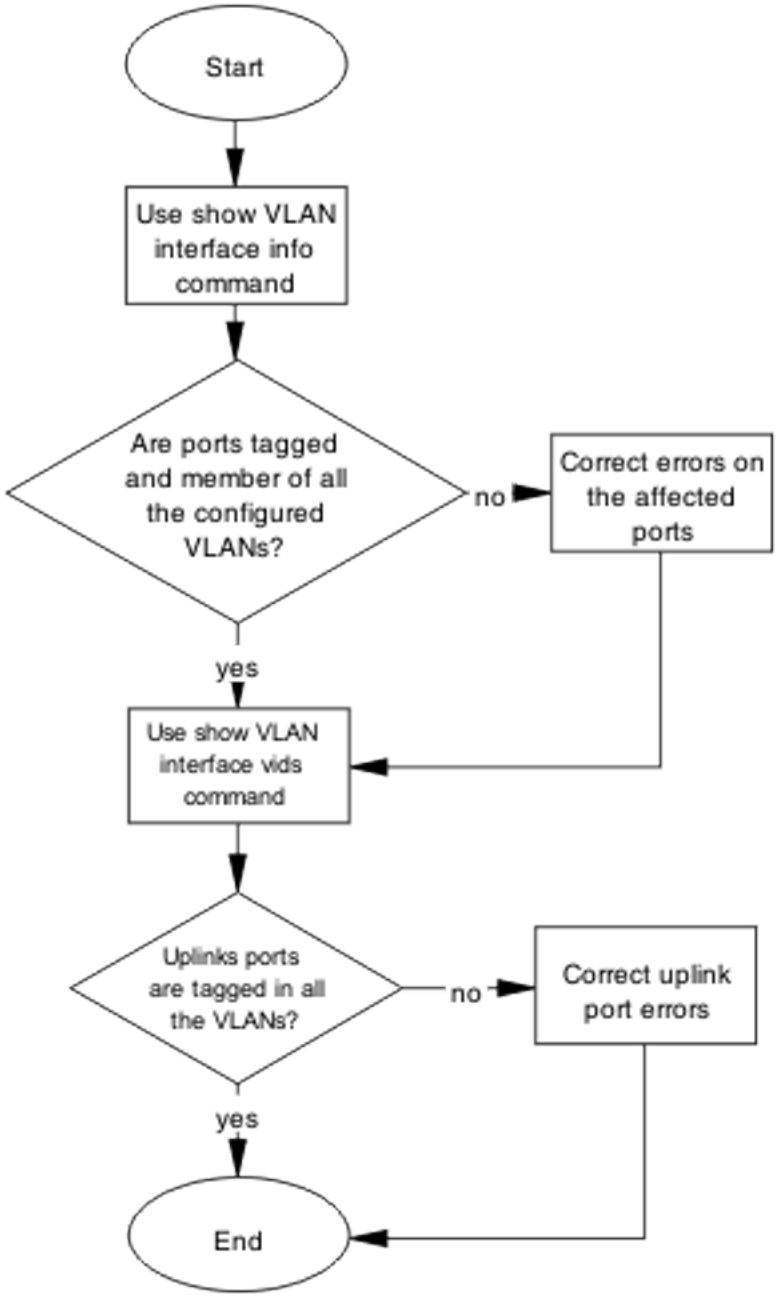


Figure 14: VLAN not tagged to uplink ports

SNMP

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

SNMP recovery tree

The following figures show the SNMP recovery tree.

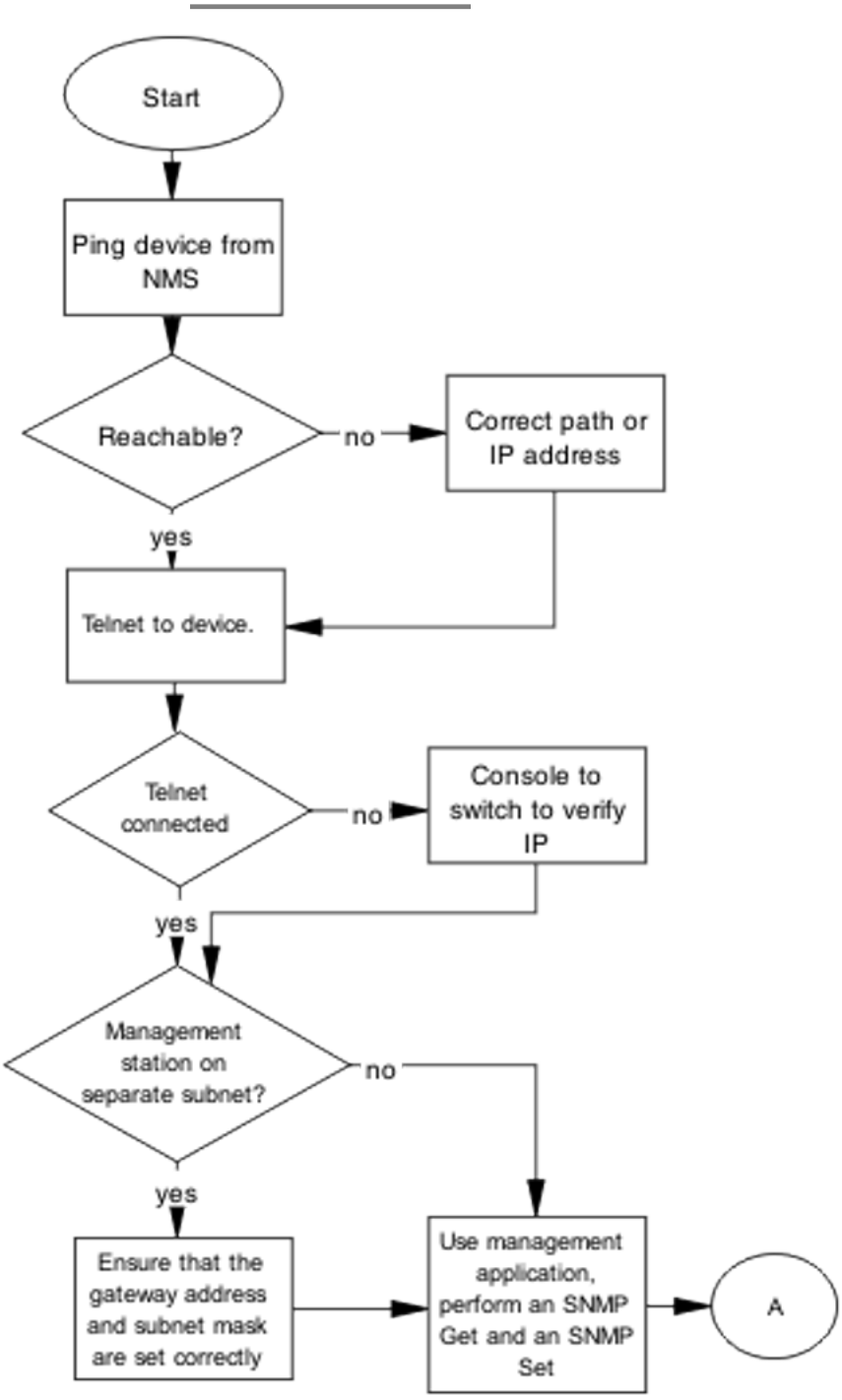


Figure 15: SNMP part 1

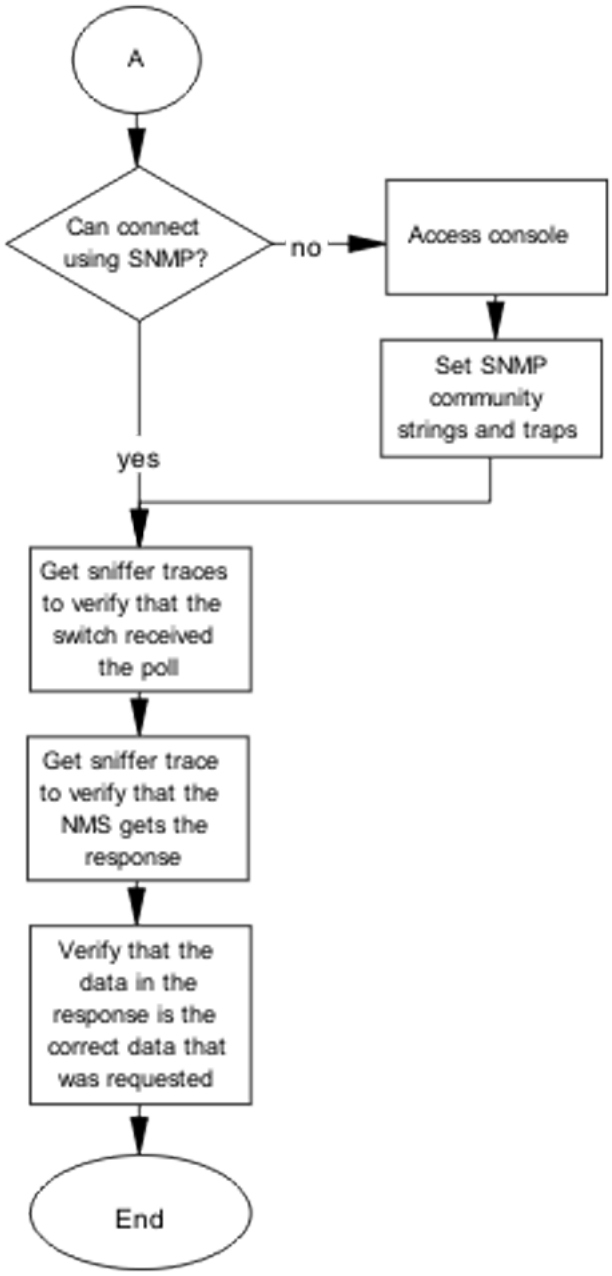


Figure 16: SNMP part 2

Stack

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

Several situation may cause stacking problems, for example:

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

Stack recovery tree

The following figures show the stack recovery tree.

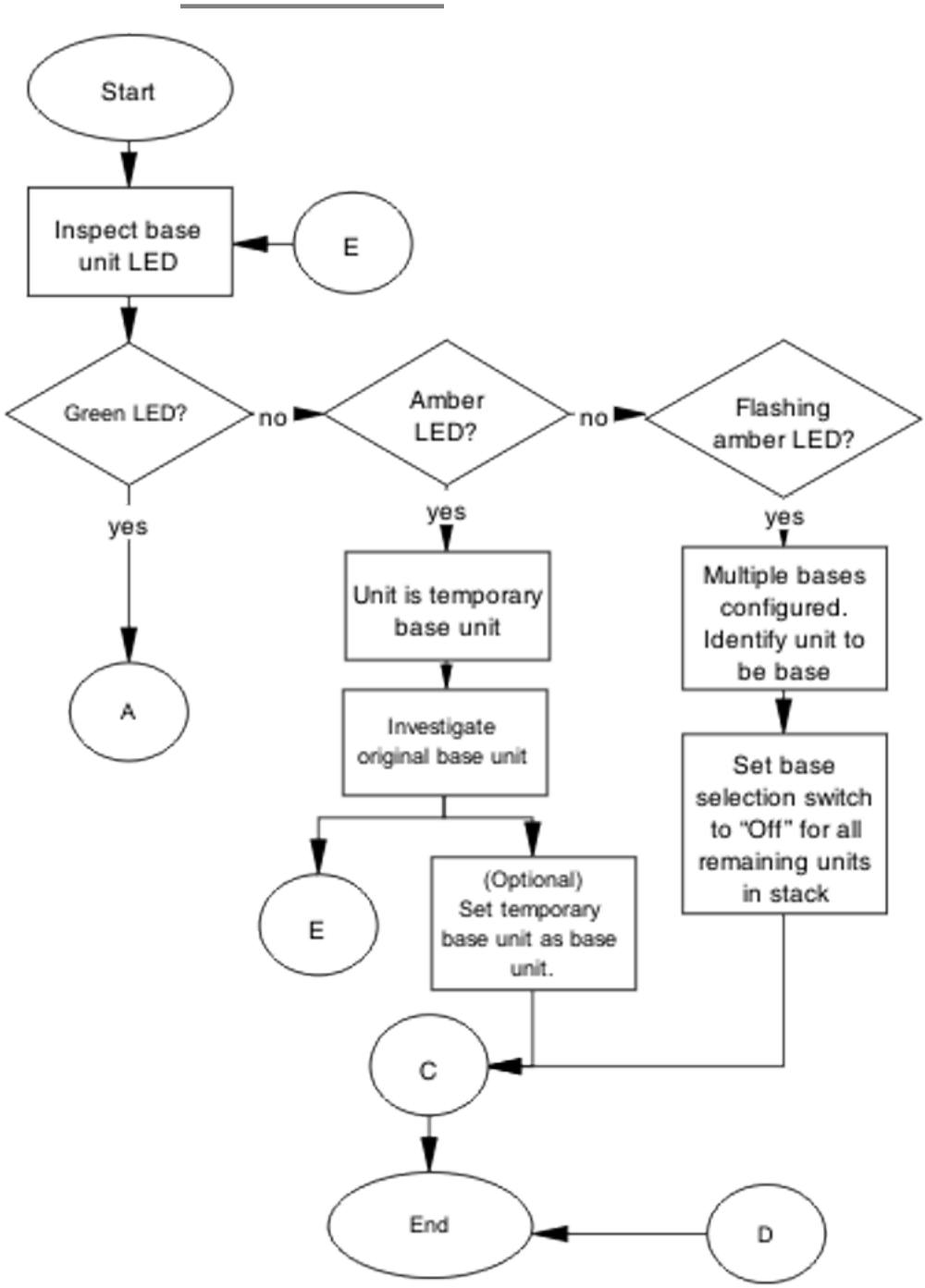


Figure 17: Stack part 1

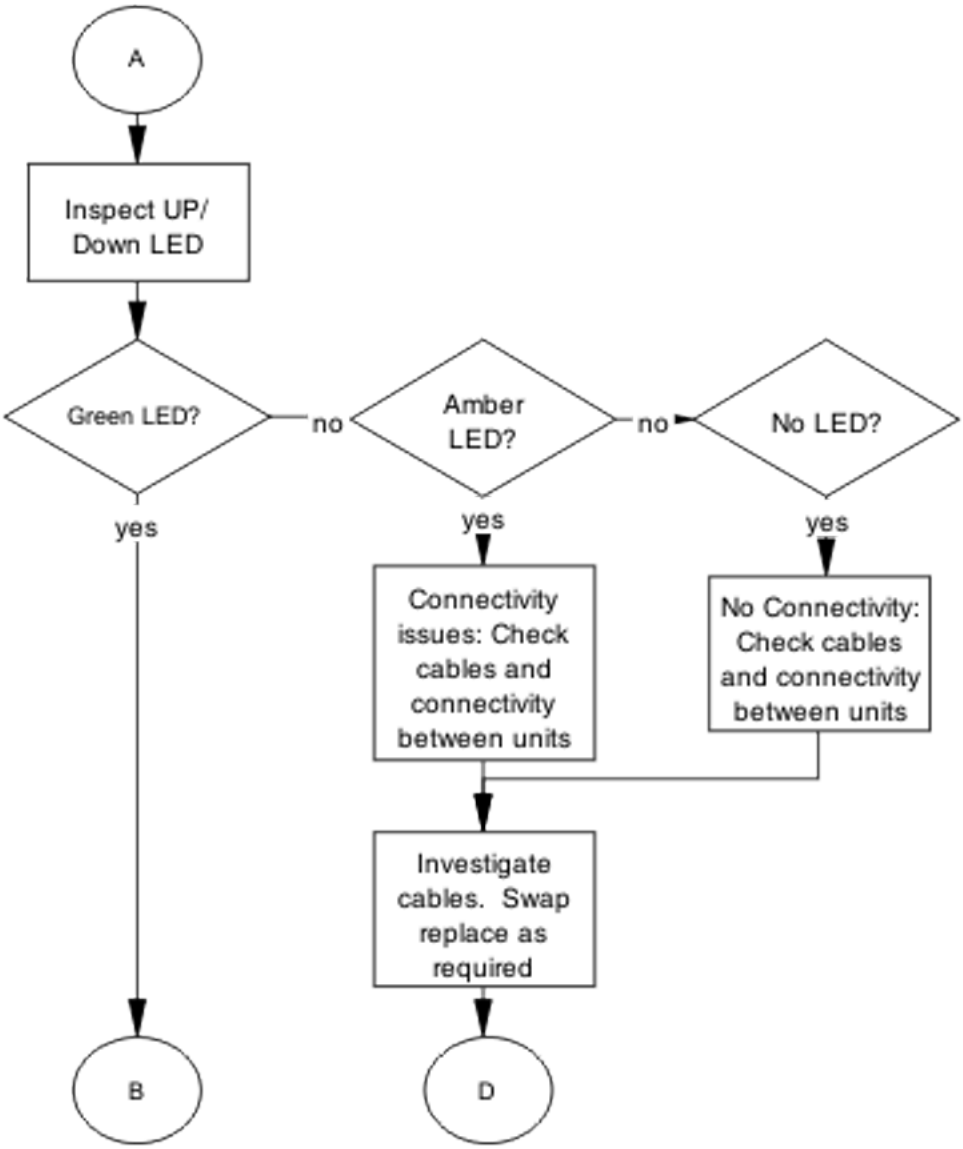


Figure 18: Stack part 2

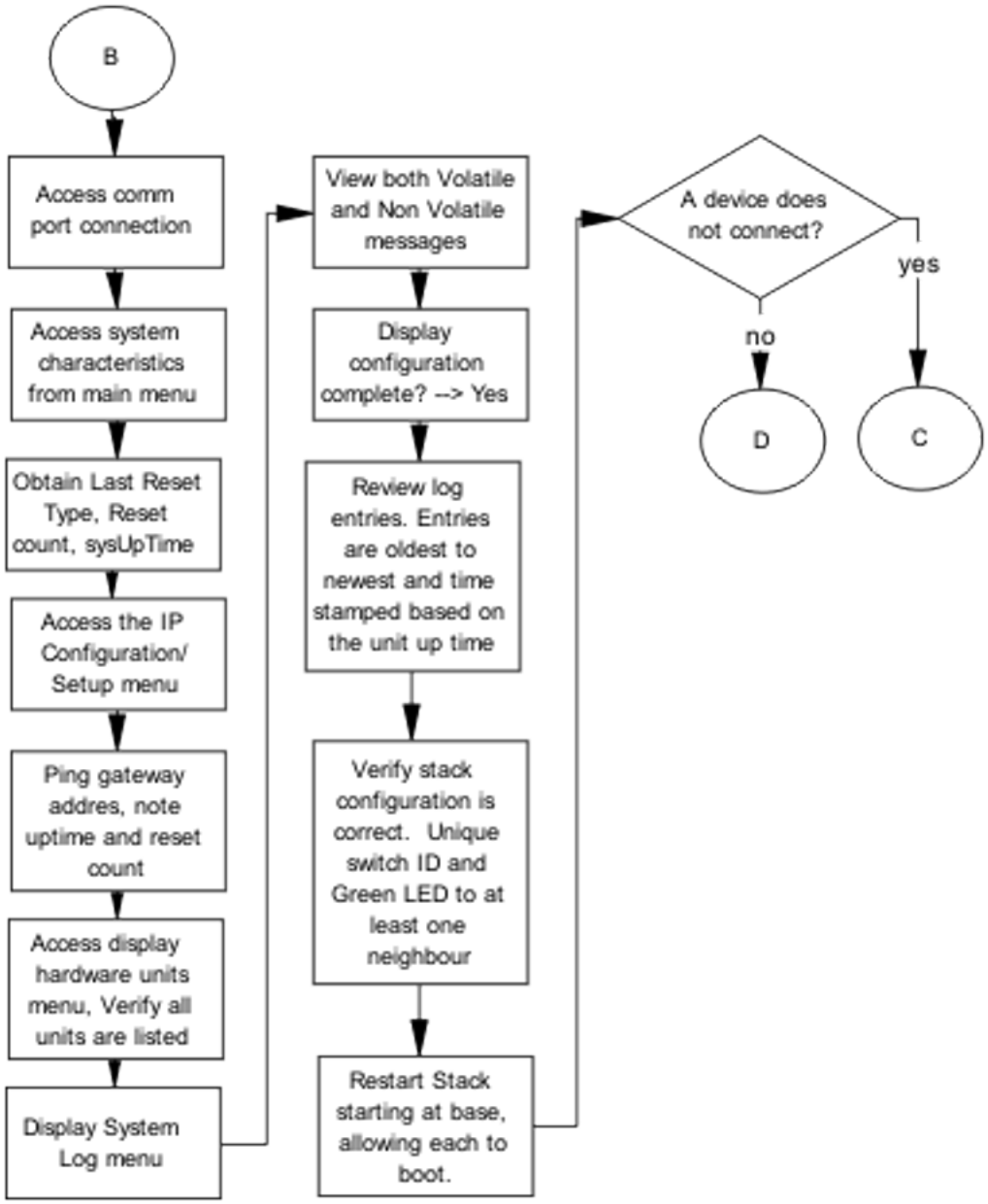


Figure 19: Stack part 3

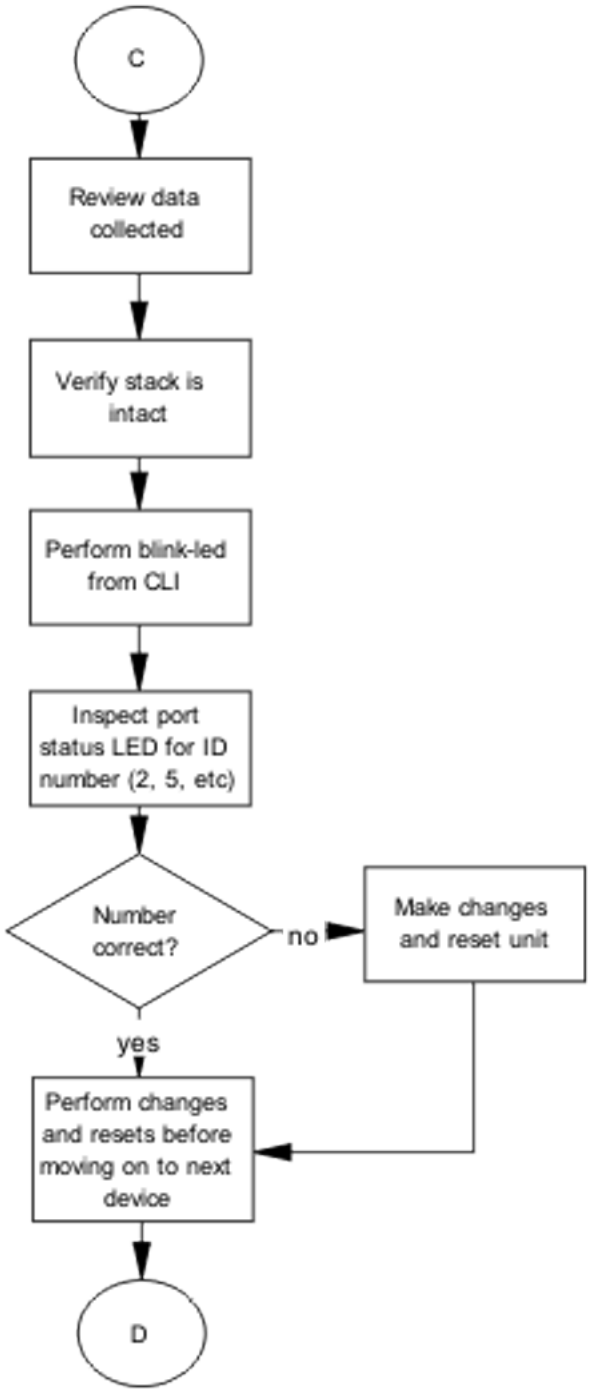


Figure 20: Stack part 4

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

The following figure shows the DHCP relay recovery tree.

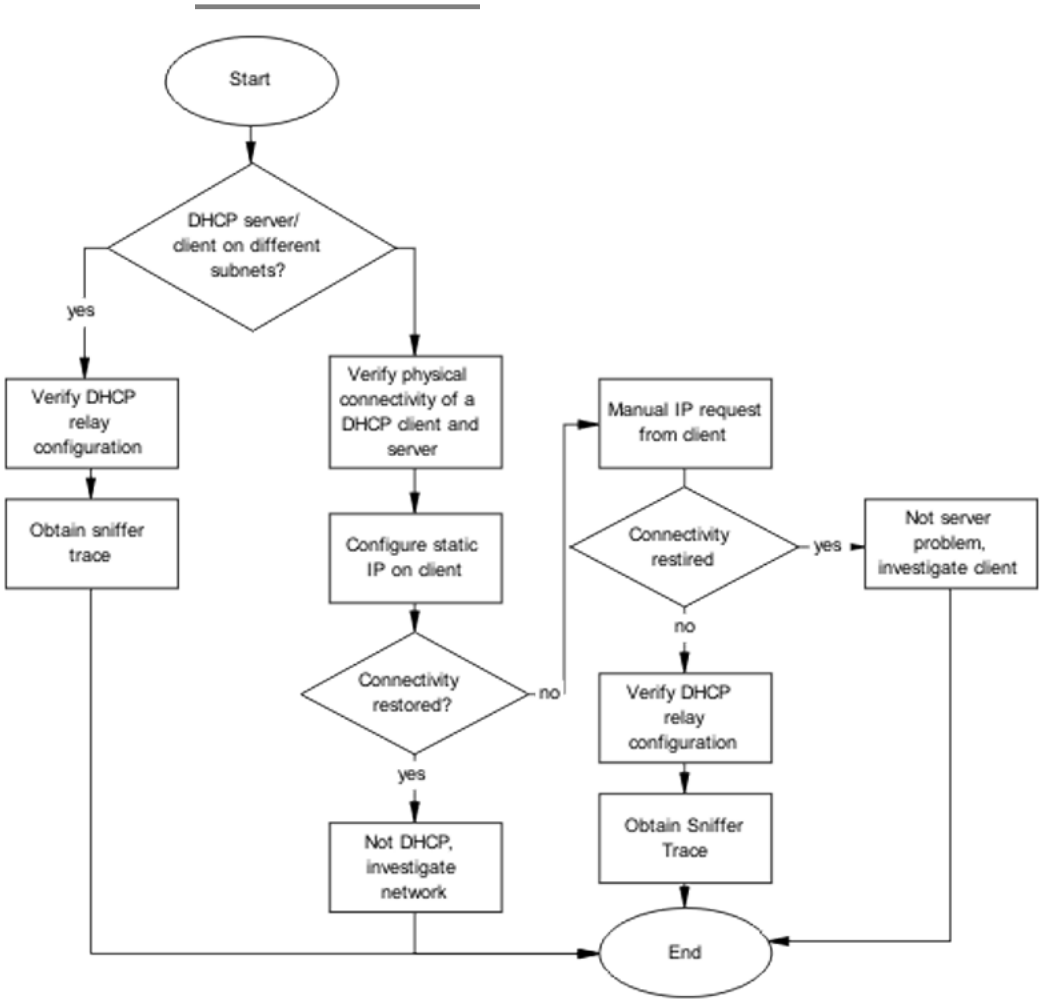


Figure 21: DHCP

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

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.

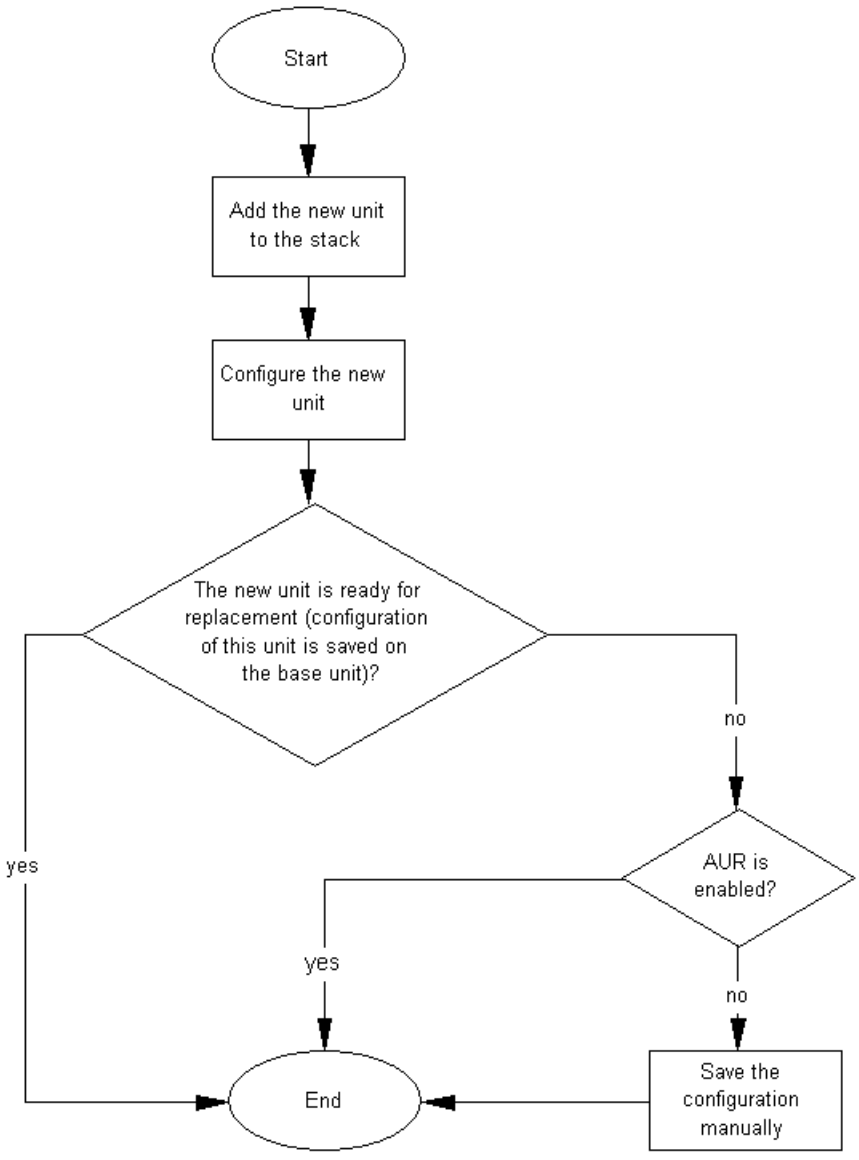


Figure 22: Configuration for the units in the stack is not saved on the base unit

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

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.

