Troubleshooting Avaya Ethernet Routing Switch 5000 Series

6.0
NN47200-700, 01.02
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

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

Link disclaimer

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

Warranty

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

Licenses

Copyright

Third-party components

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

Trademarks

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

Avaya is a registered trademark of Avaya Inc.

All other trademarks are the property of their respective owners.

Downloading documents

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

Contact Avaya Support

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

Contents

Chapter 1: New in this release

This document is the first standard version of the Ethernet Routing Switch 5500 Series Troubleshooting document. It supports all features included in software Release 5.1. The hardware models supported are: 5510, 5520, 5530-24TFD.

Chapter 2: Introduction

This document :

- Describes the diagnostic tools and utilities available for troubleshooting the Avaya Ethernet Routing Switch 5000 Series products including the Avaya Command Line Interface (ACLI) and Device Manager (DM).
- Guides you through some common problems to achieve a first tier solution to these situations
- Advises you what information to compile prior to troubleshooting or calling Avaya for help.

This documents assumes that you:

- Have basic knowledge of networks, Ethernet bridging, and IP routing.
- Are familiar with networking concepts and terminology.
- Have experience with Graphical User Interface (GUI).
- Have basic knowledge of network topologies.

Troubleshooting Tools

The Ethernet Routing Switch 5000 Series products support a range of protocols, utilities, and diagnostic tools that you can use to monitor and analyze traffic, monitor laser operating characteristics, capture and analyze data packets, trace data flows, view statistics, and manage event messages.

Certain protocols and tools are tailored for troubleshooting specific Ethernet Routing Switch 5000 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

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

First, use the *Ethernet Routing Switch 5000 Series Documentation Roadmap* (NN47200-103) to familiarize yourself with the documentation set, so you know where to get information when you need it.

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

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

- A site network map identifies where each device is physically in 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).
- You should maintain online and paper copies of your device configuration information. Ensure that all online data is stored with your site's regular data backup for your site. If your site has no backup system, copy the information onto a backup medium and store the backup offsite.
- Store passwords in a safe place. 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 list all devices and relevant information for your network. Use this inventory to easily see the device types, IP addresses, ports, MAC addresses, and attached devices.
- If your hubs or switches are not managed, you must keep a list of the MAC addresses that correlate to the ports on your hubs and switches.
- Maintain a change-control system for all critical systems. Permanently store change-control records.
- A good practice is to store the details of all key contacts, such as support contacts, support numbers, engineer details, and telephone and fax numbers. Having this information available during troubleshooting saves you time.

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

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

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

Chapter 4: Troubleshooting tools

These are the available troubleshooting tools and their applications.

Port Mirroring

ERS 5500 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 ERS 5500 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

Please refer to the *Avaya Ethernet Routing Switch 5500 Series Configuration — System* (NN47200-500) for port mirroring command information

You can 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.

Route Tracing

Identify network connection issues that are not directly related to the ERS 5500 Series device.

The **`traceroute <ip>`** command records the route (the specific gateway computers at each hop) through the Internet between your computer and a specified destination computer. The command also calculates and displays the amount of time each hop took. The command is useful for understanding where problems occur in the Internet and to get a detailed sense of the Internet itself.

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.

Two types of stack loopback tests exist. The 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, please reference the *Avaya Ethernet Routing Switch 5500 Series Configuration — System Monitoring* (NN47200-505).

Time Domain Reflectometer

Beginning with Release 5.0 software, the Avaya Ethernet Routing Switch 5000 Series device is equipped with a Time Domain Reflectometer (TDR). The TDR provides a diagnostic capability to test connected cables for defects, such as short pin and pin open. You can obtain TDR test results from the ACLI or the DM.

The cable diagnostic tests only apply to Ethernet copper ports; fiber ports cannot be tested.

The cable diagnostic tests only apply to Ethernet copper ports. Fiber ports cannot be tested. You can initiate a test on multiple ports at the same time. After you test a cable with the TDR, if the cable has a 10/100 MB/s link speed, the link is broken during the test and restored only when the test is complete. TDR test does not affect the gigabit links.

System Logs

You can use the syslog messaging feature of the ERS 5500 Series products to manage event messages. The ERS 5500 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 ERS 5500 Series device running in a network accessible to the workstation.

Auto Unit Replacement (AUR)

You must understand AUR to replace a failed device in the stack if AUR is enabled.

With the Auto Unit Replacement (AUR) feature you can 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 is not be replicated in the new unit.

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

For further detail regarding port statistics and commands, refer to *Ethernet Routing Switch 5000 series — System Configuration* (NN47200-501).

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 engine is searchable by natural-language query.

Chapter 5: General diagnostic tools

The Ethernet Routing Switch 5000 Series device has diagnostic features available with the DM, ACLI, and a Web Interface. 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 the ACLI to perform the majority of troubleshooting. For purposes of using this document, CLI and ACLI are interchangeable. Refer to *Avaya Ethernet Routing Switch 5000 Series Commands Reference* (NN47200-500) for information about moving between the two.

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

Understand the ACLI command modes and how they differ.

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

- User Executive
- Privileged EXEC
- Global configuration
- Interface configuration
- Router 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 Executive mode:

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

- Global configuration mode:

  While using the Privileged EXEC mode (also referred to as Privileged Executive mode) you can perform basic switch-level management tasks, such as downloading software images, setting passwords, and booting the switch. With the unrestricted Privileged Executive is an unrestricted mode you can view all settings on the switch. While you are logged in with write access you can access all configuration modes and commands that affect operation of the switch (such as downloading images or rebooting).

- Global configuration mode: While using 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:

  While 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.

- Router configuration mode:

  With the Router Configuration mode (also referred to as config-router mode) you can configure routing parameters for RIP, OSPF, and VRRP.

You can move between command modes on a limited basis. This concept is explained in the Common Procedures section of this document.

Chapter 6: Initial troubleshooting

The types of problems that typically occur with networks involve connectivity and performance. A good practice is to follow the OSI network architecture layers. 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 do this, you can use the **`show running-config`** command.
- System status. output from the **`show tech`** command. It displays technical information about system status and information about the hardware, software, and switch operation. This command displays more information than the similar **`show sys-info`** command.
- Information about past events. To do this, review the log files.
- The software version that is running on the device. To do this, use the **`show sys-info`** or **`show system verbose`** commands to display the software version that is running on all cards.
- 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`**: After connectivity problems occur, get information about at least five working source and destination IP pairs and five IP pairs with connectivity issues. To do this, use these commands:
    - **`show tech`**

  - `show running-config`
  - `show port-statistics <port>`
- Use the MIB web page. See *Avaya Ethernet Routing Switch 5000 Series System - Monitoring* (NN47200-502) for detailed information.
- Use the trap Web page. See *Avaya Ethernet Routing Switch 5000 Series System - Monitoring* (NN47200-502) for detailed information.

Chapter 7: Emergency recovery trees

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

Emergency recovery trees

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

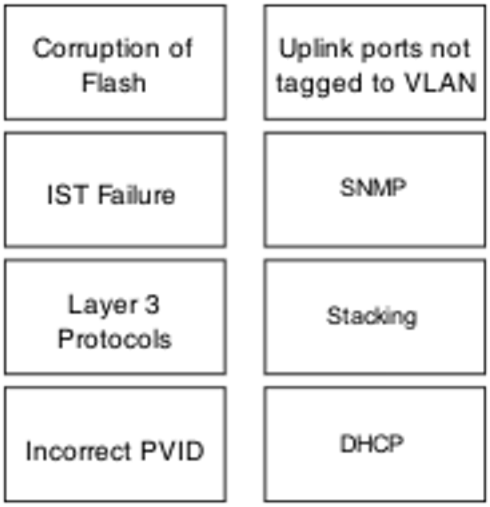


Figure 1: Emergency recovery trees

Navigation

- Corruption of flash on page 24
- IST Failure on page 25
- Layer 3 protocols on page 27
- Incorrect PVID on page 28
- VLAN not tagged to uplink ports on page 29

- SNMP on page 31
- Stack on page 33
- Dynamic Host Configuration Protocol (DHCP) on page 37

Corruption of flash

Corruption of the flash due to power outage or environmental reasons makes the configuration of the box corrupt and non-functional. Initializing of the flash is required before an RMA.

Corruption of flash recovery tree

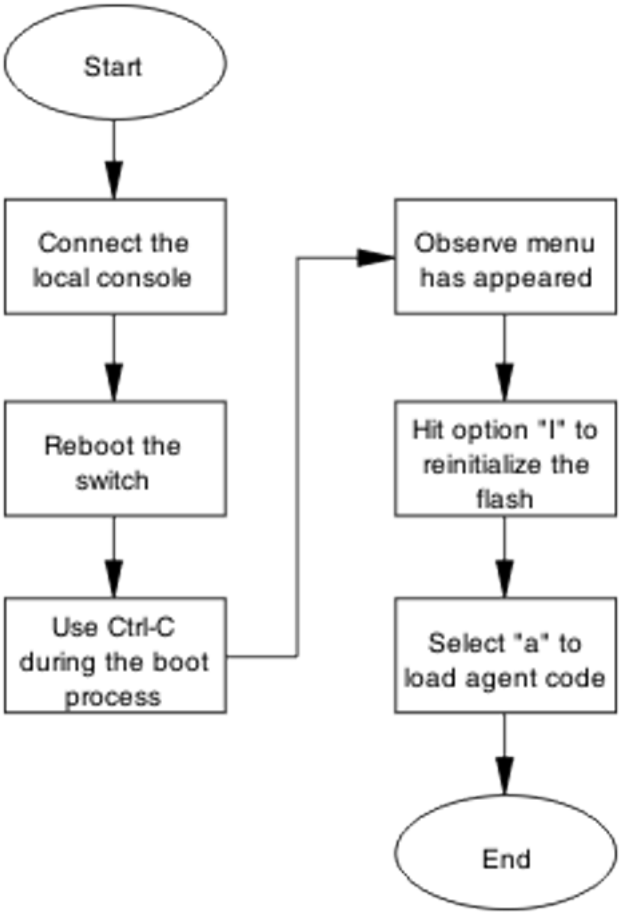

Start
Connect the local console
Reboot the switch
Use Ctrl-C during the boot process
Observe menu has appeared
Hit option "I" to reinitialize the flash
Select "a" to load agent code
End

Figure 2: Corruption of flash

IST Failure

Two ERS 5500 series devices running IST between them will experience a total loss of communication when an IST link between ERS 5500 series goes down. All critical network traffic runs on IST link therefore if IST failure, network protocol like RIP, VRRP, OSPF, VLACP start flapping and will finally cause a network outage.

IST Failure Recovery Tree

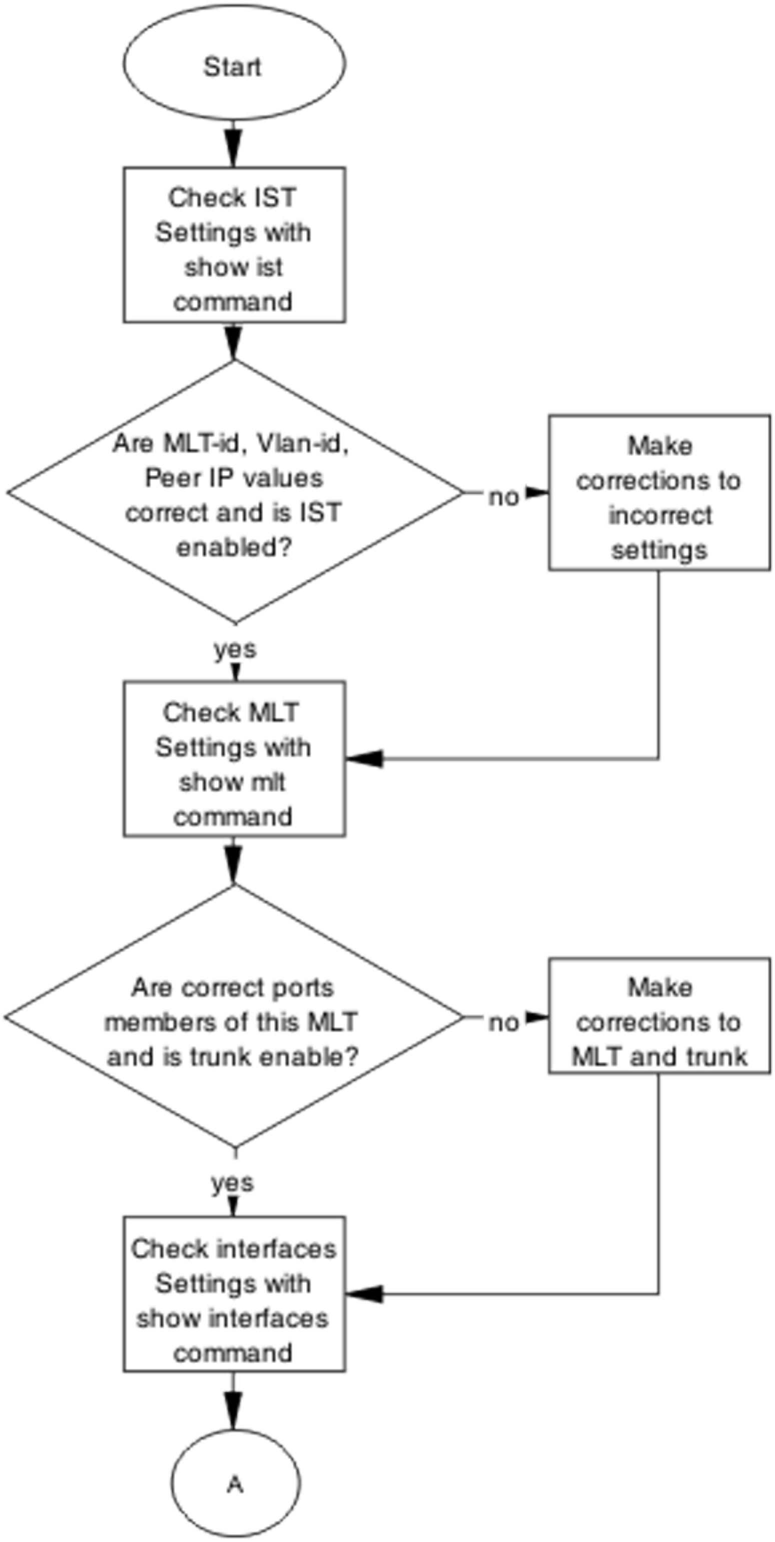

Start
Check IST Settings with show ist command
Are MLT-id, Vlan-id, Peer IP values correct and is IST enabled?
no
Make corrections to incorrect settings
yes
Check MLT Settings with show mlt command
Are correct ports members of this MLT and is trunk enable?
no
Make corrections to MLT and trunk
yes
Check interfaces Settings with show interfaces command
A

Figure 3: IST Failure part 1

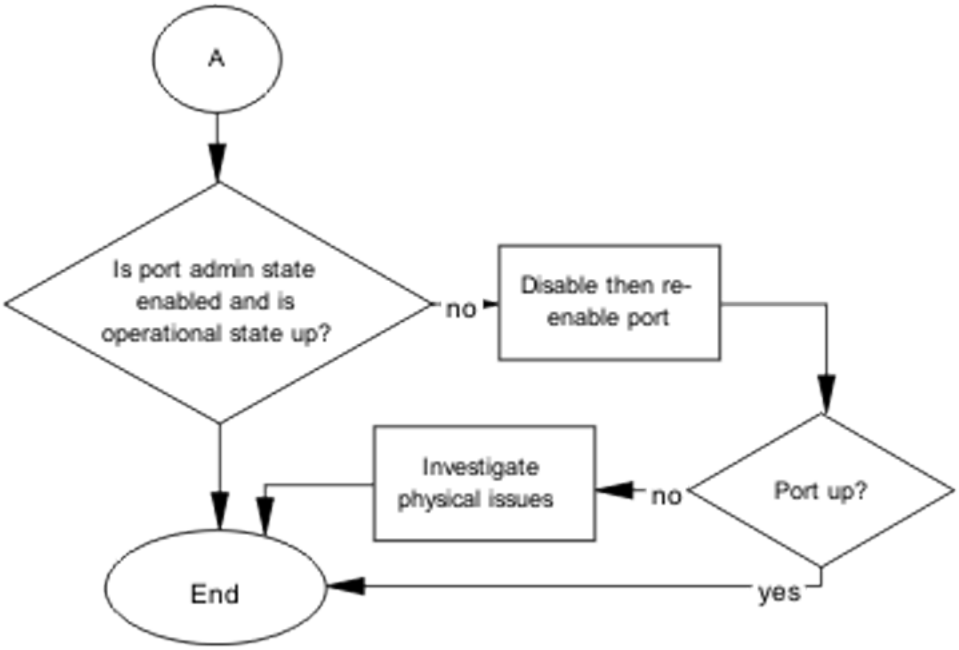

A
Is port admin state enabled and is operational state up?
no
Disable then re-enable port
Port up?
no
Investigate physical issues
yes
End

Figure 4: IST Failure part 2

Layer 3 protocols

To configure Layer-3 protocol like OSPF, VRRP and IST/SMLT on ERS 5500 series devices, require a license file to be loaded on the switch.

Layer 3 Protocols Recovery Tree

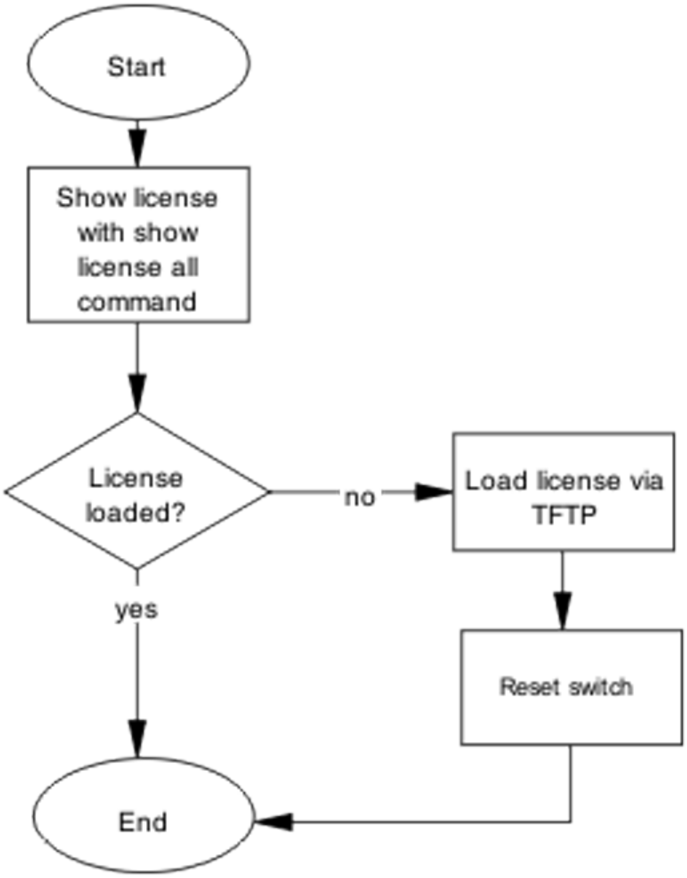


Figure 5: Layer 3 Protocols

Incorrect PVID

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

Incorrect PVID Recovery Tree

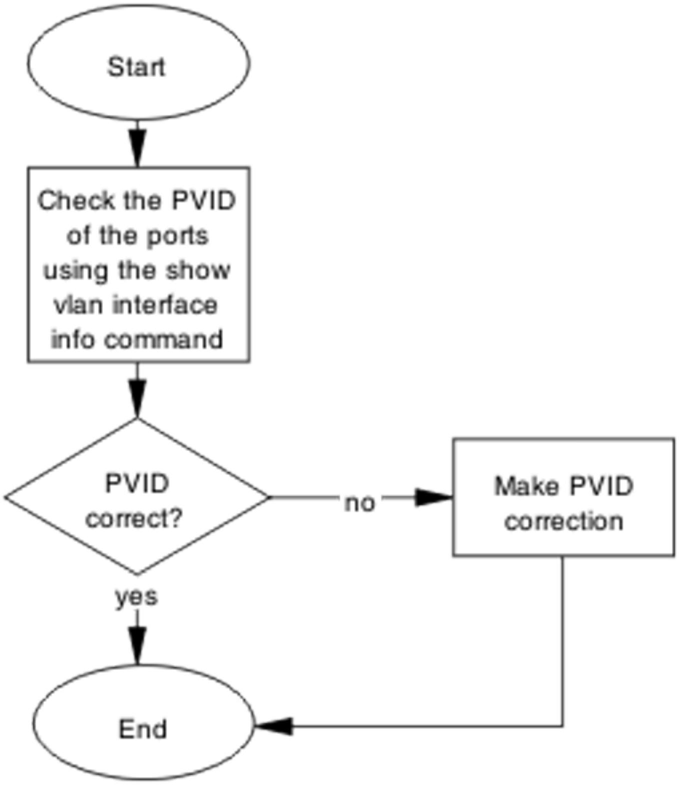

Start
Check the PVID of the ports using the show vlan interface info command
PVID correct?
no
Make PVID correction
yes
End

Figure 6: Incorrect PVID

VLAN not tagged to uplink ports

After the ERS 5500 series is connected to an ERS 8600 series and devices in a VLAN on the ERS 8600 series are not able to communicate with devices at the ERS 5500 series in the same VLAN indicates that the uplink ports are not tagged to the VLAN at the ERS 5500 series.

VLAN not tagged to uplink ports recovery tree

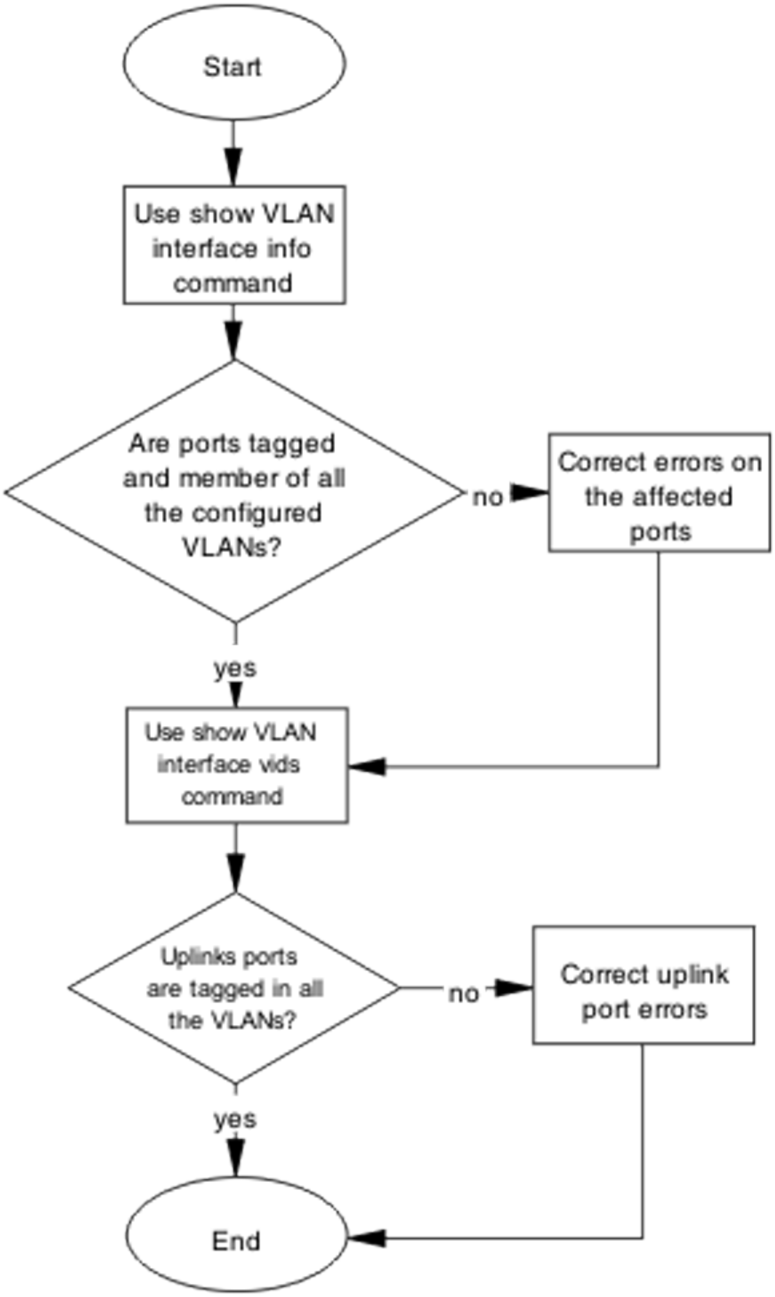

Start
Use show VLAN interface info command
Are ports tagged and member of all the configured VLANs?
no
Correct errors on the affected ports
yes
Use show VLAN interface vids command
Uplinks ports are tagged in all the VLANs?
no
Correct uplink port errors
yes
End

Figure 7: 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, verify the trap configurations (the trap destination address and the traps configured to be sent).