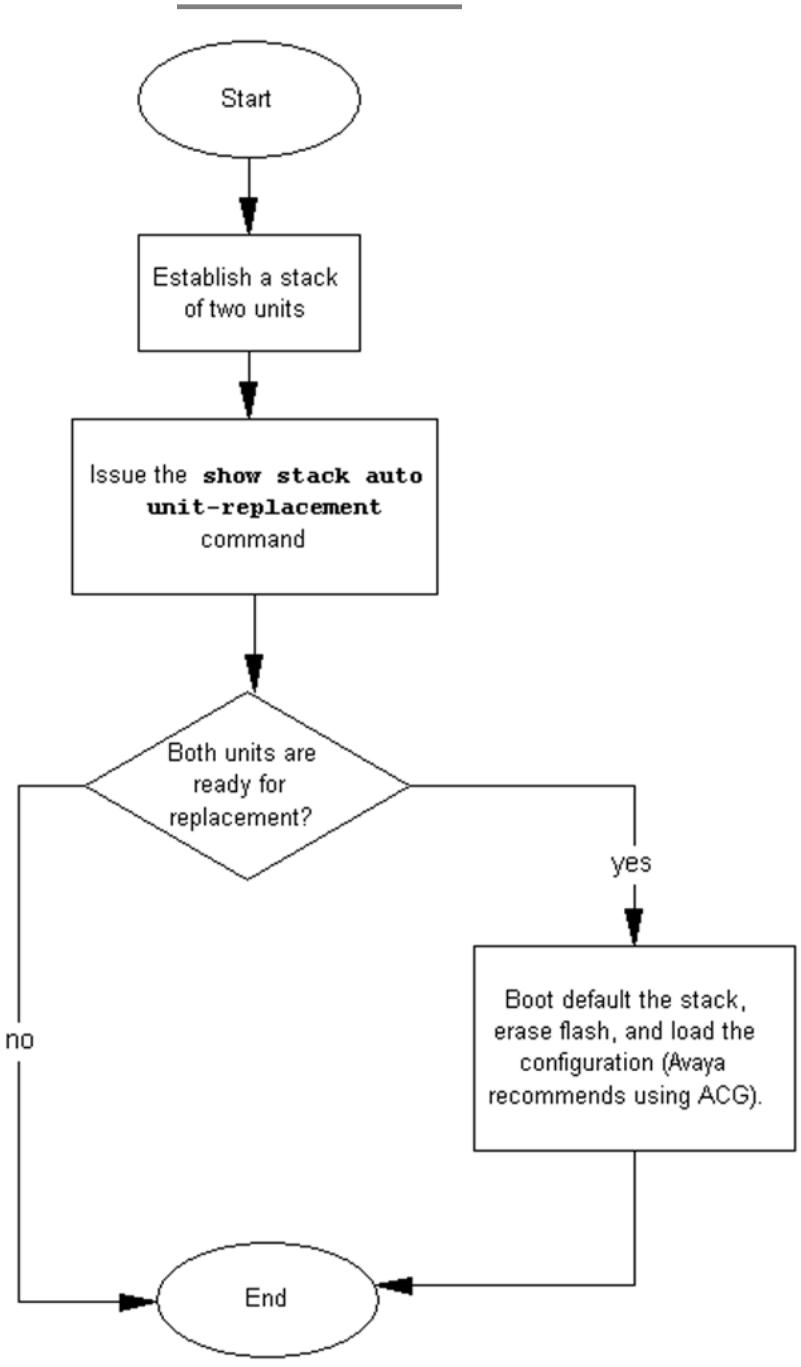


Figure 23: Both units display yes for Ready for Replacement

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

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

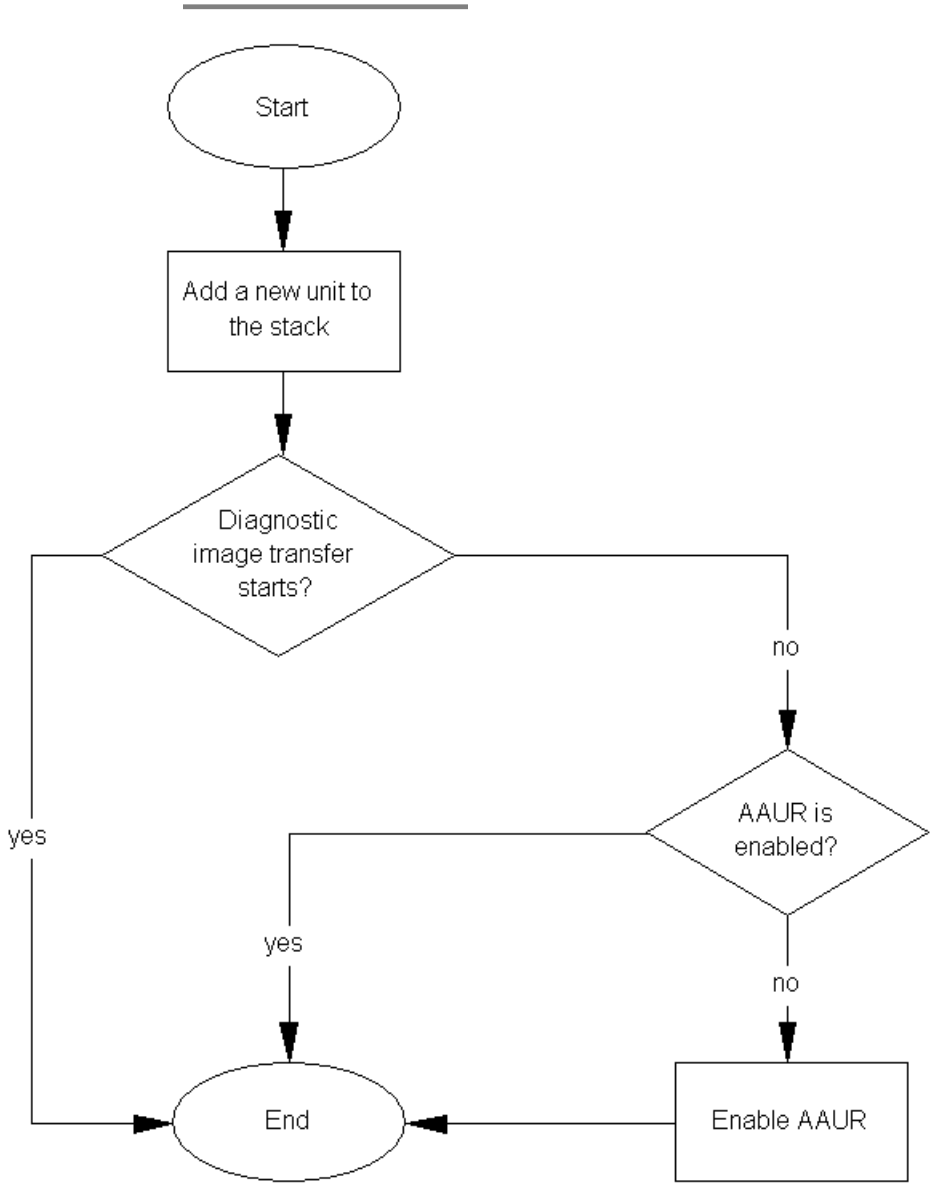


Figure 24: Diagnostic image transfer does not start

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 DM recovery tree

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.

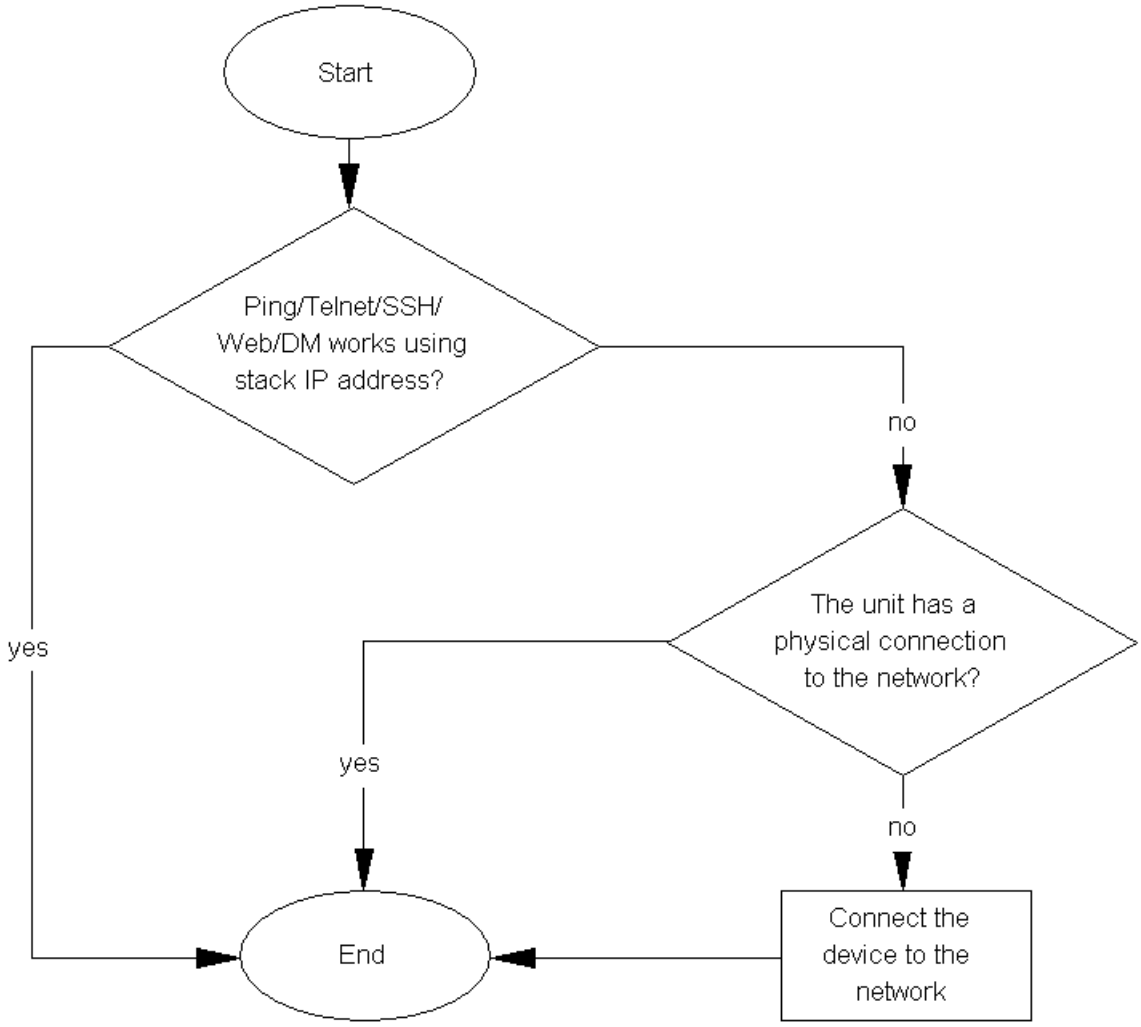


Figure 25: Ping/Telnet/SSH/Web/DM do not work when you use the stack IP address

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

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

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

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.

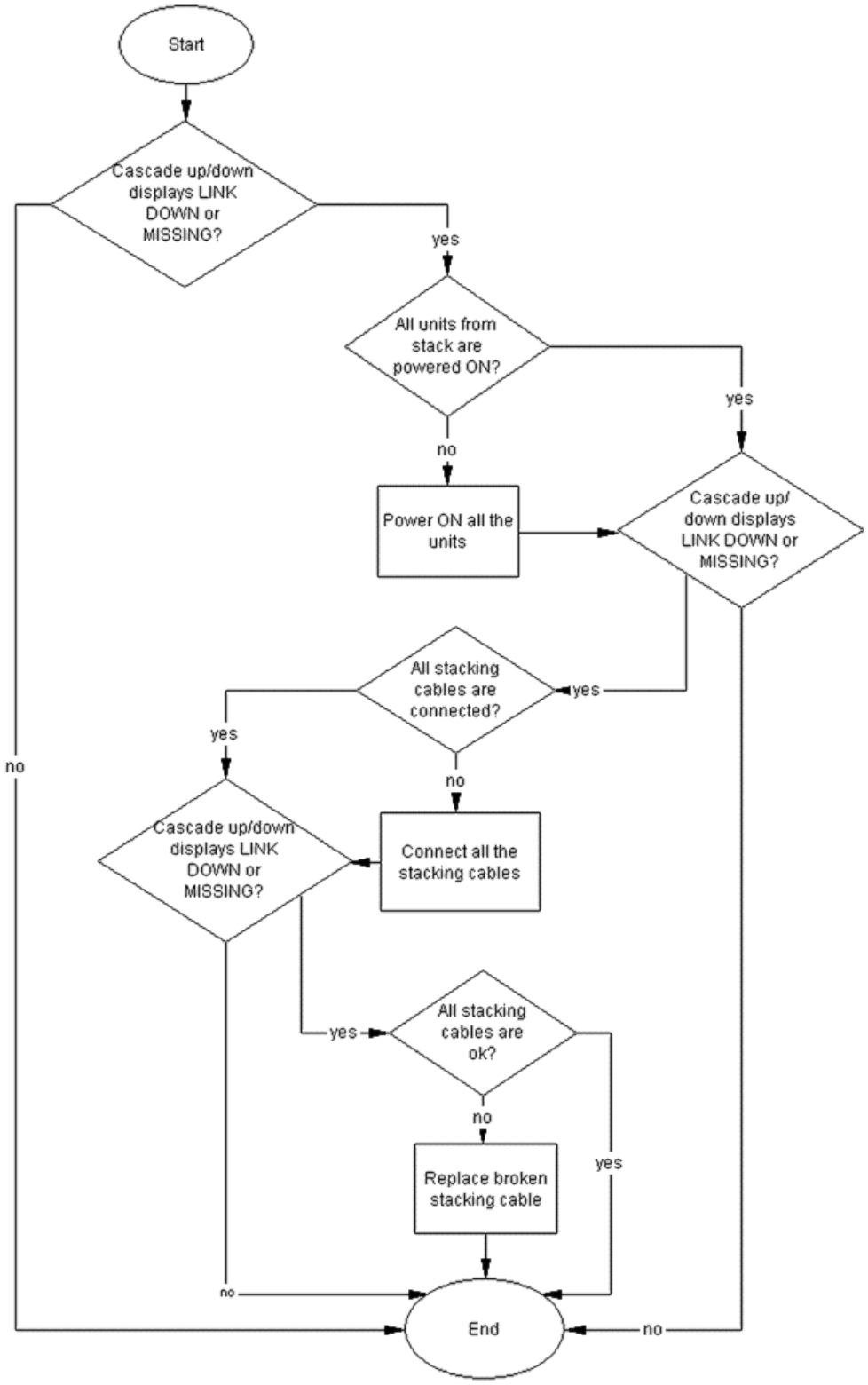


Figure 26: Stack Health Check: Cascade Up and Cascade Down columns display LINK DOWN or MISSING

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

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.

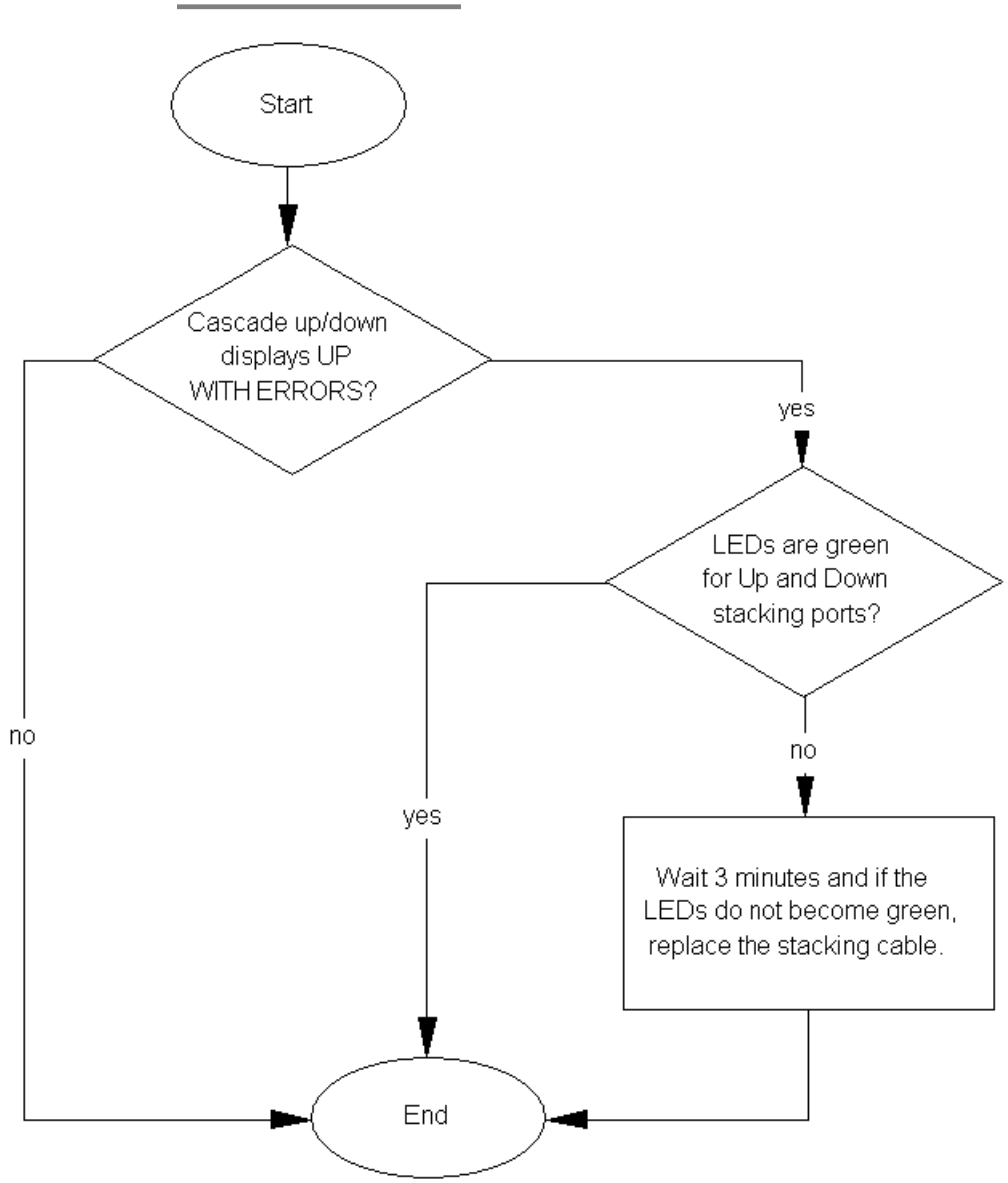


Figure 27: Stack Health Check: Cascade Up and Cascade Down columns display UP WITH ERRORS

Chapter 8: General troubleshooting of hardware

Use this section for hardware troubleshooting specific to the Avaya Ethernet Routing Switch 4500 Series.

Work flow: General troubleshooting of hardware

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

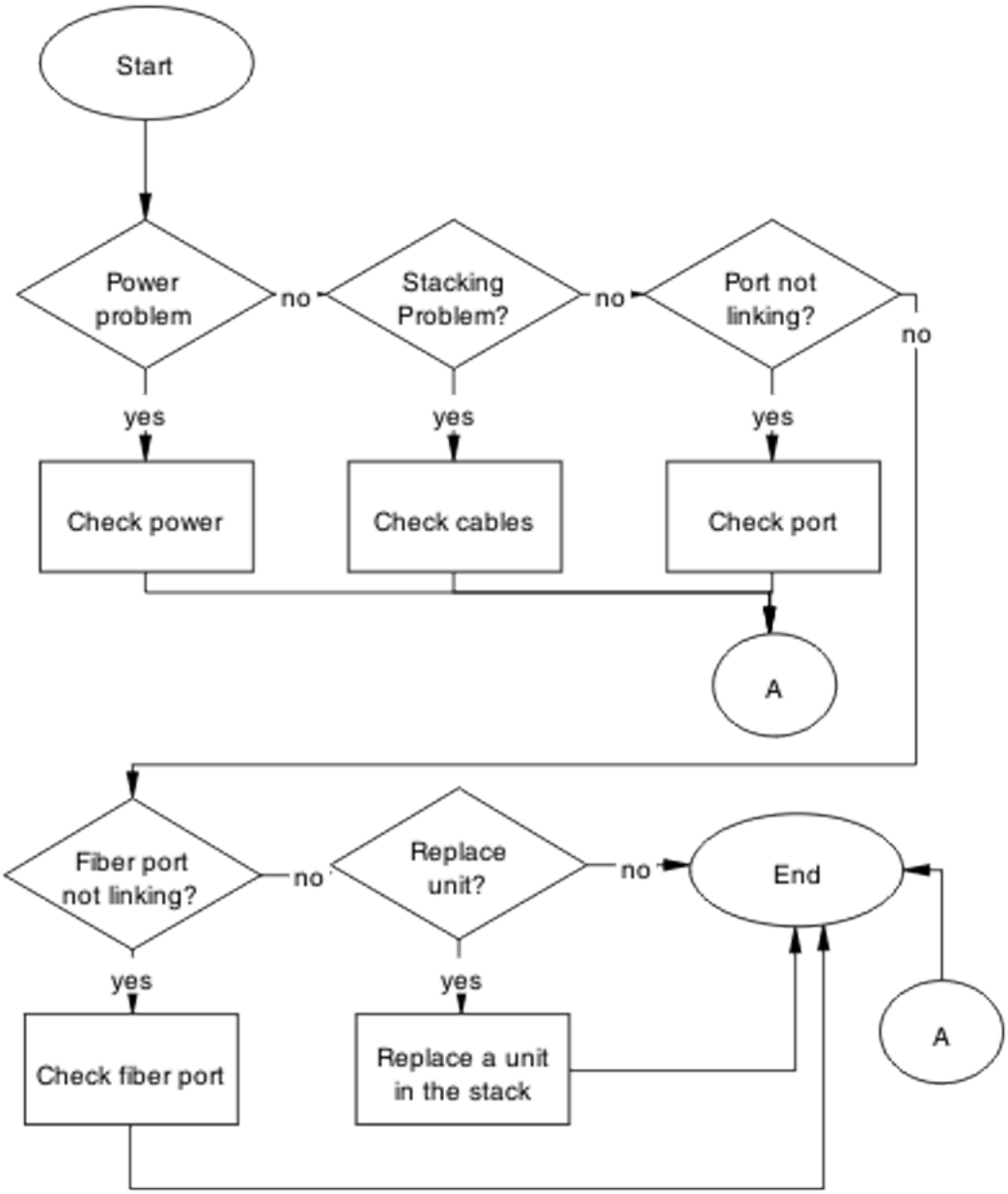


Figure 28: General troubleshooting of hardware

Navigation

Check power

Confirm power is being delivered to the device. The Avaya Ethernet Routing Switch 4500 Series utilizes a universal Power Supply Unit (PSU) that operates with voltages between 90v and 260v AC.

Task flow: Check power

The following task flow assists you to confirm that the Avaya Ethernet Routing Switch 4500 Series device is powered correctly.

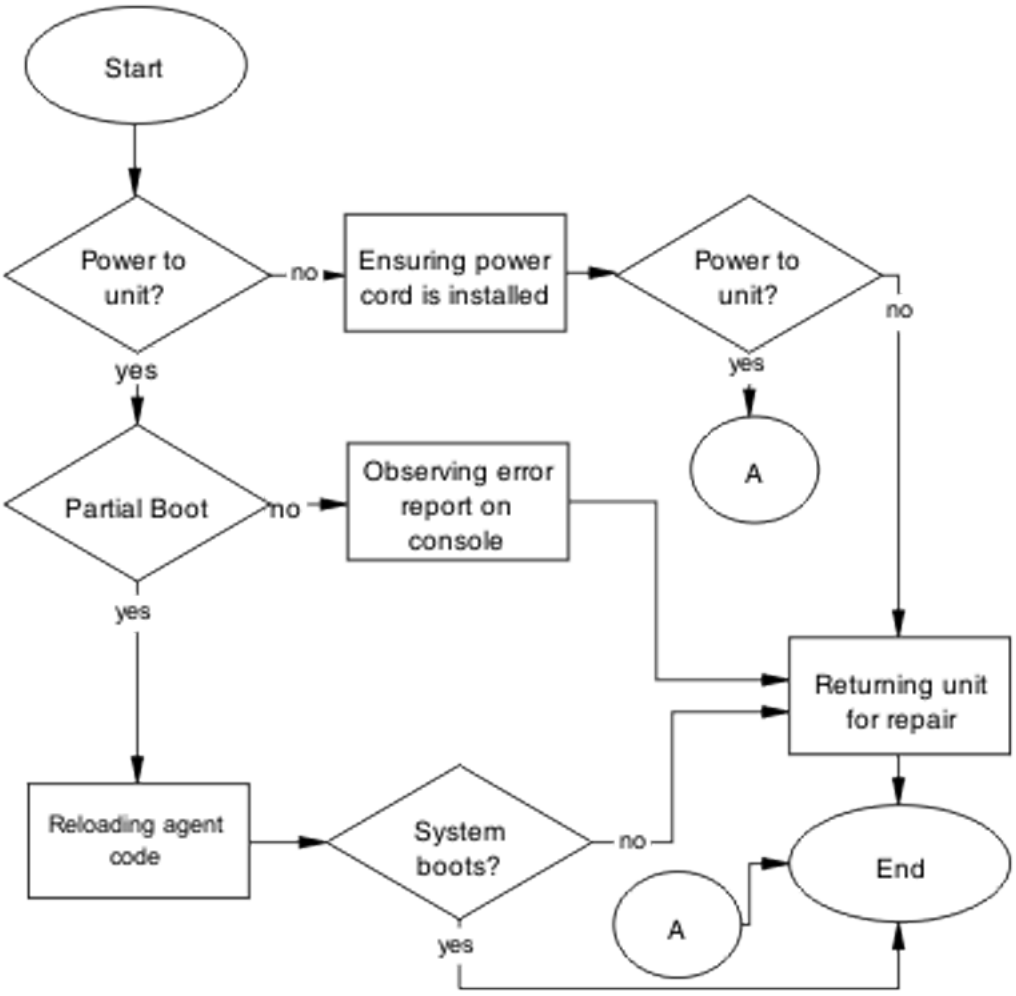


Figure 29: Check power

Result

Navigation

- Ensuring the power cord is installed on page 73
- Observing an error report on the console on page 73
- Reloading the agent code on page 73
- Returning the unit for repair on page 74

Ensuring the power cord is installed

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

See the technical document *Avaya Ethernet Routing Switch 4500 Series Installation* (NN47205-300) for power cord standards and details.

Observing an error report on the console

Interpret 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 the agent code

Reload the agent code on the Avaya Ethernet Routing Switch 4500 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 4500 Series Release 5.2 Release Notes* (NN47205-400) for information about software installation.

Replacing the power cord

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

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

Returning the unit for repair

Return a unit to Avaya for repair.

Contact Avaya for return instructions and RMA information.

Check cables

Confirm the stacking cables are correctly connected. Review the *Avaya Ethernet Routing Switch 4500 Series Installation* (NN47205-300) stacking section for cable requirements.

Task flow: Check cables

The following task flow assists you to confirm the stacking cables on the Avaya Ethernet Routing Switch 4500 Series device are installed correctly.

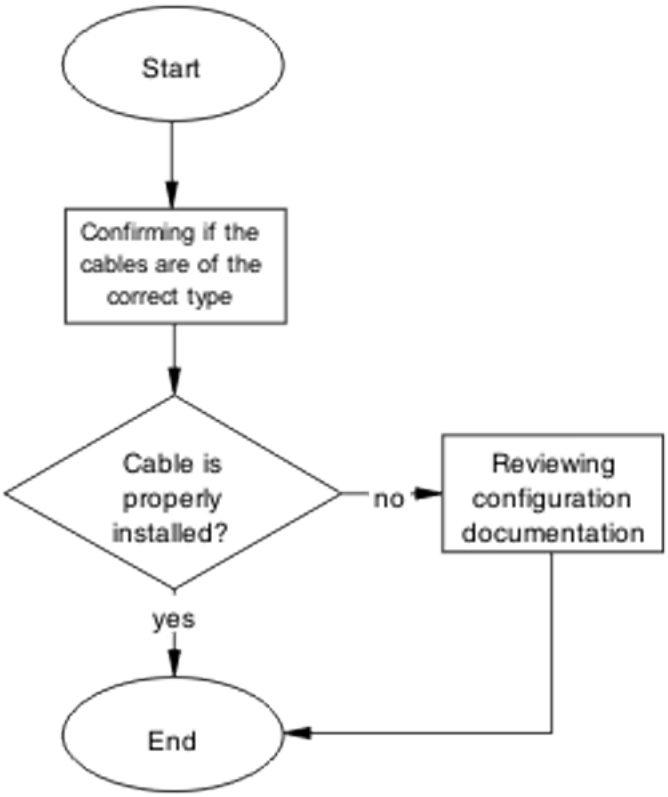


Figure 30: Check cables

Result

Navigation

- Confirming if the cables are the correct type on page 75
- Reviewing stacking configuration documentation on page 76

Confirming if the cables are the correct type

To create a stack connection, order the appropriate Avaya Ethernet Routing Switch 4500 Series cascade cables to ensure fail-safe stacking. A 1.5 foot stacking cable is included with the switch. For stacking three or more units (maximum eight units in a stack), order the 5-foot (1.5 m), 10-foot (3.0 m), 14-foot (4.3 m), or 16.4-foot (4.9 m) cables as applicable.

Reviewing stacking configuration documentation

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

Review the stacking procedure and diagram for your stack configuration (cascade up or down) in the stacking section of *Avaya Ethernet Routing Switch 4500 Series Installation* (NN47205-300).

Check port

Confirm that the port and the 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.

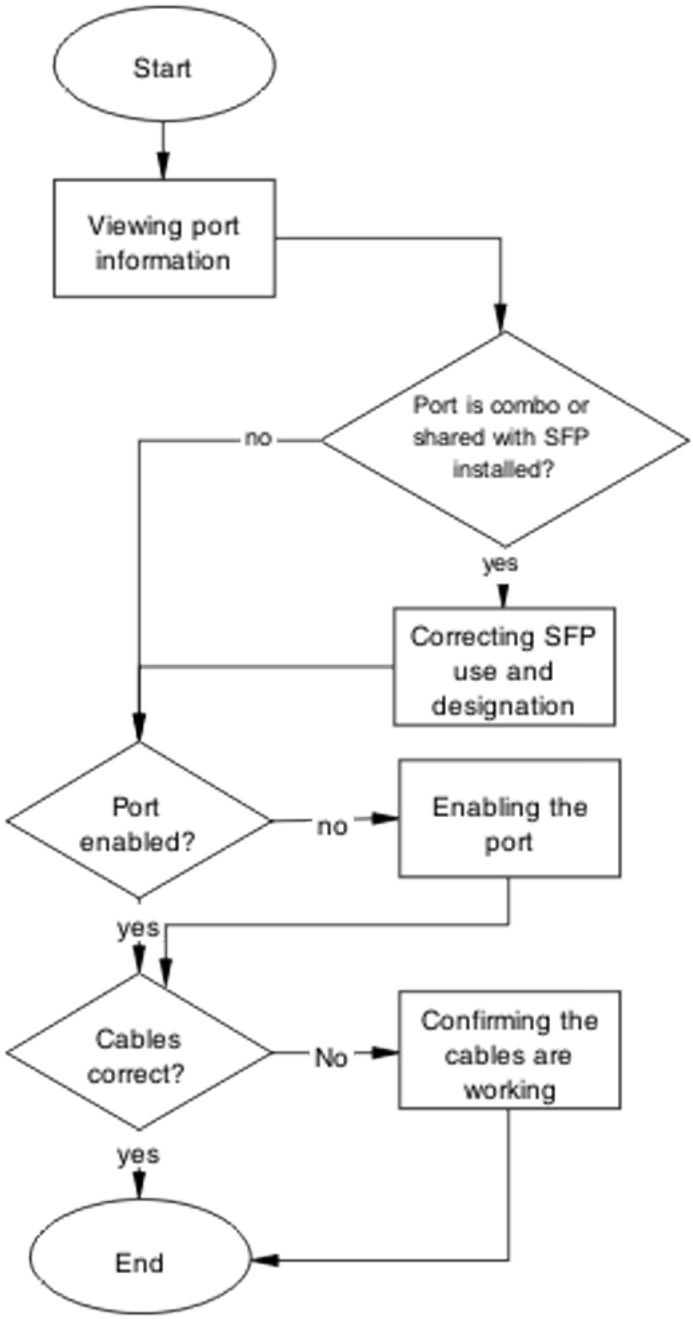


Figure 31: Check port

Result

Navigation

- Viewing port information on page 78
- Correcting SFP use and designation on page 78
- Enabling the port on page 78
- Confirming the cables are working on page 79

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.

Correcting SFP use and designation

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

For complete information about SFP transceiver use and designation, see *Avaya Ethernet Routing Switch 4500 Series Installation — SFPs and XFPs* (NN47205-301).

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.

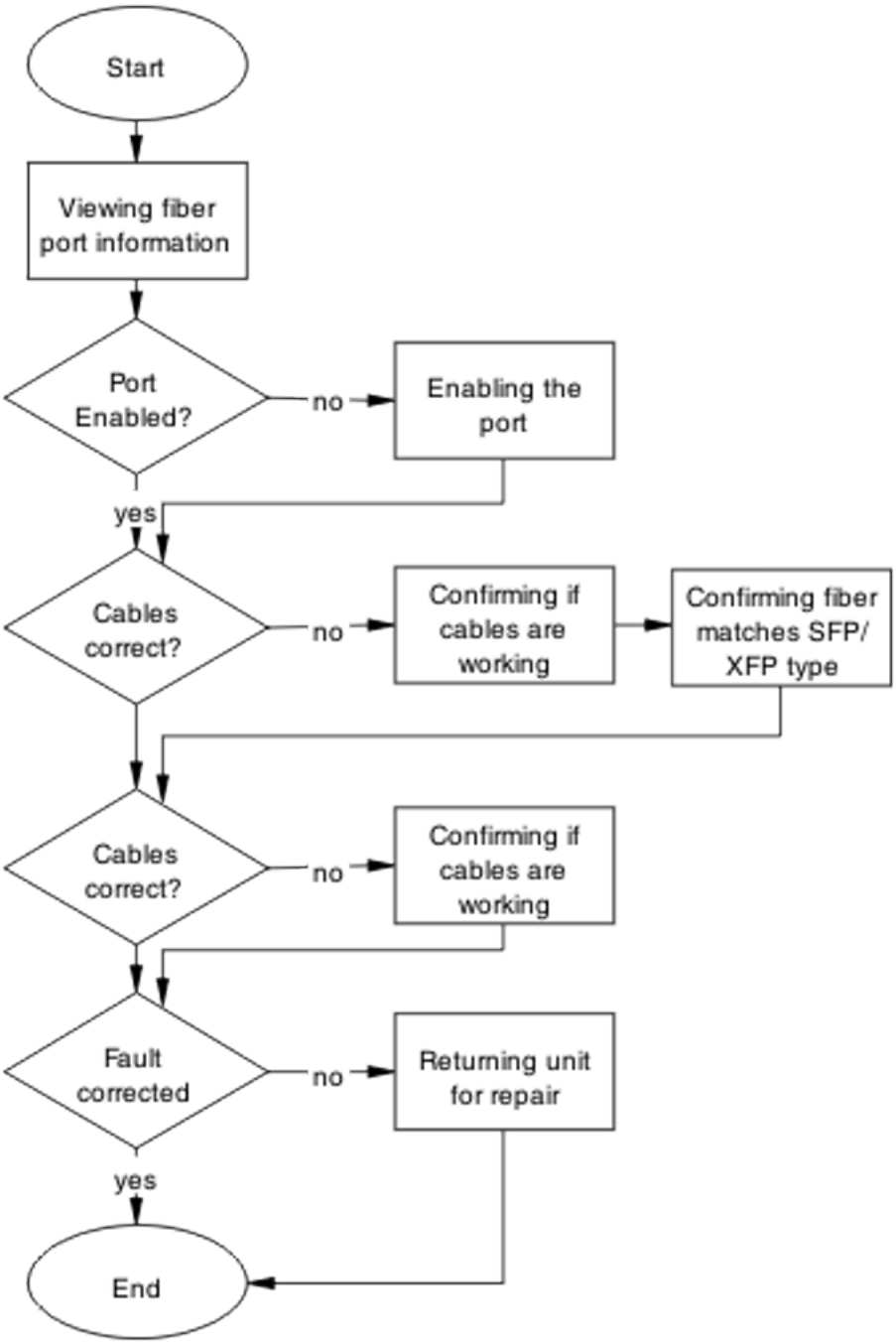


Figure 32: Check fiber port

Result

Navigation

- Viewing fiber port information on page 81
- Enabling the port on page 81
- Confirming if cables are working on page 81
- Confirming fiber matches SFP/XFP type on page 82
- Returning the unit for repair on page 82

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 Avaya Ethernet Routing Switch 4500 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 if 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.

Confirming fiber matches SFP/XFP type

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

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

Returning the unit for repair

Return unit to Avaya for repair.

Contact Avaya for return instructions and RMA information.

Replace a unit in the stack

Remove the defective unit and insert the replacement.

Caution:
Due to physical handling of the device and your physical proximity to electrical equipment, review and adhere to all safety instructions and literature included with the device and in *Avaya Ethernet Routing Switch 4500 Series Regulatory Information* (NN47205-100).

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

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

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

Important:

If the stack is only of two switches, the remaining switch enters Stack Forced Mode if that feature is enabled. Review the section Stack Forced Mode on page 19regarding this feature.

Important:

Different versions of the software and diagnostic images have different behaviors for the software and diagnostic images. Review the section Diagnostic Auto Unit Replacement (DAUR) on page 32 regarding DAUR and its expected results.

Task flow: Replace a unit in the stack

The following task flow assists you to replace one of the Avaya Ethernet Routing Switch 4500 Series devices in a stack. This is only appropriate if old software is used or AAUR is disabled. If AAUR is available (and it is turned on by default in such cases), then the procedures to verify software are not required.

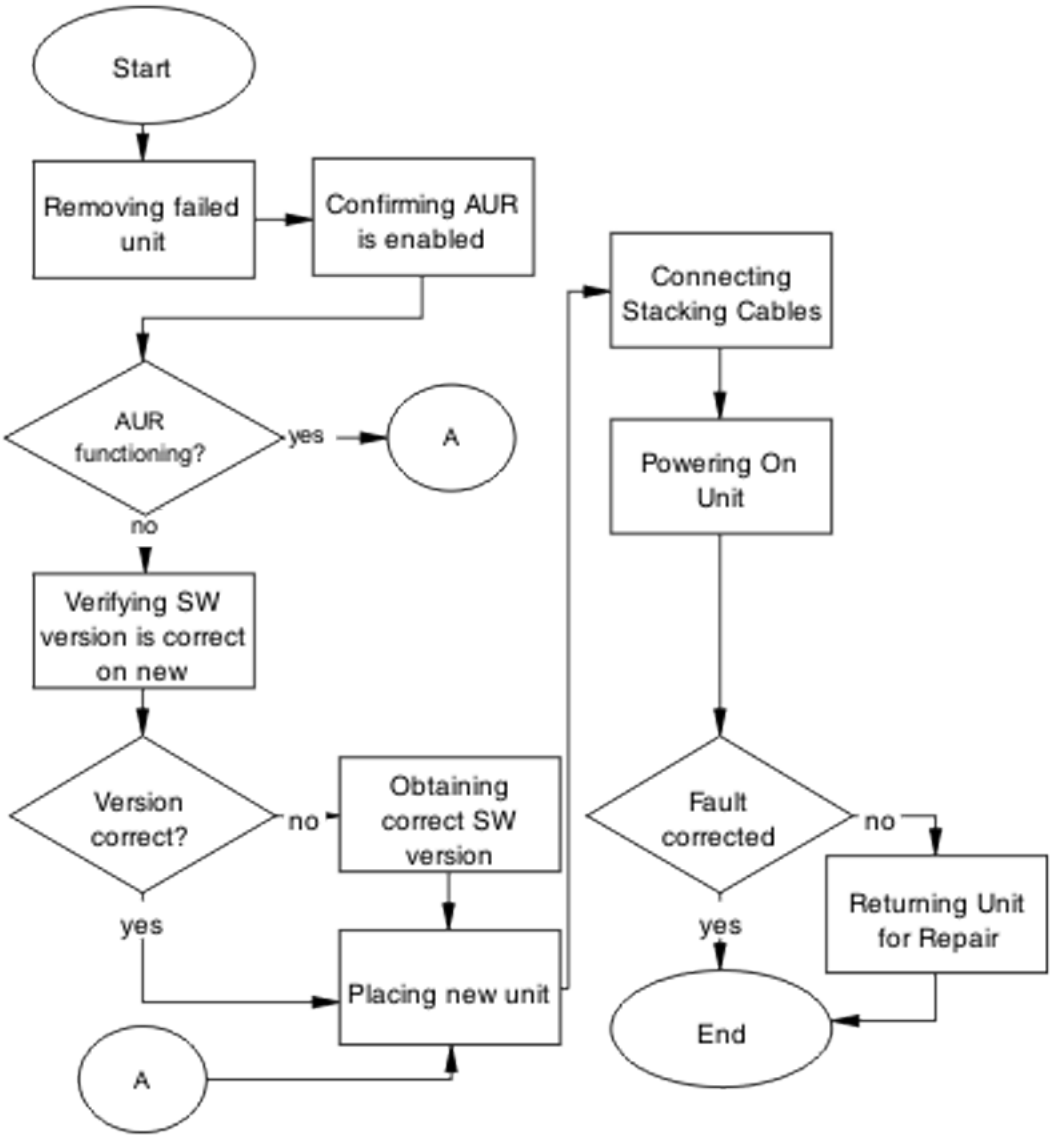


Figure 33: Replace a unit in the stack

Result

Navigation

- Removing a failed unit on page 85
- Confirming AUR is enabled on page 85
- Verifying the software version is correct on the new device on page 85
- Obtaining the correct software version on page 86
- Placing a new unit on page 86

- Connecting stacking cables on page 86
- Powering on the unit on page 86
- Returning the unit for repair on page 87

Removing a 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.

Confirming AUR is enabled

Confirm AUR is enabled in the stack.

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

Verifying the software version is correct on the 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 to 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 4500 Series Release 5.2 Release Notes* (NN47205-400) for software installation information.

Placing a new unit

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

Place the device in the stack in accordance with procedures outlined in *Avaya Ethernet Routing Switch 4500 Series Installation* (NN47205-300).

Connecting stacking cables

Reconnect the stacking cables to correctly stack the device.

1. Review the stacking section in *Avaya Ethernet Routing Switch 4500 Series Installation* (NN47205-300) 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.

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

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

Returning the unit for repair

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

You 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 as needed. Use the **`adac voice-vlan x`** command to reserve or set the VLAN number used by ADAC.

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.

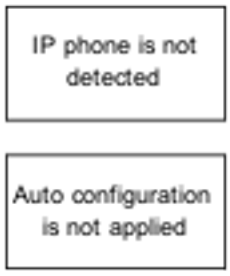


Figure 34: Troubleshooting ADAC

Navigation

- IP phone is not detected on page 90
- Auto configuration is not applied on page 96

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.

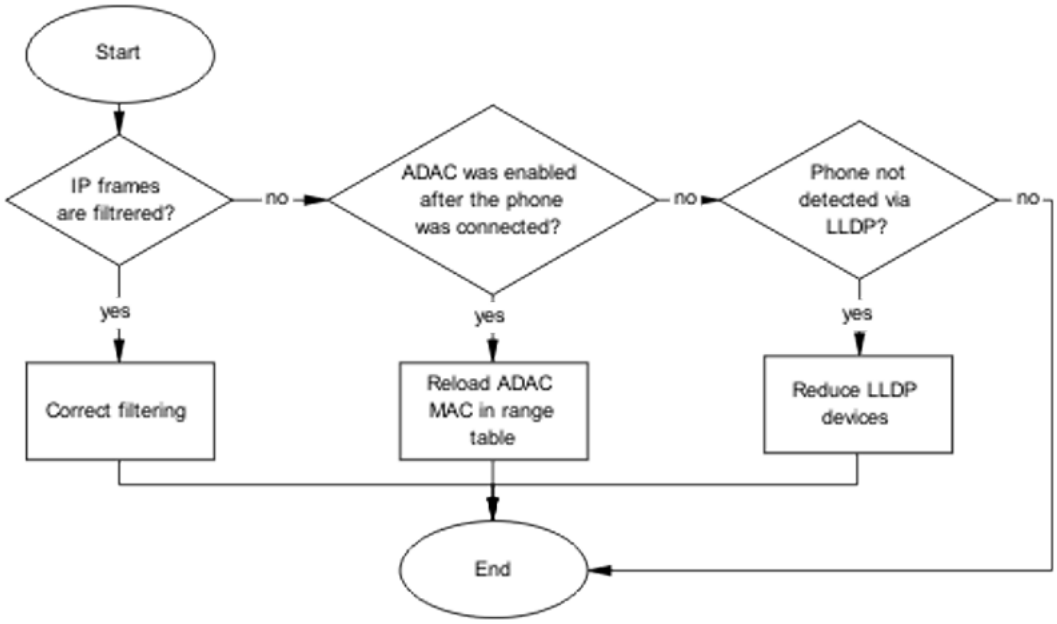


Figure 35: IP phone not detected

Navigation

- Correct filtering on page 91
- Reload ADAC MAC in range table on page 93
- Reduce LLDP devices on page 94

Correct filtering

Configure the VLAN filtering to allow ADAC.

Task flow: Correct filtering

The following task flow assists you to correct the filtering.

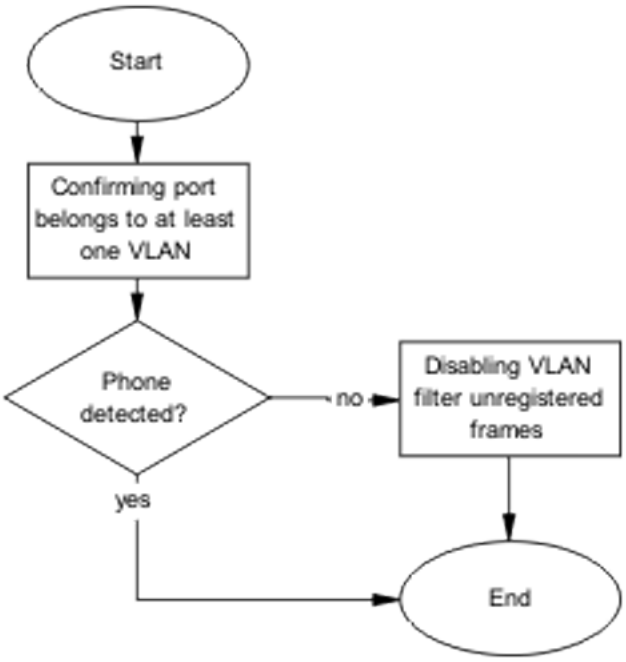


Figure 36: Correct filtering

Navigation

- Confirming port belongs to at least one VLAN on page 92
- Disabling the VLAN filtering of unregistered frames on page 92

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.

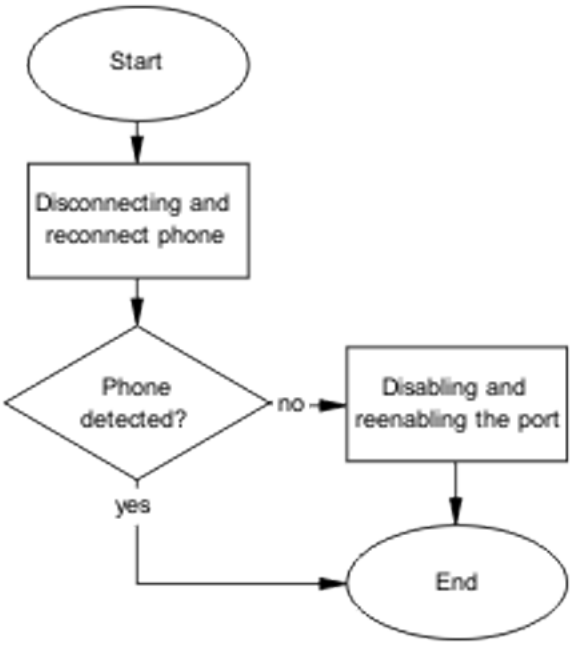


Figure 37: Reload ADAC MAC in range table

Navigation

- Disconnecting and reconnecting phone on page 94
- Disabling and enabling the port on page 94

Disconnecting and reconnecting phone

Remove the phone and then 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. After disabling and re-enabling 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.

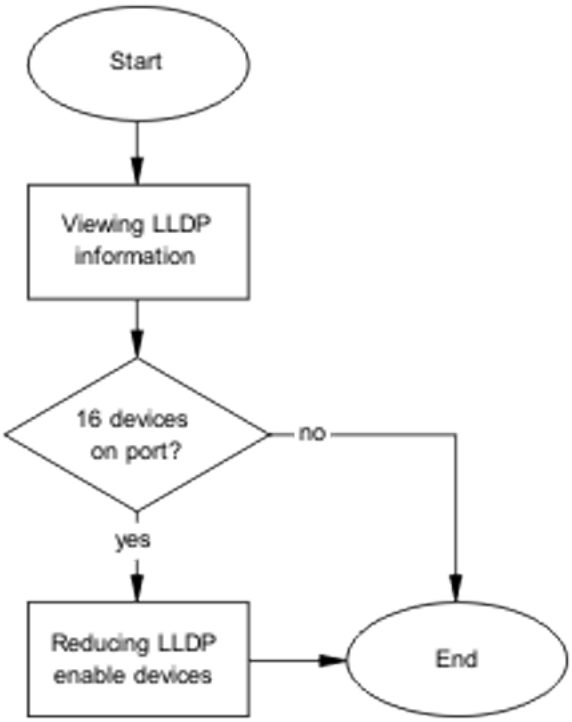


Figure 38: Reduce LLDP devices

Navigation

- Viewing LLDP information on page 95
- Reducing LLDP enabled devices on page 96

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.

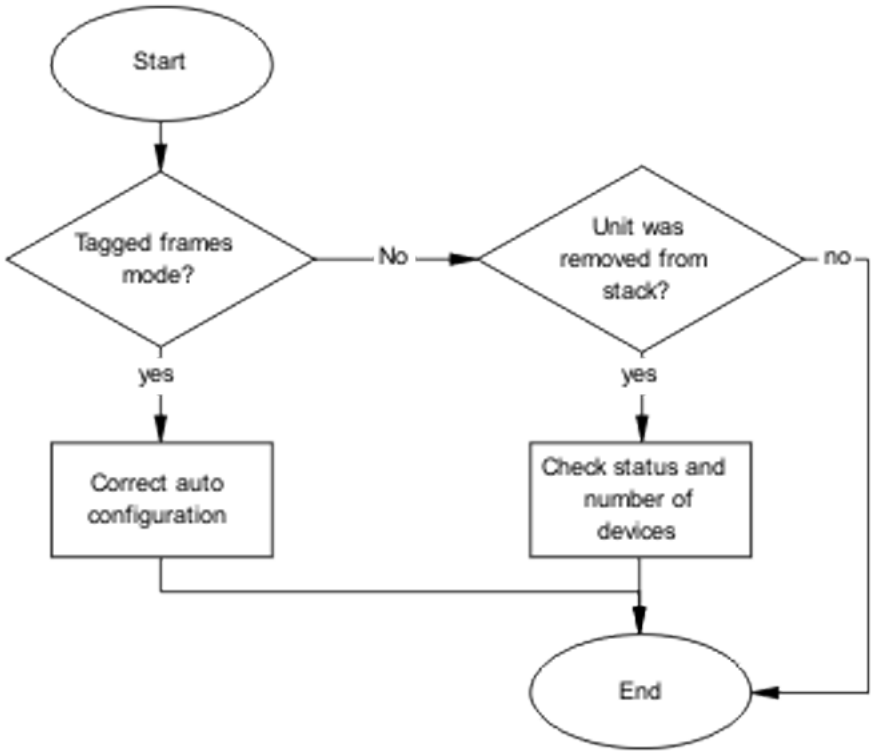


Figure 39: Auto configuration is not applied

Navigation

- Correct auto configuration on page 97
- Check status and number of devices on page 99

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.

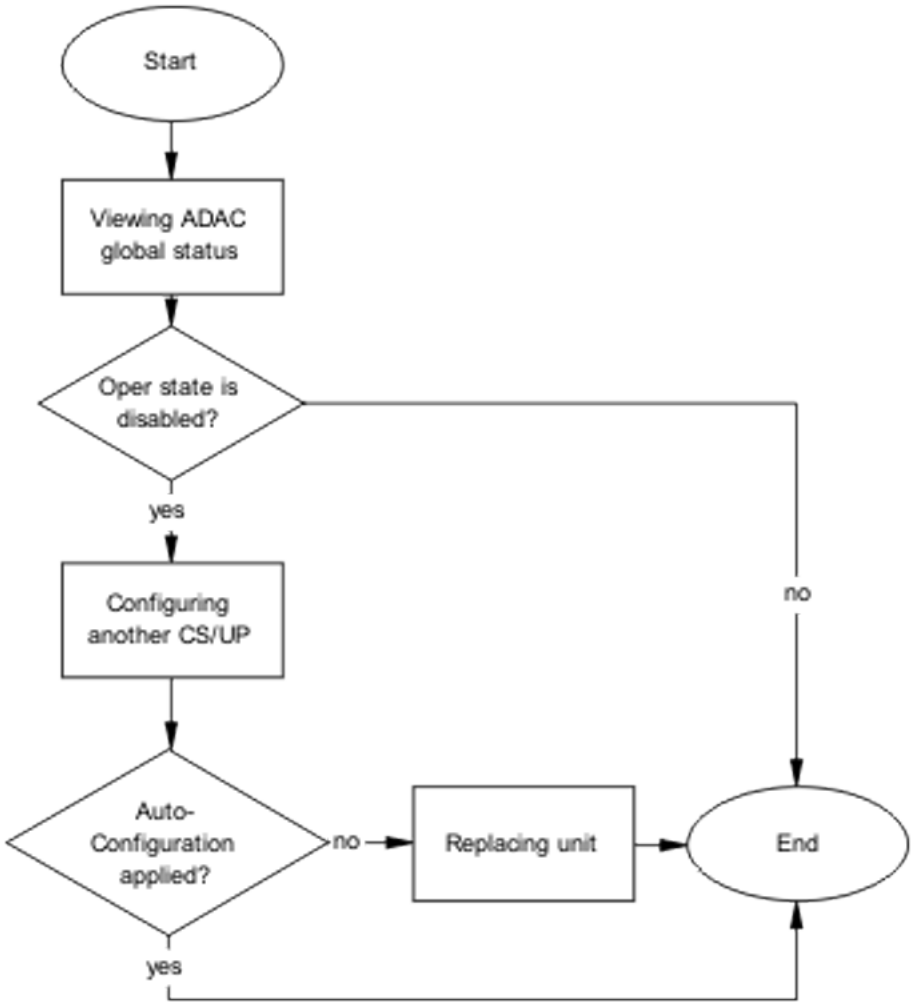


Figure 40: Correct auto configuration

Navigation

- Viewing ADAC global status on page 98
- Configuring another call server and uplink port on page 99
- Replacing the unit on page 99

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 the unit

Replace the unit to replicate configuration if AUR is enabled.

1. Follow the replacement guidelines in *Avaya Ethernet Routing Switch 4500 Series Configuration — System* (NN47205-500).
2. Refer to the unit replacement section in the Troubleshooting Hardware section of this document.

Check status and number of devices

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

Task flow: Check status and number of devices

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

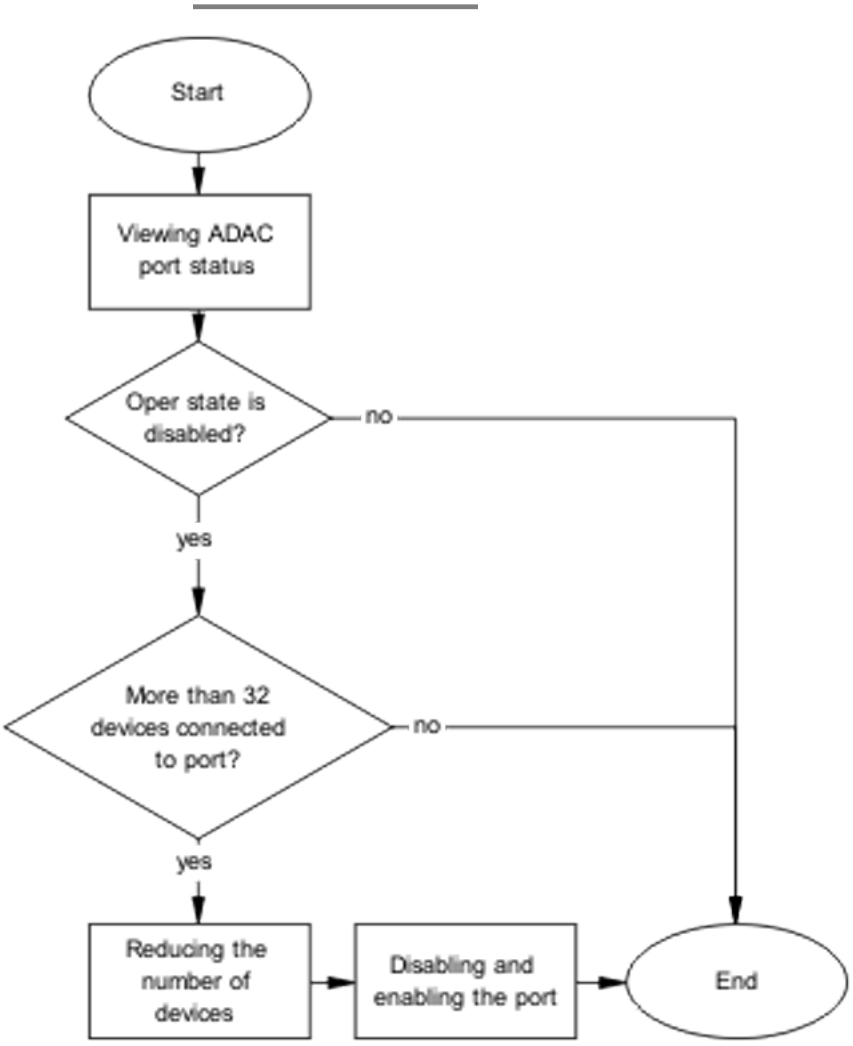


Figure 41: Check status and number of devices

Navigation

- Viewing ADAC port status on page 100
- Reducing the number of devices on page 101
- Disabling and enabling the port on page 101

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

Disabling and enabling the port

Administratively disable and enable the port to initialize the 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.

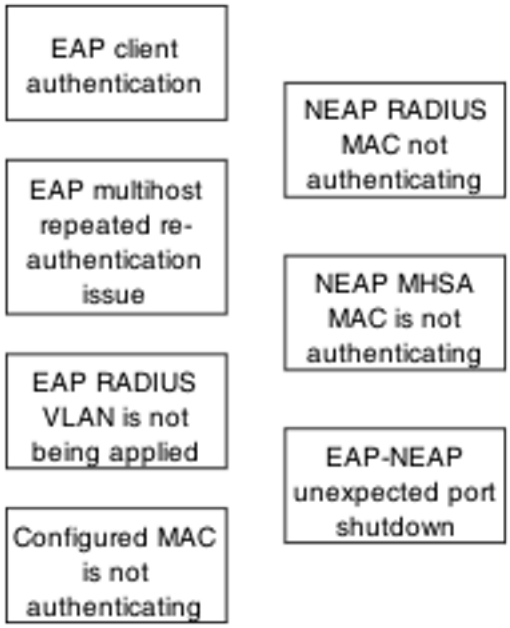


Figure 42: Troubleshooting authentication

Navigation

EAP client authentication

This section provides troubleshooting guidelines for the EAP and NEAP features on the Avaya Ethernet Routing Switch 4500 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.

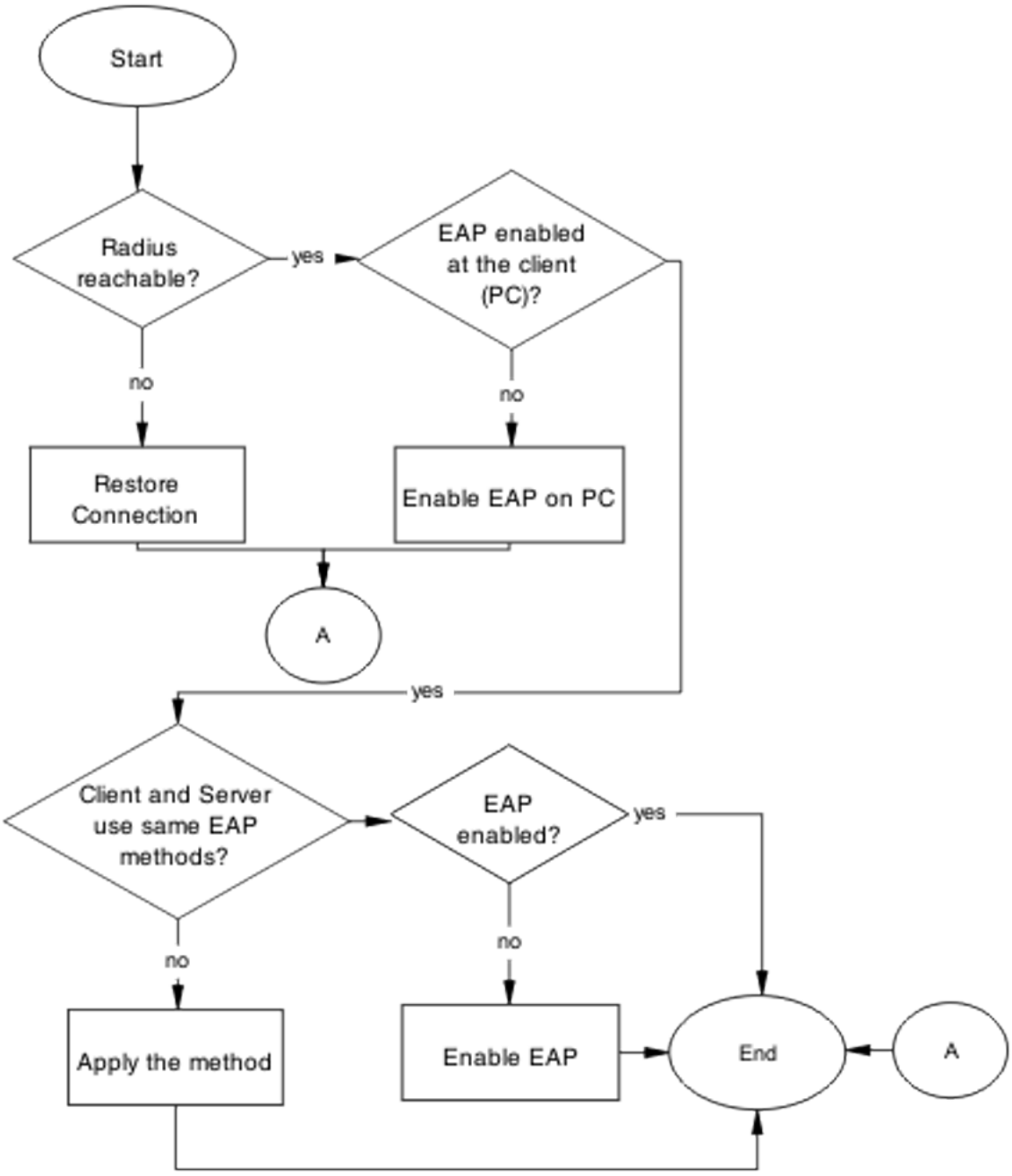


Figure 43: EAP client is not authenticating

Navigation

- Restore RADIUS connection on page 106
- Enable EAP on the PC on page 109
- Apply the method on page 110
- Enable EAP globally on page 111

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.