SNMP Recovery Tree

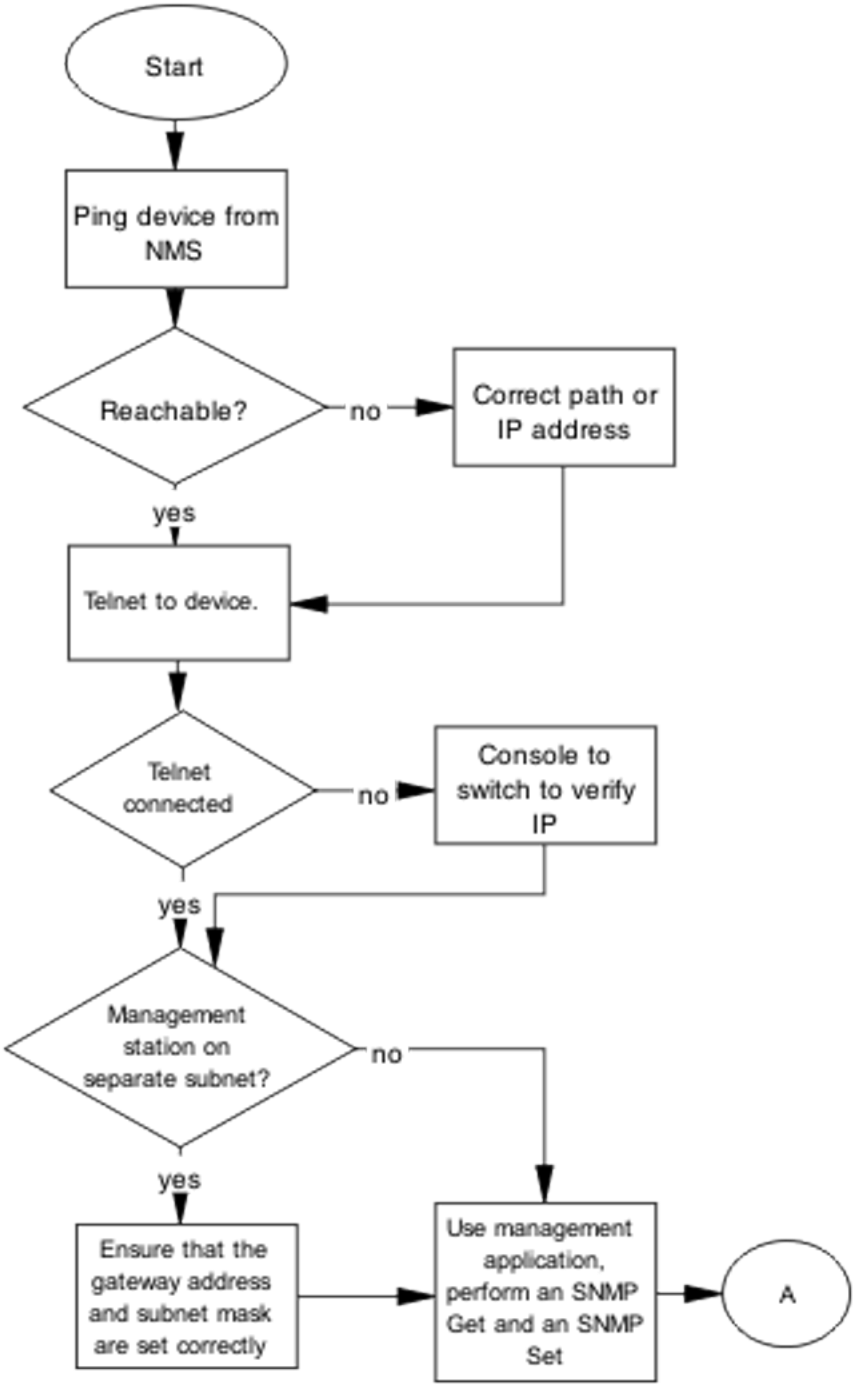

Start
Ping device from NMS
Reachable?
no
Correct path or IP address
yes
Telnet to device.
Telnet connected
no
Console to switch to verify IP
yes
Management station on separate subnet?
no
yes
Ensure that the gateway address and subnet mask are set correctly
Use management application, perform an SNMP Get and an SNMP Set
A

Figure 8: SNMP part 1

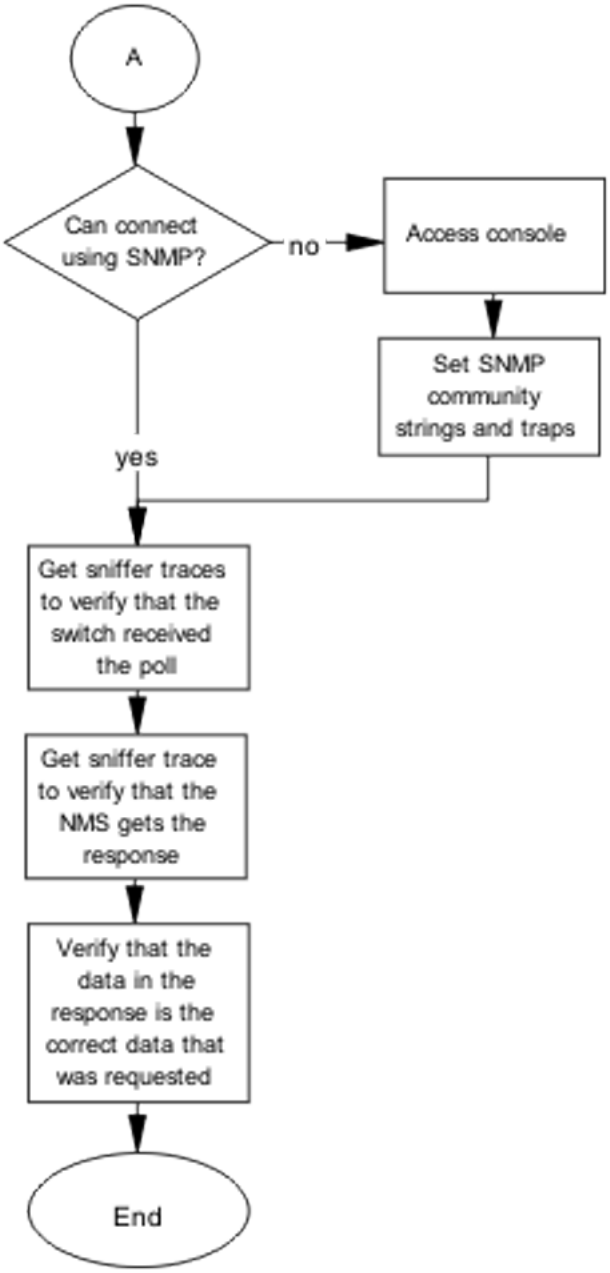

A
Can connect using SNMP?
no
Access console
Set SNMP community strings and traps
yes
Get sniffer traces to verify that the switch received the poll
Get sniffer trace to verify that the NMS gets the response
Verify that the data in the response is the correct data that was requested
End

Figure 9: SNMP part 2

Stack

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

Stack Recovery Tree

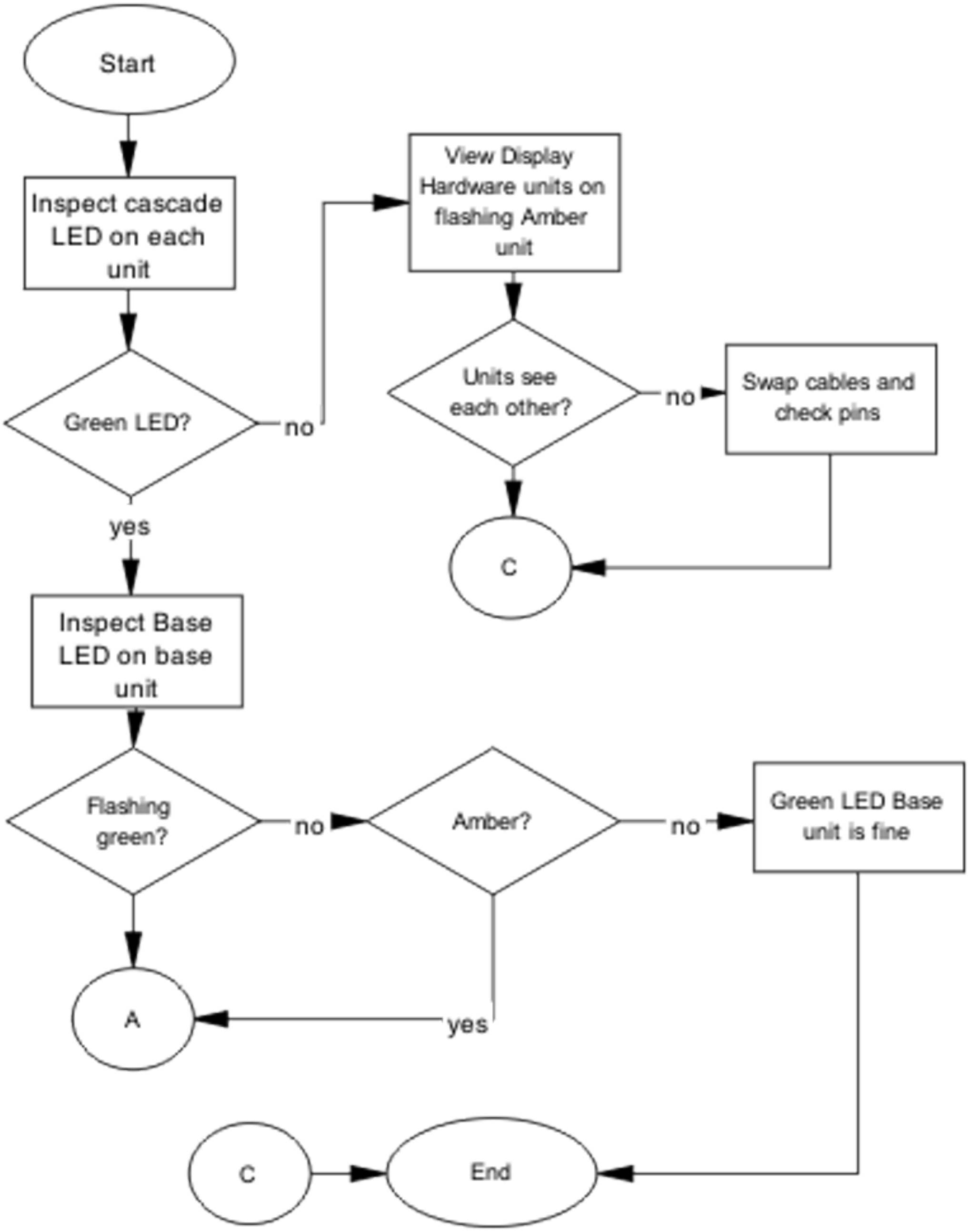

Start
Inspect cascade LED on each unit
Green LED?
no
yes
View Display Hardware units on flashing Amber unit
Units see each other?
no
Swap cables and check pins
C
Inspect Base LED on base unit
Flashing green?
no
Amber?
no
Green LED Base unit is fine
A
yes
C
End

Figure 10: Stack part 1

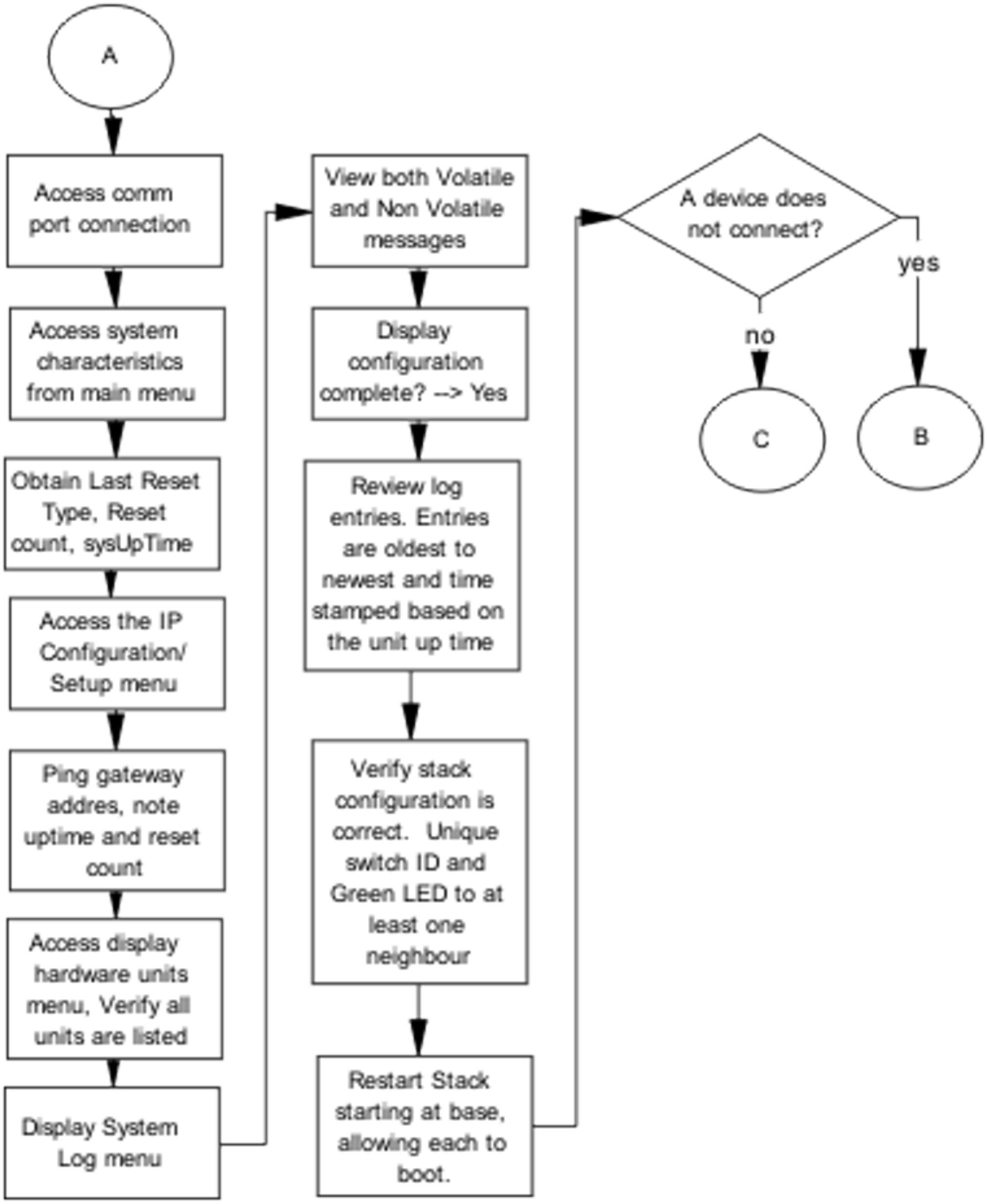

A
Access comm port connection
Access system characteristics from main menu
Obtain Last Reset Type, Reset count, sysUpTime
Access the IP Configuration/ Setup menu
Ping gateway addres, note uptime and reset count
Access display hardware units menu, Verify all units are listed
Display System Log menu
View both Volatile and Non Volatile messages
Display configuration complete? --> Yes
Review log entries. Entries are oldest to newest and time stamped based on the unit up time
Verify stack configuration is correct. Unique switch ID and Green LED to at least one neighbour
Restart Stack starting at base, allowing each to boot.
A device does not connect?
yes
no
C
B

Figure 11: Stack part 2

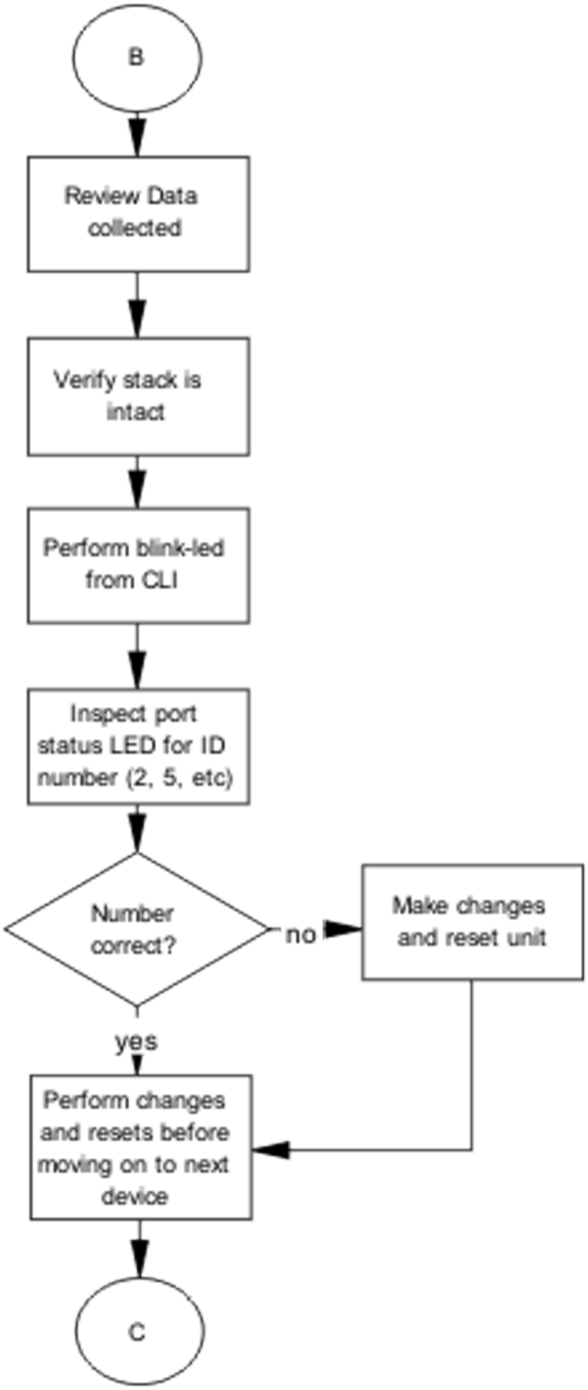

B
Review Data collected
Verify stack is intact
Perform blink-led from CLI
Inspect port status LED for ID number (2, 5, etc)
Number correct?
no
Make changes and reset unit
yes
Perform changes and resets before moving on to next device
C

Figure 12: Stack part 3

Dynamic Host Configuration Protocol (DHCP)

DHCP errors are often on the client-side of the communication. The DHCP relay configuration may be at fault when the DHCP server is not on the same subnet as the client, .

DHCP Recovery Tree

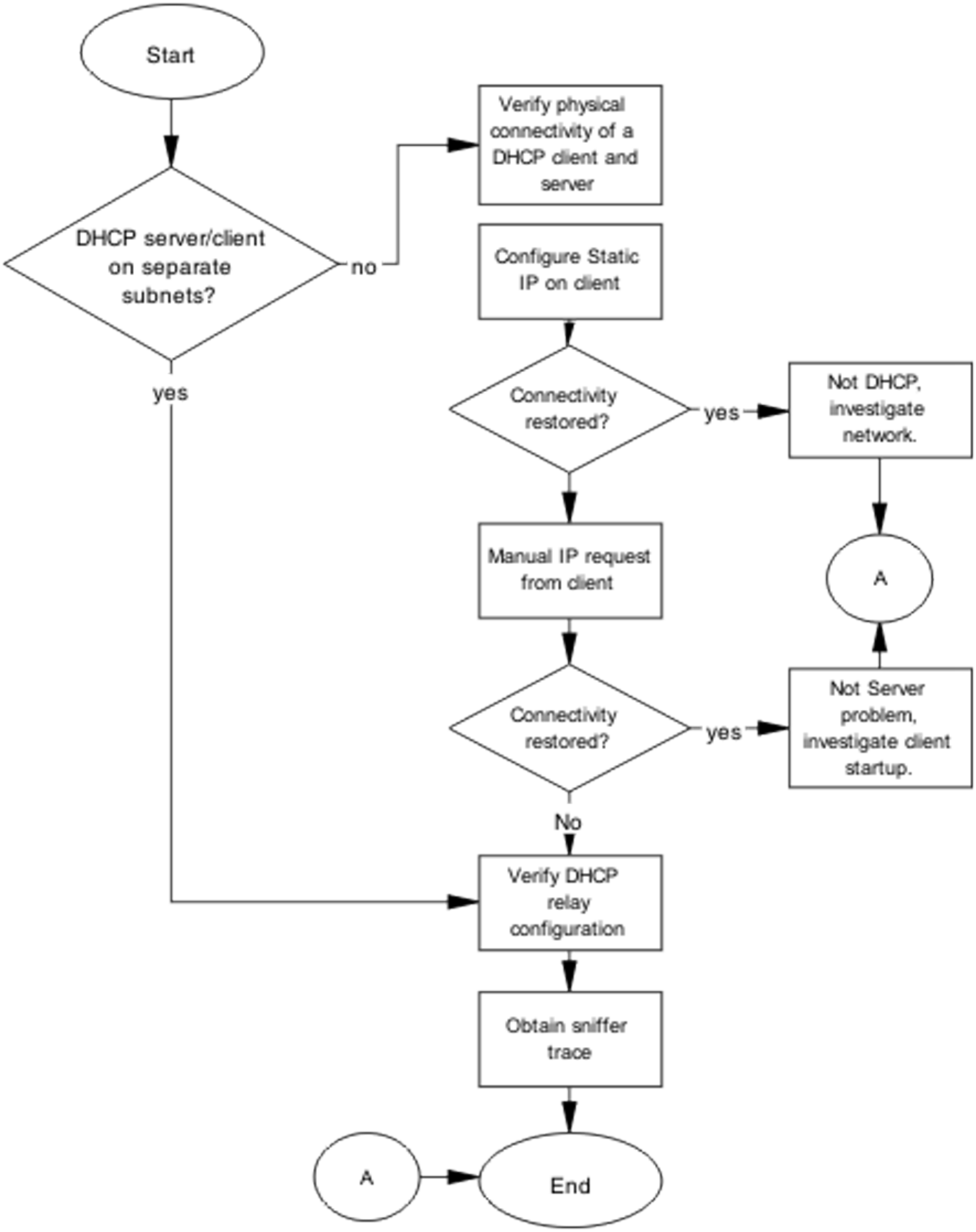

Start
DHCP server/client on separate subnets?
no
yes
Verify physical connectivity of a DHCP client and server
Configure Static IP on client
Connectivity restored?
yes
Not DHCP, investigate network.
Manual IP request from client
A
Connectivity restored?
yes
Not Server problem, investigate client startup.
No
Verify DHCP relay configuration
Obtain sniffer trace
A
End

Figure 13: DHCP

Chapter 8: Troubleshooting hardware

This sections includes hardware troubleshooting specific to the ERS 5000 series.

Work flow: Troubleshooting hardware

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

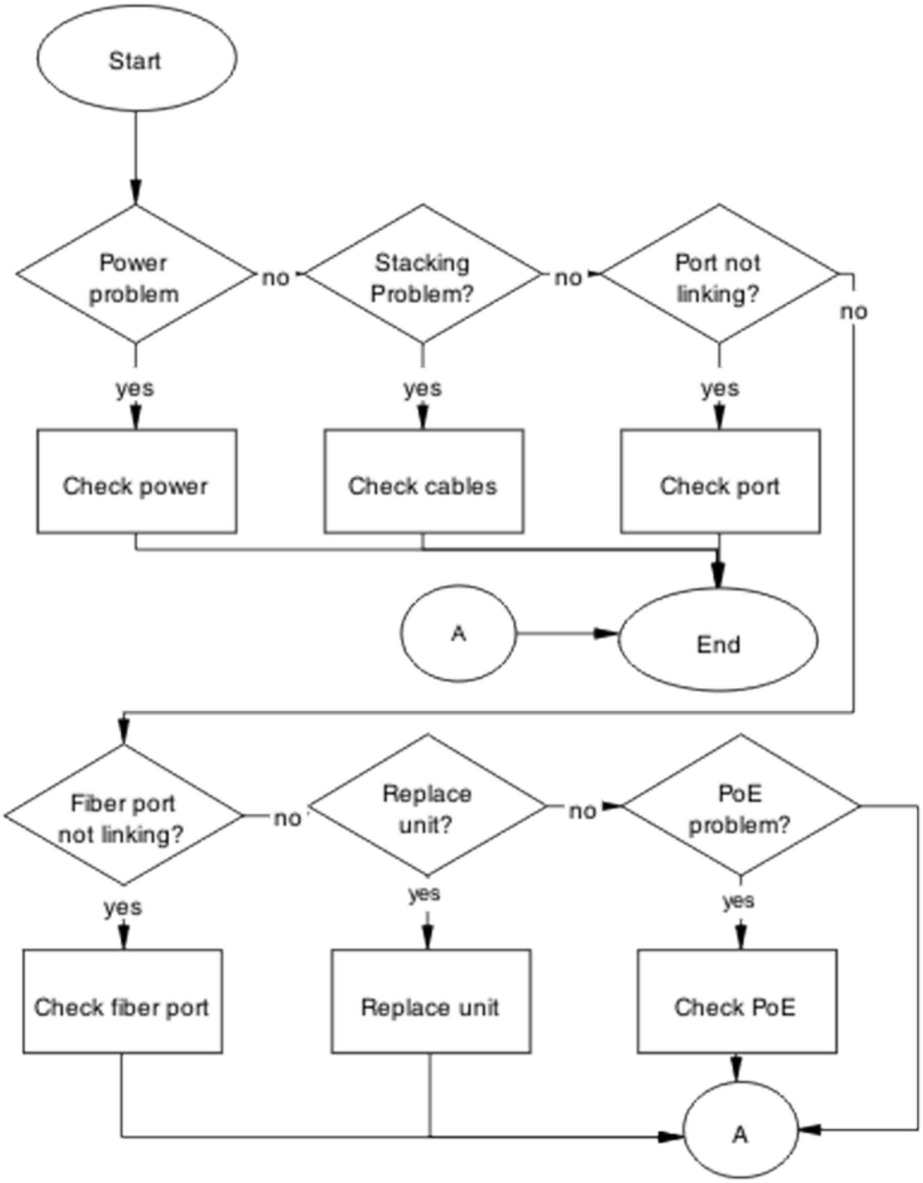


Figure 14: Troubleshooting hardware

Troubleshooting hardware navigation:

- Check power on page 41
- Check cables on page 43
- Check port on page 45
- Check fiber port on page 50
- Replace unit on page 53
- Check PoE

Check power

Confirm power is being delivered to the device.

Task flow: Check power

The following task flow assists you to confirm that the ERS 5500 series device is powered correctly.

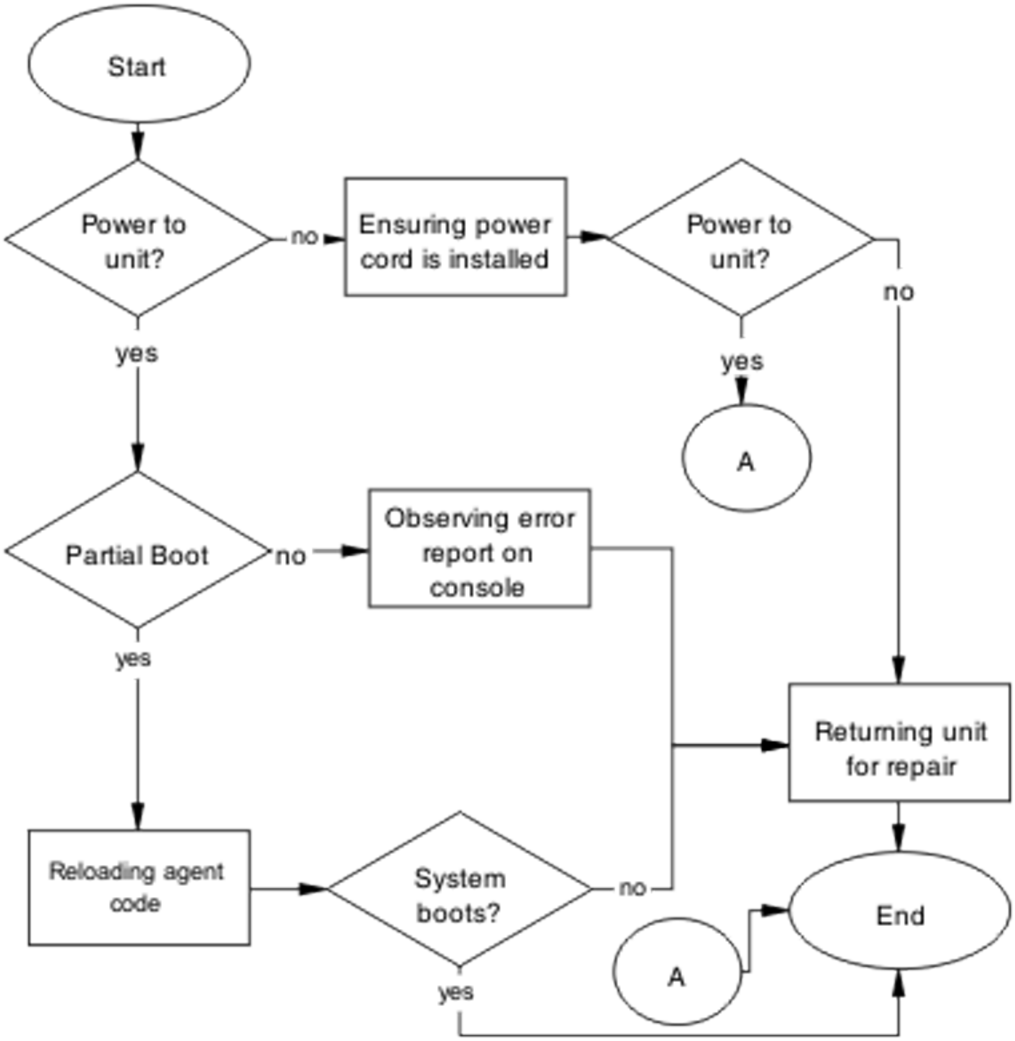


Figure 15: Check power

Check power navigation:

- Ensuring power cord is installed on page 42
- Observing error report on console on page 43
- Reloading agent code on page 43
- Returning unit for repair on page 43

Ensuring power cord is installed

Confirm the power cord is properly installed for the device.

Refer to *Avaya Ethernet Routing Switch 5500 Series - Installation* (NN47200-700) for details regarding proper cord installation.

Observing error report on console

Intrepret the message that is sent to console when it fails.

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

Reloading agent code

Reload the agent code on the ERS 5500 series device to eliminate corrupted or damaged code that causes a partial boot of the device.

⚠ **Caution:**

Ensure you adequately backup the switch 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. Refer to the *Avaya Ethernet Routing Switch 5500 Series Configuration — System* (NN47200-500) for software installation.

Returning unit for repair

Return unit to Avaya for repair

Contact Avaya for return instructions and RMA information.

Check cables

Confirm the stacking cables are correctly connected.

Task flow: Check cables

The following task flow assists you to confirm the stacking cables on the ERS 5500 series device are installed correctly.

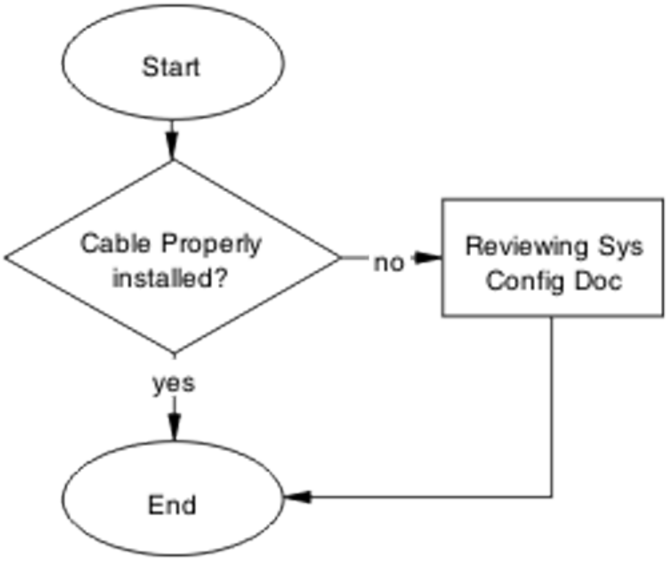


Figure 16: Check cables

Check cables navigation:

- Reviewing Sys Config Doc on page 44

Reviewing Sys Config Doc

Review the system configuration documentation to reapply the stacking cabling as is required.

Review the stacking procedures in the *Avaya Ethernet Routing Switch 5500 Series Configuration — System* (NN47200-500).

Check fiber port

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

Check port

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

Task flow: Check port

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

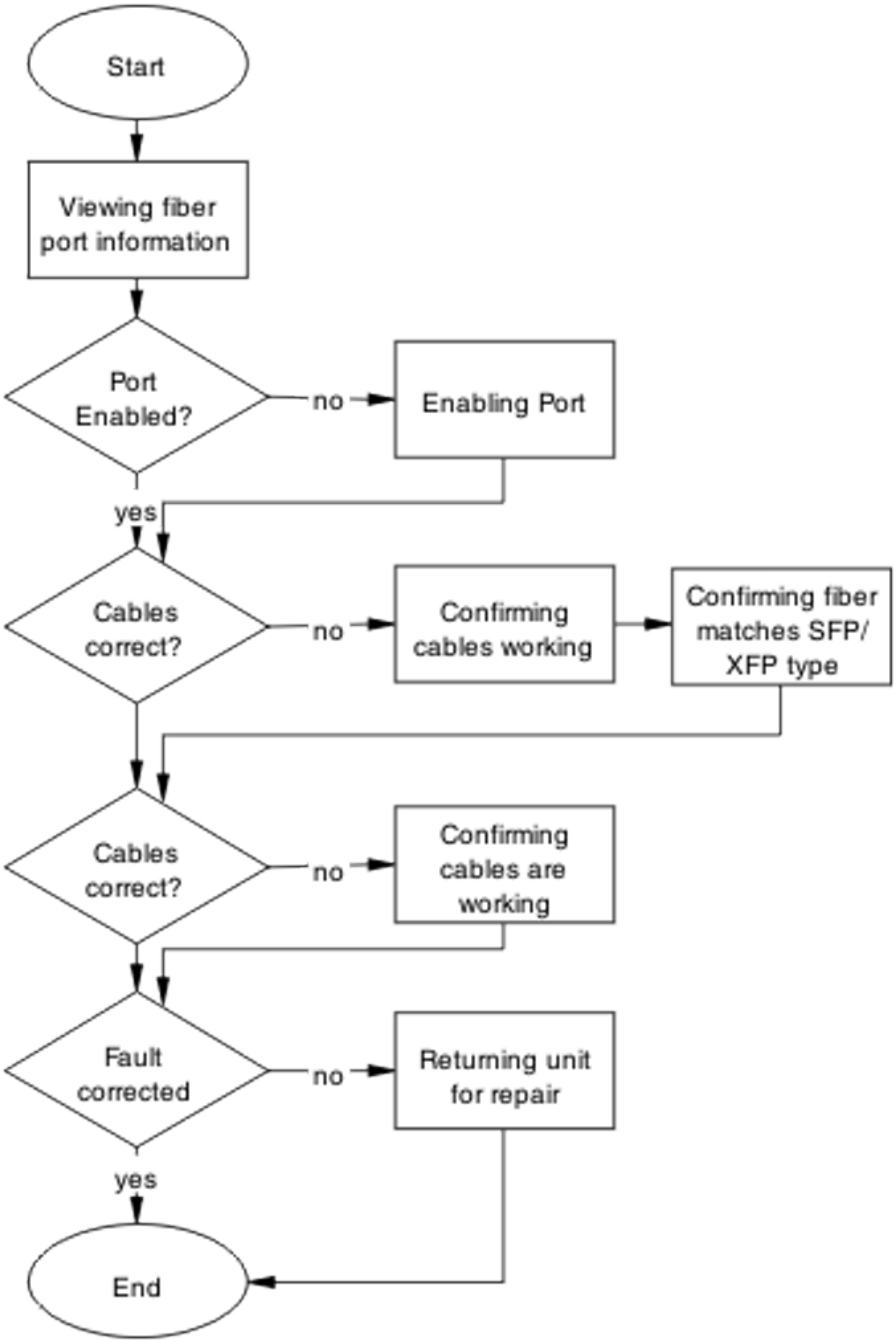

Start
Viewing fiber port information
Port Enabled?
no
Enabling Port
yes
Cables correct?
no
Confirming cables working
Confirming fiber matches SFP/ XFP type
Cables correct?
no
Confirming cables are working
Fault corrected
no
Returning unit for repair
yes
End

Figure 17: Check port

Check port navigation:

- Viewing port information on page 47
- Enabling the port on page 47
- Confirming the cables are working on page 47

Viewing port information

Review the port information to ensure it is enabled.

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

Enabling the port

Enable the port.

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

Confirming the cables are working

Ensure that the cables connecting 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.

Task flow: Check fiber port

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

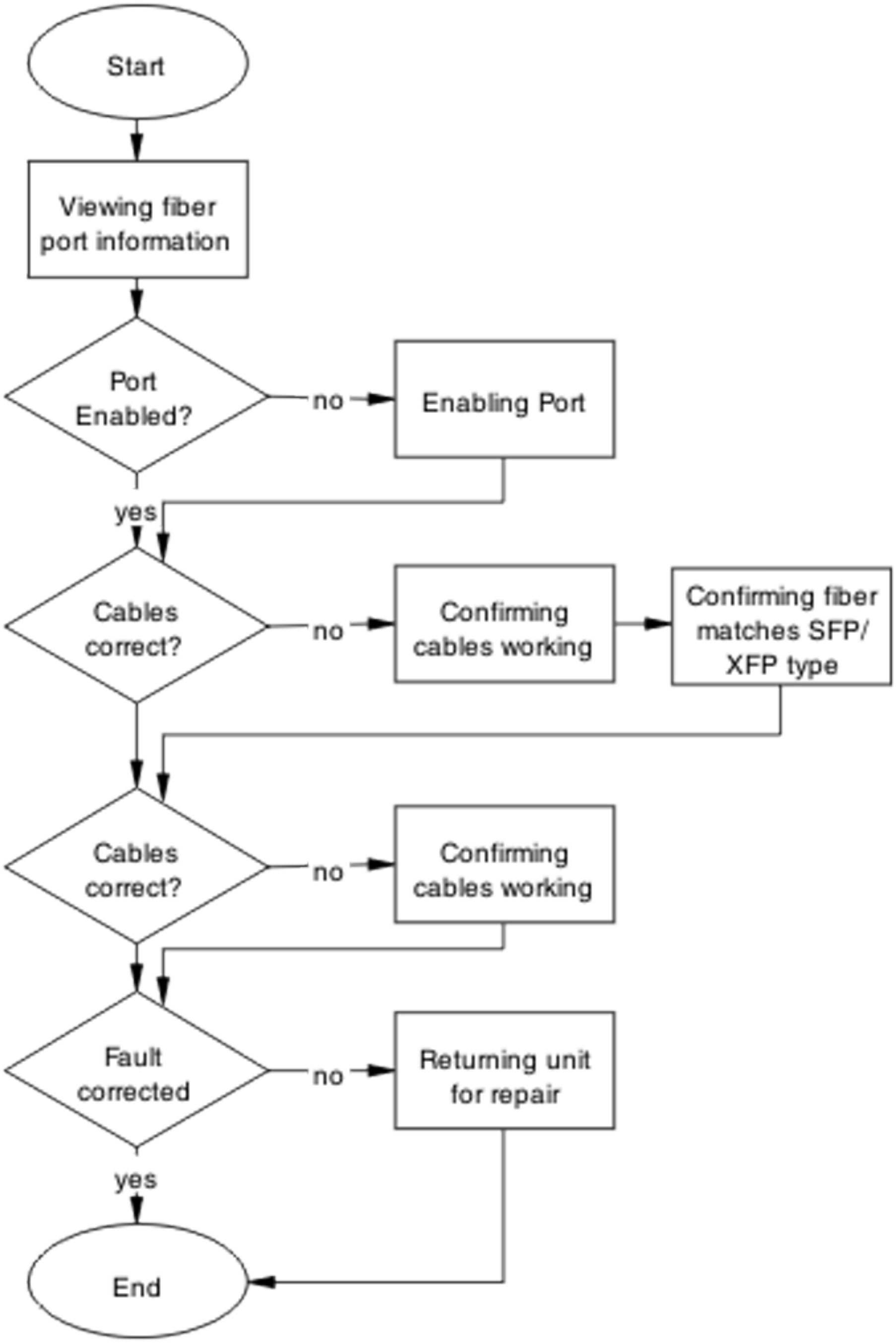

Start
Viewing fiber port information
Port Enabled?
no
Enabling Port
yes
Cables correct?
no
Confirming cables working
Confirming fiber matches SFP/ XFP type
Cables correct?
no
Confirming cables working
Fault corrected
no
Returning unit for repair
yes
End

Figure 18: Check fiber port

Check fiber port navigation:

- Viewing fiber port information on page 49
- Enabling Port on page 49
- Confirming cables working on page 49

- Confirming fiber matches SFP/XFP Type on page 49
- Returning unit for repair on page 53

Viewing fiber port information

Review the port information to ensure it is enabled.

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

Enabling Port

Ensure the port on the ERS 5500 series device is enabled.

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

Confirming cables 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

Ensue the fiber is the correct type and SFP/XFP is installed.

1. Inspect the fiber cables to ensure they are the correct type.
2. Review *Avaya Ethernet Routing Switch 5500 Series Installation — SFP* (NN47200-302) for details or RN's for list of approved SFP/XFP
3. Note the port status.

Check fiber port

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

Task flow: Check fiber port

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

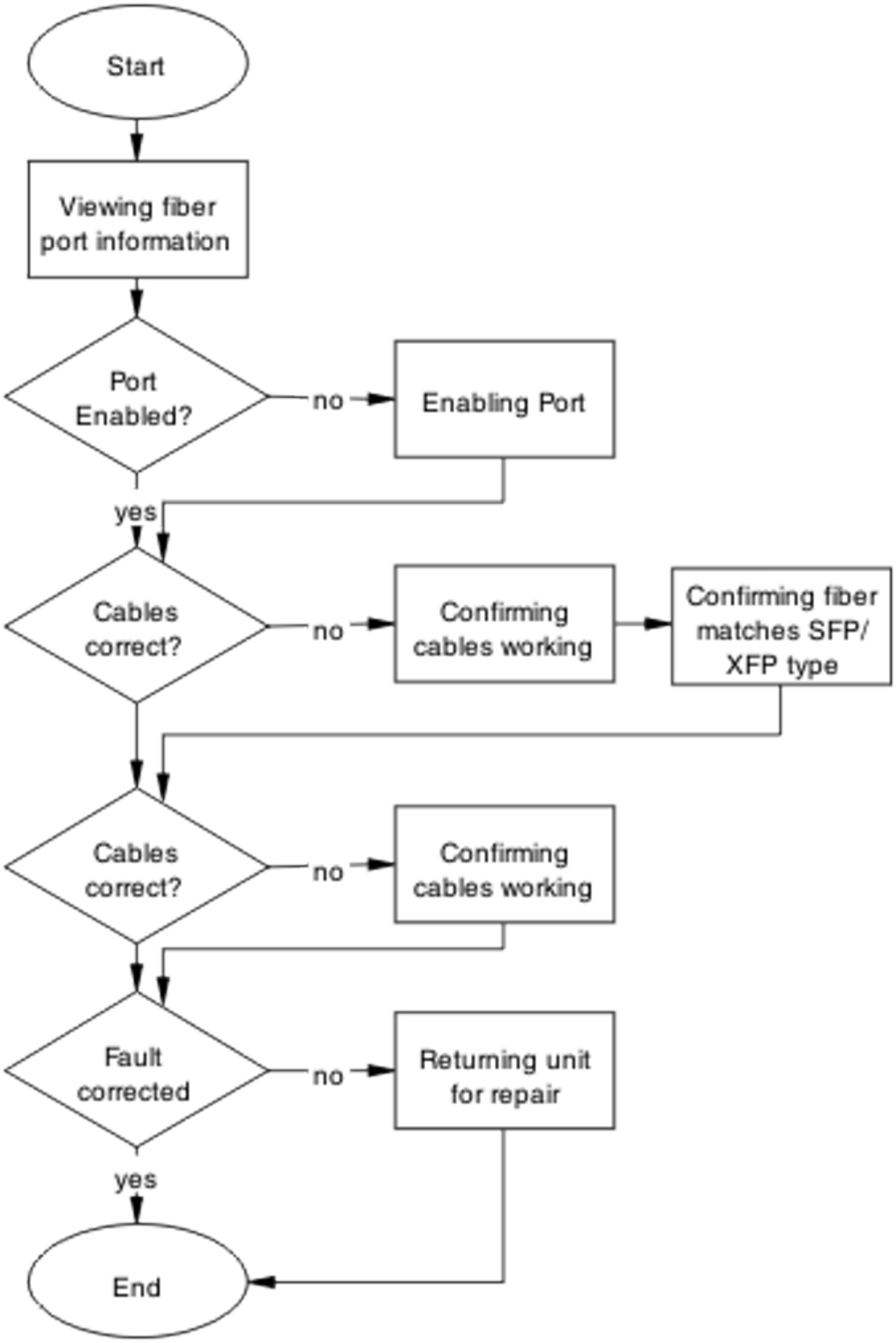

Start
Viewing fiber port information
Port Enabled?
no
Enabling Port
yes
Cables correct?
no
Confirming cables working
Confirming fiber matches SFP/ XFP type
Cables correct?
no
Confirming cables working
Fault corrected
no
Returning unit for repair
yes
End

Figure 19: Check fiber port

Check fiber port navigation:

- Viewing fiber port information on page 49
- Enabling Port on page 49
- Confirming cables working on page 49

- Confirming fiber matches SFP/XFP Type on page 49
- Returning unit for repair on page 53

Viewing fiber port information

Review the port information to ensure it is enabled.

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

Enabling Port

Ensure the port on the ERS 5500 series device is enabled.

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

Confirming cables 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

Ensue the fiber is the correct type and SFP/XFP is installed.

1. Inspect the fiber cables to ensure they are the correct type.
2. Review *Avaya Ethernet Routing Switch 5500 Series Installation — SFP* (NN47200-302) for details or RN's for list of approved SFP/XFP
3. Note the port status.

Returning unit for repair

Return unit to Avaya for repair

Contact Avaya for return instructions and RMA information.

Replace unit

Remove defective unit and insert the replacement.

Prerequisites

Caution:

Due to physical handling of the device and your physical proximity to electrical equipment, review and adhere to all safety instructions and literature included with device and in *Avaya Ethernet Routing Switch 5500 Series Installation* (NN47200-300)

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

Also understand, that if you are replacing the base unit and then another unit of the stack will be designated as the temporary base unit. After the base unit is replaced, the new unit will not resume as the base unit automatically.

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.

Task flow: Replace unit

The following task flow assists you to replace one of the ERS 5500 series devices. This in only appropriate if old software is used or AAUR is disabled. If AAUR is available (and it is turned on by default in such cases) the verify software procedures are not required.