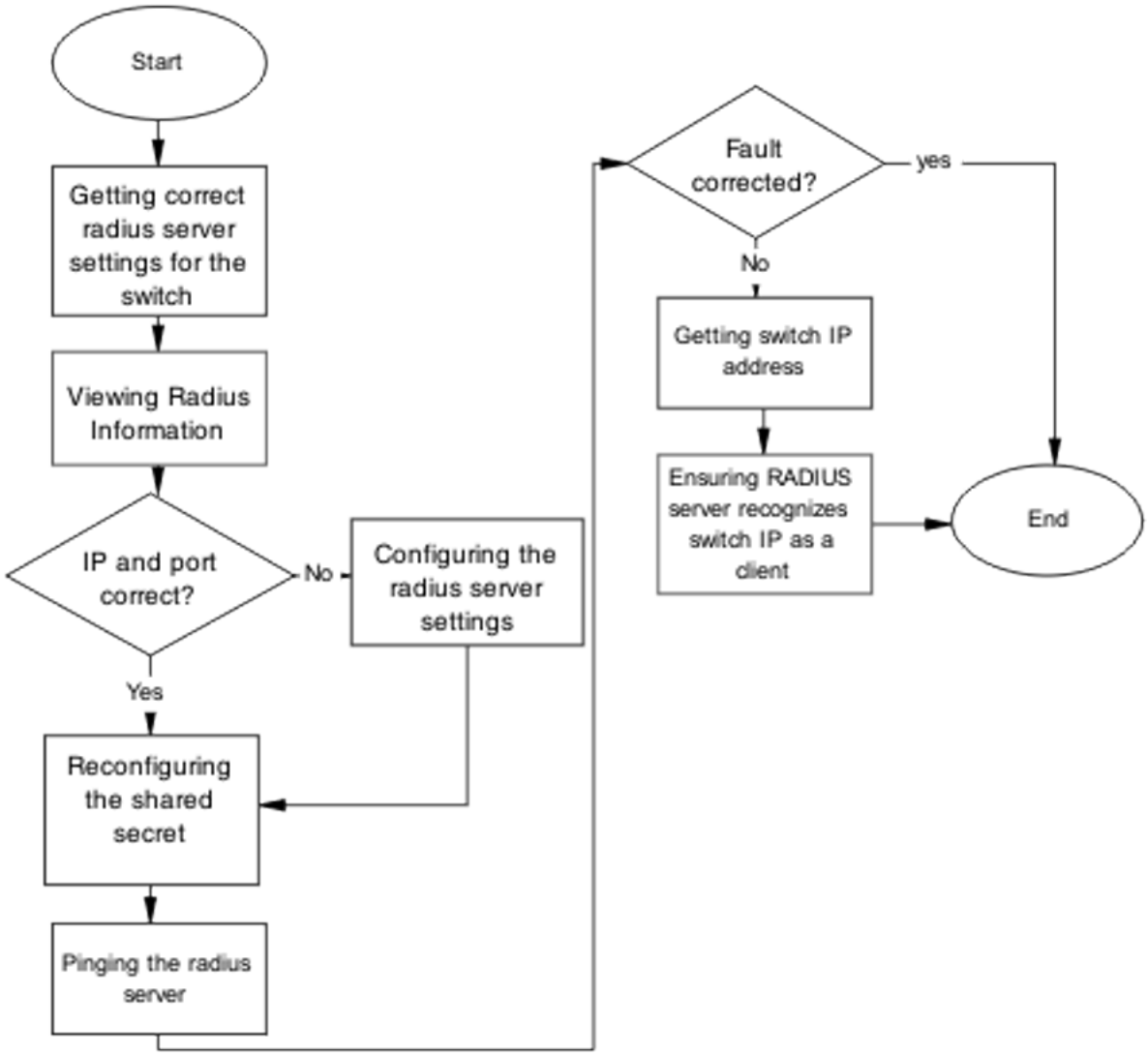


Figure 44: Restore RADIUS connection

Navigation

- Getting correct RADIUS server settings for the switch on page 108
- Viewing RADIUS information on page 108
- Configuring the RADIUS server settings on page 108
- Reconfiguring the shared secret on page 108
- Pinging the RADIUS server on page 108

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.

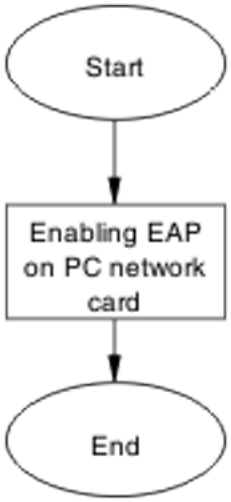


Figure 45: Enable EAP on the PC

Navigation

Enabling EAP on PC network card on page 109

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.

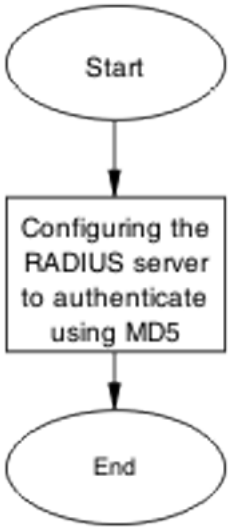


Figure 46: Apply the method

Navigation

Configuring the RADIUS server on page 111

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 4500 Series device.

Task flow: Enable EAP globally

The following task flow assists you to enable EAP globally on the Avaya Ethernet Routing Switch 4500 Series device.

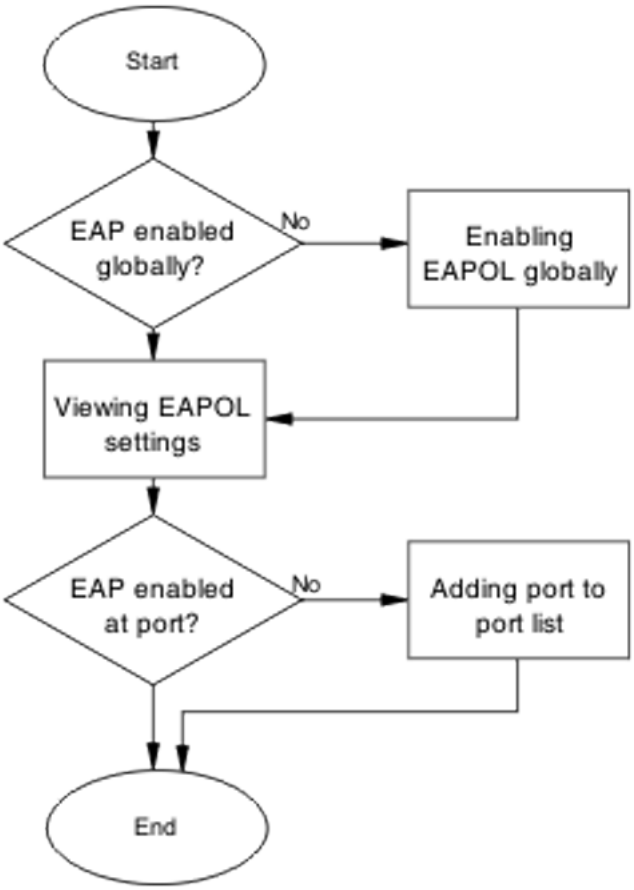


Figure 47: Enable EAP globally

Navigation

Enabling EAP globally

Enable EAP globally on the Avaya Ethernet Routing Switch 4500 Series device.

1. Use the **eapol enable** command to enable EAP globally on the Avaya Ethernet Routing Switch 4500 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.

Task flow: 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.

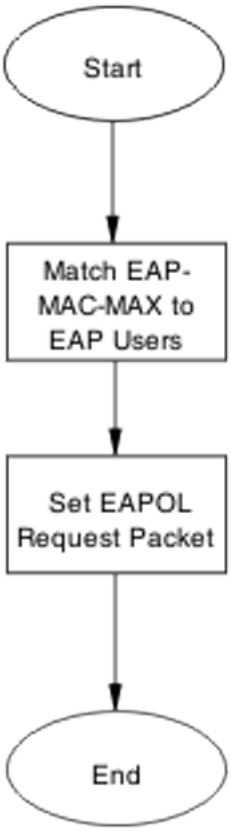


Figure 48: EAP multihost repeated re-authentication issue

Navigation

- Match EAP-MAC-MAX to EAP users on page 114
- Set EAPOL request packet on page 116

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.

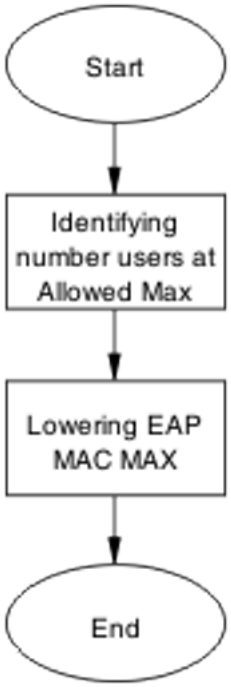


Figure 49: Match EAP-MAC-MAX to EAP users

Navigation

- Identifying number of users at allowed max on page 115
- Lowering EAP max MAC on page 116

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.

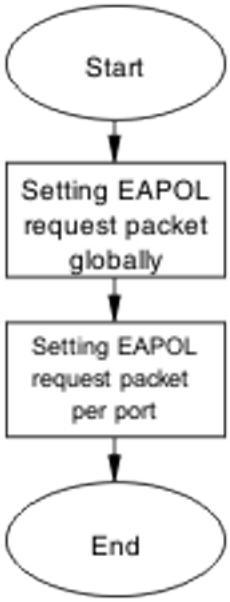


Figure 50: Set EAPOL request packet

Navigation

- Setting EAPOL request packet globally on page 117
- Setting EAPOL request packet for a port on page 117

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.

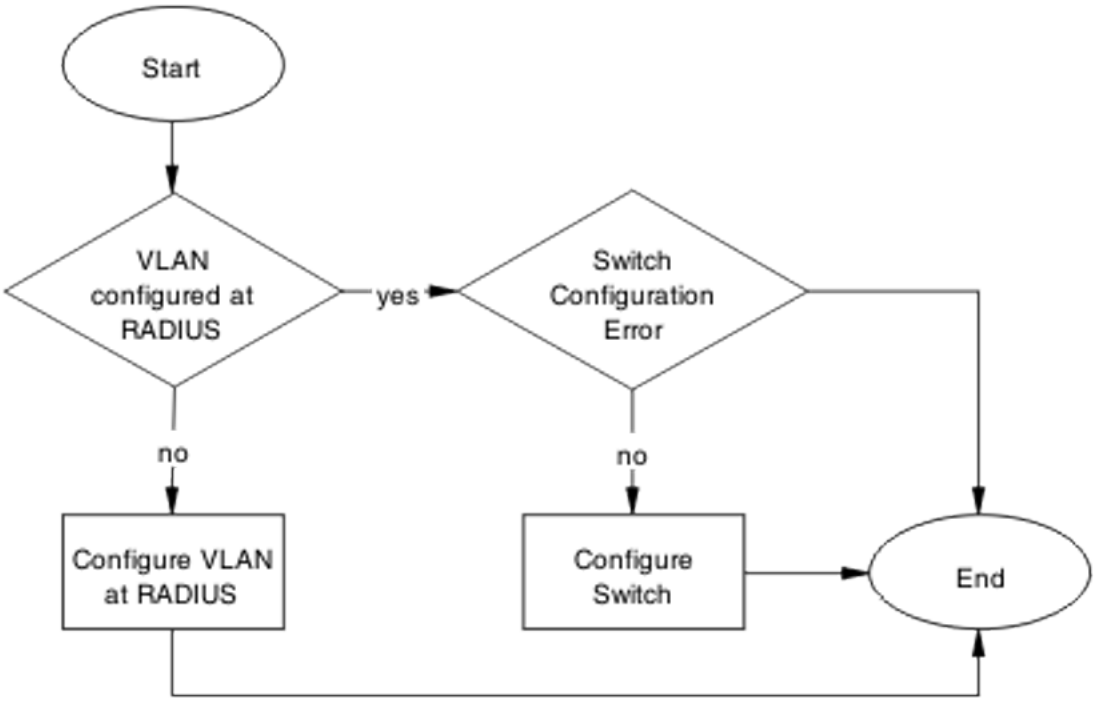


Figure 51: EAP Radius VLAN is not being applied

Navigation

- Configure VLAN at RADIUS on page 118
- Configure the switch on page 120

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.

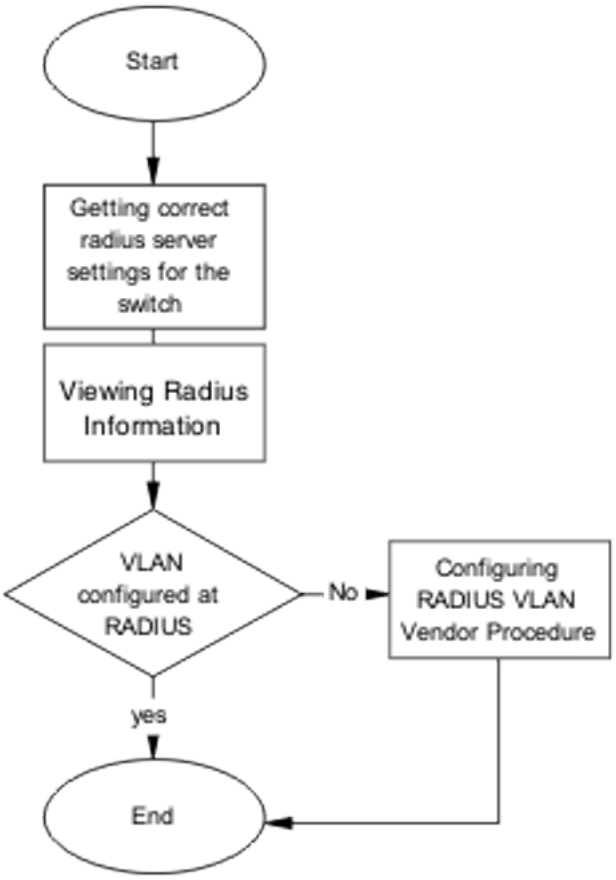


Figure 52: Configure VLAN at RADIUS

Navigation

- Getting correct RADIUS server settings on page 119
- Viewing RADIUS information on page 120
- Configuring RADIUS on page 120

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 the switch

The VLAN must be configured correctly on the Avaya Ethernet Routing Switch 4500 Series device.

Task flow: Configure switch

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

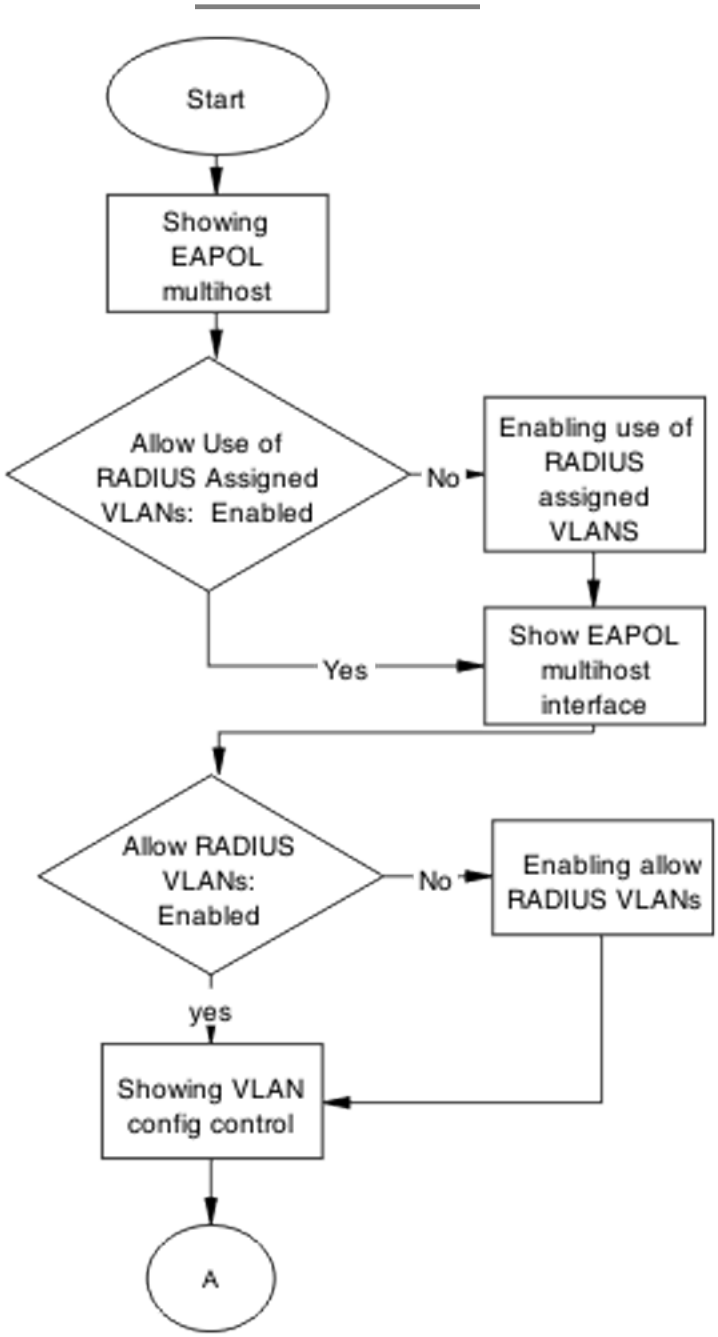


Figure 53: Configure switch task part 1

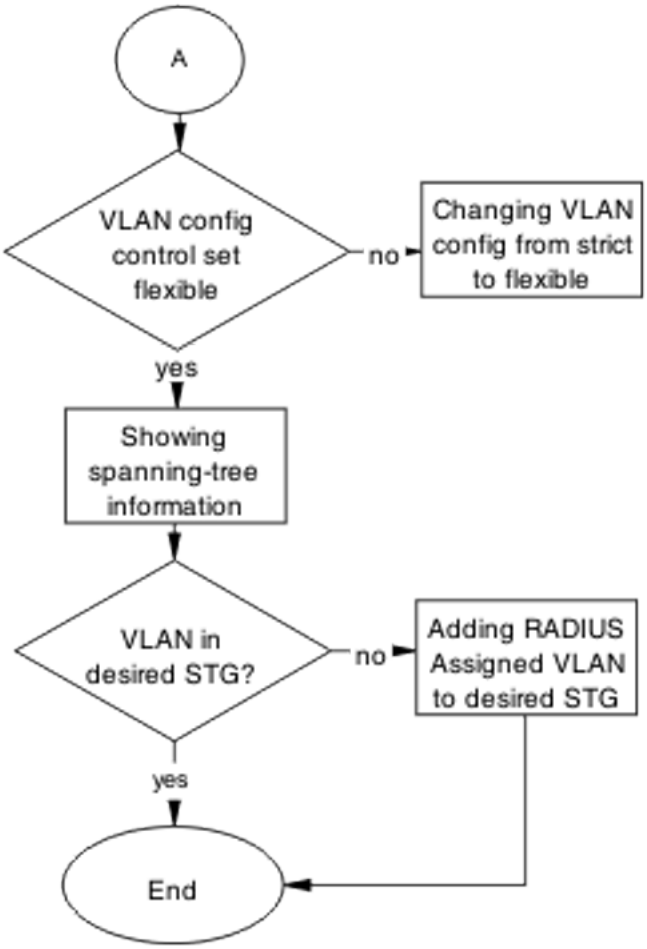


Figure 54: Configure switch task part 2

Navigation

- Showing EAPOL multihost on page 123
- Enabling use of RADIUS assigned VLANs on page 123
- Showing EAPOL multihost interface on page 123
- Showing VLAN config control on page 123
- Changing VLAN config from strict to flexible on page 124
- Showing spanning tree on page 124
- Adding RADIUS assigned VLAN to desired STG on page 124

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" setting 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 information.
2. Identify if the 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 the 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 the 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.

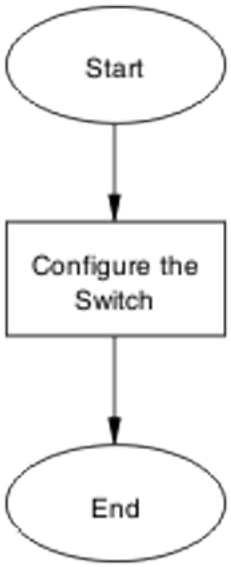


Figure 55: Configured MAC is not authenticating

Navigation

Configure the switch on page 125

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 flows assist you to ensure that the MAC is authenticating on the Avaya Ethernet Routing Switch 4500 Series device.

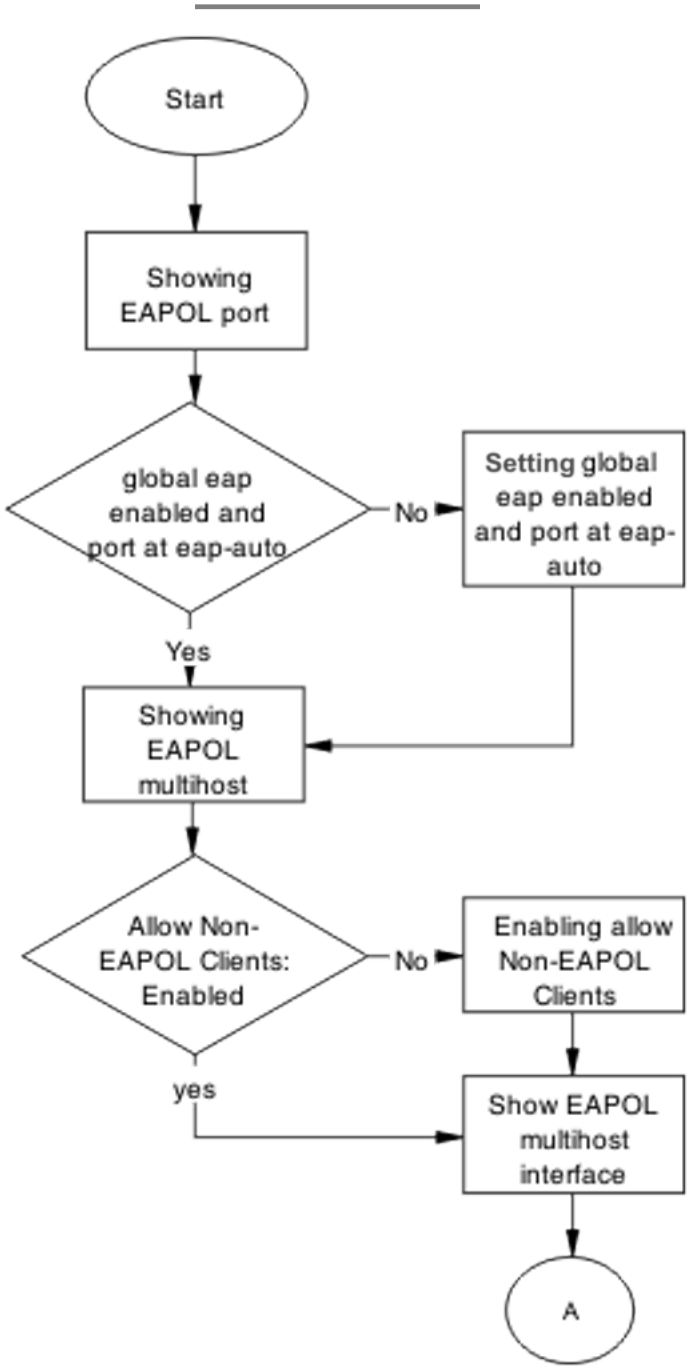


Figure 56: Configure the switch part 1

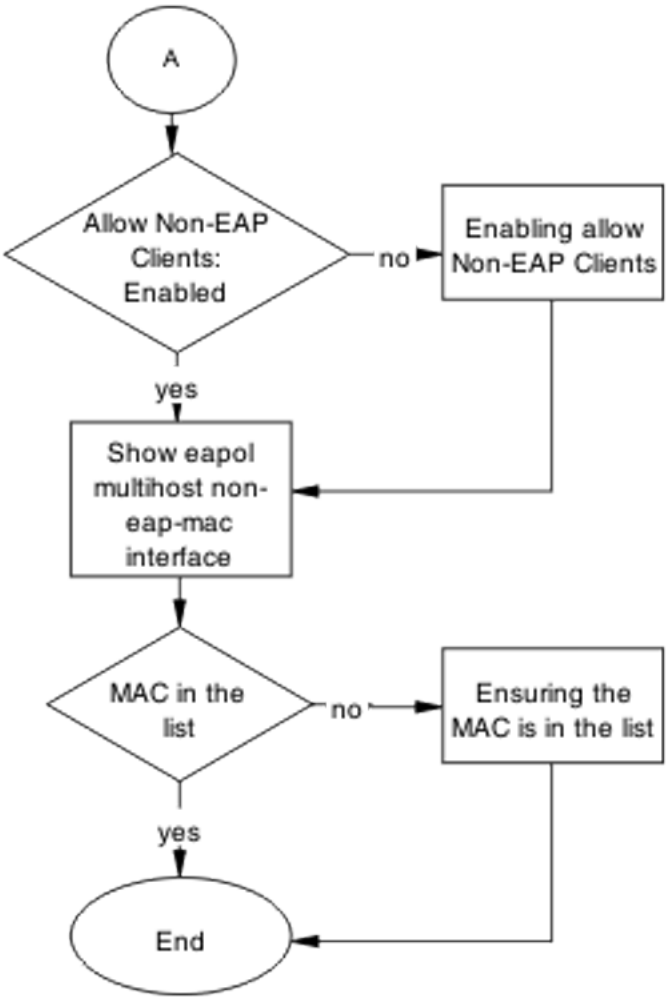


Figure 57: Configure the switch part 2

Navigation

- Showing EAPOL port on page 141
- Setting global EAP enabled and port at eap-auto on page 129
- Showing EAPOL multihost on page 129
- Enabling allow non-EAPOL clients on page 129
- Showing EAPOL multihost interface on page 130
- Enabling multihost status and allow non-EAPOL clients on page 130
- Showing EAPOL multihost non-eap-mac interface on page 130
- Ensuring MAC is in the list on page 130

Showing the 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 is 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.

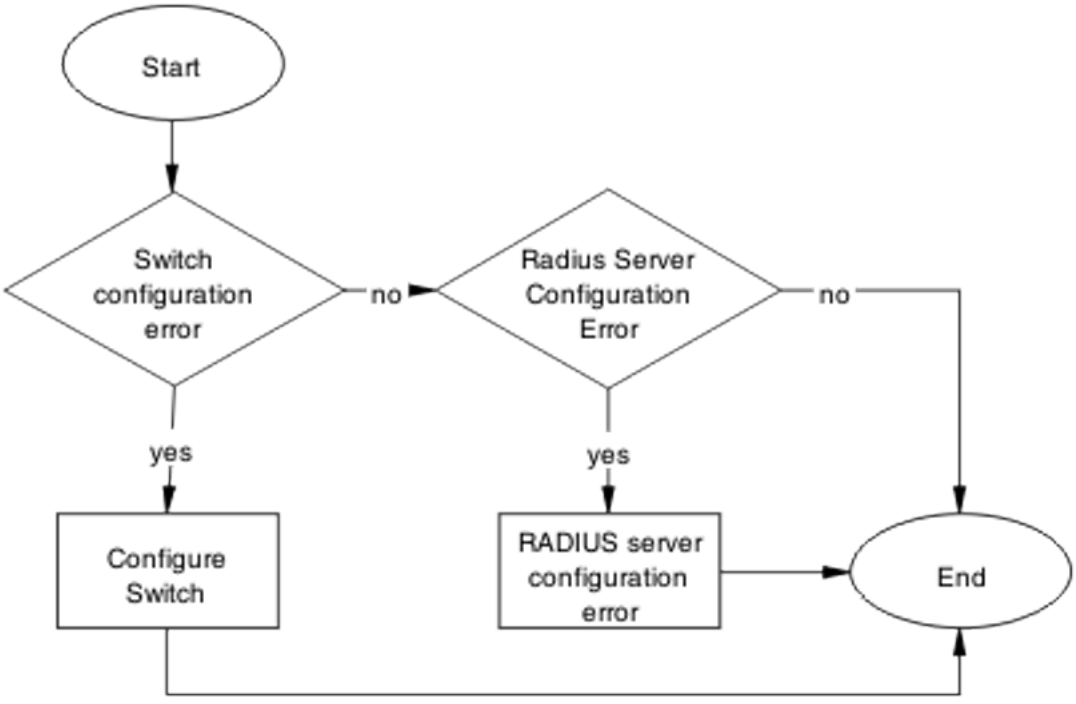


Figure 58: NEAP RADIUS MAC not authenticating

Navigation

- Configure switch on page 132
- RADIUS server configuration error on page 136

Configure switch

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

Task flow: Configure switch

The following task flows assist you to configure the Avaya Ethernet Routing Switch 4500 Series device to correct the RADIUS MAC issue.