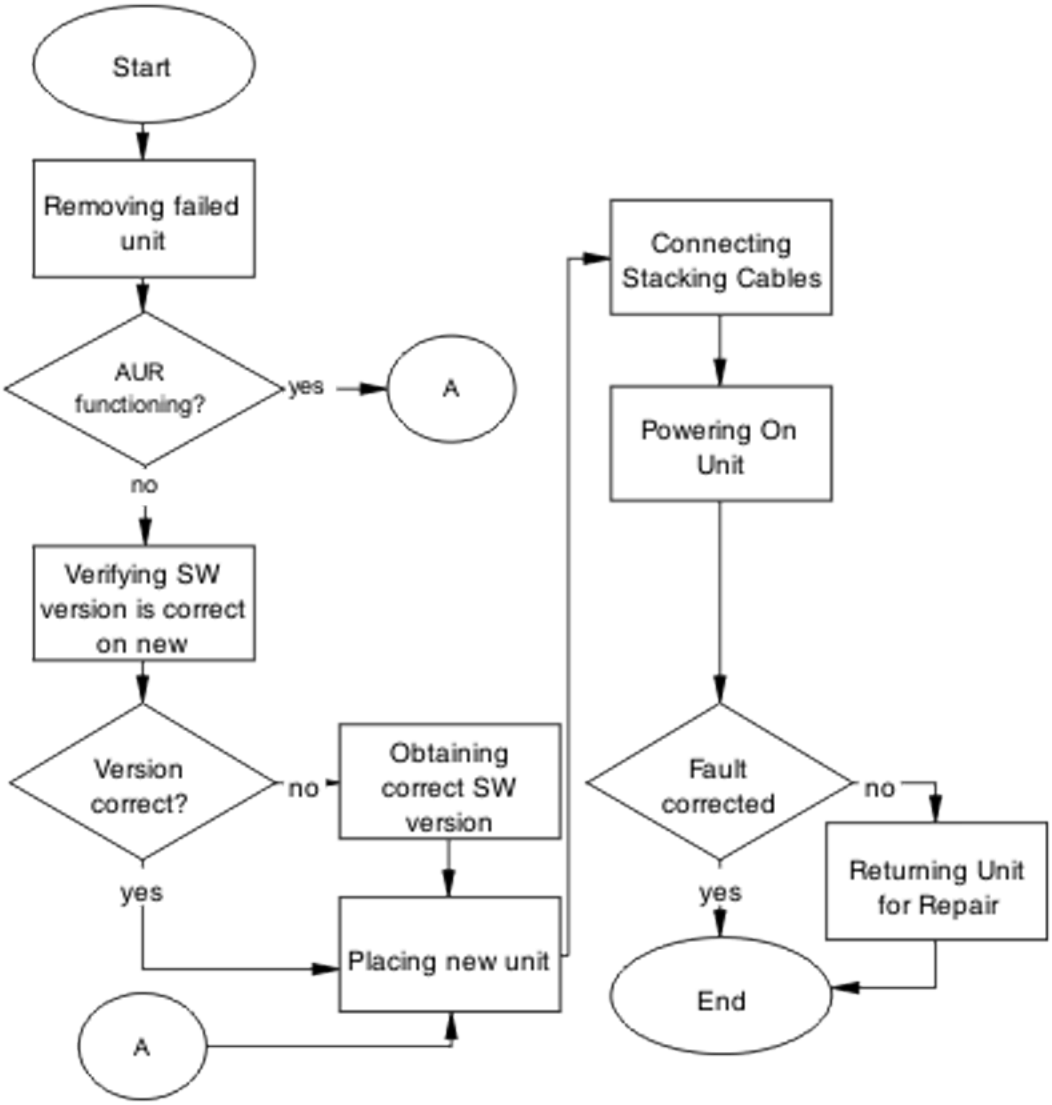


Figure 20: Replace unit

Replace unit navigation:

- Removing failed unit on page 55
- Verifying software version is correct on new device on page 55
- Obtaining correct software version on page 55
- Placing new unit on page 55
- Connecting stacking cables on page 56
- Powering on unit on page 56
- Returning unit for repair on page 56

Removing failed unit

Remove the failed unit from the stack.

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

Verifying software version is correct on new device

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

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

Obtaining correct software version

Obtain and install correct software version

⚠ **Caution:**

Ensure you backup the switch configuration prior to reloading software.

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

Refer to the *Avaya Ethernet Routing Switch 5500 Series Configuration — System* (NN47200-500) for software installation.

Placing 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 5500 Series Installation* (NN47200-300).

Connecting stacking cables

Reconnect the stacking cables to correctly stack the device.

1. Review the stacking section in *Avaya Ethernet Routing Switch 5500 Series Configuration — System* (NN47200-500) for cabling details.
2. Connect the cables in accordance with physical stack requirements.

Powering on unit

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

No requirement exists to reset the entire stack. The single device being replaced will be the only device having such action placed on it.

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

Returning unit for repair

Return unit to Avaya for repair

Contact Avaya for return instructions and RMA information.

Chapter 9: Troubleshooting authentication

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

Work flow: Troubleshooting authentication

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

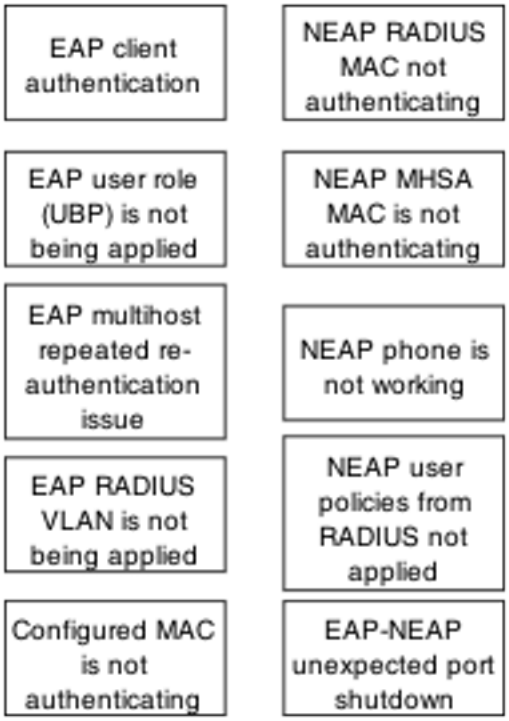

EAP client authentication
NEAP RADIUS MAC not authenticating
EAP user role (UBP) is not being applied
NEAP MHSA MAC is not authenticating
EAP multihost repeated re-authentication issue
NEAP phone is not working
EAP RADIUS VLAN is not being applied
NEAP user policies from RADIUS not applied
Configured MAC is not authenticating
EAP-NEAP unexpected port shutdown

Figure 21: Troubleshooting authentication

Troubleshooting authentication navigation:

- EAP client authentication on page 58
- EAP user role (UBP) is not being applied on page 67
- EAP multihost repeated re-authentication issue on page 81
- EAP RADIUS VLAN is not being applied on page 85

- Configured MAC is not authenticating on page 91
- NEAP RADIUS MAC not authenticating on page 97
- NEAP MHSA MAC is not authenticating on page 103
- NEAP phone is not working on page 108
- NEAP user policies from RADIUS not applied on page 116
- EAP-NEAP unexpected port shutdown on page 131

EAP client authentication

This section provides troubleshooting guidelines for the EAP and NEAP features on the ERS 5500 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.

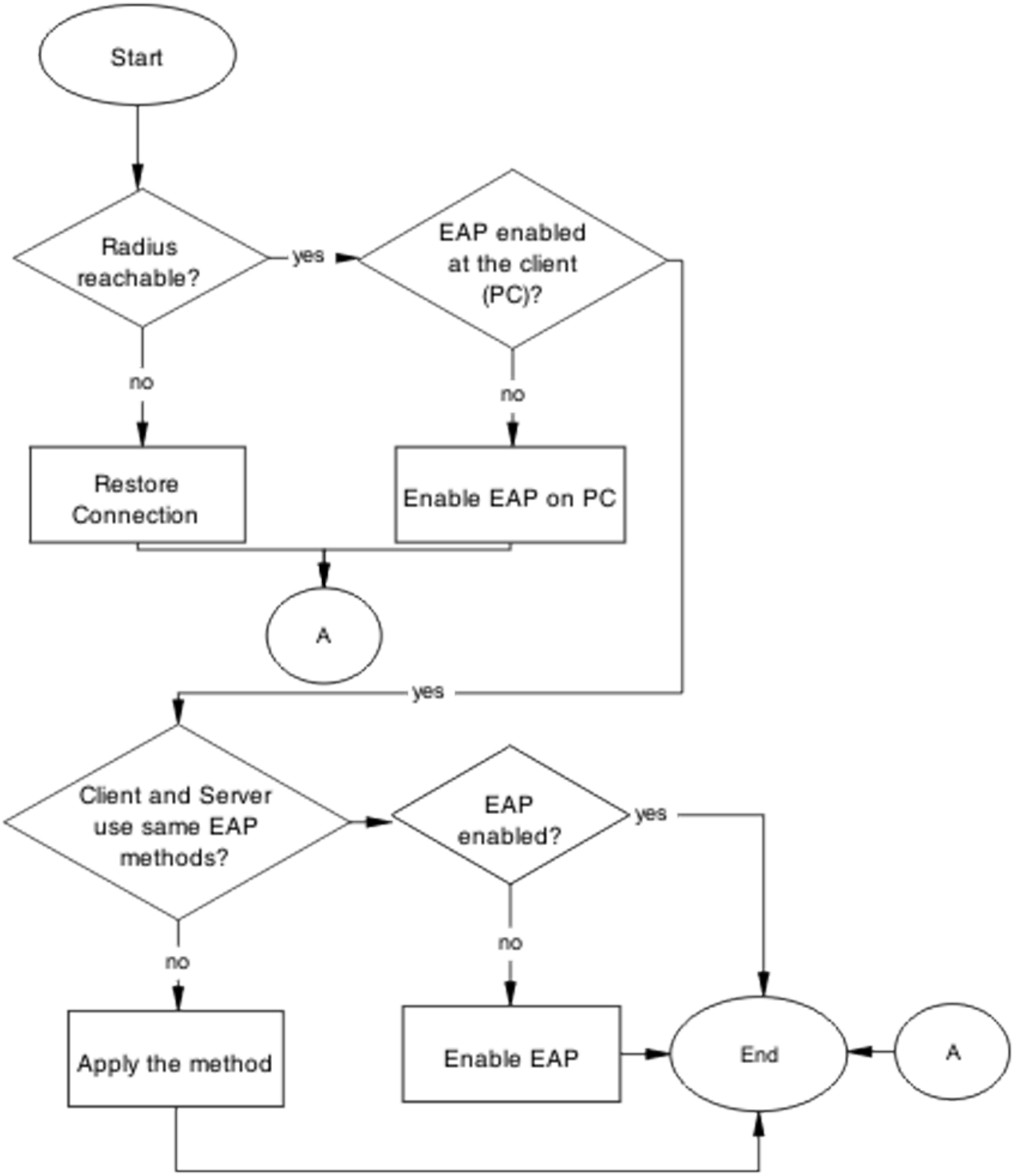


Figure 22: EAP client is not authenticating

EAP client is not authenticating navigation:

- Restore RADIUS connection on page 60
- Enable EAP on The PC on page 63
- Apply the method on page 64
- Enable EAP globally on page 65

Restore RADIUS connection

Ensure that the RADIUS server has connectivity to the device

Task flow: Restore RADIUS connection

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

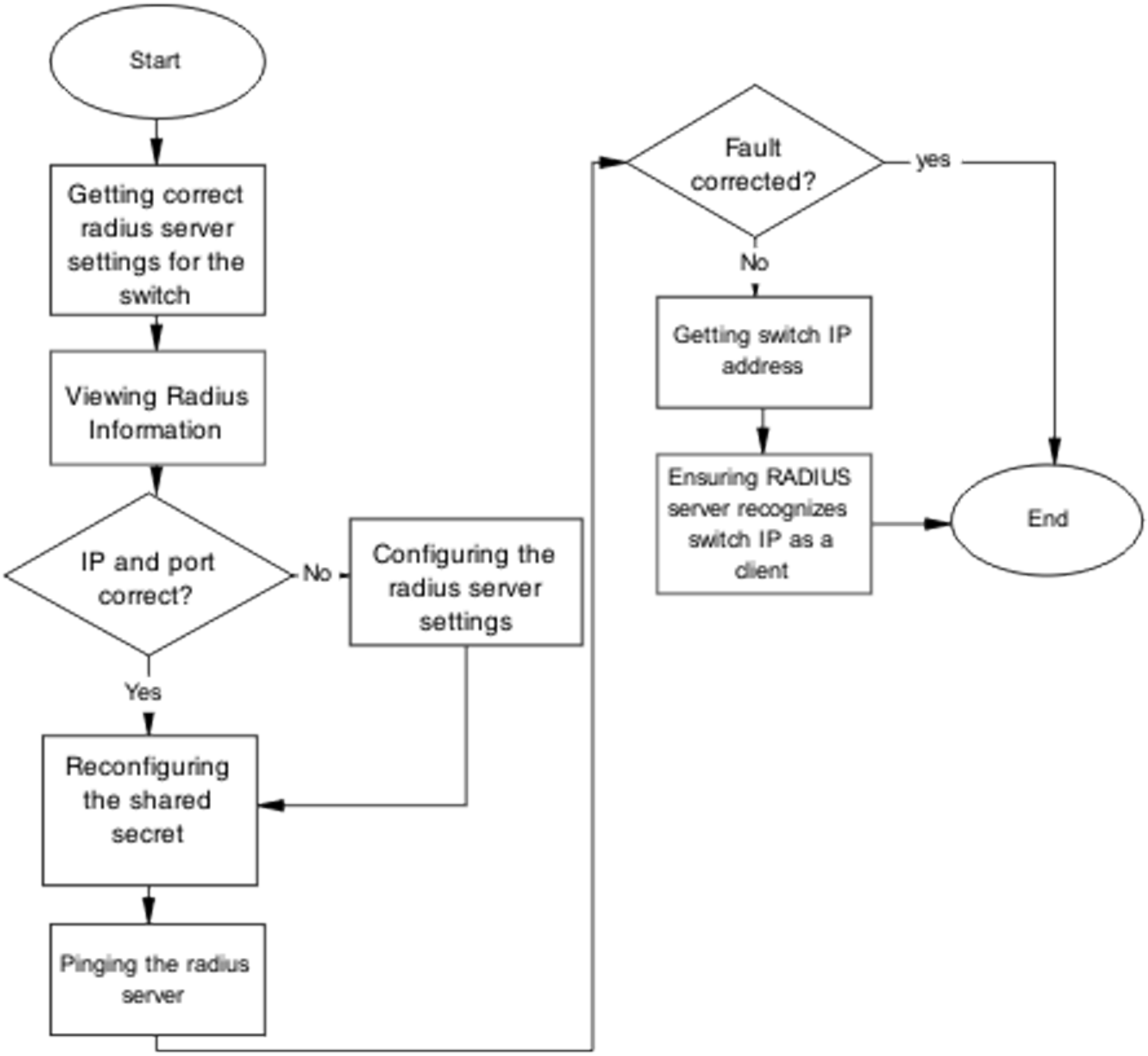

Start
Getting correct radius server settings for the switch
Viewing Radius Information
IP and port correct?
No
Configuring the radius server settings
Yes
Reconfiguring the shared secret
Pinging the radius server
Fault corrected?
yes
No
Getting switch IP address
Ensuring RADIUS server recognizes switch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

Figure 23: Restore RADIUS connection

Restore RADIUS connection navigation:

- Getting correct RADIUS server settings for the switch on page 61
- Viewing RADIUS information on page 62
- Configuring the RADIUS server settings on page 62
- Reconfiguring the shared secret on page 62
- Pinging the RADIUS server on page 62

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

To review the RADIUS server settings in the device.

Understand that default server port is 1812/UDP. Older servers will use 1645/UDP. Some older servers will not support UDP.

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 are to be correct for the network.

Follow vendor documentation to set the RADIUS server settings.

Reconfiguring the shared secret

The Shared Secret is to be reset in case there was 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 has to 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.

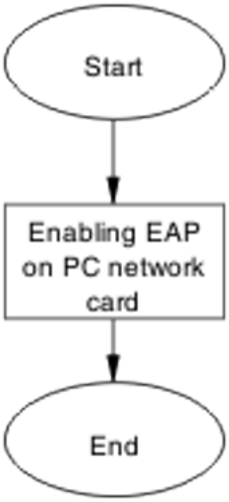


Figure 24: Enable EAP on the PC

Enable EAP on the PC navigation:

- Enabling EAP on PC network card on page 63

Enabling EAP on PC network card

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

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

Apply the method

The correct EAP method needs to be applied.

Task flow: Apply the method

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

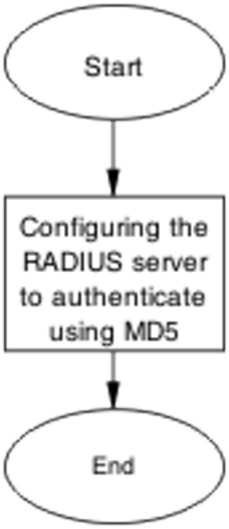


Figure 25: Apply the method

Apply the method navigation:

- Configuring the RADIUS server on page 64

Configuring the RADIUS server

The RADIUS server is to be configured to authenticate using MD5.

1. Obtain Network information for Radius Server from Planning and Engineering.
2. Save the information for reference.

Enable EAP globally

EAP is to be globally enabled on the ERS 5500 series device.

Task flow: Enable EAP globally

The following task flow assists you to enable EAP globally on the ERS 5500 series device.

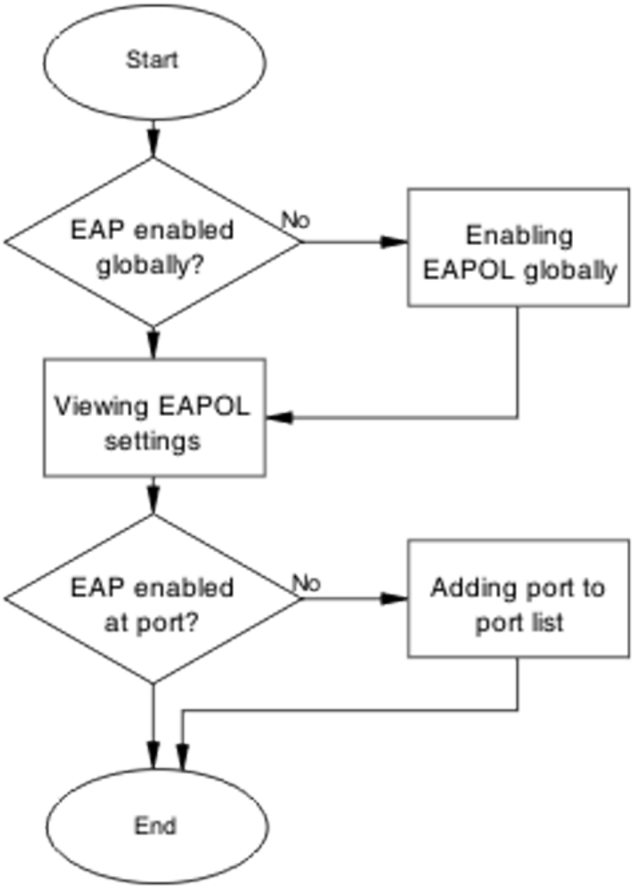


Figure 26: Enable EAP globally

Enable EAP globally navigation:

- Enabling EAP globally on page 66
- Viewing EAPOL settings on page 67
- Setting EAPOL port administrative status to auto on page 67

Enabling EAP globally

The EAP is to be globally enabled on the ERS 5500 series device.

1. Use the **`eapol enable`** command to enable EAP globally on the ERS 5500 series device.
2. Observe no errors after command execution.

Viewing EAPOL settings

The EAPOL settings is to be reviewed 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

The port is to be included in the port list.

1. Use the **`eapol status auto`** command to change the port status to auto.
2. Observe no errors after the command execution.

EAP user role (UBP) is not being applied

Determine the reason why the user role is not being applied.

Work flow: EAP user role not being applied

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

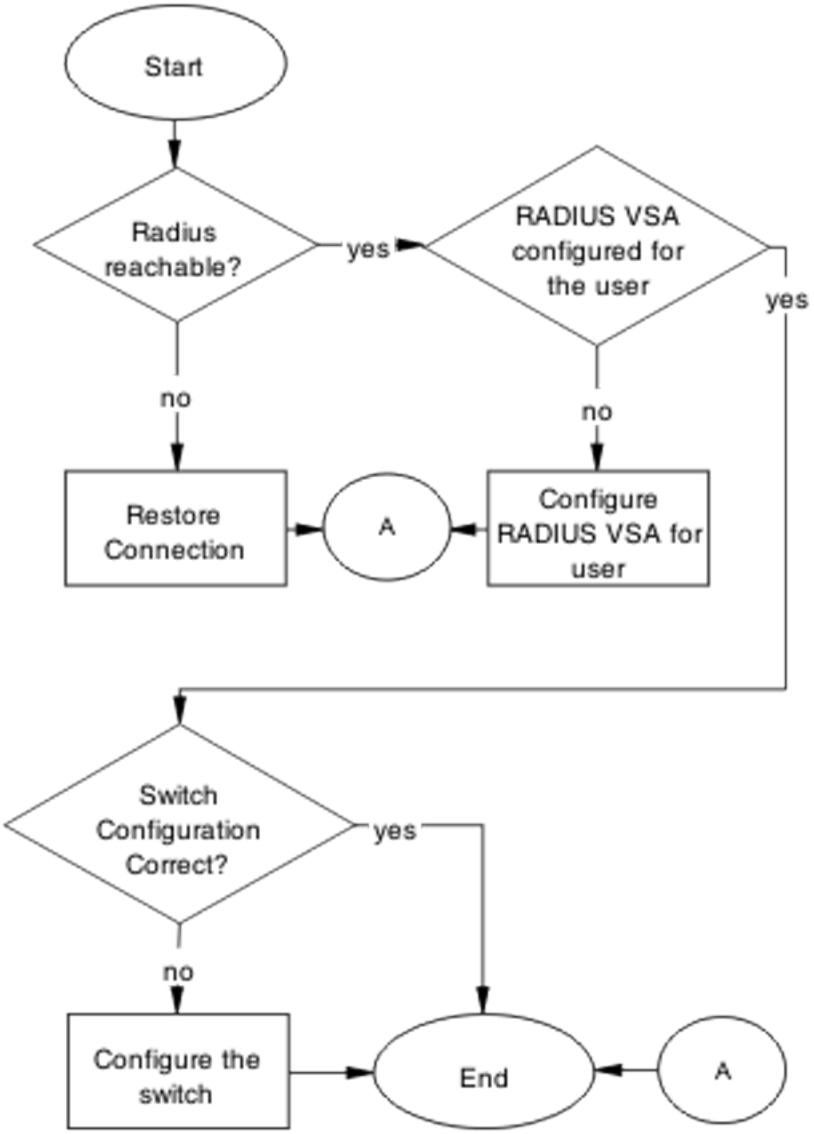

Start
Radius reachable?
yes
RADIUS VSA configured for the user
yes
no
no
Restore Connection
A
Configure RADIUS VSA for user
Switch Configuration Correct?
yes
no
Configure the switch
End
A

Figure 27: EAP user role not being applied

EAP user role not being applied navigation:

- Restore RADIUS Connection on page 68
- Configure RADIUS VSA for User on page 71
- Configure the switch on page 72

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 RADIUS connection to the device.

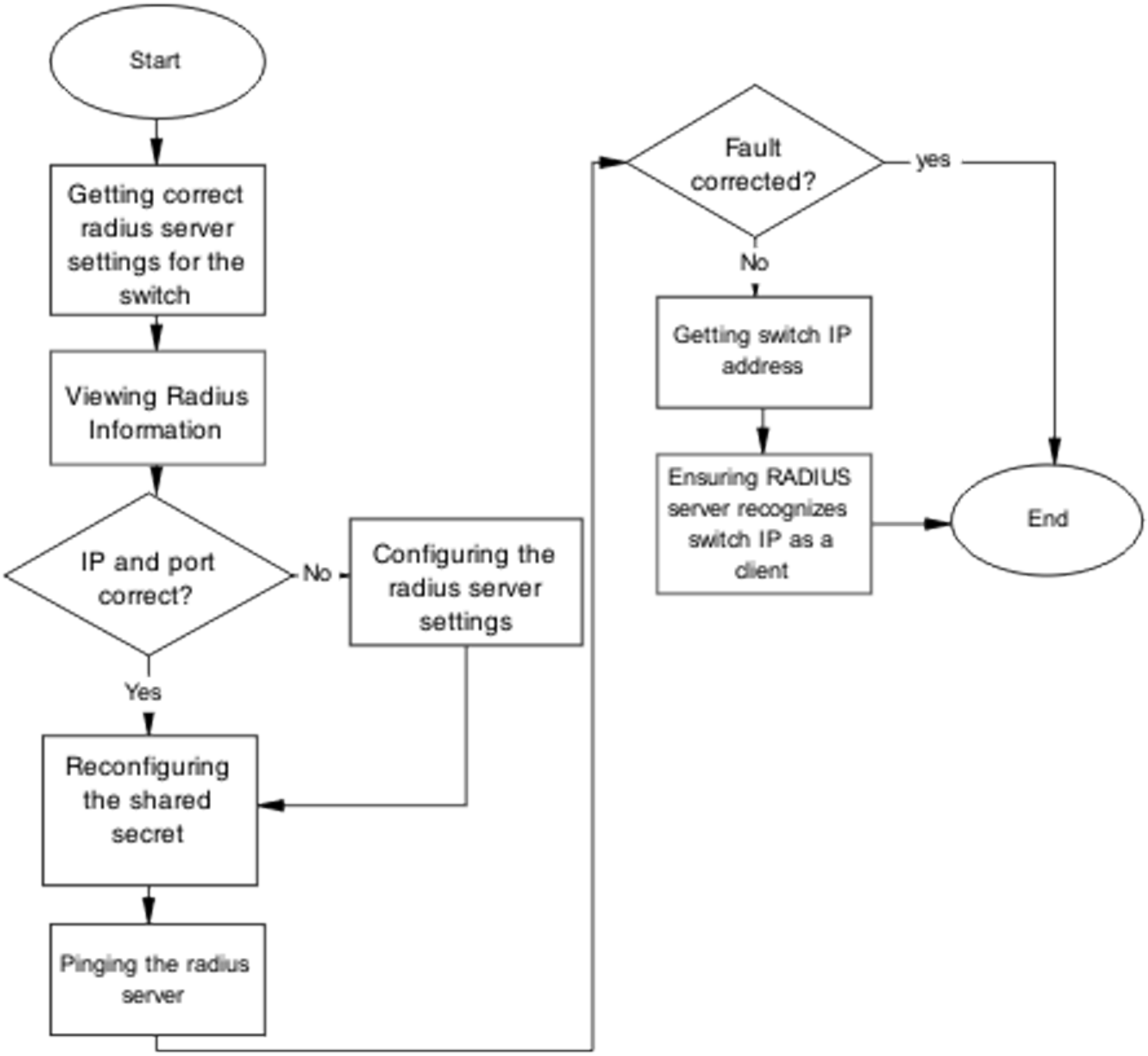

Start
Getting correct radius server settings for the switch
Viewing Radius Information
IP and port correct?
No
Configuring the radius server settings
Yes
Reconfiguring the shared secret
Pinging the radius server
Fault corrected?
yes
No
Getting switch IP address
Ensuring RADIUS server recognizes switch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

Figure 28: Restore RADIUS connection

Restore RADIUS connection navigation:

- Getting correct RADIUS server settings for the switch on page 70
- Viewing Radius Information on page 70
- Configuring the RADIUS server settings on page 70
- Reconfiguring the shared secret on page 70
- Pinging the RADIUS server on page 70

Getting correct RADIUS server settings for the switch

Obtain the Radius server settings.

1. Obtain network information for RADIUS server from Planning and Engineering.
2. Save Information for reference.

Viewing Radius Information

To review the Radius server settings in the device.

Prerequisites:

Understand that default server port is 1812/UDP. Older servers will use 1645/UDP. Some older servers will not support UDP.

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 is to be set to be correct for the network.

Follow vendor documentation to set the RADIUS server.

Reconfiguring the shared secret

The Shared Secret is to be reset in case there was 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.

Configure RADIUS VSA for User

To correct the VSA for the user on the RADIUS server.

Task flow: Configure RADIUS VSA for user

The following task flow assists you to configure the RADIUS VSA for a user.

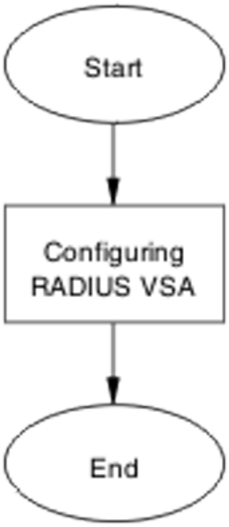


Figure 29: Configure RADIUS VSA for user

Configure RADIUS VSA for user navigation:

- Configuring RADIUS VSA for User on page 71

Configuring RADIUS VSA for User

Configure the RADIUS VSA for the user.

1. Obtain the Vendor documentation for the RADIUS server.
2. Make VSA correction for the user according to the vendor documentation. At least one UROL string is to be declared.

Configure the switch

Configure the switch for UBP globally.

Task flow: Configure the switch

The following task flows assist you to enable UBP globally on the device.

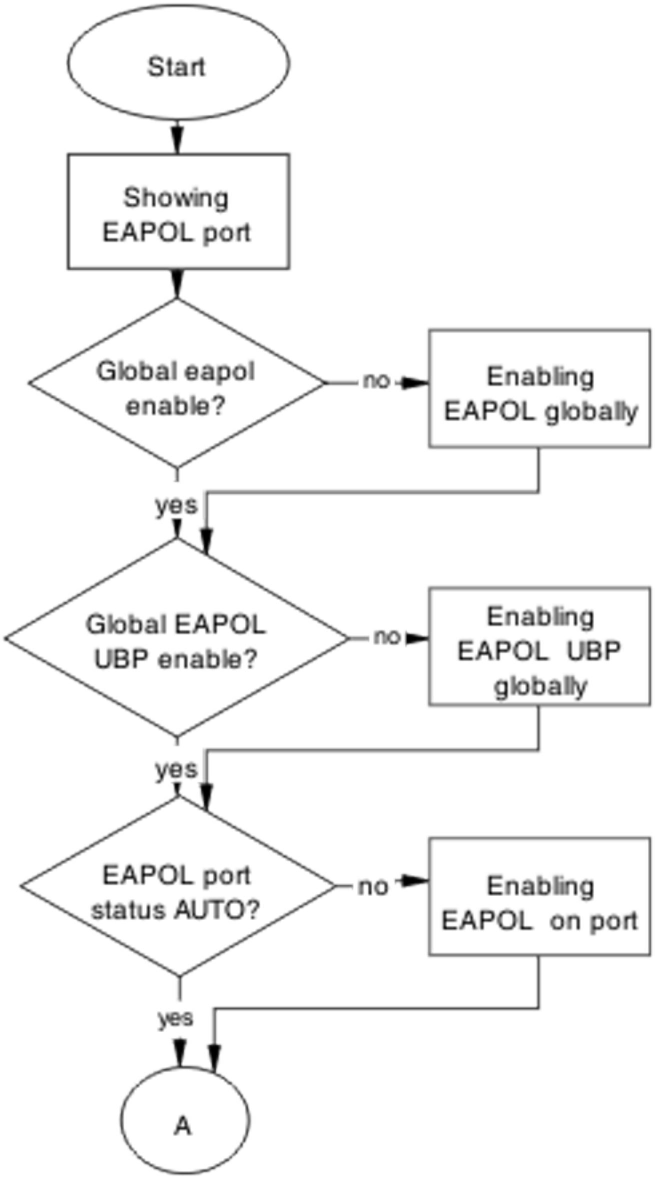


Figure 30: Configure the switch part 1

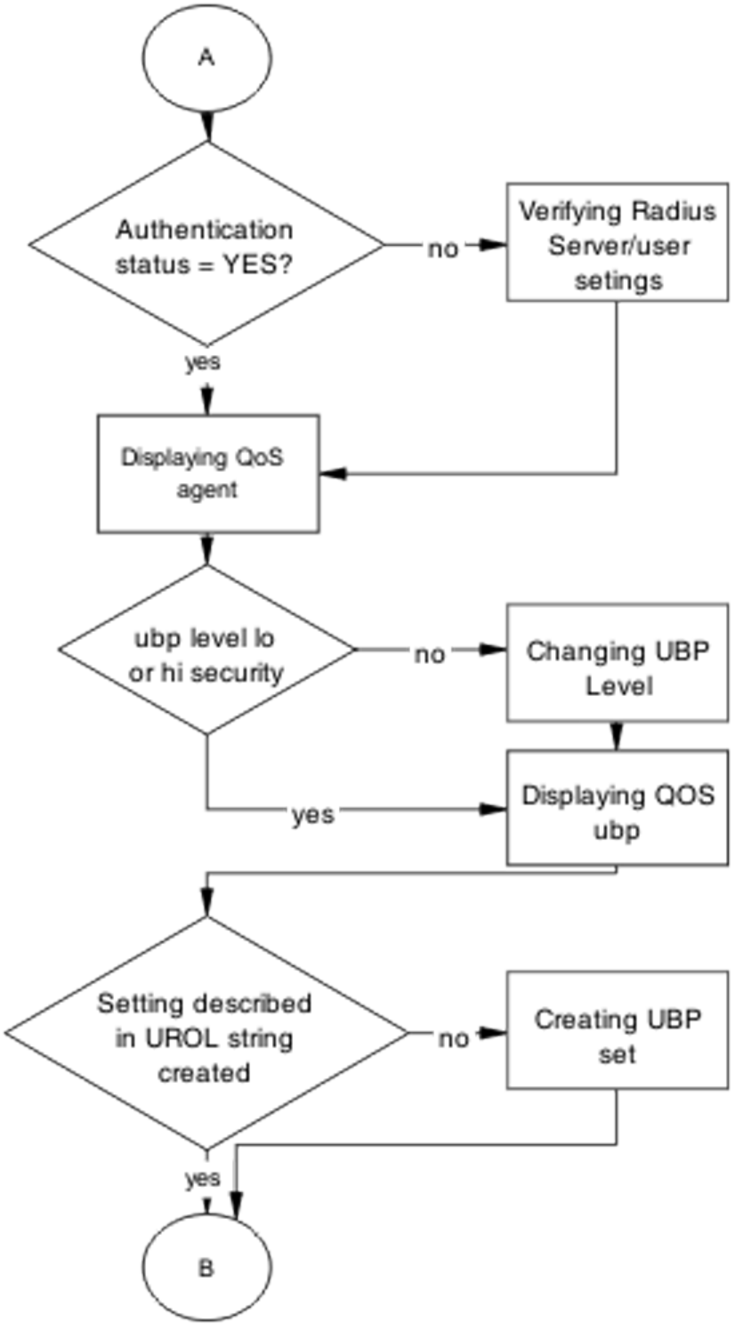

A
Authentication status = YES?
no
Verifying Radius Server/user setings
yes
Displaying QoS agent
ubp level lo or hi security
no
Changing UBP Level
yes
Displaying QOS ubp
Setting described in UROL string created
no
Creating UBP set
yes
B

Figure 31: Configure the switch part 2

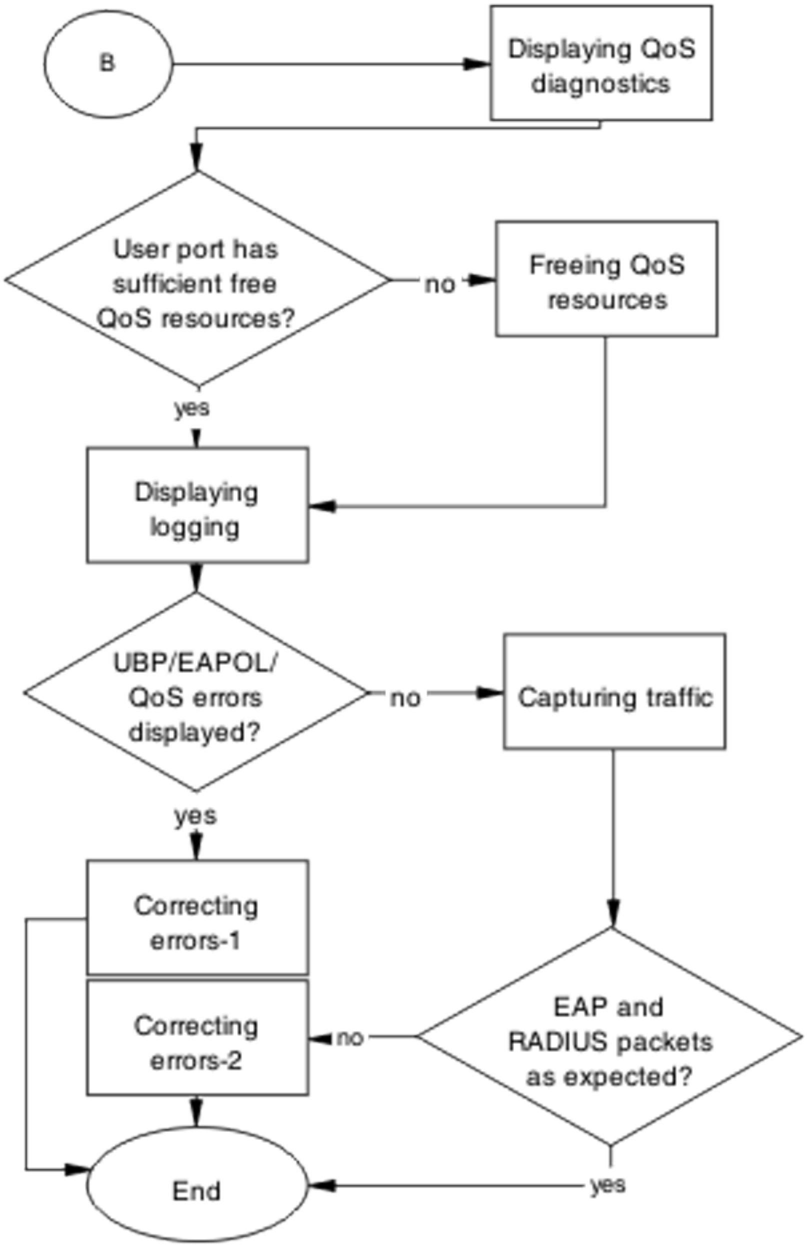

B
Displaying QoS diagnostics
User port has sufficient free QoS resources?
no
Freeing QoS resources
yes
Displaying logging
UBP/EAPOL/ QoS errors displayed?
no
Capturing traffic
yes
Correcting errors-1
Correcting errors-2
no
EAP and RADIUS packets as expected?
yes
End

Figure 32: Configure the switch part 3

Configure the switch navigation:

- Displaying EAPOL Port on page 76
- Enabling EAPOL globally on page 76
- Enabling EAPOL UBP globally on page 76
- Enabling EAPOL on port on page 77
- Verifying Radius Server/User settings on page 77

- Showing QoS Agent on page 77
- Changing UBP Level on page 78
- Displaying QoS UBP on page 78
- Creating UBP Set on page 78
- Displaying QoS Diag on page 79
- Freeing QoS resources on page 79
- Displaying logging on page 79
- Correcting errors-1 on page 79
- Capturing traffic on page 80
- Correcting errors-2 on page 80

Displaying EAPOL Port

Obtain details of the EAPOL port configuration

1. Use the **`show eapol port <port>`** command to display the port information.
2. Verify if EAPOL global setting is enable.
3. Verify if EAPOL UBP global setting is enable.
4. Verify if EAPOL port status is AUTO.

Enabling EAPOL globally

Enable EAPOL Globally for the switch.

1. Use the **`eapol enable`** command to enable EAP globally.
2. Verify if errors are displayed. No error or warning messages should be displayed.

Enabling EAPOL UBP globally

Enable EAPOL UBP globally for the switch.

1. Use the `eapol user-based-policies enable` command to enable EAPOL UBP globally.
2. Verify if errors are displayed. No error or warning messages should be displayed.

Enabling EAPOL on port

Enable EAPOL on the user port.

1. Use the `eapol port <port> status auto` command to enable EAPOL on port.
2. Verify if errors are displayed. No error or warning messages should be displayed.

Enabling EAPOL on port

Enable EAPOL on the user port.

1. Use the `eapol port <port> status auto` command to enable EAPOL on port.
2. Verify if errors are displayed. No error or warning messages should be displayed.

Verifying Radius Server/User settings

This section provides troubleshooting guidelines for to verify the user and password configured on RADIUS server match user and password used on the user PC.

Use vendor procedures to verify the information.

Showing QoS Agent

Obtain details of the QOS Agent.

1. Use the **`qos agent`** command to display the QOS agent information.
2. Verify that ubp level is low or high security.

Changing UBP Level

Change UBP level to high or low security to enable QoS UBP globally.

1. Use the **`qos agent ubp high-security-local`** or **`qos agent ubp low-security-local`** commands to enable QoS UBP on device.
2. Verify if errors are displayed. No error or warning messages should be displayed.

Displaying QoS UBP

Obtain details of QoS agent settings.

1. Use the **`show qos ubp`** command to display UBP sets.
2. Verify if UBP set name matches the UROL string configured on the Radius Server (if UBP Set is named student then the UROL string sent by the RADIUS server is to be UROL student).

Creating UBP Set

Create UBP set to configure the template policy that will be applied to the authenticated user port.

1. Use the **`qos ubp classifier`** and **`qos ubp set`** commands to create desired UBP set.
2. Verify if errors are displayed. No error or warning messages should be displayed.

Displaying QoS Diag

Obtain details of QoS resources usage.

1. Use the **`show qos diag`** command to display QoS resource utilization.
2. Verify for the port that will be used for user authentication if ((Non QoS masks + QoS mask < 16) and (Non QoS Filters + QoS Filters < 128)).

Freeing QoS resources

Delete some QoS policies that are configured on the user port or disable some of the non-qos application configured on that port.

1. Use the **`no qos policies`** command to delete some of the unnecessary.
2. Verify for the port that will be used for user authentication if ((Non QoS masks + QoS mask < 16) and (Non QoS Filters + QoS Filters < 128)).

Displaying logging

Obtain log messages for the device.

1. Use the **`show logging`** command to display device log messages.
2. Search log messages for EAPOL and QoS errors

Correcting errors-1

Verify EAPOL and/or QoS configuration if errors are displayed in log messages.

1. If error EAPOL messages are logged verify port status and user/password on the RADIUS server/user PC.
2. If QoS error messages are logged verify UBP sets for conflicts inside the set or with the QoS policies already installed on that port.

Capturing traffic

Capture traffic between user PC, DUT, and between DUT and RADIUS server.

1. Using another PC and a hub or port mirroring feature capture traffic between user PC and DUT.
2. Save data using vendor documentation.
3. Using another PC and a hub or port mirroring feature capture traffic between user PC and Radius Server.
4. Save data using vendor documentation.

Correcting errors-2

Using the captured data verify if all the expected packets are exchanged between user PC and DUT and/or between DUT and Radius Server.

1. Search dataflow captured between User PC and DUT for correct EAP packets.
2. Verify if the correct user name is sent by the user PC in the EAP packet.
3. Verify that the DUT sends EAP success packet at the end of EAP exchange.
4. If authentication fails check again user/password on the RADIUS server and user/password used on the user PC.
5. Search dataflow captured between DUT and RADIUS server for correct RADIUS packets.
6. Verify if correct VSA is sent by the RADIUS server.
7. Verify if correct user name is sent by the DUT in the request.
8. If the VSA is incorrect check the RADIUS server configuration, using vendor documentation.

EAP multihost repeated re-authentication issue

Eliminate the multiple authentication of users.

EAP Multihost repeated re-authentication issue

The following work flow assists you to determine the cause and solution of an EAP multihost has repeated authentication.

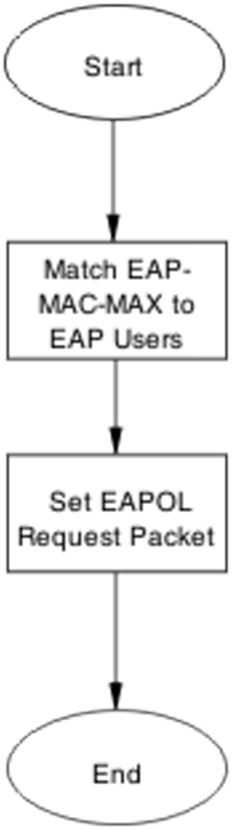


Figure 33: EAP Multihost repeated re-authentication issue

EAP Multihost repeated re-authentication issue navigation:

- Match EAP-MAC-MAX to EAP users on page 82
- Set EAPOL request packet on page 83

Match EAP-MAC-MAX to EAP users

Lower the eap-mac-max to the exact number of EAP users that will soon enter when the number of authenticated users reaches the allowed maximum 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.

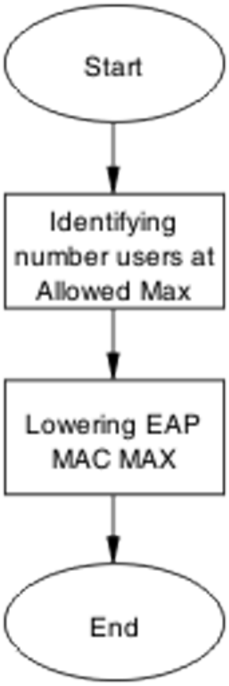


Figure 34: Match EAP-MAC-MAX to EAP users

Match EAP-MAC-MAX to EAP users navigation:

- Identifying number users at allowed max on page 82
- Lowering EAP max MAC on page 83

Identifying number users at allowed max

Obtain the exact number of eap-users that will 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 mac-max value to match the users.

1. Use the `eapol multihost eap-mac-max` command to set the mac-max value.
2. Observe 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 for unicast.

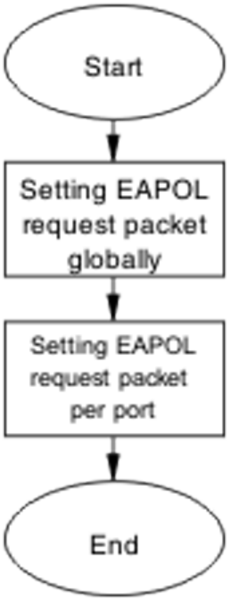

Start
Setting EAPOL request packet globally
Setting EAPOL request packet per port
End

Figure 35: Set EAPOL request packet

Set EAPOL request packet navigation:

- Setting EAPOL request packet globally on page 84
- Setting EAPOL request packet per port on page 84

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. Observe no errors after execution.

Setting EAPOL request packet per 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 is applied.

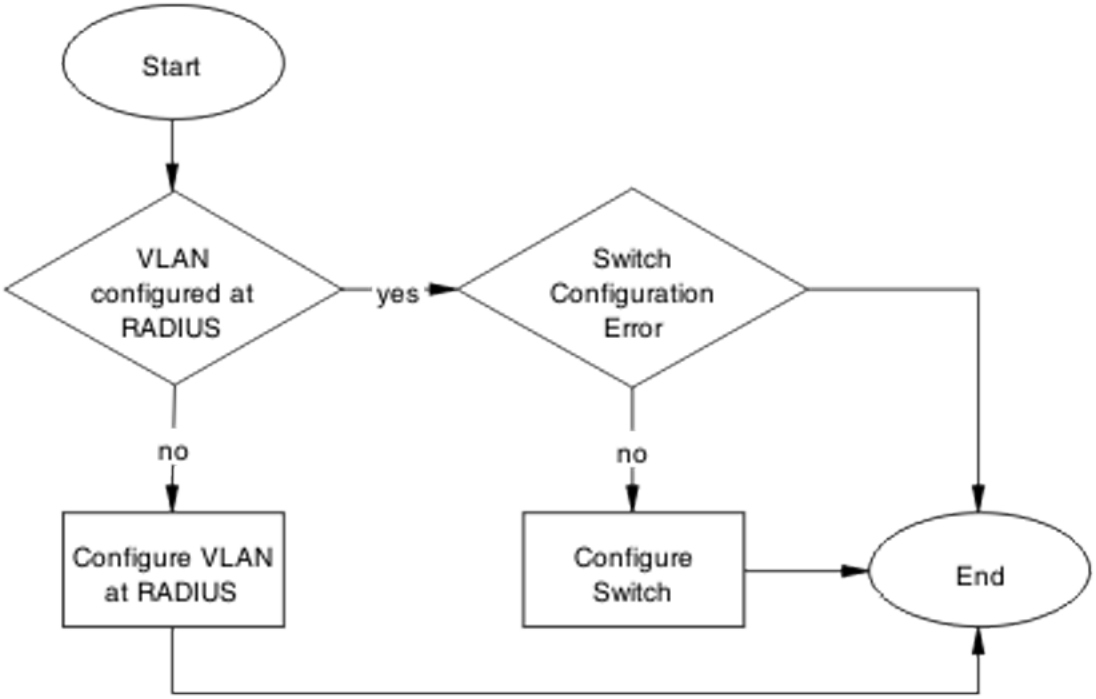


Figure 36: EAP Radius VLAN is not being applied

EAP RADIUS VLAN is not being applied navigation:

- Configure VLAN at RADIUS on page 85
- Configure Switch on page 87

Configure VLAN at RADIUS

Correct discrepancy at the RADIUS server for the VLAN information.