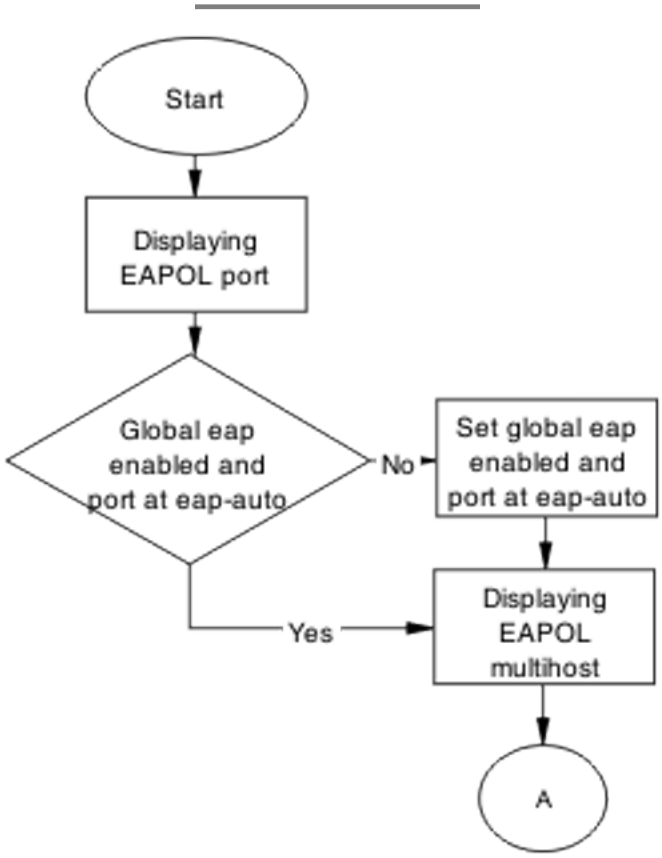


Figure 59: Configure switch part 1

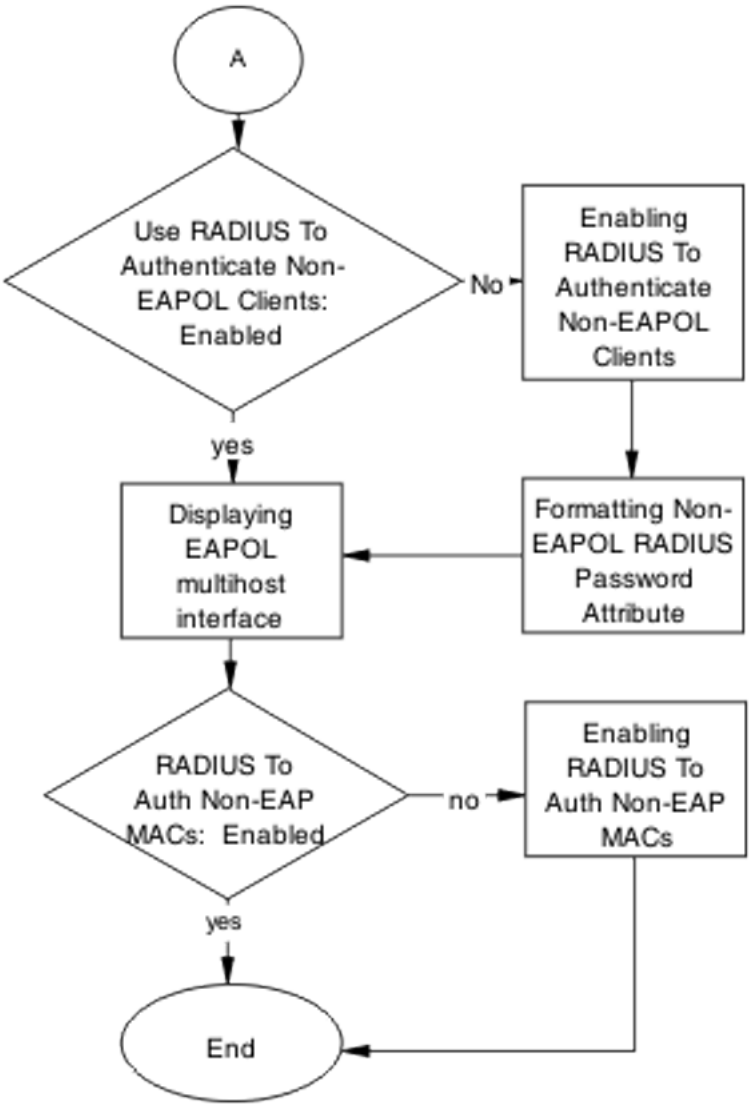


Figure 60: Configure switch part 2

Result

Navigation

- Displaying the EAPOL port on page 135
- Setting global eap enabled and port at eap-auto on page 135
- Displaying EAPOL multihost on page 135
- Enabling RADIUS to authenticate non-EAPOL clients on page 135
- Formatting non-EAPOL RADIUS password attribute on page 136

- Displaying EAPOL multihost interface on page 136
- Enabling RADIUS To Auth non-EAP MACs on page 136

Displaying the 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 status is set to 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 is 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 the RADIUS server using vendor documentation.

Formatting non-EAPOL RADIUS password attribute

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

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

Displaying EAPOL multihost interface

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 any changes to the RADIUS server using vendor documentation.

RADIUS server configuration error

The RADIUS server requires that the correct MAC address and password for the Avaya Ethernet Routing Switch 4500 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.

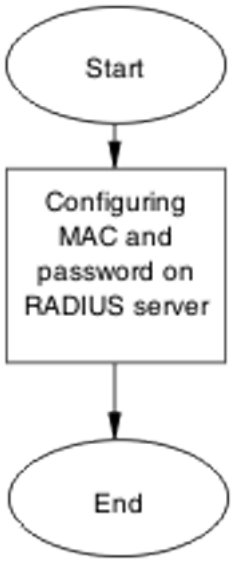


Figure 61: RADIUS server configuration error

Navigation

Configuring MAC and password on RADIUS server on page 137

Configuring MAC and password on RADIUS server

The RADIUS server requires that the MAC and password for the Avaya Ethernet Routing Switch 4500 Series device be correct. If it is incorrect, the Avaya Ethernet Routing Switch 4500 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.

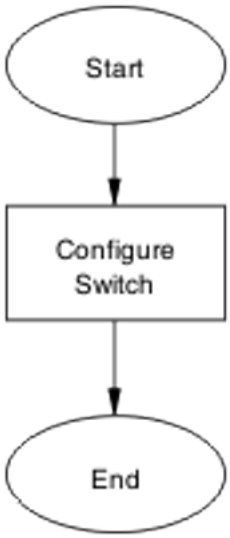


Figure 62: Non-EAP MHSA MAC is not authenticating

Navigation

Configure switch on page 138

Configure switch

Configure the switch to enable MHSA.

Task flow: Configure switch

The following task flows assist you to enable MHSA on the Avaya Ethernet Routing Switch 4500 Series device.

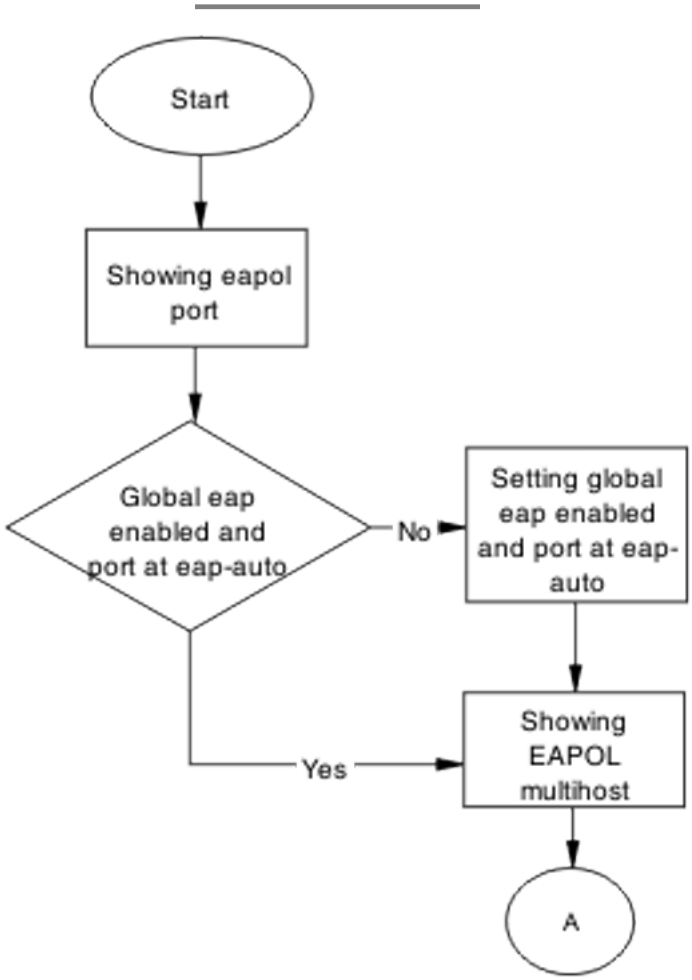


Figure 63: Configure switch part 1

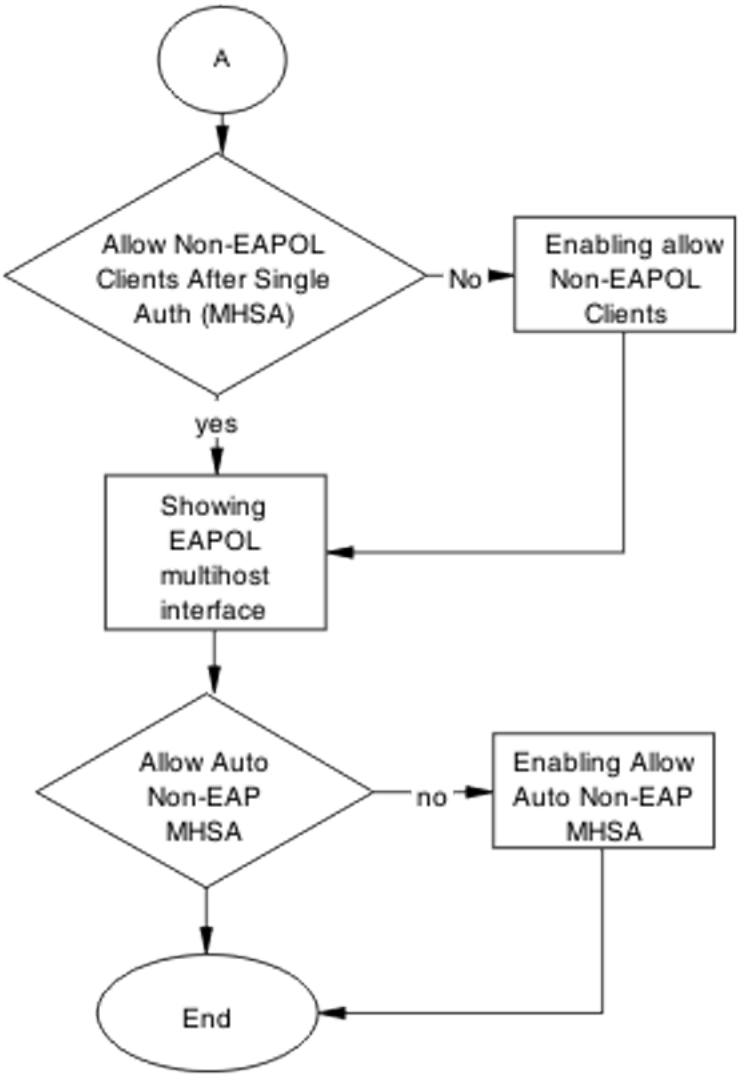


Figure 64: Configure switch part 2

Navigation

- Showing EAPOL port on page 141
- Setting global EAP enabled and port at eap-auto on page 141
- Showing EAPOL multihost on page 141
- Formatting non-EAPOL RADIUS password attribute on page 141
- Showing EAPOL multihost interface on page 141
- Enabling RADIUS to authenticate non-EAPOL clients on page 141
- Enabling RADIUS to auth non-EAP MACs on page 142

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 the 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 the RADIUS server using vendor documentation.

EAP–non-EAP unexpected port shutdown

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

Work flow: EAP–non-EAP unexpected port shutdown

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

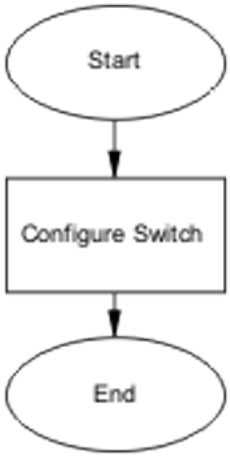


Figure 65: EAP-NEAP unexpected port shutdown

Navigation

Configure switch on page 142

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.

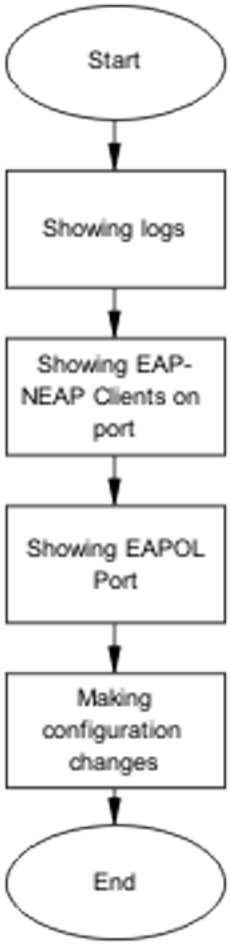


Figure 66: Configure switch

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

Chapter 11: Troubleshooting NSNA

NSNA issues can interfere in the device operation and function. The following work flow contains some common authentication problems.

Troubleshooting NSNA work flow

The following work flow contains some typical NSNAS problems. These situations are not normally dependant upon each other.

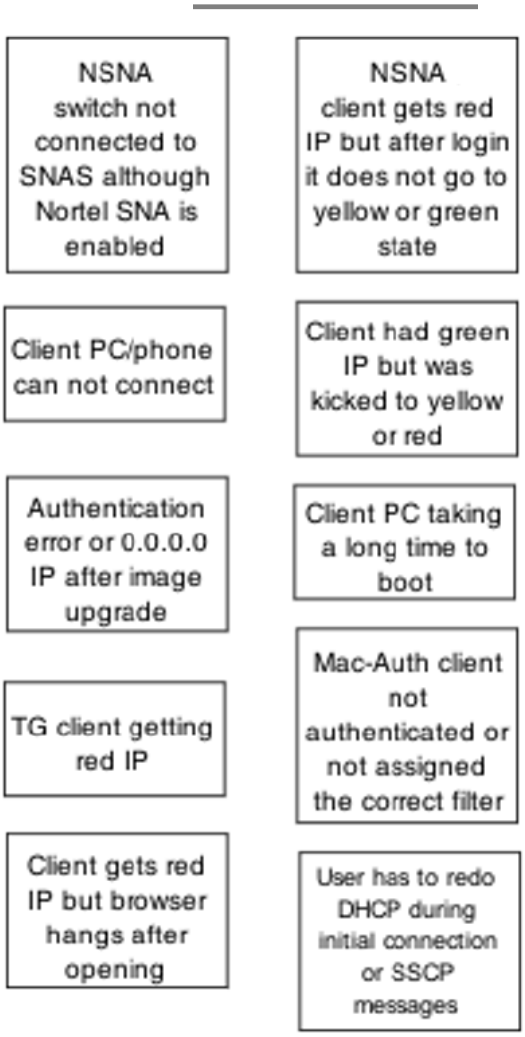


Figure 67: Troubleshooting NSNAS

Navigation

- NSNA switch not connected to NSNAS although NNA is enabled on page 147
- Client PC/phone cannot connect on page 156
- Authentication error or 0.0.0.0 IP after image upgrade on page 166
- TG client getting red IP on page 171
- Client gets red IP but browser hangs after opening on page 174

- NSNA client gets red IP but after login it does not go to yellow or green state on page 176
- Client had green IP but was moved to yellow or red on page 178
- Client PC taking a long time to boot on page 181
- Mac-Auth client not authenticated or not assigned the correct filter on page 183
- Client has no DHCP information during initial connection or SSCP messages on page 186

NSNA switch not connected to NSNAS although NNA is enabled

Ensure the NSNAS is displayed as connected to the Avaya Ethernet Routing Switch 4500 Series device.

The secure image must be running on the device to support NSNA and SSH. If you require these features, see the section on updating switch software in *Avaya Ethernet Routing Switch 4500 Series Release 5.2 Release Notes* (NN47205-400).

Work flow: NSNA switch not connected to NSNAS although NSNA is enabled

The following work flow assists you to determine the solution for an NSNA switch that does not connect to a NSNAS.

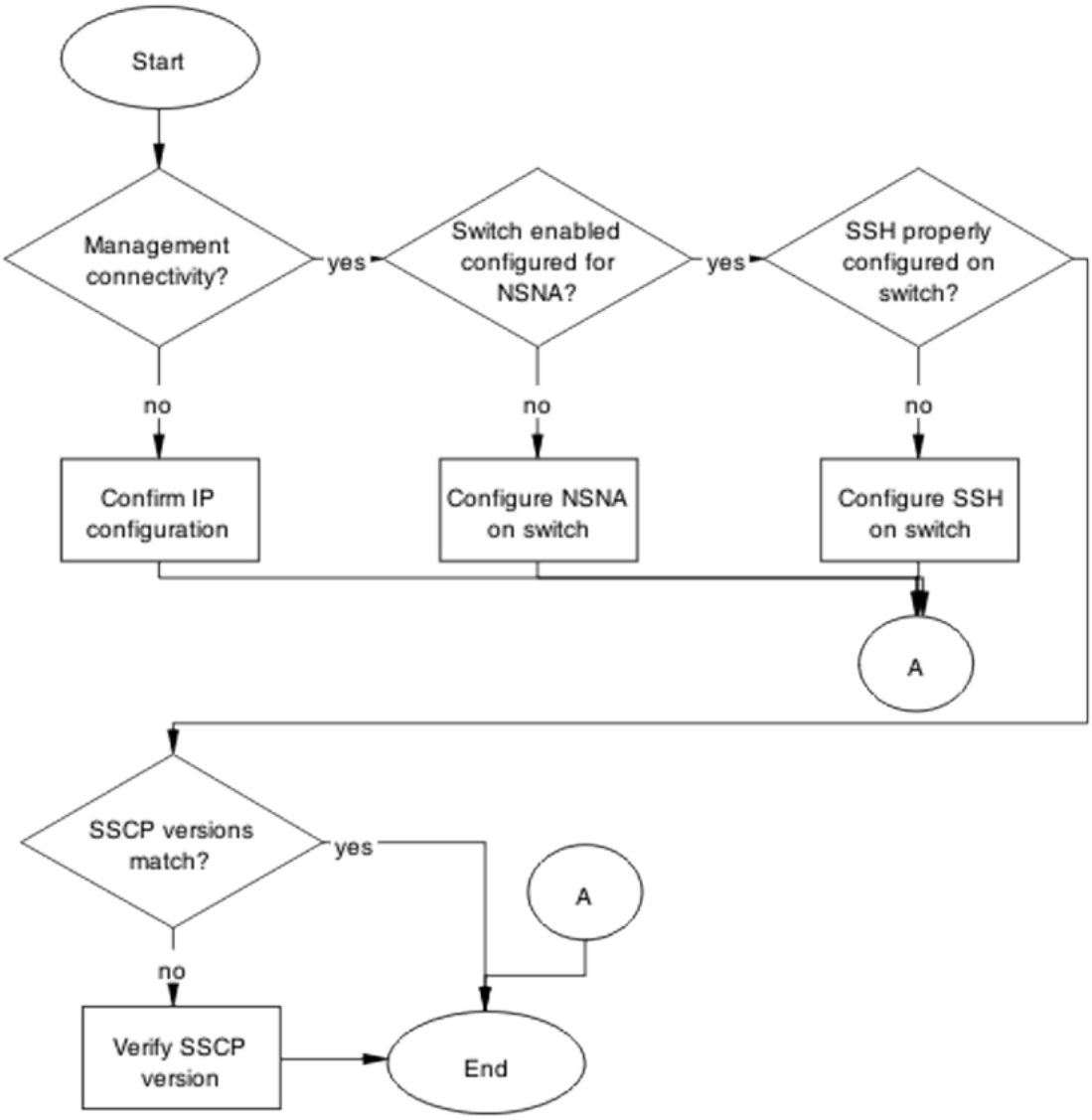


Figure 68: NSNA switch not connected to NSNAS although NSNA is enabled

Navigation

- Confirm IP configuration on page 149
- Configure NSNA on switch on page 150
- Configure SSH on switch on page 152
- Verify SSCP version on page 155

Confirm IP configuration

Correct IP connectivity to restore management connectivity.

Task flow: Confirm IP configuration

The following task flow assists you to correct IP connectivity to restore management connectivity.

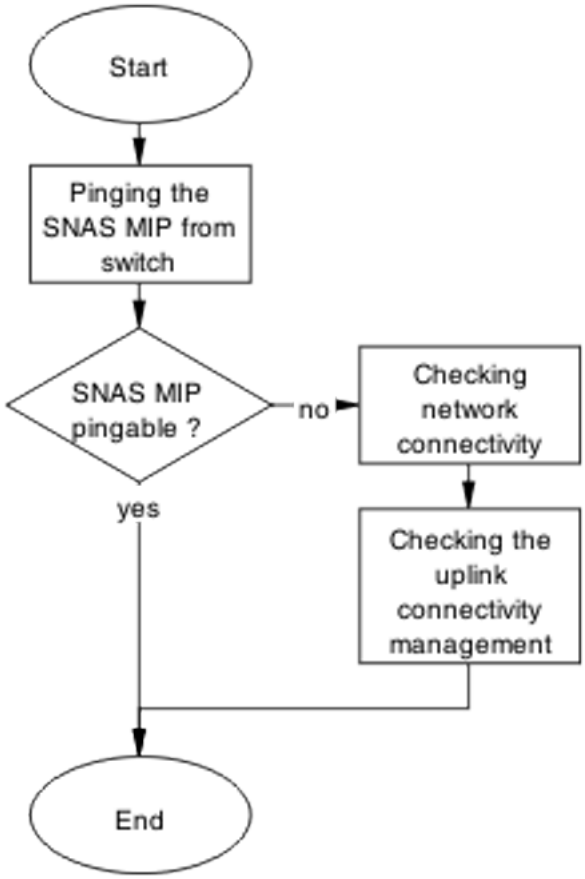


Figure 69: Confirm IP configuration

Navigation

Pinging the NSNAS MIP from switch

Confirm IP connectivity from the switch exists.

1. Use the **`ping <IP>`** command from the switch.
2. Note the ping response displayed.

Checking network connectivity from switch to router to SNAS

Confirm network connection from the switch to SNAS exists.

1. Use the **`ping <SNAS IP>`** command from the switch.
2. Note the ping response displayed.

Checking the uplink connectivity management

1. Use the **`cfg/domain 1/switch Y`** command followed by "cur" .
2. Note the response displayed.

Configure NSNA on switch

Configure and enable NSNA on the switch.

Task flow: Configure NSNA on switch

The following task flow assists you to ensure the Avaya Ethernet Routing Switch 4500 Series device has NSNA enabled.

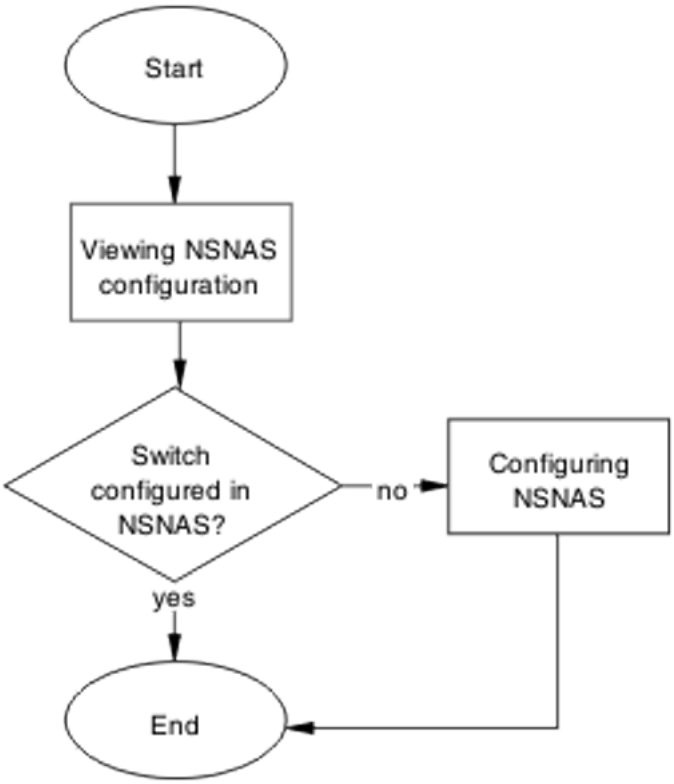


Figure 70: Configure NSNA on switch

Navigation

- Checking NSNAS configuration on page 151
- Configuring NSNA on page 152

Checking NSNAS configuration

Verify the current configuration.

1. Use the **cfg/domain 1/switch Y** command followed by "cur" .
2. Note if the switch is configured in the NSNAS.

Configuring NSNA

Configure NSNA for the switch.

1. Create the VLANs on the switch using the following commands:
   - **vlan create 210 type port**
   - **vlan create 220 type port**
   - **vlan create 230 type port**
   - **vlan create 240 type port**
2. Use the **NSNA NSNAs <IP>/<subnet> port <port>** command to configure the NSNAS IP address/subnet and the TCP communication port.
3. Set the created VLANs as NSNA VoIP, RED, YELLOW, and GREEN VLANs using the following commands:
   - **NSNA vlan 240 color voip**
   - **NSNA vlan 210 color red filter RED**
   - **NSNA vlan 220 color yellow filter YELLOW yellow-subnet 10.200.201.0/24**
   - **NSNA vlan 230 color green filter GREEN**
4. Set ports as NSNA uplink and dynamic using the following commands:
   - **interface fast Ethernet all**
   - **NSNA port 47-48 uplink vlans 210,220,230,240**
   - **NSNA port 1-46 dynamic voip-vlans 240**

Configure SSH on switch

Correct the SSH configuration on the switch.

Task flow: Configure SSH on switch

The following task flow assists you to ensure SSH is configured on the Avaya Ethernet Routing Switch 4500 Series device.

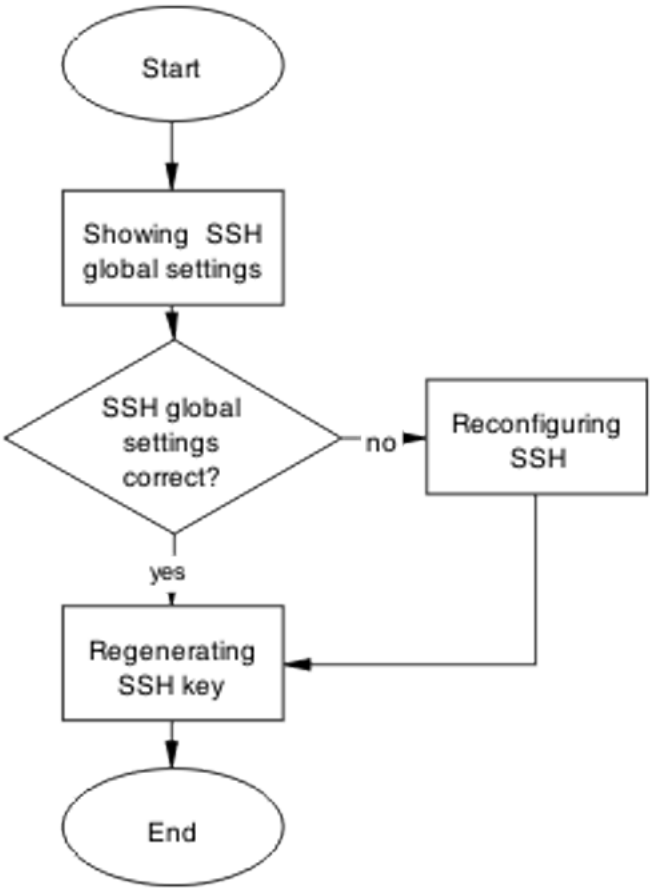


Figure 71: Configure SSH on switch

Navigation

- Showing SSH globally on page 154
- Reconfiguring SSH on page 154
- Regenerating SSH key on page 154

Showing SSH globally

Display the SSH configuration of the switch.

1. Use the **show ssh global** command to display the current configuration.
2. Confirm the SSH setting is correct.

Reconfiguring SSH

Change the SSH settings to be correct.

1. Use the **no ssh dsa-auth-key** command to delete the SSH DSA auth key.
2. Use the **ssh download-auth-key address <IP> key-name snaskey.pub** command to download the correct NSNAS public key.
3. Use the **ssh** command to enable SSH globally.

Regenerating SSH key

Regenerate the SSH key if all SSH settings are correct and the problem still exists.

1. Enter the **no NSNA** command.
2. Enter the **no ssh** command.
3. Enter the **no ssh dsa-auth-key** command.
4. Enter the **ssh** command.
5. Enter the **NSNA enable** command.
6. On the NSNAS, navigate to /cfg/domain 1/switch 1/sshkey and import the switch SSH key using the **SSH Key# import** command.
7. Enter the **apply** command to keep the changes.
8. Enter the **show NSNA** command to review the changes.

Verify SSCP version

Ensure the correct SSCP version is on the switch.

Task flow: Verify SSCP version

The following task flow assists you to verify the SSCP version on the Avaya Ethernet Routing Switch 4500 Series device.

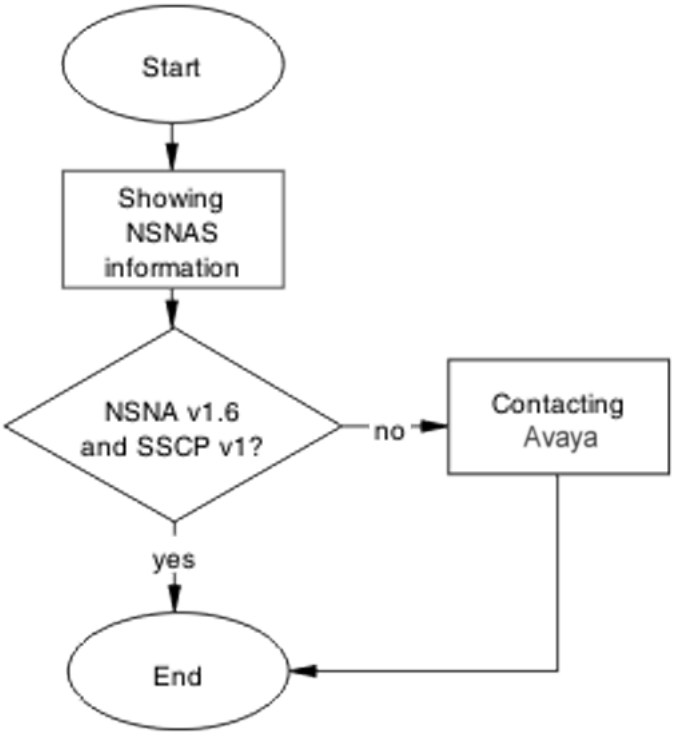


Figure 72: Verify SSCP version

Navigation

- Showing NSNA on page 156
- Contacting Avaya on page 156

Showing NSNA

Display the NSNA information for review.

1. Enter the **`show NSNA`** command to display the configuration.
2. Enter the **`/info/local`** command to display the software version on the NSNAS side.
3. Ensure the following is on the switch:

   NSNAS Connection Version: SSCPv1

   Higher versions are backward compatible.
4. Verify that the SNAS has the following:

   Software version: 1.6.1.2

   Higher versions are backward compatible.

Contacting Avaya

Engage Avaya in the troubleshooting by advising of the software discrepancy.

Follow the Avaya customer service procedures at your convenience.

Client PC/phone cannot connect

Use the procedures in this section to correct connection issues between the PC or phone and the switch.

Work flow: Client PC/phone can not connect

The following work flow assists you to determine the solution for a client PC or phone that cannot connect.