Task flow: Configure VLAN at RADIUS

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

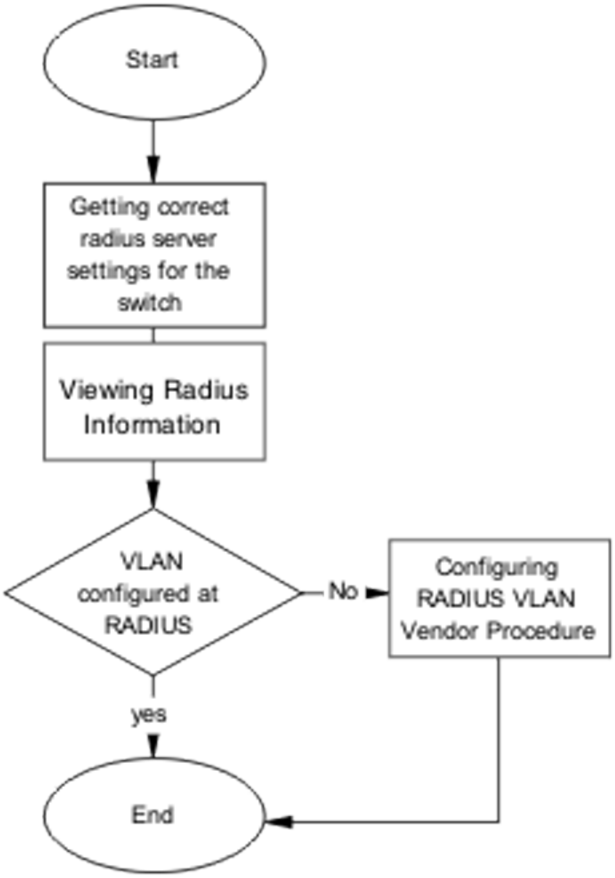

Start
Getting correct radius server settings for the switch
Viewing Radius Information
VLAN configured at RADIUS
No
Configuring RADIUS VLAN Vendor Procedure
yes
End

Figure 37: Configure VLAN at RADIUS

Configure VLAN at RADIUS navigation:

- Getting correct RADIUS server settings on page 86
- Viewing RADIUS information on page 87
- Configuring RADIUS on page 87

Getting correct RADIUS server settings

This section provides troubleshooting guidelines to obtain what the RADIUS server settings are to be.

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

Viewing RADIUS information

Obtain the RADIUS information to identify its settings.

Use vendor documentation to obtain settings display.

Configuring RADIUS

Reconfigure the RADIUS server with the correct VLAN information.

Use vendor documentation to make the required changes.

Prerequisites

Three attributes exist that the RADIUS server sends back to the NAS(switch) for RADIUS assigned VLANs. The attributes are the same for all RADIUS vendors:

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

Configure Switch

The VLAN has to be configured correctly on the ERS 5500 series device.

Task flow: Configure switch

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

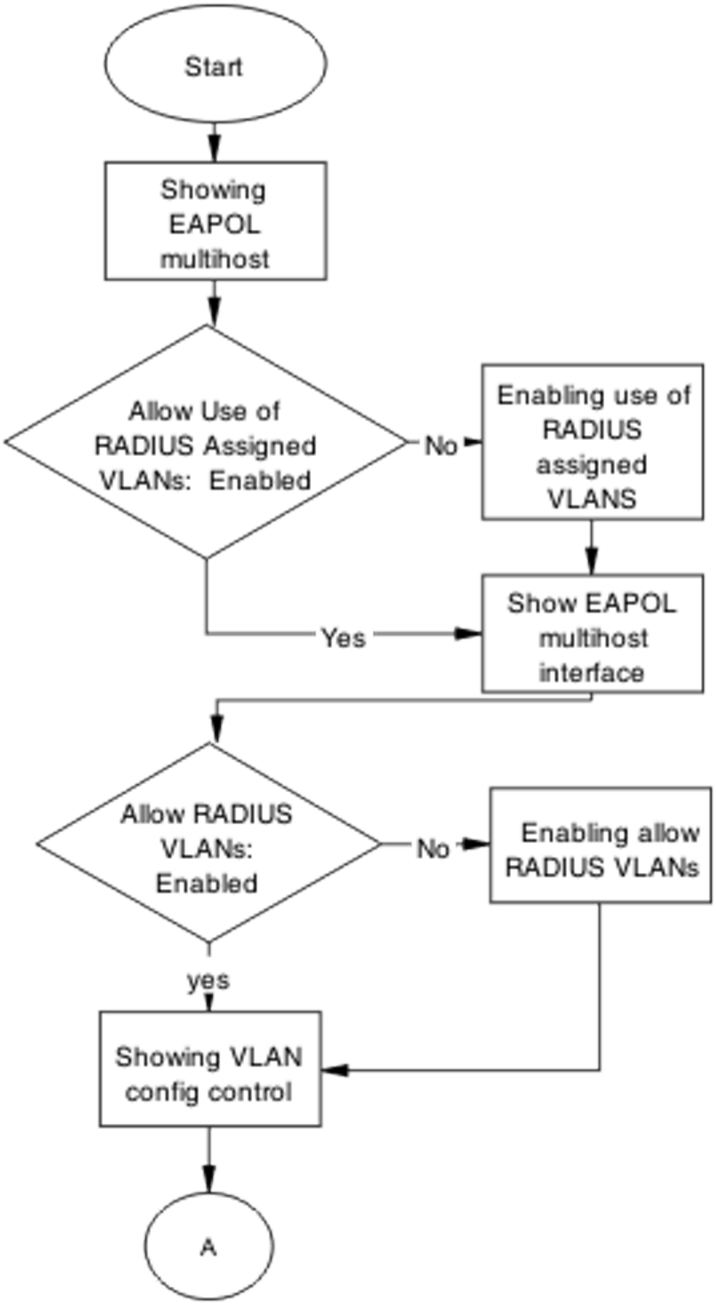

Start
Showing EAPOL multihost
Allow Use of RADIUS Assigned VLANs: Enabled
No
Enabling use of RADIUS assigned VLANS
Yes
Show EAPOL multihost interface
Allow RADIUS VLANs: Enabled
No
Enabling allow RADIUS VLANs
yes
Showing VLAN config control
A

Figure 38: Configure switch task part 1

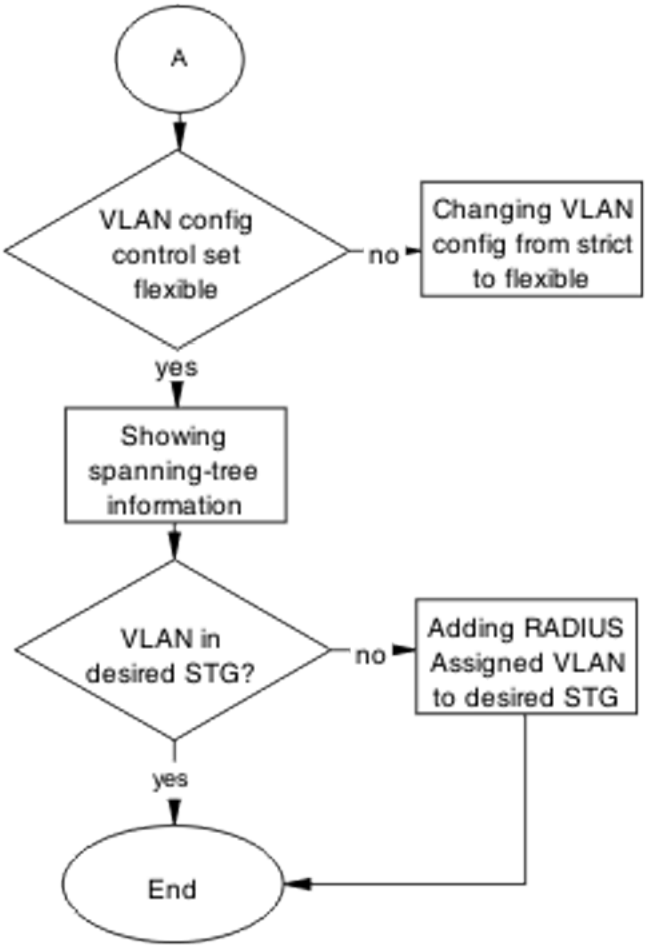

A
VLAN config control set flexible
no
Changing VLAN config from strict to flexible
yes
Showing spanning-tree information
VLAN in desired STG?
no
Adding RADIUS Assigned VLAN to desired STG
yes
End

Figure 39: Configure switch task part 2

Configure switch navigation:

- Showing EAPOL Multihost on page 89
- Enabling allow RADIUS VLANs on page 90
- Showing EAPOL multihost interface on page 90
- Enabling allow RADIUS VLANs on page 90
- Showing VLAN config control on page 90
- Changing VLAN config from strict to flexible on page 90
- Showing Spanning Tree on page 91
- Adding RADIUS assigned VLAN to desired STG on page 91

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 allow RADIUS VLANs

Change the allow RADIUS assigned VLAN to enable.

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

Showing EAPOL multihost interface

Display the EAPOL Interface.

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

Showing VLAN config control

Display the VLAN config control information.

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

Changing VLAN config from strict to flexible

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

1. Use the **`vlan config control flexible`** command to set the VLAN config control to flexible.
2. Observe no errors after execution.

Showing Spanning Tree

Display the VLANs added to the desired STG.

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

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

Adding RADIUS assigned VLAN to desired STG

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

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

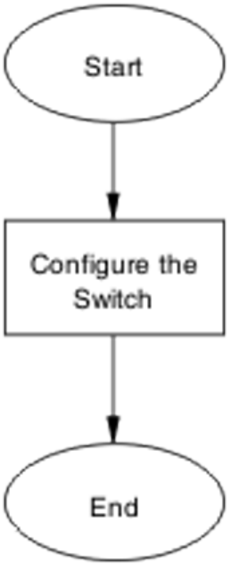


Figure 40: Configured MAC is not authenticating

Configured MAC is not authenticating navigation:

- Configure the switch on page 92

Configure the switch

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

Task flow: Configure the switch

The following task flow assists you to ensure the MAC is authenticating on the ERS 5500 series device.

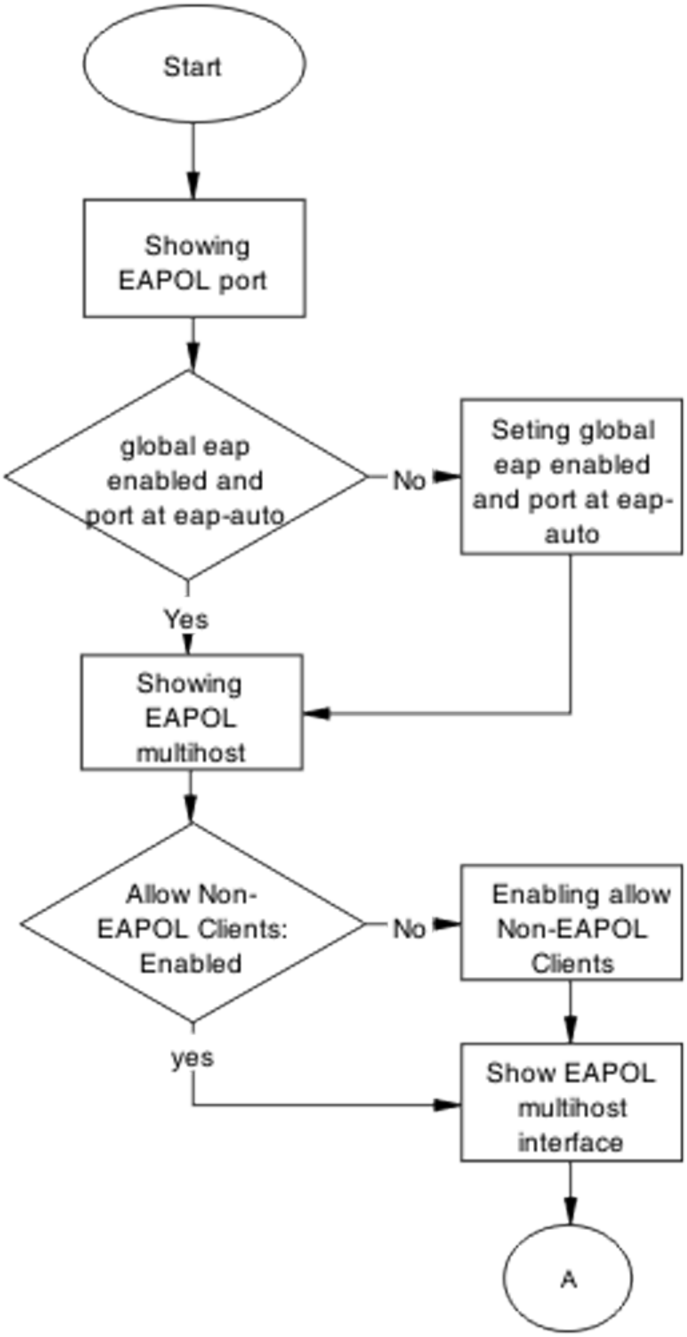

Start
Showing EAPOL port
global eap enabled and port at eap-auto
No
Seting global eap enabled and port at eap-auto
Yes
Showing EAPOL multihost
Allow Non-EAPOL Clients: Enabled
No
Enabling allow Non-EAPOL Clients
yes
Show EAPOL multihost interface
A

Figure 41: Configure the switch part 1

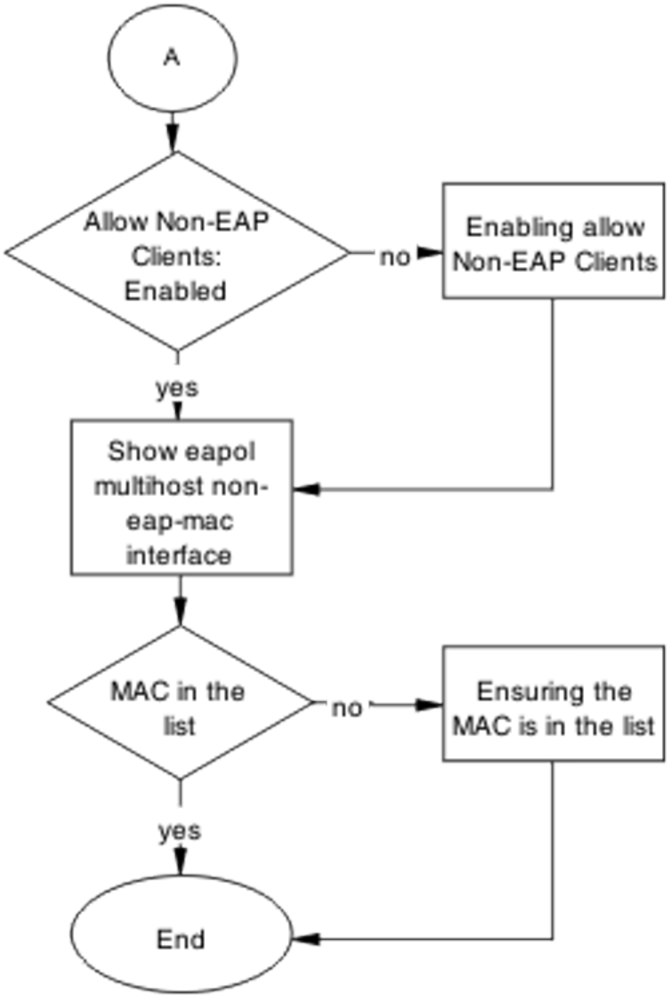

A
Allow Non-EAP Clients: Enabled
no
Enabling allow Non-EAP Clients
yes
Show eapol multihost non-eap-mac interface
MAC in the list
no
Ensuring the MAC is in the list
yes
End

Figure 42: Configure the switch part 2

Configure the switch navigation:

- Showing EAPOL port on page 95
- Setting global EAP enabled and port at eap-auto on page 95
- Showing EAPOL multihost on page 95
- Enabling Allow Non-EAPOL Clients on page 95
- Showing EAPOL multihost interface on page 96
- Enabling multihost status and allow non-EAPOL clients on page 96
- Showing EAPOL multihost non-eap-mac interface on page 96
- Ensuring MAC in the list on page 96

Showing EAPOL port

Display the EAPOL port information

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

Setting global EAP enabled and port at eap-auto

Make the corrections to ensure the settings as required.

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. 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 enable.
2. Observe 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. Allow Non-EAPOL clients is enabled.
3. 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 enable.
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 the MAC is in the list.

Ensuring MAC in the list

Add the MAC to the list if the case 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.

NEAP RADIUS MAC not authenticating

Correct a NEAP RADIUS MAC that is not authenticating.

Work flow: NEAP RADIUS MAC not authenticating

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

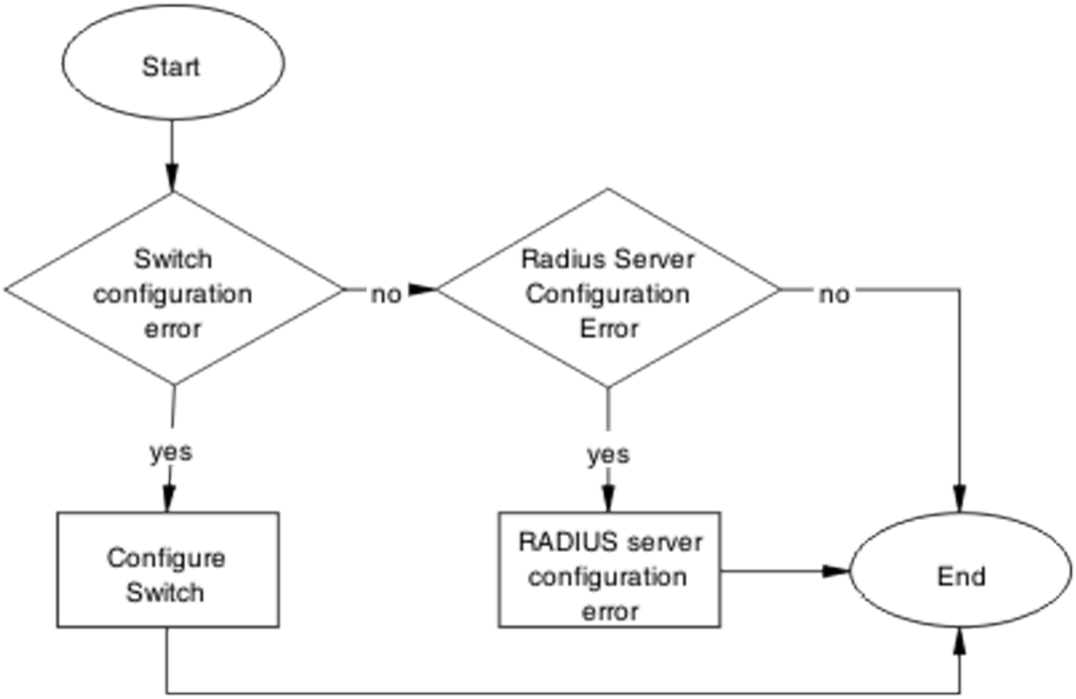

Start
Switch configuration error
no
Radius Server Configuration Error
no
yes
yes
Configure Switch
RADIUS server configuration error
End

Figure 43: NEAP RADIUS MAC not authenticating

NEAP RADIUS MAC not authenticating navigation:

- Configure Switch on page 98
- RADIUS server configuration error on page 102

Configure Switch

Correct switch configuration to correct issue with RADIUS MAC.

Task flow: Configure switch

The following task flow assists you to configure the ERS 5500 series device to correct the RADIUS MAC issue.

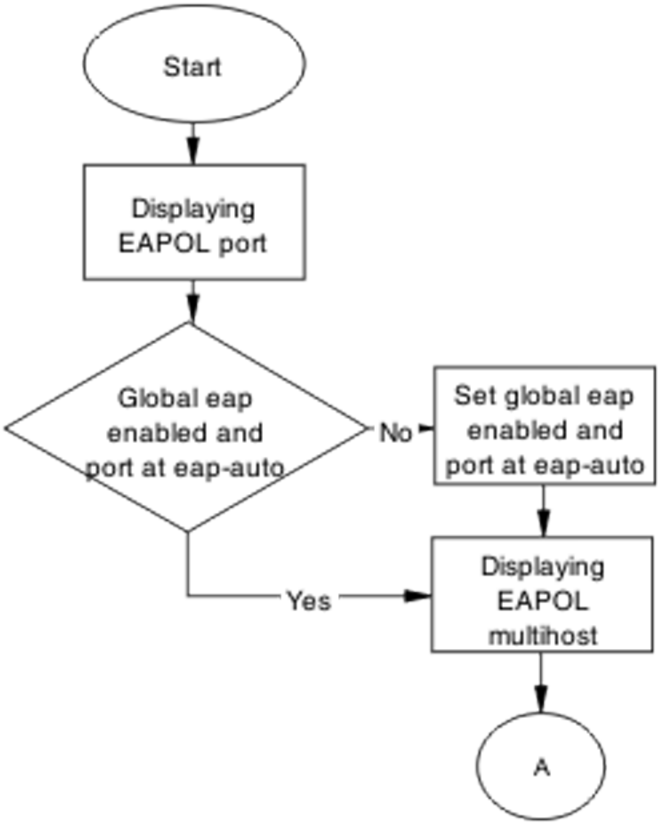

Start
Displaying EAPOL port
Global eap enabled and port at eap-auto
No
Set global eap enabled and port at eap-auto
Yes
Displaying EAPOL multihost
A

Figure 44: Configure switch part 1

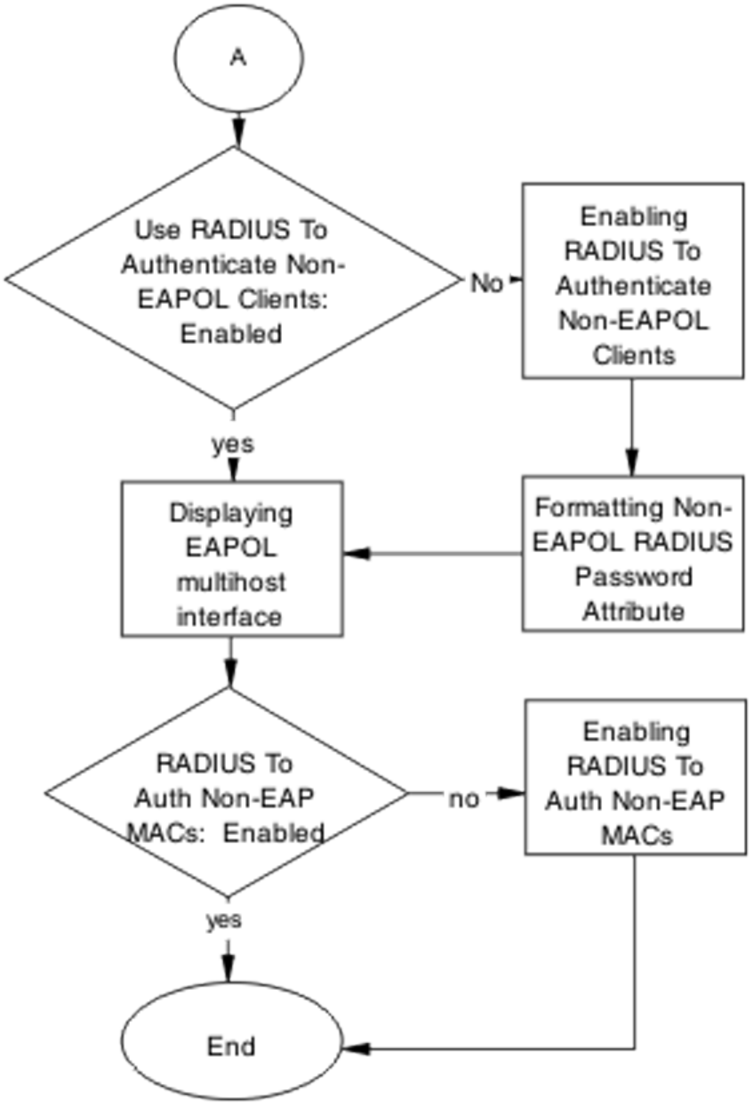

A
Use RADIUS To Authenticate Non-EAPOL Clients: Enabled
No
Enabling RADIUS To Authenticate Non-EAPOL Clients
yes
Displaying EAPOL multihost interface
Formatting Non-EAPOL RADIUS Password Attribute
RADIUS To Auth Non-EAP MACs: Enabled
no
Enabling RADIUS To Auth Non-EAP MACs
yes
End

Figure 45: Configure switch part 2

Configure switch navigation:

- Displaying EAPOL port on page 101
- Setting global eap enabled and port at eap-auto on page 101
- Displaying EAPOL multihost on page 101
- Enabling RADIUS to authenticate non-EAPOL clients on page 101
- Formatting non-EAPOL RADIUS password attribute on page 102
- Displaying EAPOL multihost interface on page 102
- Enabling RADIUS To Auth Non-EAP MACs on page 102

Displaying EAPOL port

Display the EAPOL port information for review.

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

Setting global eap enabled and port at eap-auto

Make the required changes to ensure the settings are correct.

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

Display the EAPOL Multihost information for review.

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

Enabling RADIUS to authenticate non-EAPOL clients

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

Apply changes to RADIUS server using vendor documentation.

Formatting non-EAPOL RADIUS password attribute

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

RADIUS server is to use the format changed to IpAddr.MACAddr.PortNumber.

Displaying EAPOL multihost interface

Display the EAPOL Multihost information for review.

1. Enter the **`show eapol multihost interface <port#>`** command to display the information
2. Verify the following:

   Use RADIUS To Authenticate Non EAP MACs is enabled

Enabling RADIUS To Auth Non-EAP MACs

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

Apply changes to RADIUS server using vendor documentation.

RADIUS server configuration error

The RADIUS server requires that the correct MAC address and password for the ERS 5500 series device be configured.

Task flow: RADIUS server configuration error

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

Start
Configuring MAC and password on RADIUS server
End

Figure 46: RADIUS server configuration error

RADIUS server configuration error navigation:

Configuring MAC and password on RADIUS server on page 103

Configuring MAC and password on RADIUS server

The RADIUS server requires that the MAC and password for the ERS 5500 series device be correct. If it is not correct the ERS 5500 series device will not authenticate.

Reference the vendor documentation for the RADIUS server

NEAP MHSA MAC is not authenticating

Ensure that the switch is configured correctly.

Work flow: NEAP MHSA MAC is not authenticating

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

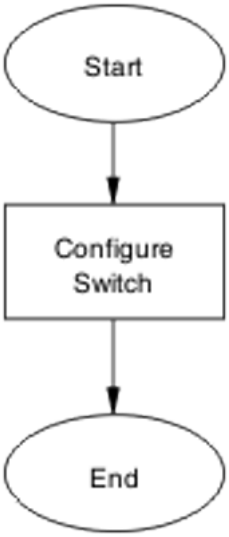


Figure 47: NEAP MHSA MAC is not authenticating

NEAP MHSA MAC is not authenticating navigation:

- Configure switch on page 104

Configure switch

Configure the switch to enable MHSA.

Task flow: Configure switch

The following task flow assists you to enable MHSA on the ERS 5500 series device.

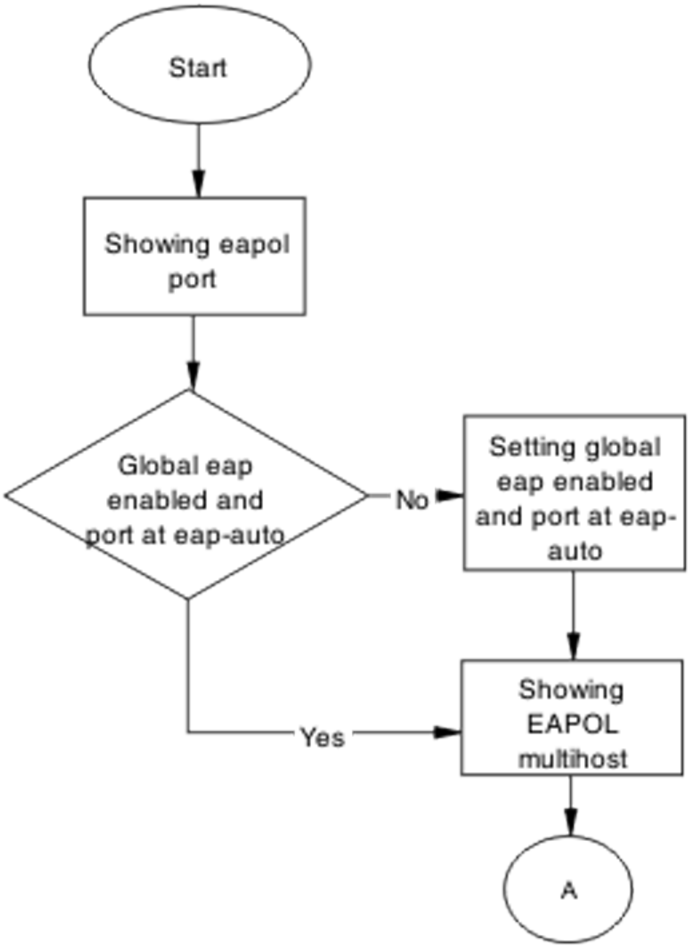

Start
Showing eapol port
Global eap enabled and port at eap-auto
No
Setting global eap enabled and port at eap-auto
Yes
Showing EAPOL multihost
A

Figure 48: Configure switch part 1

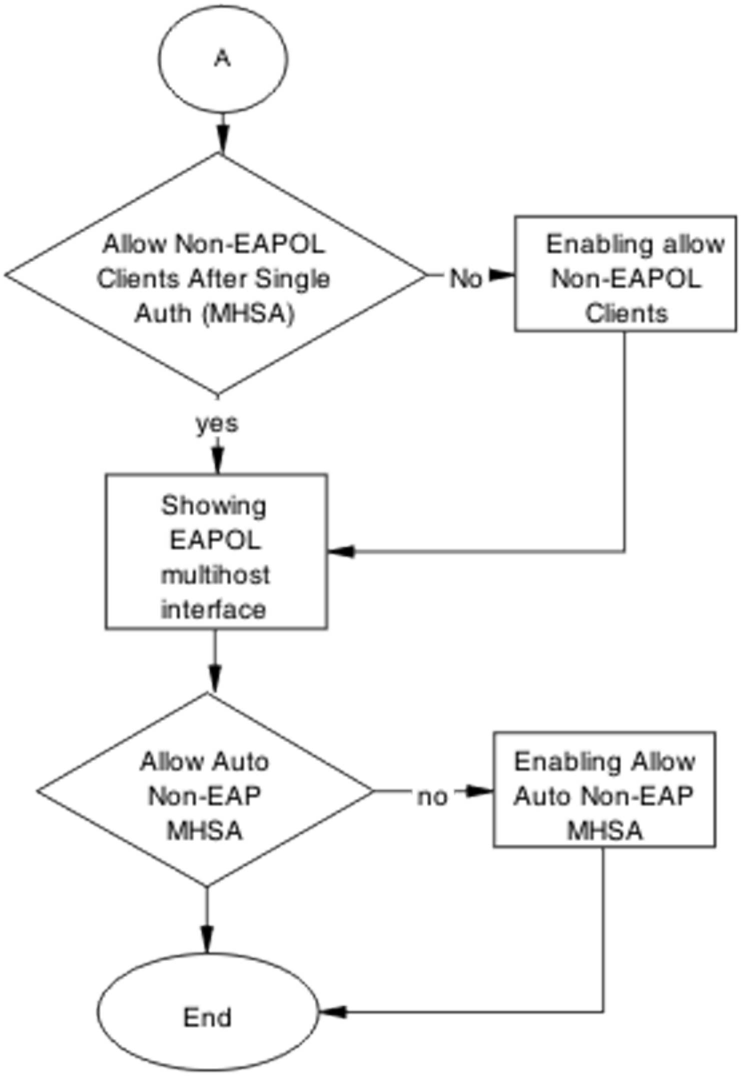

A
Allow Non-EAPOL Clients After Single Auth (MHSA)
No
Enabling allow Non-EAPOL Clients
yes
Showing EAPOL multihost interface
Allow Auto Non-EAP MHSA
no
Enabling Allow Auto Non-EAP MHSA
End

Figure 49: Configure switch part 2

Configure switch navigation:

- Showing EAPOL port on page 107
- Setting global EAP enabled and port at eap-auto on page 107
- Showing EAPOL multihost on page 107
- Formatting non-EAPOL RADIUS password attribute on page 107
- Showing EAPOL multihost interface on page 108
- Enabling RADIUS to auth Non-EAP MACs on page 108

Showing EAPOL port

Display the EAPOL port information for review.

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

Setting global EAP enabled and port at eap-auto

Make the required changes to ensure the settings are correct.

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 for review.

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

   Use RADIUS To Authenticate NonEAPOL Clients is enabled

Formatting non-EAPOL RADIUS password attribute

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

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

Enabling RADIUS to Authenticate NON-EAPOL Clients

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

Apply changes to RADIUS server using vendor documentation.

Showing EAPOL multihost interface

Display the EAPOL Multihost information for review.

1. Enter the **`show eapol multihost interface <port#>`** command to display the information.
2. Note the following:

   Allow Auto Non-EAP MHSA: Enabled

Enabling RADIUS to auth Non-EAP MACs

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

Apply changes to RADIUS server using vendor documentation.

NEAP phone is not working

Rectify a NEAP phone that is not working.

Task flow: NEAP phone is not working

The following task flow assists you to establish a connection between a NEAP phone and the ERS 5500 series device.

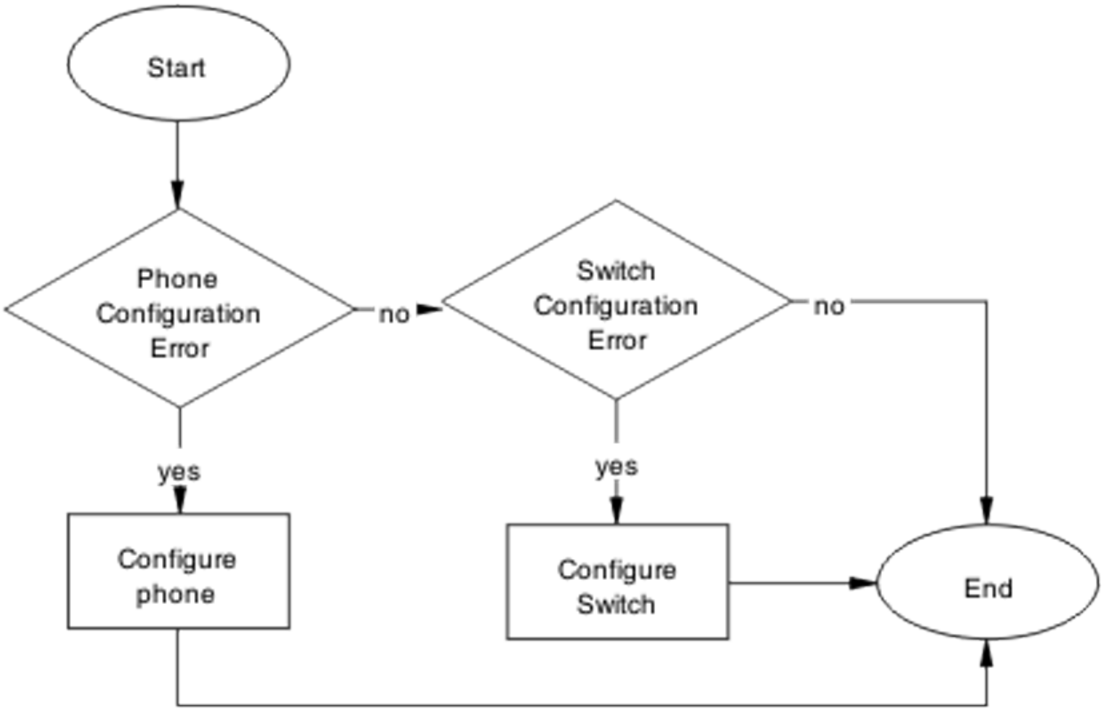


Figure 50: NEAP phone is not working

NEAP phone is not working navigation:

- Configure phone on page 109
- Configure the switch on page 110

Configure phone

Change phone configuration to ensure it is configured correctly.

Task flow: Configure phone

The following task flow assists you to configure the phone to work with the ERS 5500 series device.

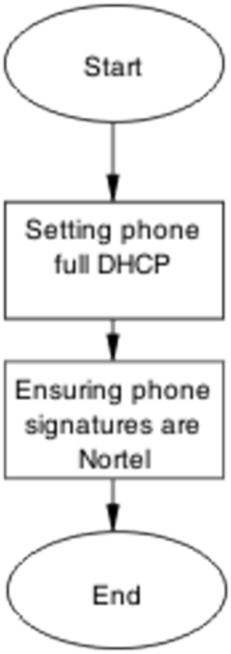


Figure 51: Configure phone

Configure phone:

- Setting Phone full DHCP on page 110
- Ensuring phone signatures are Avaya on page 110

Setting Phone full DHCP

Configure the phone as full DHCP to obtain network information.

Use vendor documentation for the phone to configure phone for full DHCP.

Ensuring phone signatures are Avaya

Configure the phone with Avaya signatures.

Use vendor documentation for the phone to ensure phone signatures are Avaya.

Configure the switch

The switch has to be configured to support the phone correctly.

Task flow: Configure the switch

The following task flow assists you to configure the ERS 5500 series device to support the phone.

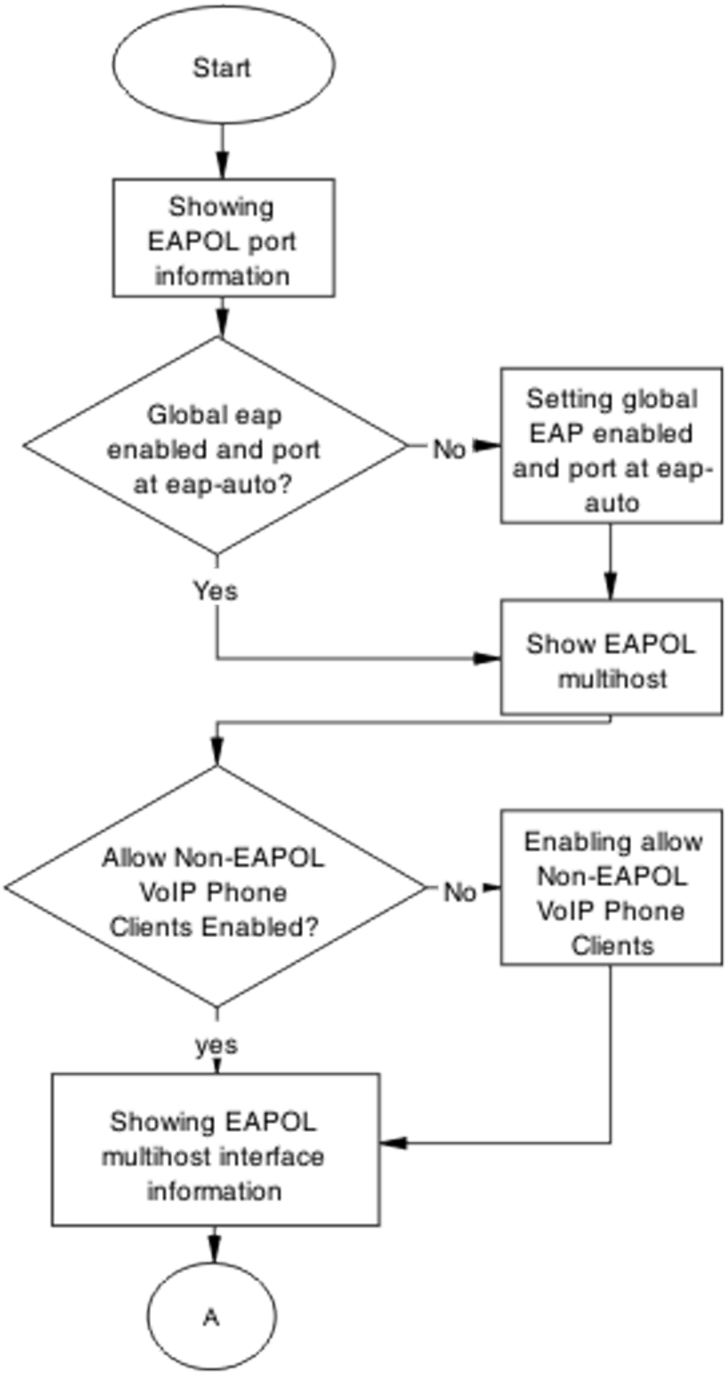

Start
Showing EAPOL port information
Global eap enabled and port at eap-auto?
No
Setting global EAP enabled and port at eap-auto
Yes
Show EAPOL multihost
Allow Non-EAPOL VoIP Phone Clients Enabled?
No
Enabling allow Non-EAPOL VoIP Phone Clients
yes
Showing EAPOL multihost interface information
A

Figure 52: Configure the switch part 1

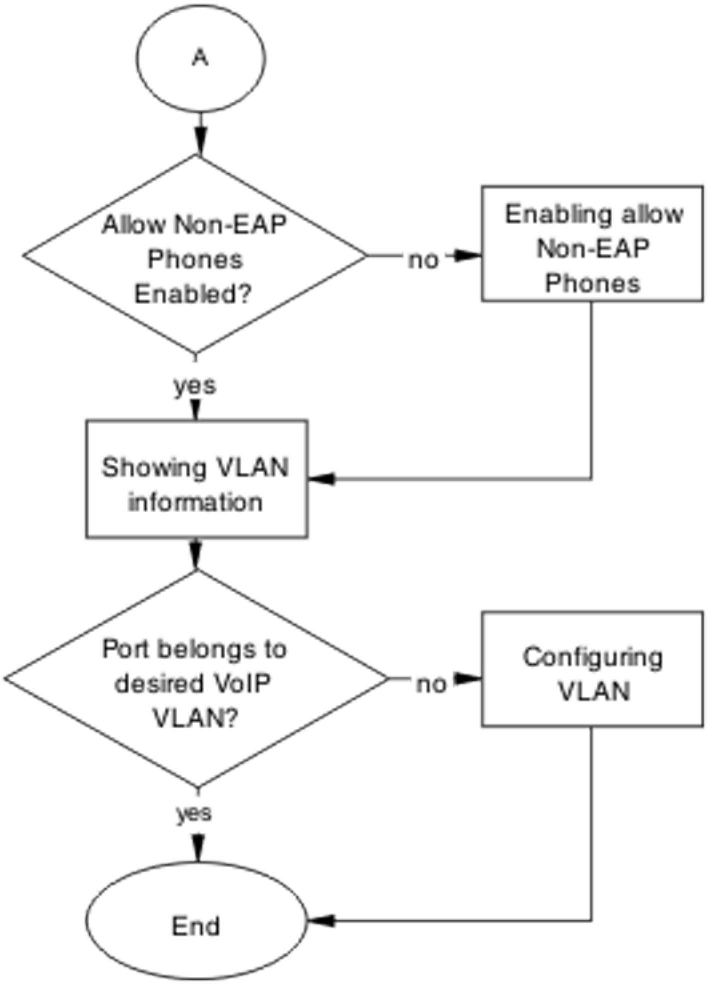

A
Allow Non-EAP Phones Enabled?
no
Enabling allow Non-EAP Phones
yes
Showing VLAN information
Port belongs to desired VoIP VLAN?
no
Configuring VLAN
yes
End

Figure 53: Configure the switch part 2

Configure the switch navigation:

- Showing EAPOL port on page 114
- Setting global eap enabled and port at eap-auto on page 114
- Showing EAPOL multihost on page 114
- Enabling allow non-EAPOL VoIP phone clients on page 114
- Showing EAPOL multihost interface on page 115
- Enabling allow Non-EAP phones on page 115
- Showing VLAN information on page 115
- Configuring VLAN on page 115

Showing EAPOL port

Display the EAPOL port information for review.

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

Setting global eap enabled and port at eap-auto

Make the required changes to ensure the settings are correct.

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 for review.

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

   Allow Non-EAPOL VoIP Phone Clients: Enabled

Enabling allow non-EAPOL VoIP phone clients

Display the EAPOL Multihost information for review.

1. Use the **`eapol multihost non-eap-phone-enable`** command to allow NEAP Phone.
2. Observe no errors after execution.

Showing EAPOL multihost interface

Display the EAPOL Multihost information for review.

1. Enter the **`show eapol multihost interface <port#>`** command to display the information.
2. Note the following:

   Allow Non-EAP Phones: Enabled

Enabling allow Non-EAP phones

Change the multihost setting to allow non-EAP phones.

1. Use the **`eapol multihost non-eap-phone-enable`** command to allow NEAP Phones .
2. Observe no errors after execution.

Showing VLAN information

Display the VLAN information for review.

1. Enter the **`show vlan`** command to display the information.
2. Verify the following:

   Ensure port belongs to desired Voip VLAN.

Configuring VLAN

Change the VLAN setting to use the correct port.

1. Use the **`vlan members add <1-4094> <port>`** command to move the port to desired VLAN.
2. Observe no errors after execution.

NEAP user policies from RADIUS not applied

Correct possible faults that ause NEAP user policies from the RADIUS server to not be applied.

Work flow: NEAP user policies from RADIUS not applied

The following work flow assists you to determine the solution for user policies from the RADIUS server not being applied.

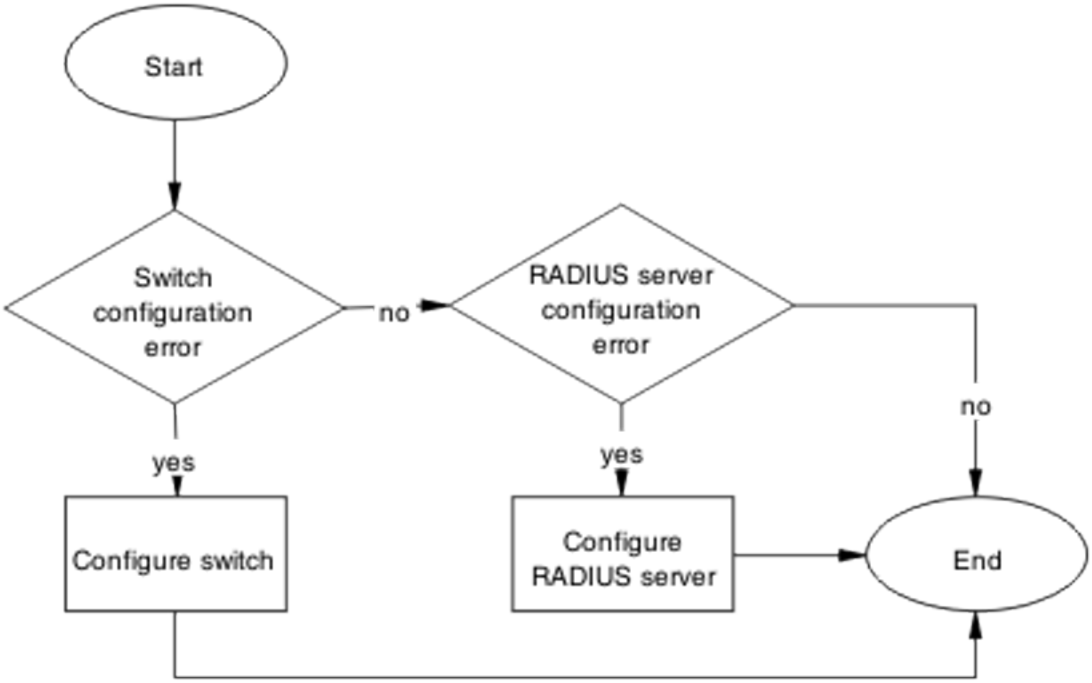


Figure 54: NEAP user policies from RADIUS not applied

NEAP user policies from RADIUS not applied navigation:

- Configure Switch on page 117
- RADIUS Server Configuration on page 130

Configure Switch

Switch configuration is configured to ensure policies are correct.

Task flow: Configure switch

The following task flow assists you to configure the ERS 5500 series device with the correct policies.