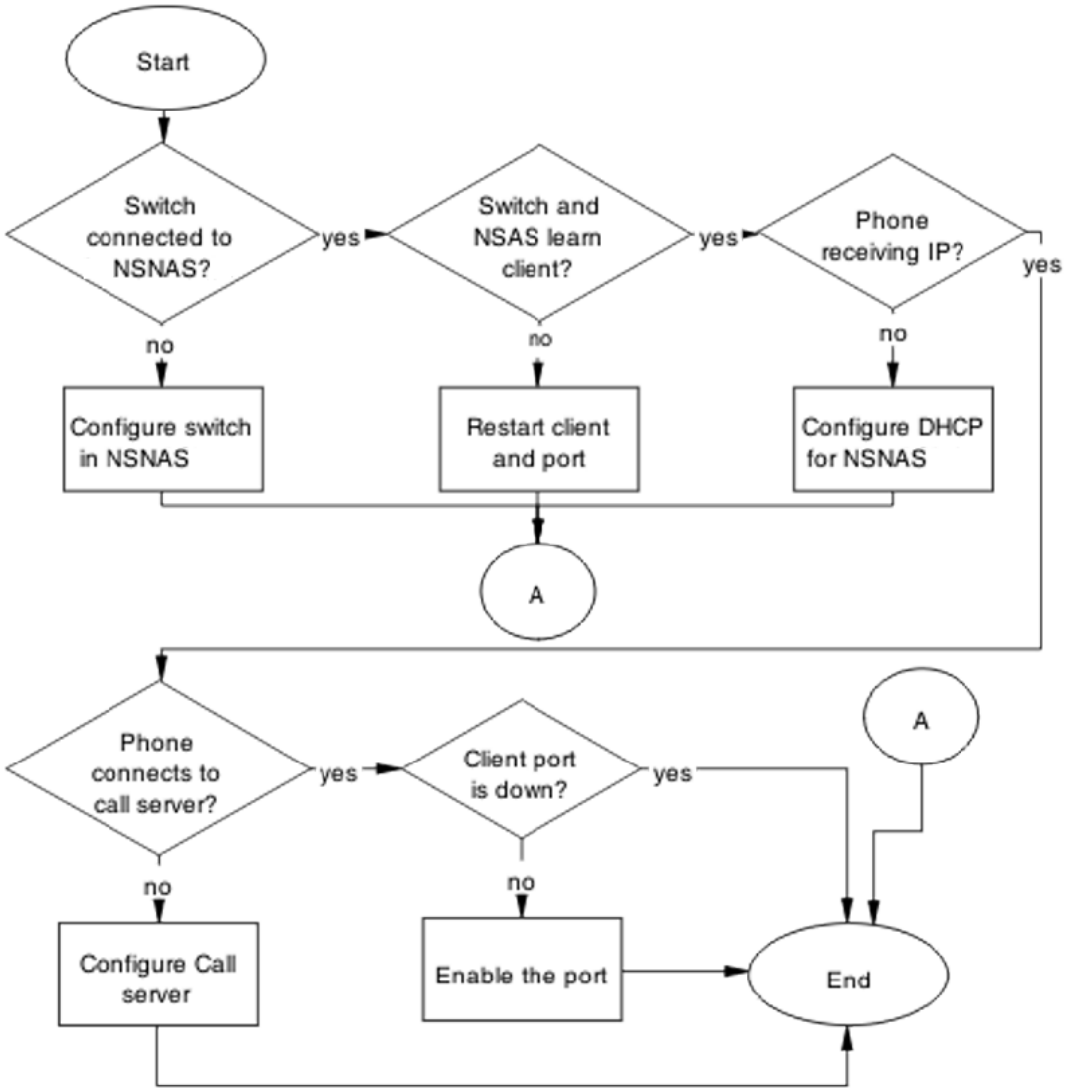


Figure 73: Client PC/phone can not connect

Navigation

- Configure switch on NSNAS on page 158
- Restart client and port on page 159
- Configure DHCP for NSNAS on page 161
- Configure call server on page 163
- Enable the port on page 164

Configure switch on NSNAS

Configure and enable the switch on the NSNAS.

Task flow: Configure the switch on NSNAS

The following task flow assists you to enable the Avaya Ethernet Routing Switch 4500 Series device on the NSNAS.

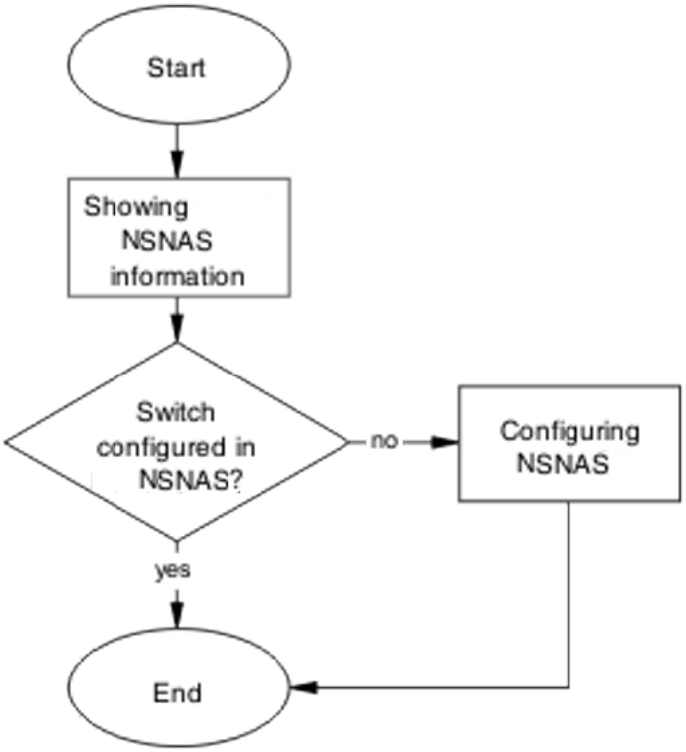


Figure 74: Configure the switch on NSNAS

Showing NSNA information

Verify the current configuration.

1. Use the **`cfg/domain 1/switch Y`** command followed by "cur".
2. Note if the switch is configured in the NNAS.

Configuring NSNAS

Configure the NSNAS with the settings for the Avaya Ethernet Routing Switch 4500 Series device.

Review the NSNAS documentation for configuration information and procedures.

Restart client and port

Ensure that the client and port are restarted.

Task flow: Restart client and port

The following task flow assists you to restart both the client and port.

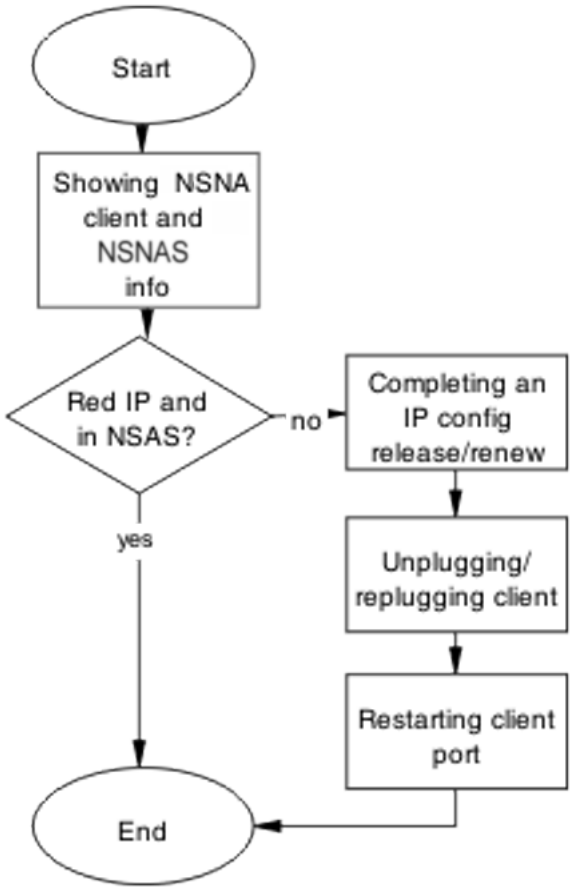


Figure 75: Restart client and port

Navigation

- Showing NSNA client and NSNAS info on page 160
- Completing an IP config release/renew on page 161
- Unplugging/replugging client on page 161
- Restarting client port on page 161

Showing NSNA client and NSNAS info

Display the NSNA client information

1. Use the **show NSNA client** command.
2. Note the output.
3. Use the **info/switch 1 n** command on the NSNAS.
4. Both are to be showing a consistent status.

Completing an IP config release/renew

Force a full IP config release and renew of IP information.

1. Using vendor documentation, perform an ipconfig release on the client PC.
2. Using vendor documentation, perform an ipconfig renew on the client PC.

Unplugging/replugging client

Physically disconnect the client from the network.

1. Following local network procedures, unplug the client PC from the network.
2. Wait a minimum of 10 seconds.
3. Following local network procedures, connect the client PC to the network.

Restarting client port

Shut down the client port, and then restart it.

Follow vendor procedures to shut down and restart the client port.

Configure DHCP for NSNAS

If the phone is still not getting an IP, eliminate DHCP configuration issues.

Task flow: Configure DHCP for NSNA

The following task flow assists you to configure DHCP for NSNA.

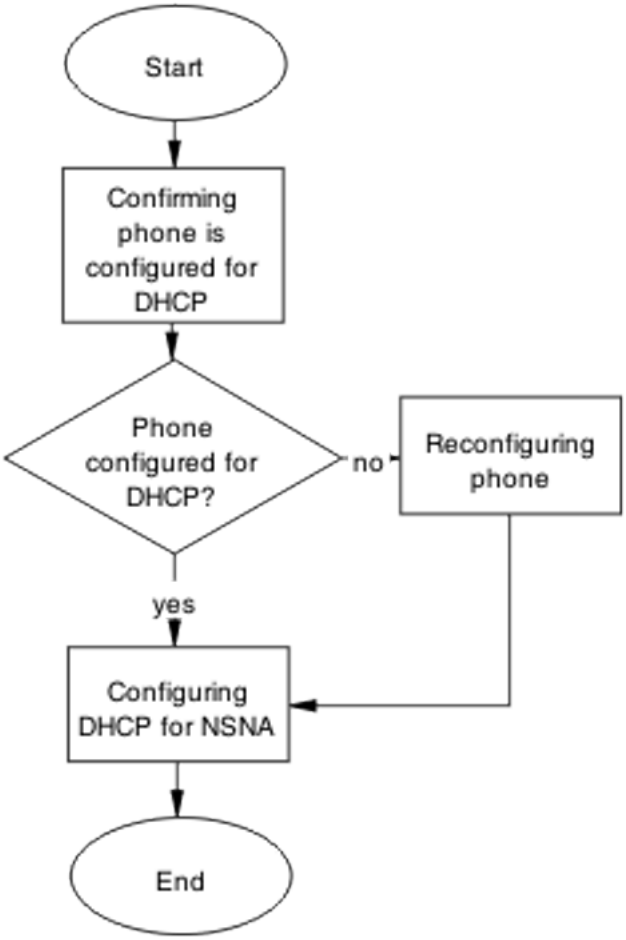


Figure 76: Configure DHCP for NSNA

Confirming phone is configured for DHCP

Ensure the phone is configured as a DHCP client.

Review vendor documentation to ensure the phone is properly configured for DHCP.

Reconfiguring phone

Change the phone settings so it is configured as a DHCP client.

Review vendor documentation to change settings of the phone to act as a DHCP client.

Configuring DHCP for NSNA

Change the DHCP server to work with NSNA.

Review vendor documentation to change settings of the DHCP server.

Configure call server

Ensure the call server is properly configured.

Task flow: Configure call server

The following task flow assists you to configure the call server.

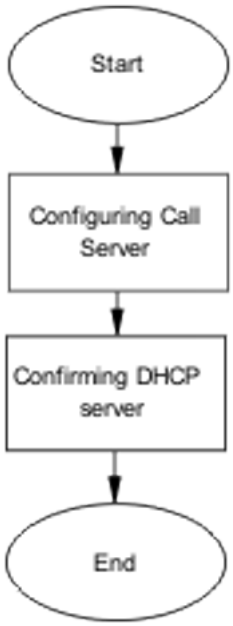


Figure 77: Configure call server.

Navigation

- Configuring call server on page 164
- Configuring DHCP server on page 164

Configuring call server

Ensure the call server is properly configured.

Review vendor documentation of the call server and ensure all configurations are correct.

Configuring DHCP server

Ensure the DHCP server is properly configured.

Review vendor documentation of the DHCP server and ensure all configurations are correct.

Enable the port

Enable the port after a new client PC/Phone (behind a hub) is unable to get an IP or connect, or if the Avaya Ethernet Routing Switch 4500 Series client port is down.

Task flow: Enable the port

The following task flow assists you to enable the port.

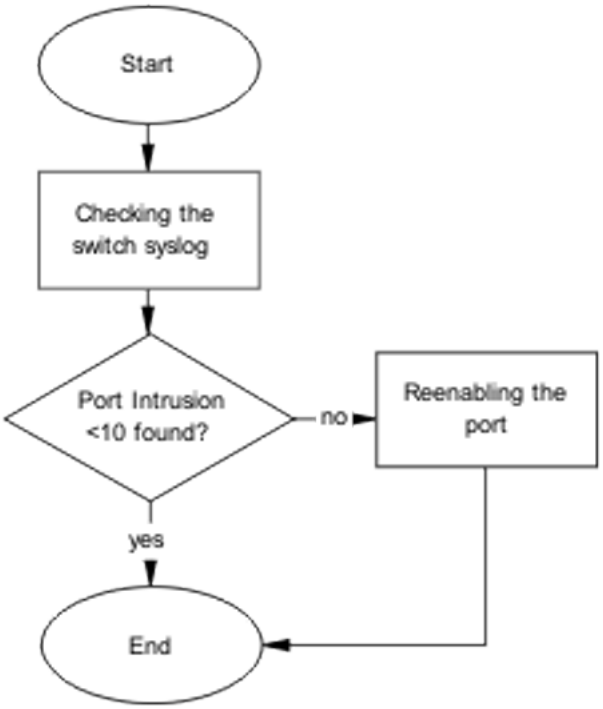


Figure 78: Enable the port

Navigation

- Checking the switch log on page 165
- Reenabling the port on page 165

Checking the switch log

Review the switch log to determine if more than 10 intruders have been detected.

1. Use the command **`show logging`** to view the log messages.
2. Review the information in the log messages.

Reenabling the port

Enable the port after it was shut down due to detected intrusion.

1. Use the command **no shutdown <port>** to enable a port that was disabled.
2. Observe no errors after execution.

Authentication error or 0.0.0.0 IP after image upgrade

Eliminate some common problems after an image upgrade that can lead to errors.

Work flow: Authentication error or 0.0.0.0 IP after image upgrade

The following work flow assists you to determine the solution for authentication errors or an IP address of 0.0.0.0 immediately following an upgrade of the image.

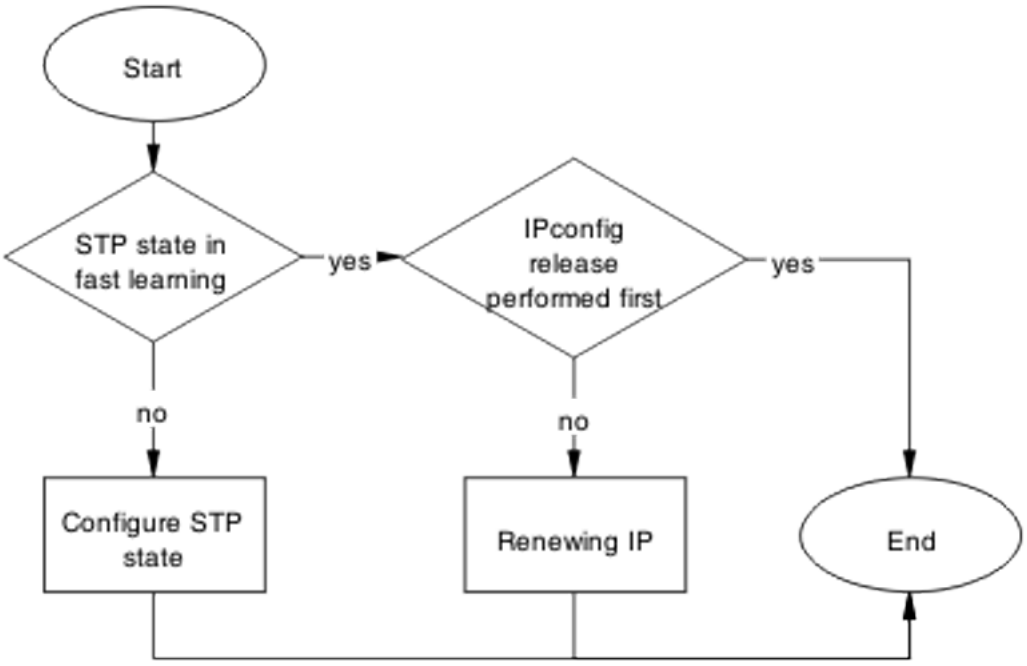


Figure 79: Authentication error or 0.0.0.0 IP after image upgrade

Navigation

- Configure STP state on page 167
- Renewing IP on page 169

Configure STP state

Place the STP state in fast learning if the ports come up too fast.

Important:
Ensure that you clearly understand the consequences of performing this action on an uplink to prevent loops.

Task flow: Configure STP state task flow

The following task flow assists you to configure the STP for fast learning.

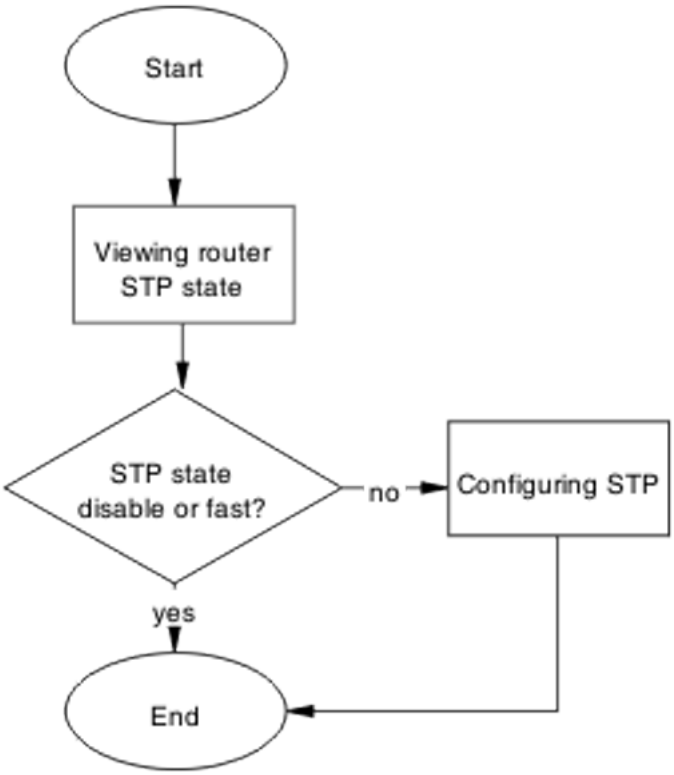


Figure 80: Configure STP state

Navigation

- Viewing Router STP state on page 168
- Configuring STP state on page 169

Viewing Router STP state

Identify what the STP state is on the router.

1. Use the **`show spanning-tree port`** command to show the router STP state.
2. Note the following:

   STP State is disable or fast

Configuring STP state

Set the STP state to fast learning.

1. Use the **`spanning-tree port 1 learning fast`** command to set the STP state to fast learning.
2. Observe no errors after execution.

Renewing IP

Renew the IP properly to restore the connection.

Task flow: Renewing IP

The following task flow assists you to properly release and renew an IP address.

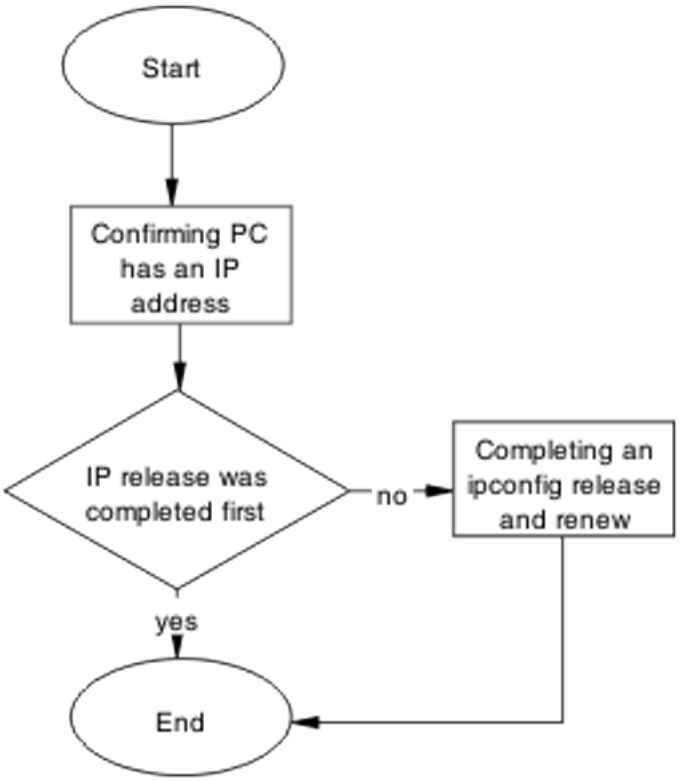


Figure 81: Renewing IP

Navigation

- Confirming PC has IP address on page 170
- Completing and ipconfig release and renew on page 171

Confirming PC has IP address

Confirm the PC has a proper IP.

1. Using vendor documentation, use the **`ipconfg /all`** command to view the IP information of the PC.
2. Note the IP address and other IP information.

Completing and ipconfig release and renew

Perform a proper ipconfig /release prior to an ipconfig /renew.

1. Using vendor documentation, use the **`ipconfg /release`** command to release the IP information of the PC.
2. Using vendor documentation, use the **`ipconfg /renew`** command to renew the IP information of the PC.

TG client getting red IP

Eliminate the switch blocking traffic to SNAS.

Work flow: TG Client getting red IP

The following work flow assists you to determine the solution for a TG client that obtains a red IP.

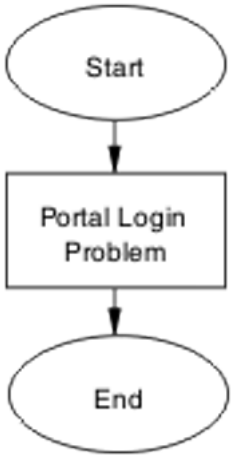


Figure 82: TG Client getting red IP

Navigation

Portal Login Problem on page 172

Portal Login Problem

Eliminate the location of the interruption to properly configure the NSAS port IP if required.

Task flow: Portal login problem

The following task flow assists you to eliminate the interruption to configure the NSAS port IP.

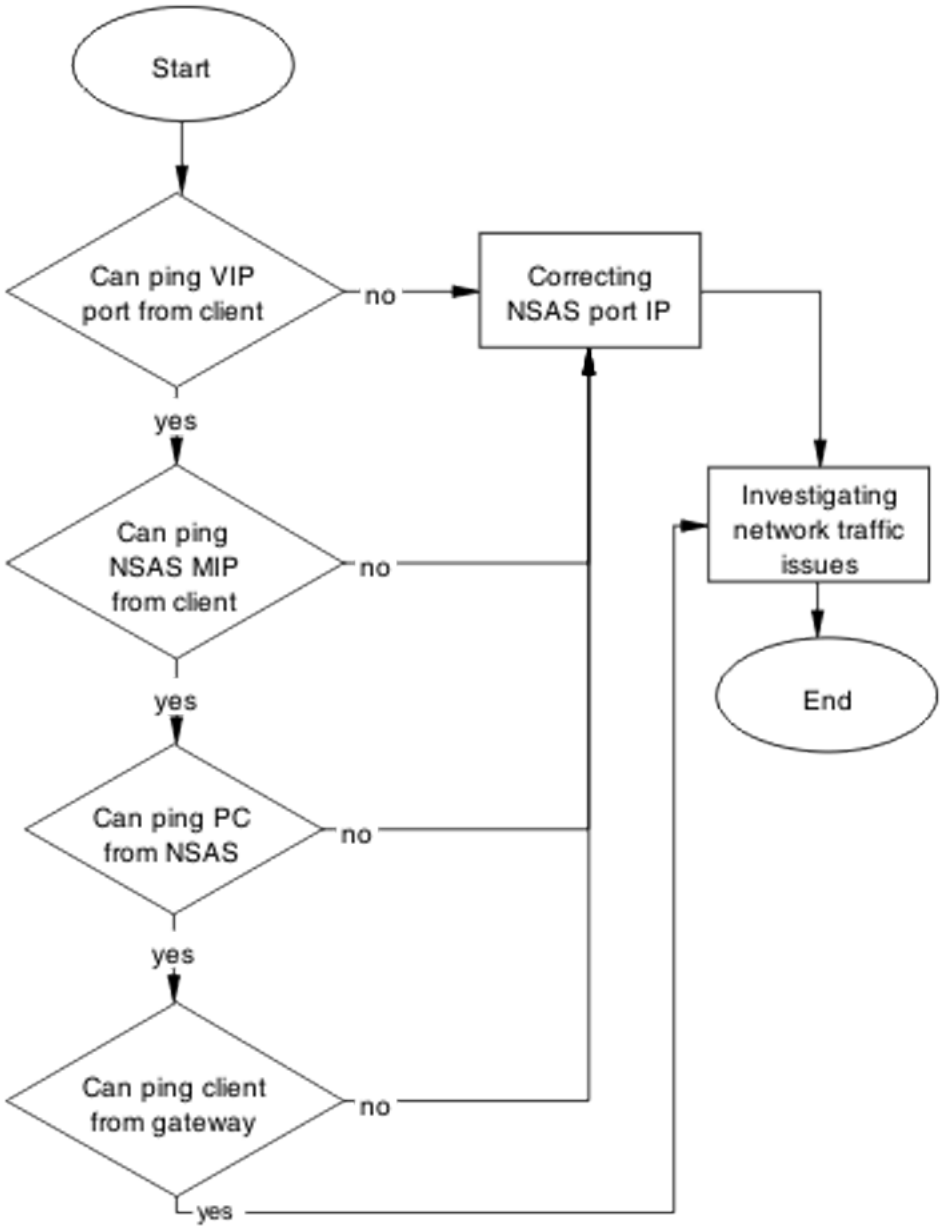


Figure 83: Portal login problem

Navigation

- Correcting NSAS port IP on page 174
- Investigating network traffic issues on page 174

Correcting NSAS port IP

Make changes to NSAS port IP.

1. Use the **`/info/domain`** command in the NSNAS CLI. Portal VIP addr(s) for the domain is the IP address.
2. Use the **`/info/sys`** command in the NSNAS CLI. Management IP (MIP) address is the IP address.

Investigating network traffic issues

Eliminate network traffic issues that may impede the browser.

Use local documentation and protocol to investigate network traffic issues. The Planning and Engineering document may be of assistance.

Client gets red IP but browser hangs after opening

Restart the browser to correct a browser hanging issue.

Work flow: Client gets red IP but browser hangs after opening

The following work flow assists you to determine the solution for a client that obtains a red IP but the browser hangs after it appears.

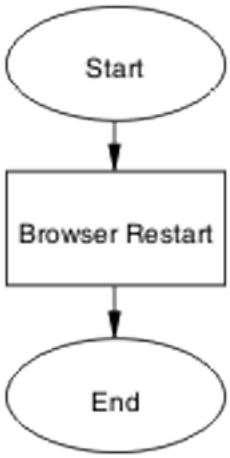


Figure 84: Client gets red IP but browser hangs after opening

Navigation

Browser restart on page 175

Browser restart

Restart the browser to regain connectivity.

Task flow: Browser restart

The following task flow assists you to restart the browser.

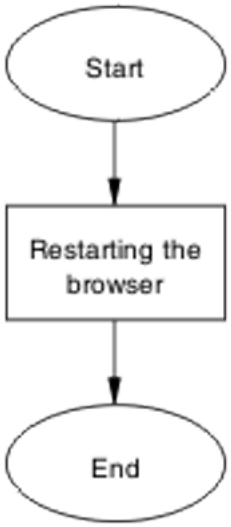


Figure 85: Browser restart

Navigation

Restarting the browser on page 176

Restarting the browser

Fully close and restart a browser.

1. Following local procedures and guidelines, close all instances of the browser.
2. Restart the browser.
3. Navigate to the portal.

NSNA client gets red IP but after login it does not go to yellow or green state

Made corrections to prevent the client from maintaining a red state for too long due to NSNA communication failure.

Work flow: NSNA client gets red IP but after login it does not go to yellow or green state

The following work flow assists you to determine the solution for a NSNA client that obtains a red IP but fails to move to yellow or green state after login.

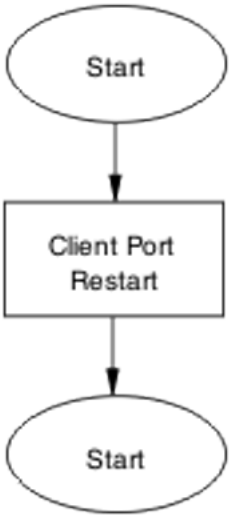


Figure 86: NSNA client gets red IP but after login it does not go to yellow or green state

Navigation

Client port restart on page 177

Client port restart

Set the client link down and then up.

Task flow: Client port restart

The following task flow assists you to restart the client port.

Figure 87: Client port restart

Restarting client port link

Shut down the client port, then restart it.

Follow vendor procedures to shut down and restart the client port.

Client had green IP but was moved to yellow or red

Correct the communication issue causing the IP status to change.

Work flow: Client had green IP but was moved to yellow or red

The following work flow assists you to determine the solution for a client that has had a green IP but changes to yellow or red.

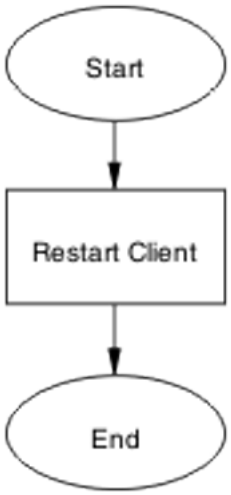


Figure 88: Client had green IP but was moved to yellow or red

Navigation

Restart client on page 179

Restart client

Shut down the client, then start to regain proper communication.

Task flow: Restart client

The following task flow assists you to restart the client.

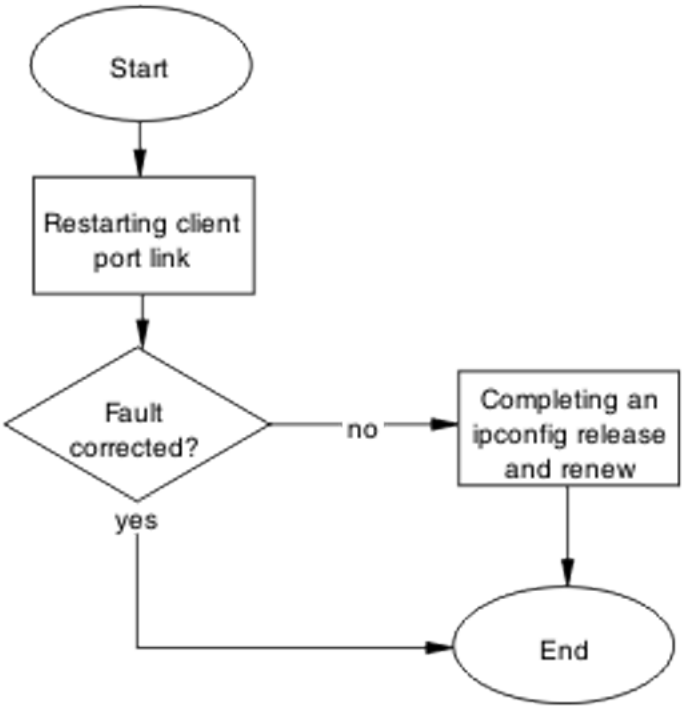


Figure 89: Restart client

Navigation

- Restarting client port link on page 180
- Completing an ipconfig release and renew on page 180

Restarting client port link

Shut down the client port, then restart it.

Follow vendor procedures to shut down and restart the client port.

Completing an ipconfig release and renew

Perform a proper ipconfig /release prior to an ipconfig /renew.

1. Using vendor documentation, use the **`ipconfg /release`** command to release the IP information of the PC.
2. Using vendor documentation, use the **`ipconfg /renew`** command to renew the IP information of the PC.

Client PC taking a long time to boot

Correct a port configuration issue that is causing the PC to have a long boot time.

Work flow: Client PC taking a long time to boot

The following work flow assists you to determine the solution for a client PC that takes an unusually long time to boot.

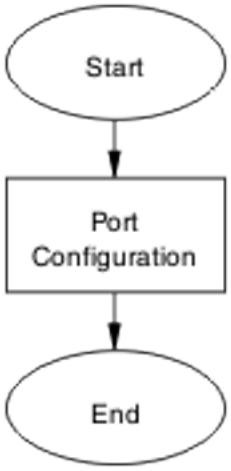


Figure 90: Client PC taking a long time to boot

Navigation

Port configuration on page 182

Port configuration

Identify and open the necessary ports that are being used by the client PC domain login in the red VLAN.

Task flow: Port configuration

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

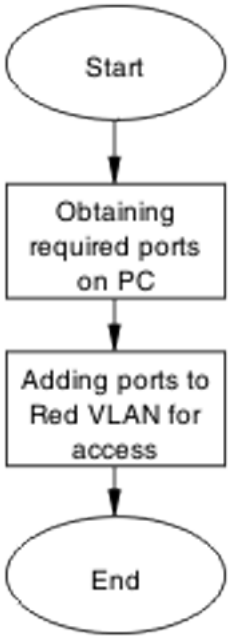


Figure 91: Port configuration

Navigation

- Obtaining required ports on PC on page 183
- Adding ports to red VLAN for access on page 183

Obtaining required ports on PC

Identify the correct ports that are required for the VLAN.

Following local procedures and vendor documentation, identify the ports that are required for the PC.

Adding ports to red VLAN for access

Ensure the ports identified are added to the red VLAN so all traffic can gain access.

1. Refer to *Avaya Ethernet Routing Switch 4500 Series Configuration — Quality of Service* (NN47205-504) for command syntax to add ports to the red VLAN.
2. Repeat previous step as required for multiple ports.

Result

Example of adding ports to a VLAN

1. In Global Configuration mode, enter **`qos nsna classifier name red protocol 17 dst-port-min 427 dst-port-max 427 ethertype 0x0800 drop-action disable block RED eval-order 101`**.
2. In Global Configuration mode, enter **`qos nsna classifier name red protocol 6 dst-port-min 524 dst-port-max 524 ethertype 0x0800 drop-action disable block RED eval-order 102`**.

Mac-Auth client not authenticated or not assigned the correct filter

Correct the client that is not authenticating. Authentication can fail if the correct filter is not assigned.

Work flow: Mac-Auth client not authenticated or not assigned the correct filter

The following work flow assists you to determine the solution for a MAC authentication client that does not authenticate or is not assigned the proper filter.

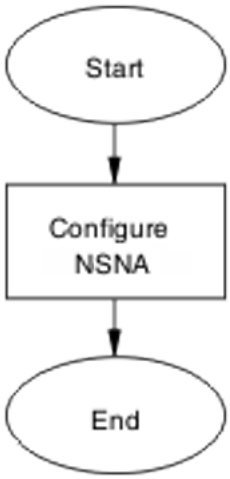


Figure 92: Mac-Auth client not authenticated or not assigned the correct filter

Navigation

Configure NSNAS on page 184

Configure NSNAS

Change the NSNAS settings to ensure authentication can occur.

Task flow: Configure NSNAS

The following task flow assists you to configure the NSNAS to allow authentication.

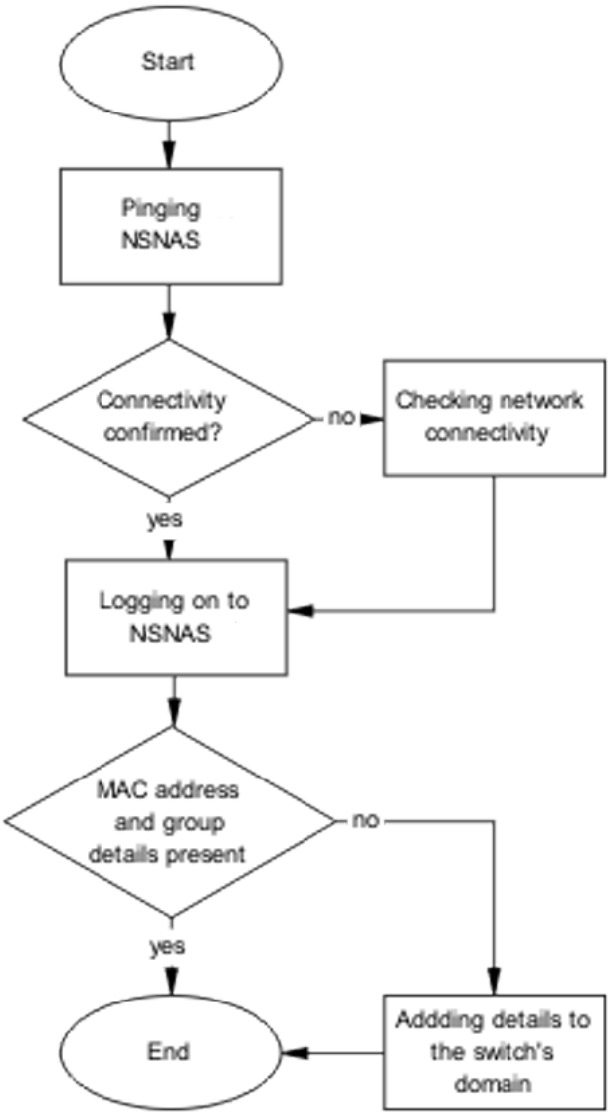


Figure 93: Configure NSNAS

Navigation

- Pinging NSNAS on page 186
- Checking network connectivity on page 186
- Logging on to NSNAS on page 186
- Adding details to the switch domain on page 186

Pinging NSNAS

Verify the network connectivity using ping.

1. Use the **ping <NSNASIP>** command to ensure connectivity.
2. Observe the details delivered.

Checking network connectivity

Verify that the network has no other network issues preventing the connection.

Use local protocol and network information to correct network issues.

Logging on to NSNAS

Log on to the NSNAS to view more information.

1. Use vendor procedure to log on to the NSNAS.
2. Observe the following:

   The macdb list for the switch's domain

Adding details to the switch domain

Add the MAC address and group details to the switch domain.

Follow vendor documentation to add the mac-address and group details.

Client has no DHCP information during initial connection or SSCP messages

Reestablish the identification of a client to the SNAS.

Work flow: Client has no DHCP information during initial connection or SSCP messages

The following work flow assists you to have a client recognized by SNAS after initial connection. If the DHCP information fails to be sent to the client, you can redo DHCP. If the client starts within five seconds after the connection is initialized, the client may be unable to log in.

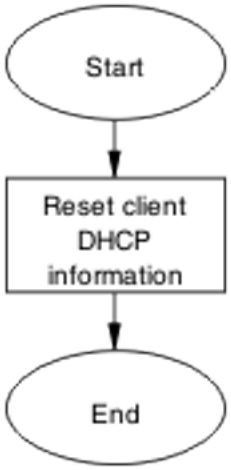


Figure 94: Client has no DHCP information during initial connection or SSCP messages

Navigation

Disconnect and reconnect client on page 187

Disconnect and reconnect client

Shut down the client, then start to regain proper identification.

Task flow: Disconnect and reconnect client

The following task flow assists you to disconnect and reconnect the client.

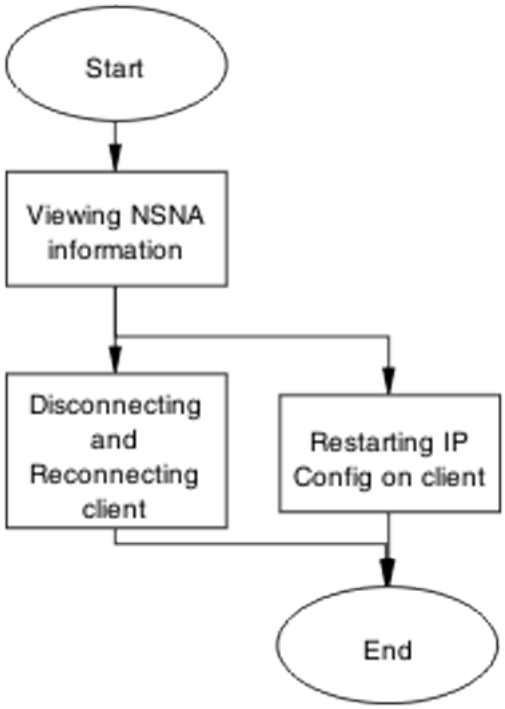


Figure 95: Disconnect and reconnect client

Navigation

- Viewing NSNA information on page 188
- Disconnecting and reconnecting client on page 189
- Restarting IP Config on client on page 189

Viewing NSNA information

View the NSNA information for the device or stack.

1. Use the **`show nsna`** command to display the NSNA information.
2. Observe the displayed information and identify the client that is not recognized.

Disconnecting and reconnecting client

Perform a proper ipconfig /release prior to an ipconfig /renew.

1. Using vendor documentation, use the **`ipconfg /release`** command to release the IP information of the PC.
2. Using vendor documentation, use the **`ipconfg /renew`** command to renew the IP information of the PC.

Restarting IP Config on client

Perform a proper ipconfig /release prior to an ipconfig /renew.

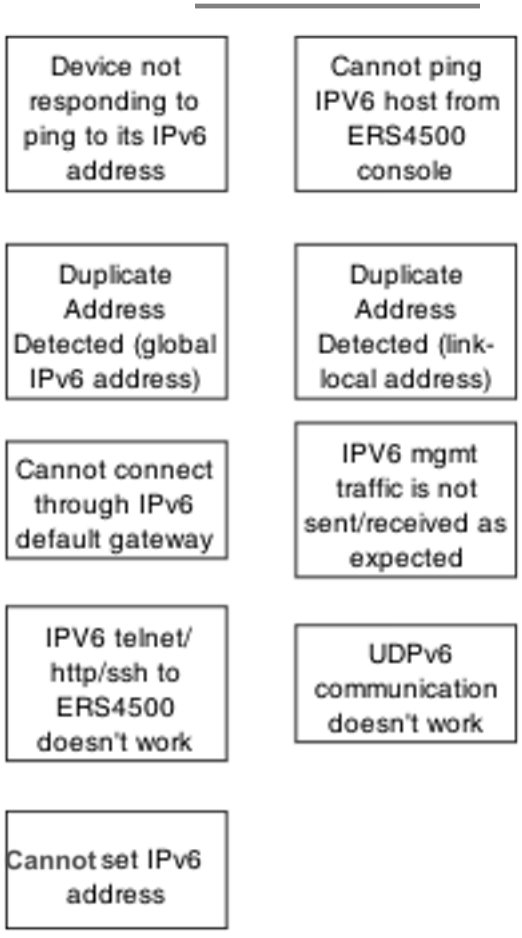
1. Using vendor documentation, use the **`ipconfg /release`** command to release the IP information of the PC.
2. Using vendor documentation, use the **`ipconfg /renew`** command to renew the IP information of the PC.

Chapter 12: Troubleshooting IPv6

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

Troubleshooting IPv6 work flow

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



Navigation

Device not responding to ping to its IPv6 address

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

Device not responding to ping to its IPv6 address task flow

Use these task flows to restore the connectivity through IPv6.

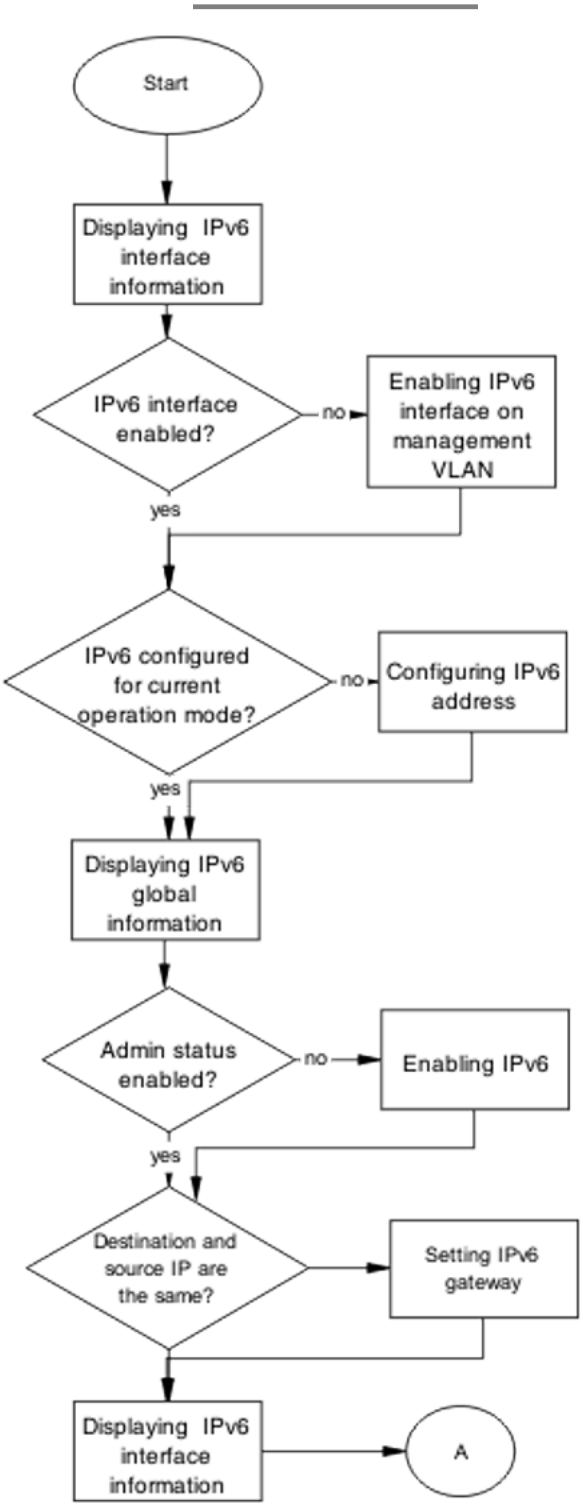


Figure 96: Task flow: Device not responding to ping to its IPv6 address part 1

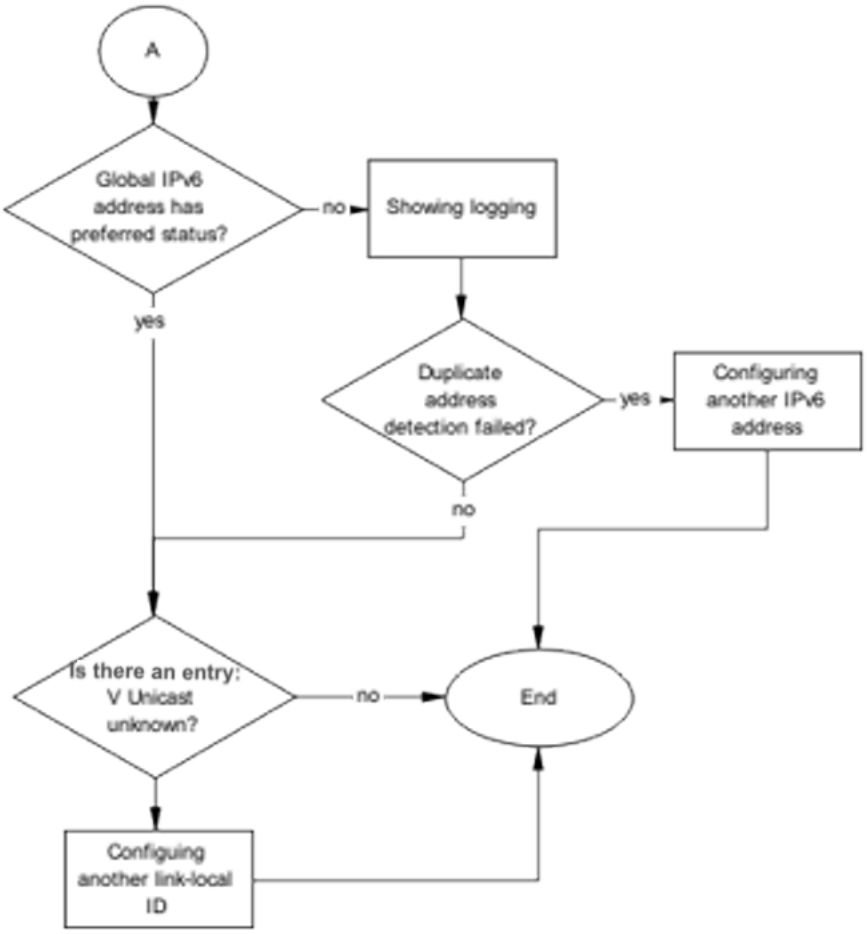


Figure 97: Task flow: Device not responding to ping to its IPv6 address part 2

Navigation

- Displaying IPv6 interface information on page 195
- Enabling IPv6 interface on management VLAN on page 195
- Configuring IPv6 address on page 195
- Displaying IPv6 global information on page 196
- Enabling IPv6 on page 196
- Setting IPv6 gateway on page 196
- Displaying IPv6 interface information on page 196
- Showing logging on page 197

- Configuring another IPv6 address on page 197
- Configuring another link-local ID on page 197

Displaying IPv6 interface information

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

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

Enabling IPv6 interface on management VLAN

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

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

Configuring IPv6 address

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

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

Displaying IPv6 global information

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

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

Enabling IPv6

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

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

Setting IPv6 gateway

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

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

Displaying IPv6 interface information

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

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

Showing logging

Use the procedure in this section to display logging information.

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

Configuring another IPv6 address

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

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

Configuring another link-local ID

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

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

Cannot ping IPV6 host from device console

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

Cannot ping IPV6 host from device console task flow

Use this task flow to restore the connectivity through IPv6.

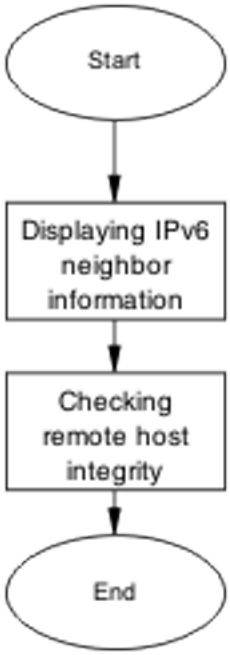


Figure 98: Task flow: Cannot ping IPV6 host from device console

Navigation

- Displaying IPv6 neighbor information on page 199
- Checking remote host integrity on page 199

Displaying IPv6 neighbor information

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

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

Checking remote host integrity

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

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

Duplicate address detected (global IPv6 address)

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

Duplicate address detected (global IPv6 address)

Use this task flow to restore the connectivity through IPv6.

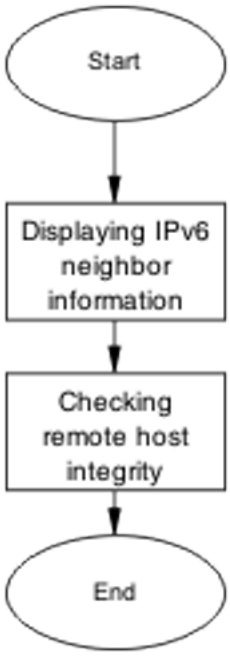


Figure 99: Task flow: Duplicate Address Detected (global IPv6 address)

Navigation

- Displaying IPv6 neighbor information on page 200
- Checking remote host integrity on page 201

Displaying IPv6 neighbor information

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

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

Checking remote host integrity

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

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

Duplicate address detected (link-local address)

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

Duplicate address detected (link-local address)

Use this task flow to restore the connectivity through IPv6.

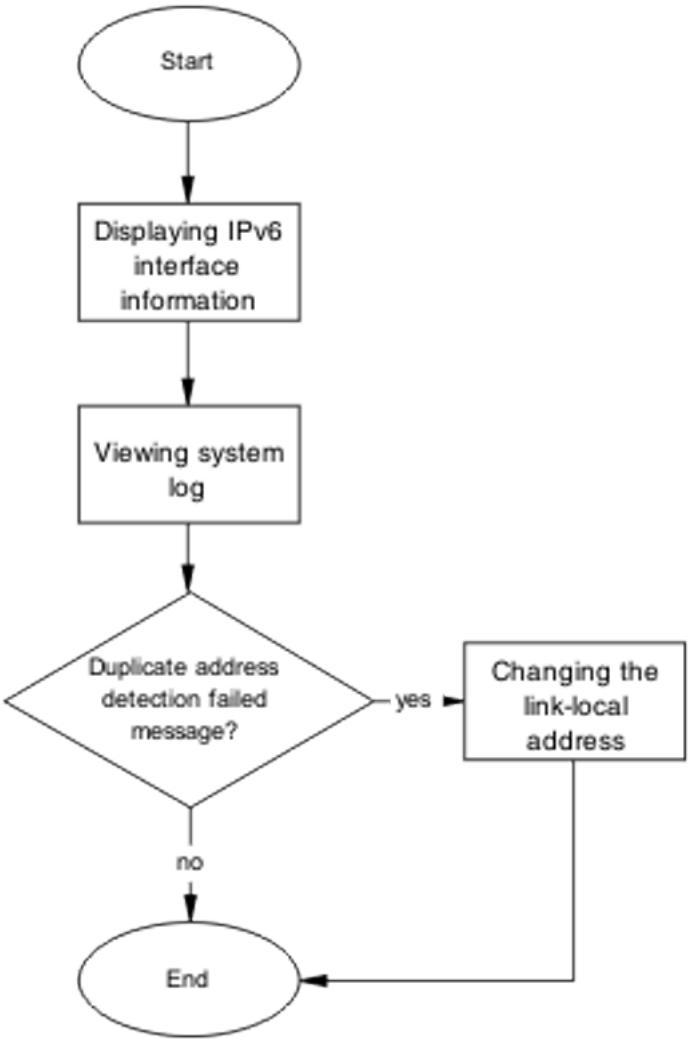


Figure 100: Task flow: Duplicate Address Detected (link-local address)

Navigation

- Displaying IPv6 interface information on page 203
- Viewing the system log on page 203
- Changing the link-local address on page 203

Displaying IPv6 interface information

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

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

Viewing the system log

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

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

Changing the link-local address

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

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

Cannot connect through IPv6 default gateway

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

Cannot connect through IPv6 default gateway

Use this task flow to restore the connectivity through IPv6.

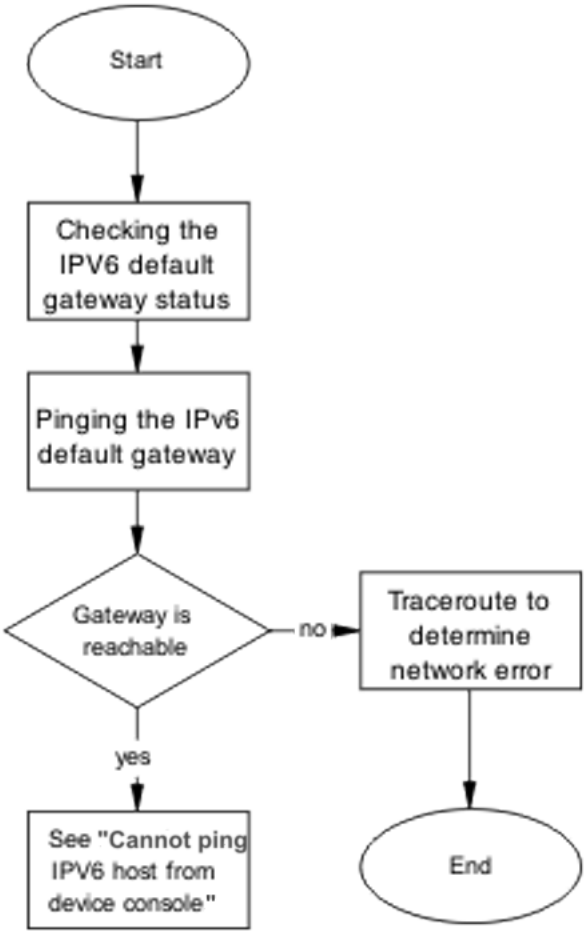


Figure 101: Task flow: Cannot connect through IPv6 default gateway

Navigation

- Checking the IPV6 default gateway status on page 205
- Pinging the IPv6 default gateway on page 205
- Using traceroute to determine network error on page 205

Checking the IPV6 default gateway status

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

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

Pinging the IPv6 default gateway

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

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

Using traceroute to determine network error

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

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

IPv6 management traffic is not sent/received as expected

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

IPv6 management traffic is not sent/received as expected

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

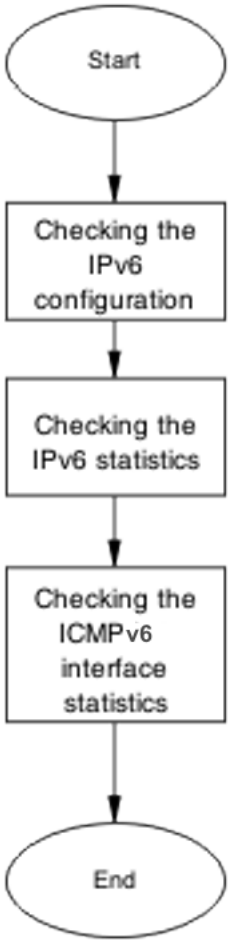


Figure 102: Task flow: IPv6 management traffic is not sent/received as expected

Navigation

- Checking the IPv6 configuration on page 207
- Checking the IPv6 statistics on page 207
- Checking the ICMPv6 statistics on page 207

Checking the IPv6 configuration

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

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

Checking the IPv6 statistics

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

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

Checking the ICMPv6 statistics

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

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

IPV6 telnet/http/ssh to device does not work

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

IPV6 telnet/http/ssh to device does not work

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

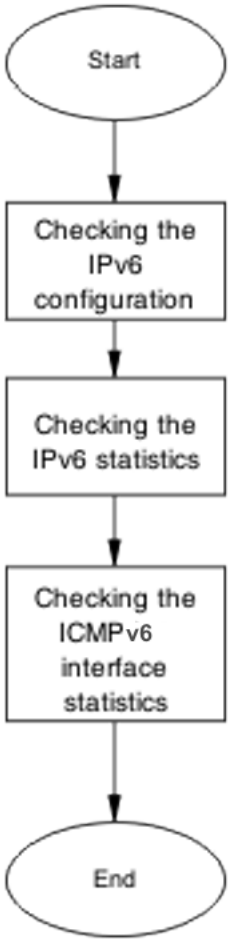


Figure 103: Task flow: IPV6 telnet/http/ssh to device does not work

Navigation

- Checking the IPv6 configuration on page 207
- Checking TCP statistics on page 209

Checking the IPv6 configuration

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

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

Checking TCP statistics

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

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

UDPv6 communication does not work

This task flow assists you to correct UDPv6 connectivity issues.

UDPv6 communication does not work

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

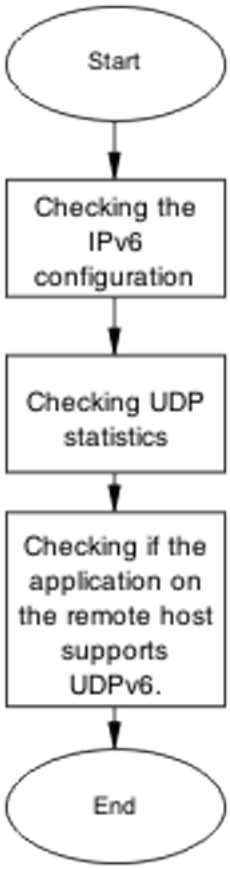


Figure 104: Task flow: UDPv6 communication does not work

Navigation

- Checking the IPv6 configuration on page 210
- Checking UDP statistics on page 211
- Checking if the application on the remote host supports UDPv6. on page 211

Checking the IPv6 configuration

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

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

Checking UDP statistics

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

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

Checking if the application on the remote host supports UDPv6.

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

Cannot set IPv6 address

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

Cannot set IPv6 address

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

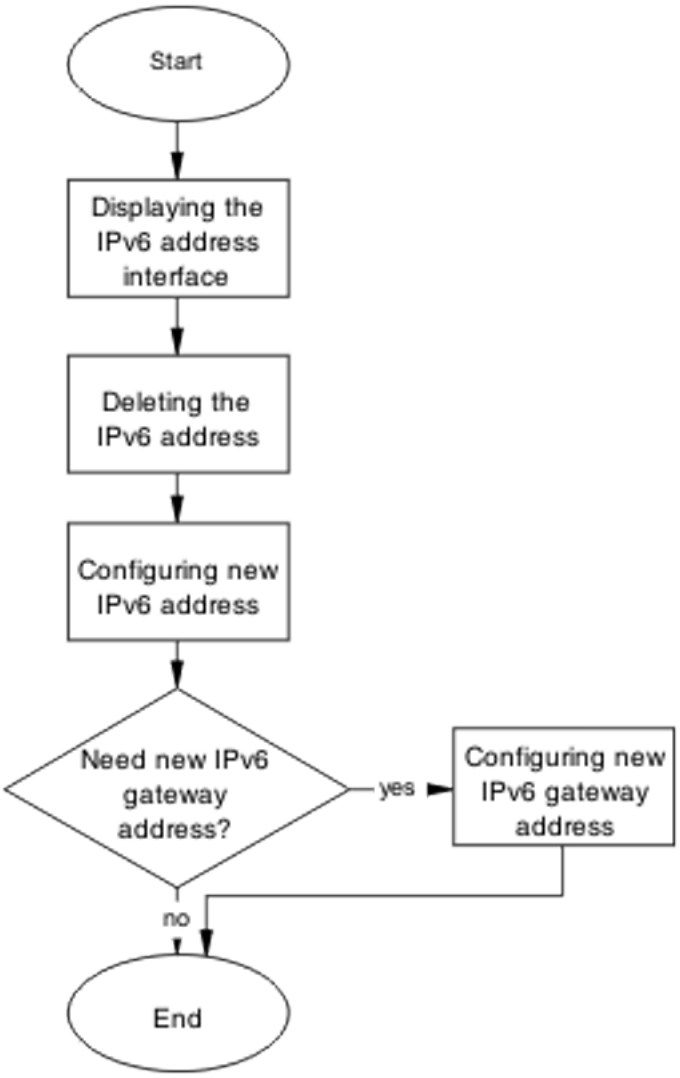


Figure 105: Task flow: Cannot set IPv6 address

Displaying the IPv6 address interface

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

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

Deleting the IPv6 address

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

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

Configuring new IPv6 address

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

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

Configuring new IPv6 gateway address

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

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

Chapter 13: Troubleshooting XFP/SFP

This sections assists you to resolve a problem detecting supported XFP or SFPdevices.

Troubleshooting XFP/SFP workflow

The following workflow assists you to resolve issues related to detecting SFPs or XFPs.

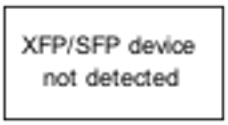


Figure 106: Work flow: Troubleshooting XFP/SFP

Result

Navigation

Troubleshooting XFP/SFP on page 215

XFP/SFP device not detected

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

XFP/SFP device not detected task flow

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

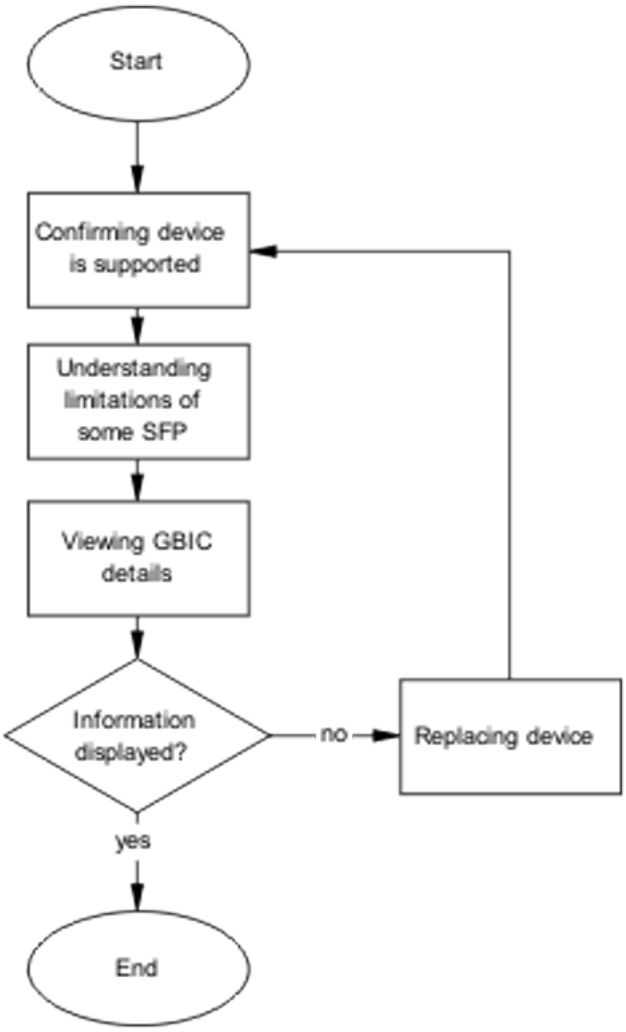


Figure 107: Task flow: XFP/SFP device not detected

Navigation

- Confirming device is supported on page 217
- Understanding limitations of some SFPs on page 217
- Viewing GBIC details on page 217
- Replacing device on page 218

Confirming device is supported

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

- *Avaya Ethernet Routing Switch 4500 Series Installation — SFPs and XFPs* (NN47205-301)
- *Avaya Ethernet Routing Switch 4500 Series Release 5.2 Release Notes* (NN47205-400)

Understanding limitations of some SFPs

Use this procedure to understand some limitations regarding unsupported XFPs or SFPs.

1. Use the **`show stack-info`** command to display device information.
2. Use the **`show interfaces gbic-info`** command to display device information.
3. Confirm that SFP AA1419075-E6 1-port T1 SFP and AA1419074-E6 1-port 100Base-FX SFP is only connected to a 4526T, 4526T-PWR, 4526FX, 4524GT, 4550T , or 4550T-PWR.

Viewing GBIC details

Use this procedure to display the GBIC device details.

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

Replacing device

Use this procedure to replace a device.

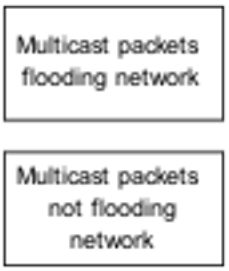
1. See XFP and SFP documentation to familiarize yourself with the installation instructions.
2. Connect the SFP or XFP to a different SFP or XFP cage.

Chapter 14: Troubleshooting IGMP

This sections assists you to resolve multicast flooding issues.

Troubleshooting IGMP workflow

The following workflow assists you to resolve multicast flooding.



Result

Navigation

- Multicast packets flooding network on page 219
- Multicast packets not flooding network on page 224

Multicast packets flooding network

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

Multicast packets flooding network task flow

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

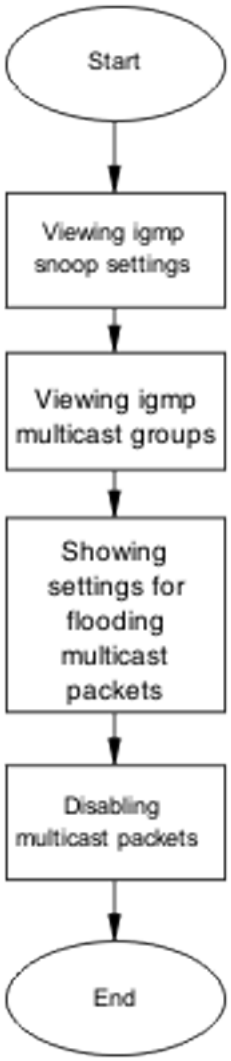


Figure 108: Task flow: Multicast packets flooding network

Result

Navigation

- Viewing IGMP snoop settings on page 221
- Viewing IGMP multicast groups on page 222
- Showing settings for flooding multicast packets on page 223
- Disabling multicast packets on page 224

Viewing IGMP snoop settings

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

1. Use the **`show vlan igmp [vlan ID <value>]`** command to display the information.
2. Observe the displayed information.

Variable Definitions

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

Job aid

The following table describes the output of the command.

Field	Description
Snooping	Indicates the status of snooping as either enable or disable. Default is disable.
Proxy	Indicates the status of igmp proxy. Disabled proxy will allow forwarding of all received host reports. Default is disable.
Robust Value	Indicates how many times a membership query is sent before a host connection is aged out. The default is 2.
Query Time	Indicates how fast a router or a host connection is aged out. The larger the interval, the longer the wait. Default is 125 seconds. Age out time equals “Query Time” times “Robust Value”.
IGMPv1 static Router Ports	Indicates the v1 static router ports (set by you) that receive all multicast streams in the VLAN. Static router ports(v1 or v2) never expire.

Field	Description
IGMPv2 static Router Ports	Indicates the v2 static router ports (set by you) that receive all multicast streams in the VLAN.

Viewing IGMP multicast groups

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

1. Use the **`show vlan multicast membership [vlan ID <value>]`** command to display the information.
2. Observe the displayed information.

Variable Definitions

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

Job aid

The following table describes the output of the command.

Field	Description
Number of groups	Indicates the number of multicast groups learned between 0 and 512.
Multicast Group Address	Specifies the group IP of a multicast group in the format a.b.c.d.
Unit	Indicates the unit where the group has been learned.
Port	Indicates the port on which the group has been learned.

Showing settings for flooding multicast packets

Use this procedure to display the settings for flooding packets with unknown multicast addresses and the list of multicast MAC addresses for which flooding is allowed.

1. Use the **`show vlan unknown-mcast-no-flood`** command to show unknown multicast flooding status.
2. Use the **`show vlan igmp unknown-mcast-allow-flood`** command to show multicast addresses.

Job aid

The following table describes the output of the **`show vlan igmp unknown-mcast-allow-flood`** command.

Field	Description
Unknown Multicast No-Flood	Indicates whether flooding packets with unknown multicast address (addresses for which no groups are created) is enabled or disabled. When it is enabled, all packets that have as destination a multicast MAC address for which an IGMP group is not created are discarded. Otherwise, if this option is disabled, the unknown multicast traffic is forwarded on all ports. Default is disabled.

Job aid

The following table describes the output of the **`show vlan igmp unknown-mcast-no-flood`** command.

Field	Description
Allowed Multicast Addresses	Indicates the MAC addresses for which the multicast traffic is not pruned when the option igmp unknown-mcast-no-flood is enabled.

Disabling multicast packets

Use this procedure to disable the multicast flooding.

1. Use the **unknown-mcast-no-flood** command to disable multicast flooding.
2. Observe the command output.

Multicast packets not flooding network

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

Multicast packets not flooding network task flow

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

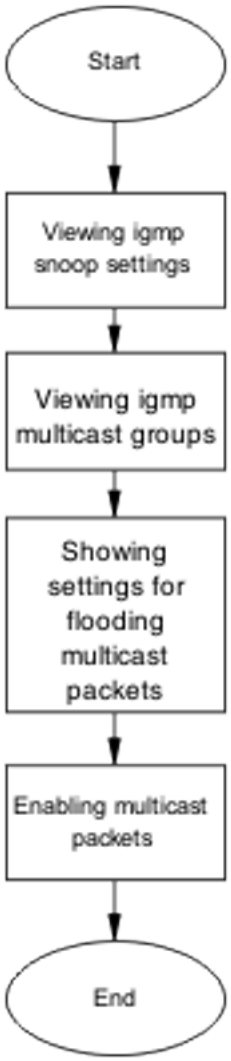


Figure 109: Task flow: Multicast packets not flooding network

Result

Navigation

- Viewing IGMP snoop settings on page 226
- Viewing IGMP multicast groups on page 227
- Showing settings for flooding multicast packets on page 228
- Enabling multicast packets on page 229

Viewing IGMP snoop settings

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

1. Use the **`show vlan igmp [vlan ID <value>]`** command to display the information.
2. Observe the displayed information.

Variable Definitions

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

Job aid

The following table describes the output of the command.

Field	Description
Snooping	Indicates the status of snooping as either enable or disable. Default is disable.
Proxy	Indicates the status of igmp proxy. Disabled proxy will allow forwarding all received host reports. Default is disable.
Robust Value	Indicates how many times a membership query will be sent before a host connection is aged out. The default is 2.
Query Time	Indicates how fast a router or a host connection is aged out. The larger the interval, the longer the wait. Default is 125 seconds. Age out time equals “Query Time” times “Robust Value”.
IGMPv1 static Router Ports	Indicates the v1 static router ports (set by you) that receive all multicast streams in the VLAN. Static router ports(v1 or v2) never expire.

Field	Description
IGMPv2 static Router Ports	Indicates the v2 static router ports (set by you) that receive all multicast streams in the VLAN.

Viewing IGMP multicast groups

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

1. Use the **`show vlan multicast membership [vlan ID <value>]`** command to display the information.
2. Observe the displayed information.

Variable Definitions

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

Job aid

The following table describes the output of the command.

Field	Description
Number of groups	Indicates the number of multicast groups learned between 0 and 512.
Multicast Group Address	Specifies the group IP of a multicast group in the format a.b.c.d.
Unit	Indicates the unit where the group has been learned.
Port	Indicates the port on which the group has been learned.

Showing settings for flooding multicast packets

Use this procedure to display the setting for flooding packets with unknown multicast addresses and the list of multicast MAC addresses for which flooding is allowed.

1. Use the **`show vlan unknown-mcast-no-flood`** command to show unknown multicast flooding status.
2. Use the **`show vlan igmp unknown-mcast-allow-flood`** command to show multicast addresses.

Job aid

The following table describes the output of the **`show vlan igmp unknown-mcast-allow-flood`** command.

Field	Description
Unknown Multicast No-Flood	Indicates whether flooding packets with unknown multicast address (addresses for which no groups are created) is enabled or disabled. When it is enabled, all packets that have as destination a multicast MAC address for which an IGMP group is not created are discarded. Otherwise, if this option is disabled, the unknown multicast traffic is forwarded on all ports. Default is disabled.

Job aid

The following table describes the output of the **`show vlan igmp unknown-mcast-no-flood`** command.

Field	Description
Allowed Multicast Addresses	Indicates the MAC addresses for which the multicast traffic is not pruned when the option igmp unknown-mcast-no-flood is enabled.

Enabling multicast packets

Use this procedure to enable the multicast flooding.

1. Use the **unknown-mcast-allow-flood** command to enable multicast flooding.
2. Observe the command output.

Chapter 15: Troubleshooting RSTP SNMP traps

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

Troubleshooting RSTP SNMP traps workflow

The following workflow assists you to resolve RSTP trap issues.

Figure 110: Work flow: Troubleshooting RSTP SNMP traps

Navigation

[No RSTP SNMP traps are received](#) on page 231

No RSTP SNMP traps are received

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

No RSTP SNMP traps are received task flow

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

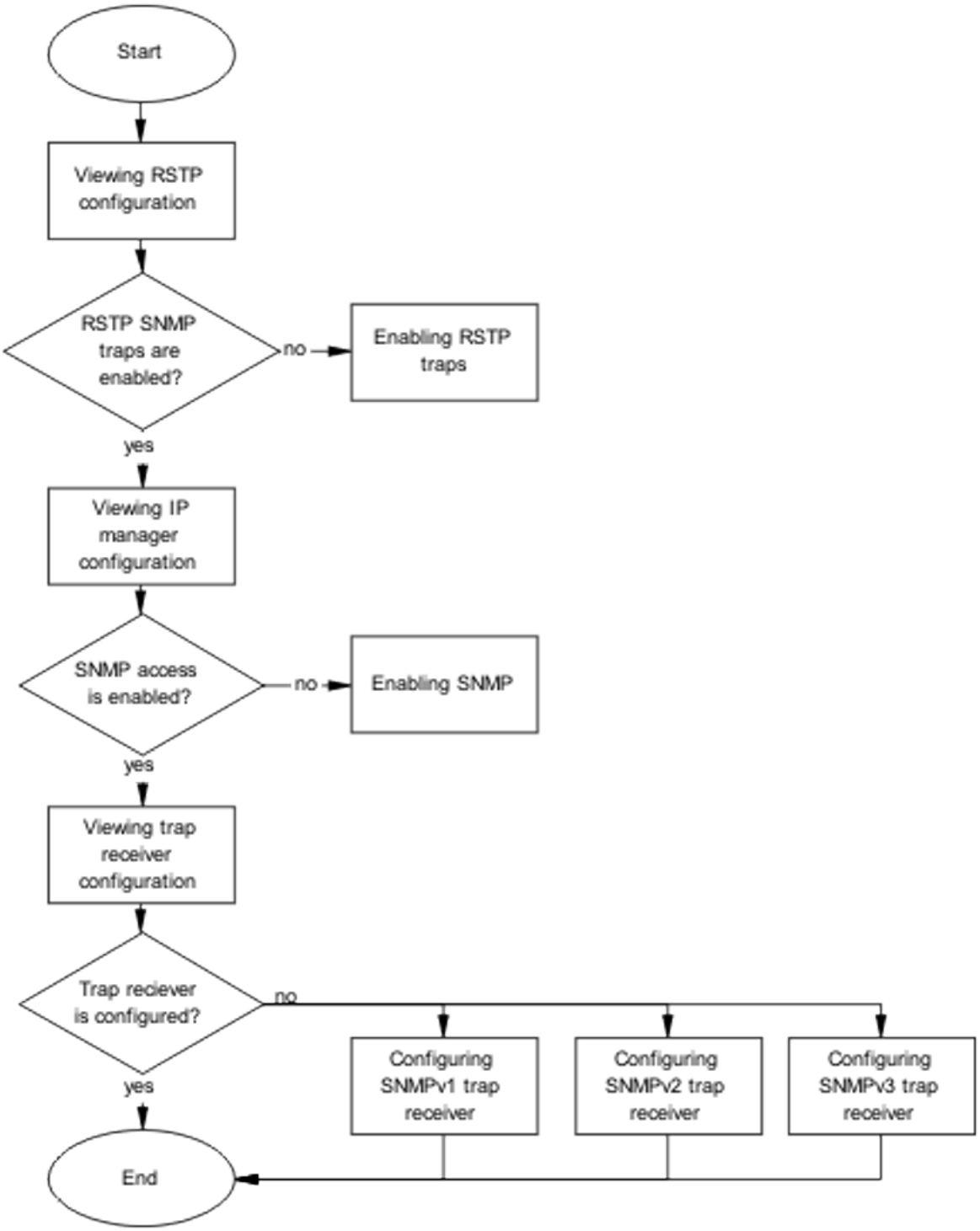


Figure 111: Task flow: No RSTP SNMP traps are received

Navigation

Viewing RSTP configuration

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

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

Job aid

The following is an example of output from the command.

```
Priority (hex):                 8000

Stp Version:                    Rstp Mode

Bridge Max Age Time:            20 seconds

Bridge Hello Time:              2 seconds

Bridge Forward Delay Time:      15 seconds
```

```
Tx Hold Count:                          3

Path Cost Default Type:                 32-bit

STP Traps:                              Disabled
```

Enabling RSTP traps

Use the procedure in this section to enable RSTP traps.

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

Viewing IP manager configuration

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

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

Job aid

The following is an example of output from the command.

```
TELNET Access:                          Enabled

SNMP Access:                            Disabled

WEB Access:                             Enabled

SSH Access:                             Enabled
```

Enabling SNMP

Use the procedure in this section to enable SNMP.

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

Viewing trap receiver configuration

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

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

Configuring SNMPv1 trap receiver

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

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

Variable Definitions

Variable	Definition
IP address	IPv4 address of the server host

Configuring SNMPv2 trap receiver

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

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

Variable Definitions

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

Configuring SNMPv3 trap receiver

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

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

Variable Definitions

Variable	Definition
IP address	IPv4 address of the server host

Variable	Definition
user	The user that has been defined for sending SNMPv3 traps

Chapter 16: Troubleshooting DHCP/BootP relay

Bootp/DHCP Relay serves the purpose of IP configuration for Bootp/DHCP clients that do not have a BootP/DHCP Server configured in the same subnet.

Troubleshooting DHCP/BootP relay work flow

The following workflow helps you to identify some common issues.

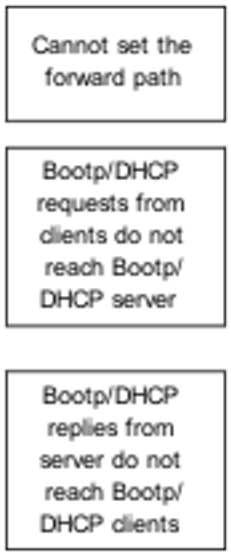


Figure 112: Work flow: Troubleshooting DHCP/BootP relay

Navigation

Cannot set the forward path

This task flow assists you to resolve the following error message if it appears:

```
% Cannot modify settings
% Error agent/server does not exist
```

Cannot set the forward path task flow

The following task flow helps you to verify that the relay agent IP address is the same as the one configured on the VLAN where relay is performed.

Figure 113: Task flow: Cannot set the forward path

Navigation

Viewing VLAN IP information on page 241

Viewing VLAN IP information

Use this procedure to verify that the relay agent IP address from the forward path command is the same as the one on the VLAN where relay is to be performed.

1. Use the **`show vlan ip`** command to display the information.
2. Verify that the relay agent IP address from the forward path command is the same as the one on the VLAN where relay is to be performed.

Bootp/DHCP requests from clients do not reach Bootp/DHCP server

This section assists you to identify and correct connectivity issues between a client and the DHCP or BootP server.

Bootp/DHCP requests from clients do not reach Bootp/DHCP server task flow

The following task flows identify the procedures to identify and correct connectivity issues between a client and the DHCP or BootP server.

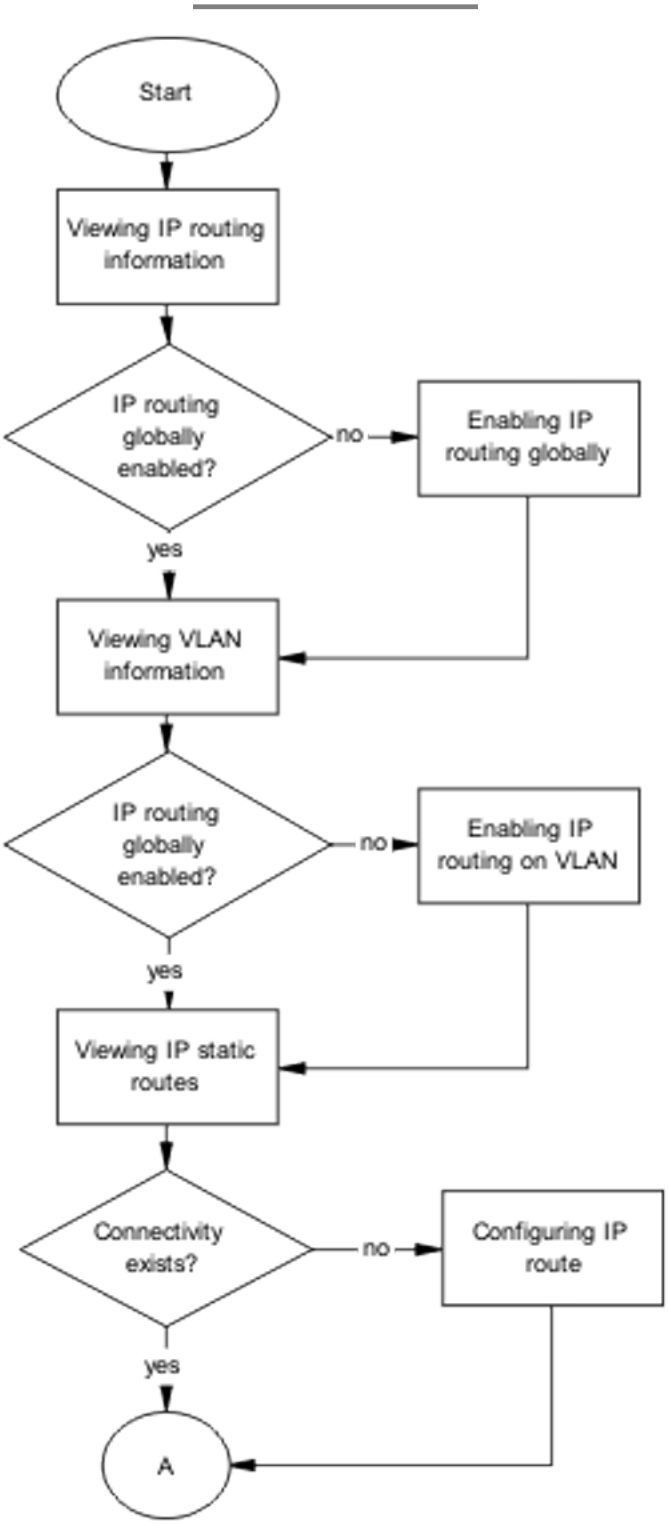


Figure 114: Task flow: Bootp/DHCP requests from clients do not reach Bootp/DHCP server part 1

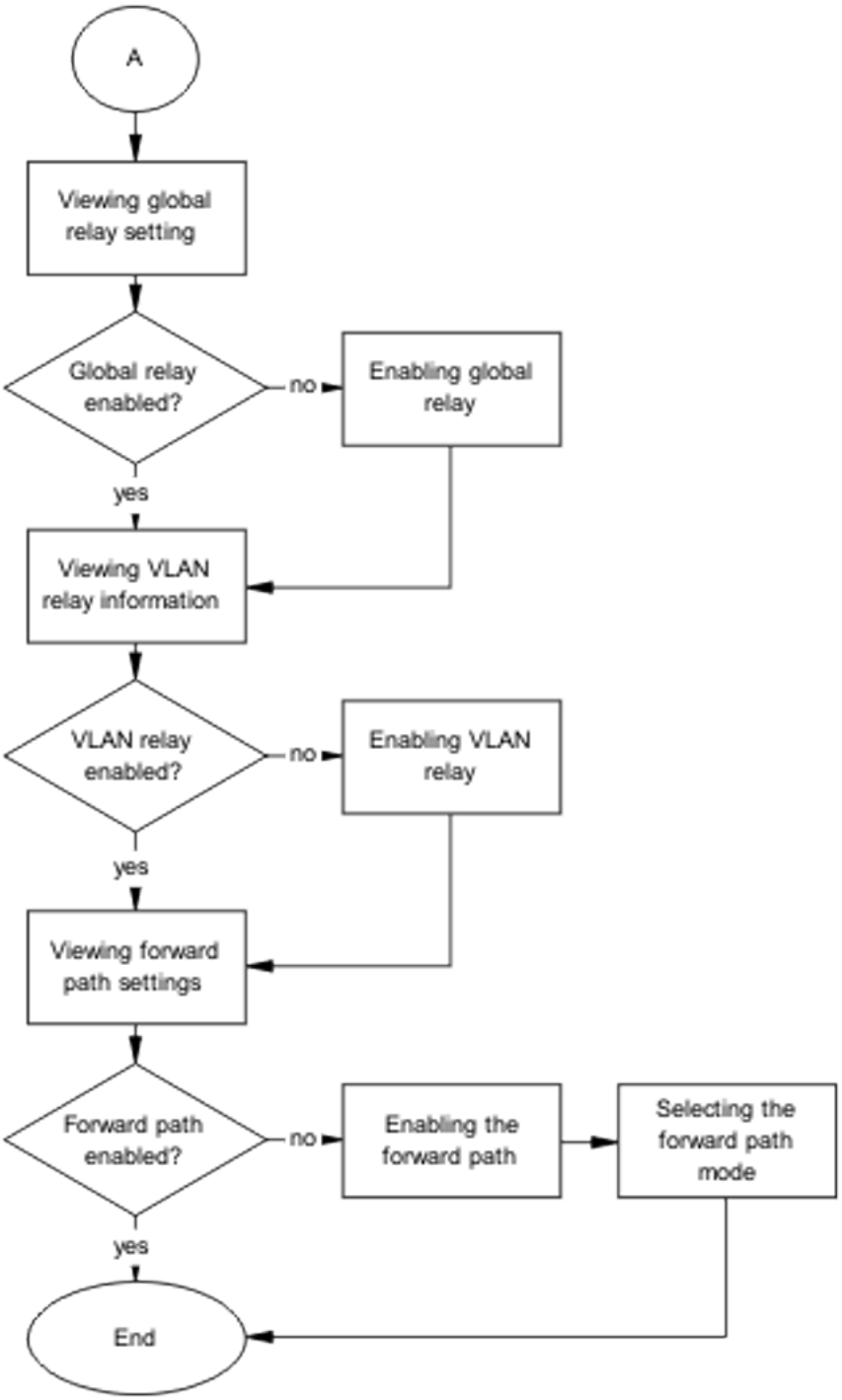


Figure 115: Task flow: Bootp/DHCP requests from clients do not reach Bootp/DHCP server part 2

Viewing IP routing information

Use the procedure in this section to view IP routing information.

1. Enter the **`show ip routing`** command to view IP routing information.
2. Identify that IP routing is enabled.

Enabling IP routing globally

Use the procedure in this section to enable IP routing globally.

1. Enter the **`ip routing`** command to enable IP routing globally.
2. Enter the **`show ip routing`** command to confirm that global IP routing is now enabled.

Viewing VLAN information

Use the procedure in this section to view VLAN information.

1. Enter the **`show vlan ip`** command to view VLAN information.
2. Verify that the interfaces are enabled under the Offset Routing column.

Enabling IP routing on VLAN

Use the procedure in this section to enable IP routing on a VLAN.

1. Enter the **interface vlan <VLANID>** command to select the VLAN interface to be modified.
2. Enter the **ip routing** command to enable IP routing on the interface.

Variable Definitions

Variable	Definition
VLANID	Unique ID of the VLAN

Viewing IP static routes

Use the procedure in this section when the server is not connected to the same Ethernet Routing Switch and configure a client with static IP for connectivity purposes. From that client, ping the server. If the ICMP echo requests do not reach the server, verify that a route is configured on the switch for the server.

1. Enter the **show ip route static** command to display the IP static route information.
2. Observe the command output.

Configuring IP route

Use the procedure in this section to configure the IP route.

1. Enter the **ip route <server.ip.address.class> <netmask> <next.hop.ip.address> <cost>** command to configure the IP route.
2. Observe the command output.

Viewing global relay setting

Use the procedure in this section to view the global relay configuration.

1. Enter the **`show ip dhcp-relay`** command to display the global relay configuration.
2. Observe the command output and confirm DHCP relay is enabled.

Enabling global relay

Use the procedure in this section to enable DHCP relay globally.

1. Enter the **`ip dhcp-relay`** command to enable DHCP relay globally.
2. Observe the command output.

Viewing VLAN relay information

Use the procedure in this section to display the VLAN relay configuration.

1. Enter the **`show vlan dhcp-relay`** command to display the VLAN relay configuration.
2. Observe the command output.

Enabling VLAN relay

Use the procedure in this section to enable VLAN relay.

1. Enter the **interface vlan <VLANID>** command to select the VLAN interface to be modified.
2. Enter the **ip dhcp-relay** command to enable DHCP relay on the interface.

Variable Definitions

Variable	Definition
VLANID	Unique ID of the VLAN

Viewing forward path settings

Use the procedure in this section to display the forward path settings.

1. Enter the **show ip dhcp-relay fwd-path** command to display the forward path configuration.
2. Ensure that the interface is enabled.

Enabling the forward path

Use the procedure in this section to enable the forward path.

1. Enter the **ip dhcp-relay fwd-path <interface address> <server address> enable** command to enable the forward path.
2. Ensure that the command completes.

Variable Definitions

Variable	Definition
interface address	IPv4 address of the interface

Variable	Definition
server address	IPv4 address of the server

Selecting the forward path mode

Use the procedure in this section to configure the forward path mode.

1. Enter the **ip dhcp-relay fwd-path <interface address> <server address> mode [boot | dhcp | boot-dhcp]** command to configure the forward path mode.
2. Ensure that the command completes.

Variable Definitions

Variable	Definition
interface address	IPv4 address of the interface
server address	IPv4 address of the server

Bootp/DHCP replies from server do not reach Bootp/DHCP clients

This section helps you to resolve issues related to Bootp/DHCP replies from the server that do not reach Bootp/DHCP clients.

Bootp/DHCP replies from server do not reach Bootp/DHCP clients task flow

The following task flow identifies the procedure to resolve issues related to Bootp/DHCP replies from the server that do not reach Bootp/DHCP clients.

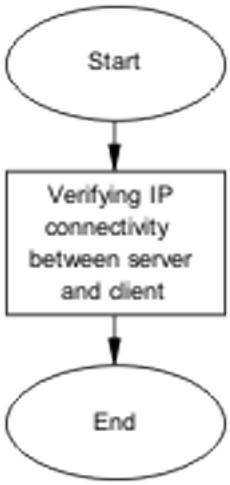


Figure 116: Task flow: Bootp/DHCP replies from server do not reach Bootp/DHCP clients

Navigation

Verifying IP connectivity between server and client on page 249

Verifying IP connectivity between server and client

Prerequisites

The server is not connected to the same Ethernet Routing Switch.

Use the procedure in this section to verify the connectivity between the DHCP server and its client.

1. Use the **`show ip route static`** command to ensure ICMP requests from the client reach the server.
2. From the server, ping the client configured with a static IP address.
3. Verify that a route is configured on the server and the route points to the subnet of the client.
4. Using the server documentation, configure the route if it does not exist.