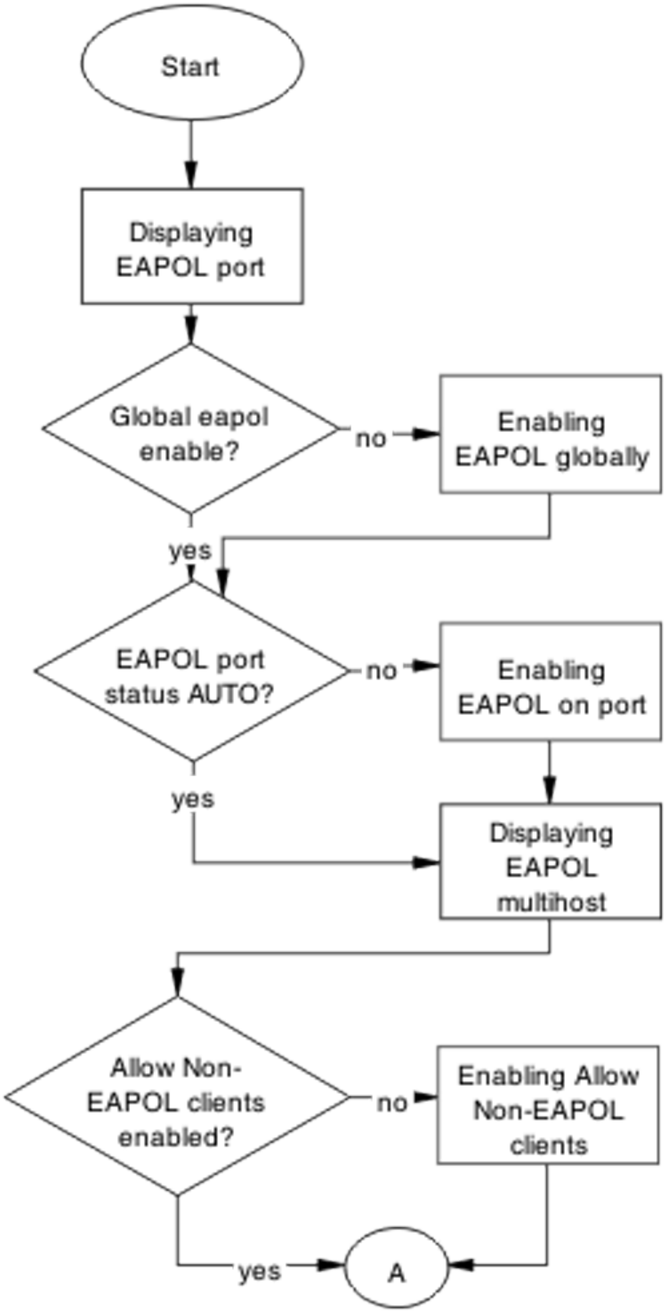


Figure 55: Configure switch part 1

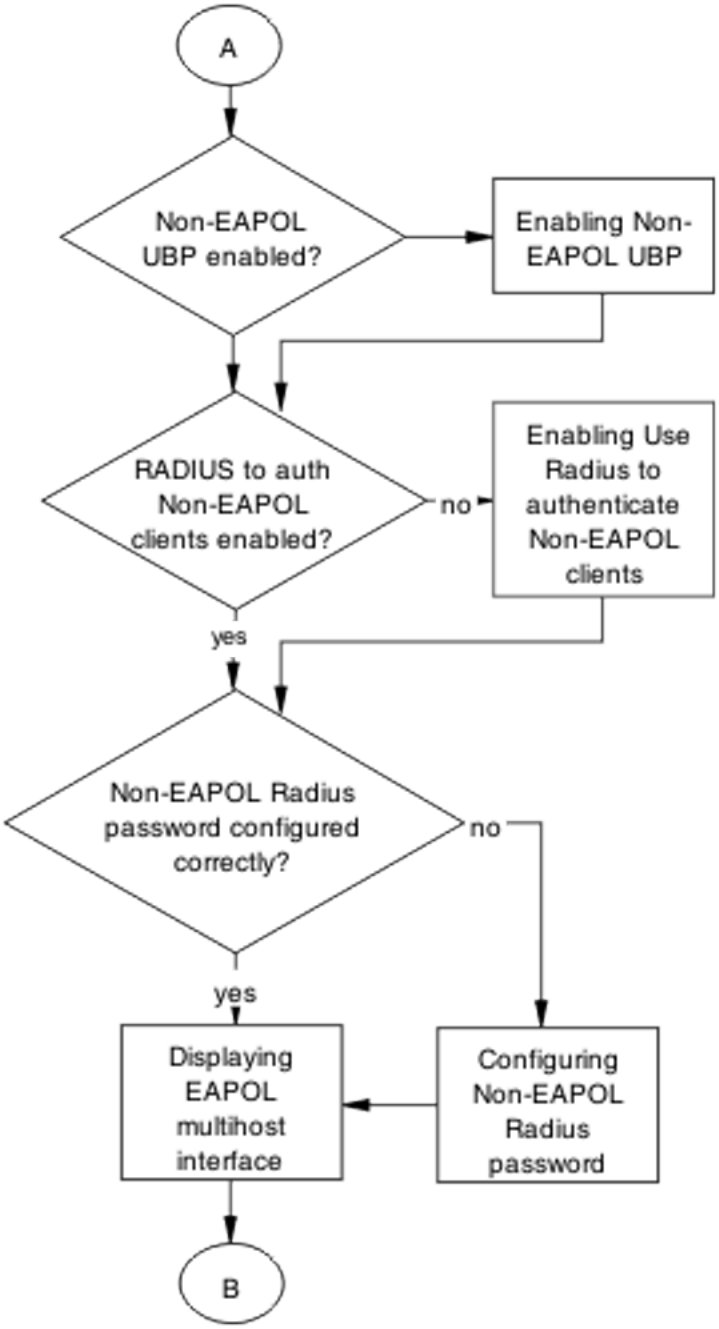

A
Non-EAPOL UBP enabled?
Enabling Non-EAPOL UBP
RADIUS to auth Non-EAPOL clients enabled?
no
Enabling Use Radius to authenticate Non-EAPOL clients
yes
Non-EAPOL Radius password configured correctly?
no
yes
Displaying EAPOL multihost interface
Configuring Non-EAPOL Radius password
B

Figure 56: Configure switch part 2

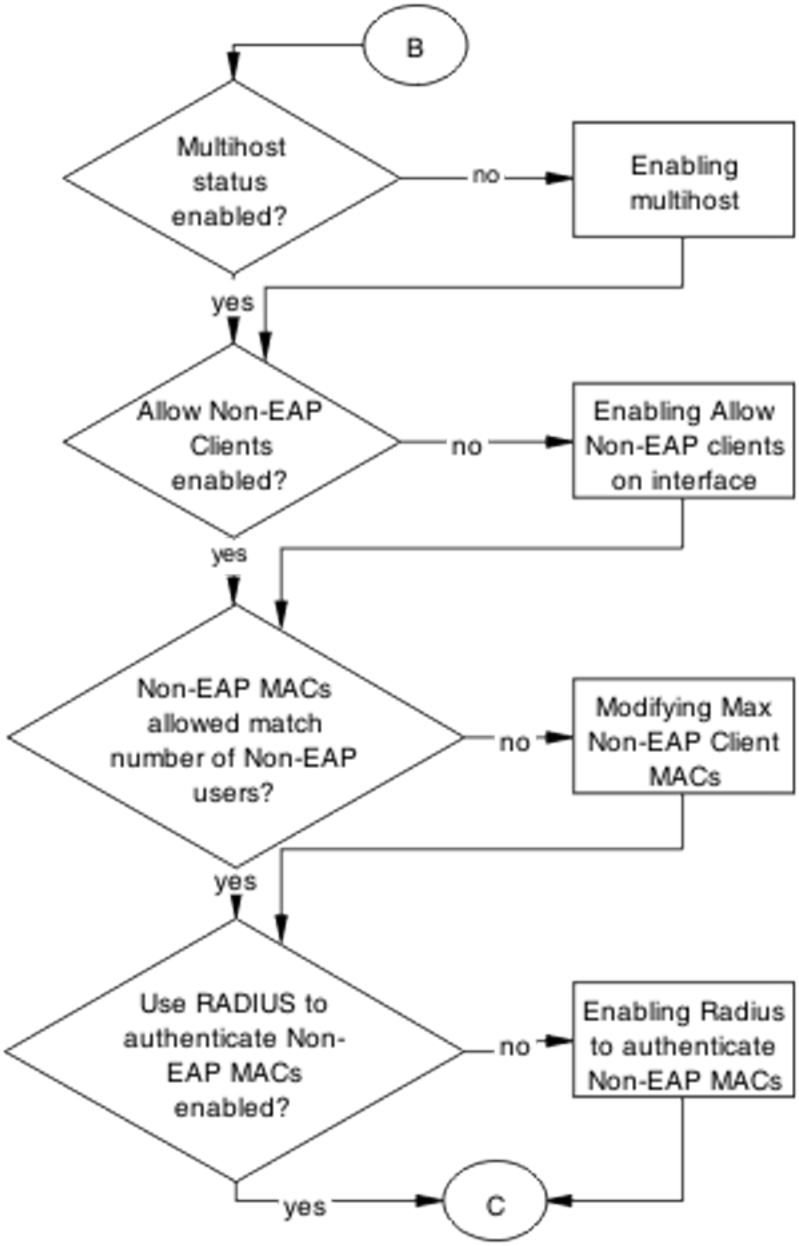

B
Multihost status enabled?
no
Enabling multihost
yes
Allow Non-EAP Clients enabled?
no
Enabling Allow Non-EAP clients on interface
yes
Non-EAP MACs allowed match number of Non-EAP users?
no
Modifying Max Non-EAP Client MACs
yes
Use RADIUS to authenticate Non-EAP MACs enabled?
no
Enabling Radius to authenticate Non-EAP MACs
yes
C

Figure 57: Configure switch part 3

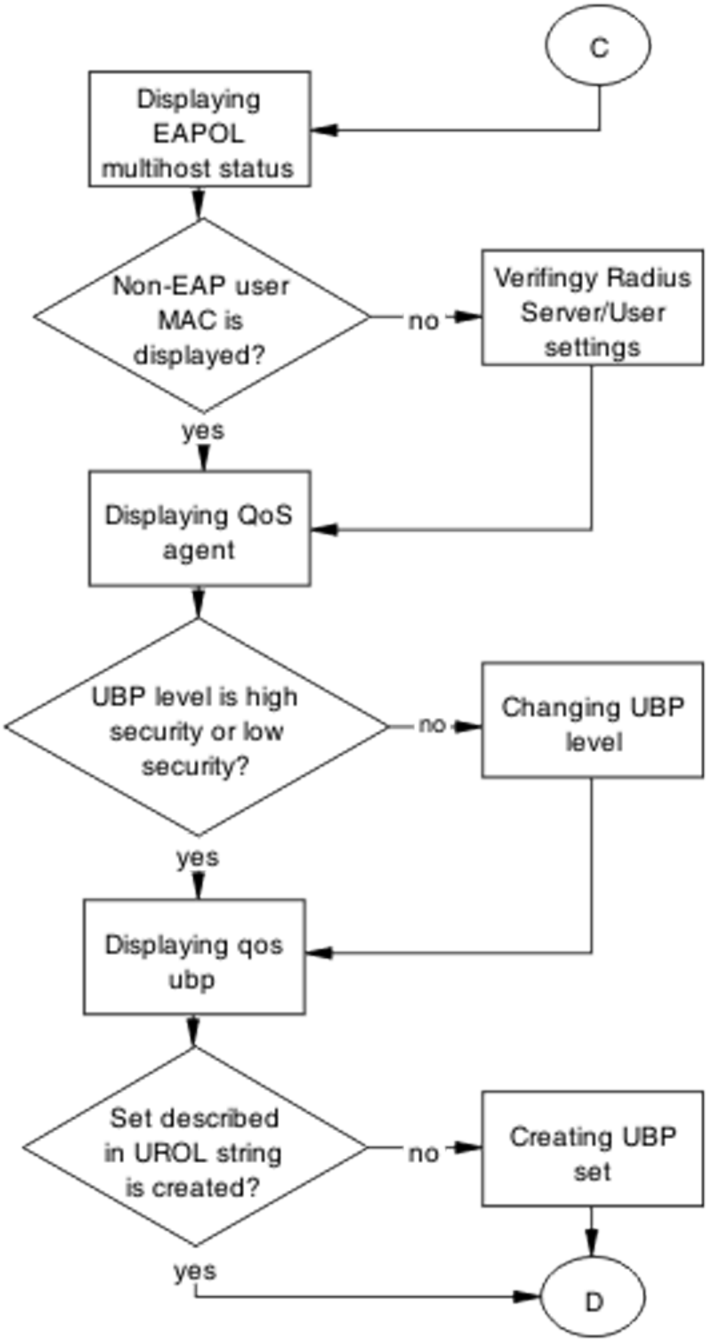

C
Displaying EAPOL multihost status
Non-EAP user MAC is displayed?
no
Verifingy Radius Server/User settings
yes
Displaying QoS agent
UBP level is high security or low security?
no
Changing UBP level
yes
Displaying qos ubp
Set described in UROL string is created?
no
Creating UBP set
yes
D

Figure 58: Configure switch part 4

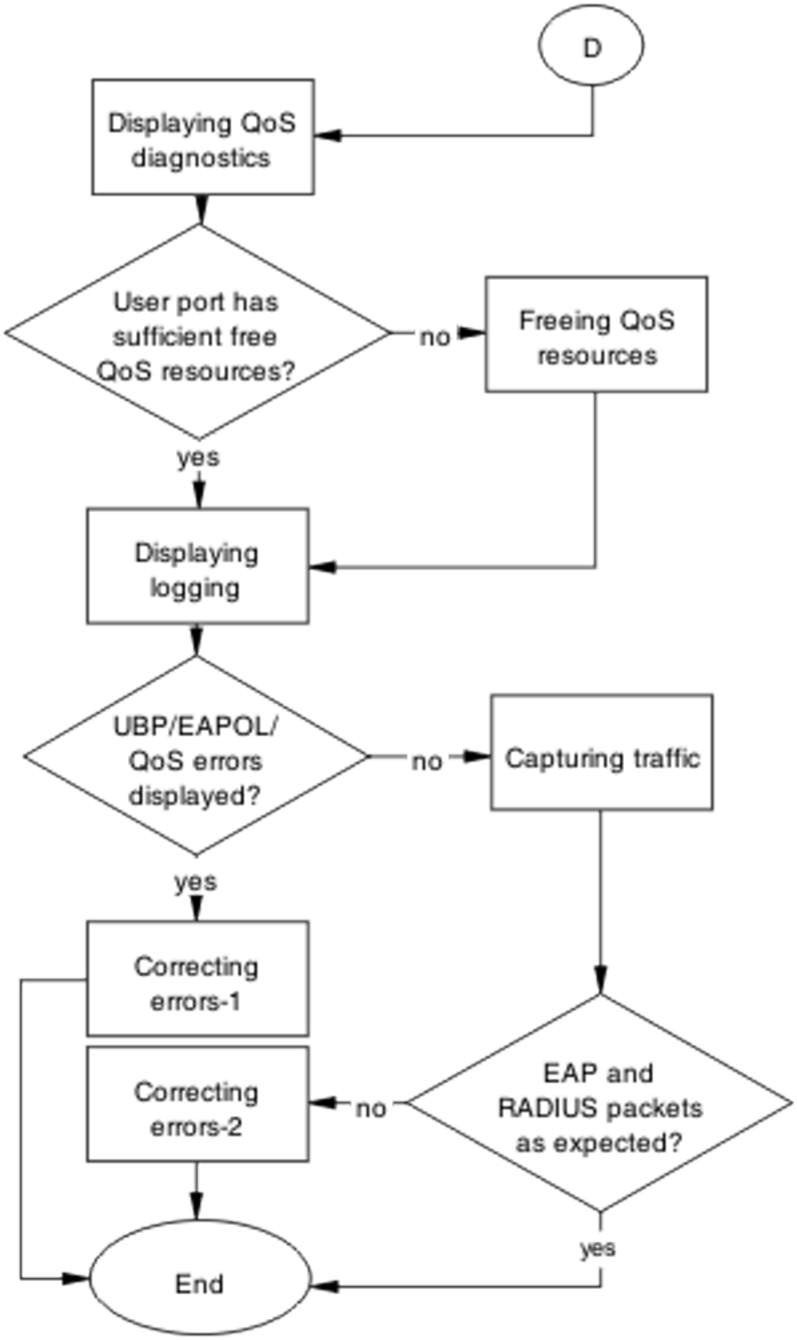

D
Displaying QoS diagnostics
User port has sufficient free QoS resources?
no
Freeing QoS resources
yes
Displaying logging
UBP/EAPOL/ QoS errors displayed?
no
Capturing traffic
yes
Correcting errors-1
Correcting errors-2
no
EAP and RADIUS packets as expected?
yes
End

Figure 59: Configure switch part 5

Configure switch navigation:

- Displaying EAPOL port on page 123
- Enabling EAPOL globally on page 124
- Enabling EAPOL UBP globally on page 124

Displaying EAPOL port

Obtain details of the EAPOL port configuration.

1. Use the **`show eapol port <port>`** command to display the port information.
2. Verify the following information:
   - EAPOL global setting is enabled
   - EAPOL UBP global setting is enabled
   - EAPOL port status is AUTO

Enabling EAPOL globally

Enable EAPOL globally for the switch.

1. Use the **`eapol enable`** command to enable EAPOL globally.
2. Check that no error or warning message is displayed.

Enabling EAPOL UBP globally

Enable EAPOL UBP globally for the switch.

1. Use the **`eapol user-based-policies enable`** command to enable EAPOL globally.
2. Check that no error or warning message is displayed.

Enabling EAPOL on port

Enable EAPOL on the user port.

1. Use the **`eapol port <port>`** command to enable EAPOL on port.
2. Check that no error or warning message is displayed.

Displaying EAPOL multihost

Obtain the details for EAPOL multihost global settings.

1. Use the **`show eapol multihost`** command to display EAPOL multihost settings.
2. Verify the following:
    - Allow Non-EAP clients is enabled
    - Non-EAP UBP is enabled
    - Use Radius to authenticate Non-EAP clients is enabled

- Allow Non-EAP clients is Radius Non-EAP password is configured correctly

Enabling allow Non-EAPOL clients

Enable processing for non-eapol clients.

1. Use the **`eapol multihost allow-non-eap-enabled`** command to enable Allow Non-EAPOL on DUT.
2. Verify if errors are displayed. No error or warning messages should be displayed.

Enabling Non-EAP UBP

Enable Non-EAP UBP.

1. Use the **`eapol multihost non-eap-user-based-policies enable`** command to enable Non-EAPOL UBP on DUT.
2. Verify if errors are displayed. No error or warning messages should be displayed.

Enabling use RADIUS to authenticate Non-EAPOL clients

Enable authentication using Radius Server for Non-EAP clients.

1. Use the **`eapol multihost RADIUS-non-eap-enabled`**command to enable authentication using Radius Server for Non-EAPOL clients.
2. Verify if errors are displayed. No error or warning messages should be displayed.

Configuring Non-EAPOL RADIUS password

Configure password to be used in Radius authentication for Non-EAPOL clients.

1. Use the **`eapol multihost non-eap-pwd-fmt [ip-aadr|mac-addr|port-number]`** command to configure password used in Radius authentication.
2. Verify if errors are displayed. No error or warning messages should be displayed.

Displaying EAPOL multihost interface

Obtain the details for EAPOL multihost interface settings.

1. Use the **`show eapol multihost interface <port>`** command to display EAPOL multihost settings.
2. Verify the following:
    - multihost on interface is enabled
    - Allow Non-EAP clients on interface is enabled
    - Max number of Non-EAP MACs is configured correctly

Enabling multihost on interface

Enable processing for multihost on the specified interface.

1. Use the **`eapol multihost port <port> enable`** command to enable multihost processing on that interface.
2. Verify if errors are displayed. No error or warning messages should be displayed.

Enabling allow non-EAP clients

Enable processing for Non-EAPOL clients on the specified interface.

1. Use the **`eapol multihost port <port> allow-non-eap-enabled`** command to enable Allow Non-EAPOL on that interface.
2. Verify if errors are displayed. No error or warning messages should be displayed.

Modifying max non-EAP client MACs

Modify Max Non-EAP Client MACs to match the number of Non-EAPOL clients on that interface.

1. Use the **`eapol multihost port <port> non-eap-mac-max`**command to modify the number of allowed Non-EAPOL clients on that interface.
2. Verify if errors are displayed. No error or warning messages should be displayed.

Displaying EAPOL multihost status

Obtain the status for EAPOL multihost interface.

1. Use the **`show eapol multihost status <port>`** command to display authenticated MACs on that port.
2. Verify if user MAC is displayed.

Verifying RADIUS server/user settings

Verify if user/password configured on Radius Server match Non-EAPOL user MAC/ password (created by the DUT).

Refer to vendor documentation for the RADIUS server configuration.

Displaying QoS agent

Obtain details of QoS agent settings.

1. Use the **`show qos agent`** command to display QoS Agent settings.
2. Verify if QoS UBP is set to low or high security.

Changing UBP Level

Change UBP level to high or low security to enable QoS UBP globally.

1. Use the **`qos agent ubp high-security-local`** or **`qos agent ubp low-security-local`** command to enable QoS UBP on device.
2. Verify if errors are displayed. No error or warning messages should be displayed.

Displaying QoS UBP

Obtain details of QoS agent settings.

1. Use the **`show qos ubp`** command to display UBP sets.
2. Verify if UBP set name matches the UROL string configured on the RADIUS server (if UBP Set is named student then the UROL string sent by the RADIUS server is to be UROLstudent) .

Creating UBP Set

Create UBP set to configure the template policy that will be applied to the authenticated user port.

1. Use the **`qos ubp classifier`** and **`qos ubp set`**commands to create desired UBP set.
2. Verify if errors are displayed. No error or warning messages should be displayed.

Displaying QoS Diag

Obtain details of QoS resources usage.

1. Use the **`show qos diag`** command to display QoS resource utilization.
2. Verify for the port that will be used for user authentication if ((Non QoS masks + QoS mask < 16) and (Non QoS Filters + QoS Filters < 128)).

Freeing QoS resources

Delete some QoS policies that are configured on the user port or disable some of the non-qos application configured on that port.

1. Use the **`no qos policies`** command to delete some of the unnecessary policies on the used port or use another port with free QoS resources.
2. Verify the port that will be used for user authentication if ((Non QoS masks + QoS mask < 16) and (Non QoS Filters + QoS Filters < 128)).

Displaying logging

Obtain log messages for the device.

1. Use the **`show logging`** command to display device log messages.
2. Search log messages for EAPOL and QoS errors.

Correcting errors-1

Verify EAPOL and/or QoS configuration if errors are displayed in log messages.

1. If error EAPOL messages are logged verify port status and user/password on the RADIUS server and Non-EAP user MAC/created password.
2. If QoS error messages are logged verify UBP sets for conflicts inside the set or with the QoS policies already installed on that port.

Capturing traffic

Capture traffic between user PC, DUT, and between DUT and RADIUS server.

1. Using another PC and a hub or port mirroring feature capture traffic between user PC and DUT. Save data.
2. Using another PC and a hub or port mirroring feature capture traffic between user PC and Radius Server. Save data.

Correcting errors -2

Using the captured data verify if all the expected packets are exchanged between user PC and DUT and/or between DUT and RADIUS Server.

1. Search dataflow captured between User PC and DUT for correct EAP packets. Verify the following:
   - the correct MAC is sent by the user PC in the EAP packet.
   - the DUT sends EAP success packet at the end of EAP exchange.
2. If authentication fails check again user/password on the Radius Server and MAC/ created password.
3. Search dataflow captured between DUT and RADIUS server for correct RADIUS packets. Verify the following:
   - the correct VSA is sent by the RADIUS server.
   - the correct MAC is sent by the DUT in the request.
4. If the VSA is incorrect check the RADIUS server configuration.

RADIUS Server Configuration

Correct the RADIUS server configuration.

Task flow: RADIUS server configuration

The following task flow assists you to configure the RADIUS server attributes.

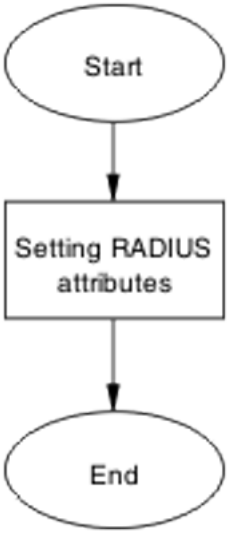


Figure 60: RADIUS server configuration

RADIUS server configuration navigation:

- Setting RADIUS attributes on page 131

Setting RADIUS attributes

Ensure that the RADIUS attributes are exactly as for EAP user based policies.

Please refer to the vendor documentation to ensure the attributes are set correctly.

EAP-NEAP unexpected port shutdown

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

Work flow: EAP-NEAP unexpected port shutdown

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

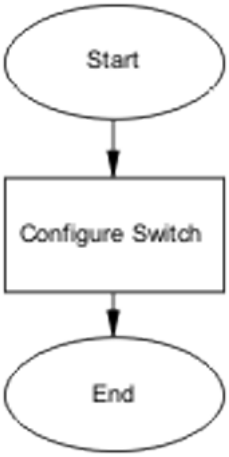


Figure 61: EAP-NEAP unexpected port shutdown

EAP-NEAP unexpected port shutdown navigation:

Configure Switch on page 132

Configure Switch

Configure ports to allow more unauthorized clients.

Task flow: Configure switch

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

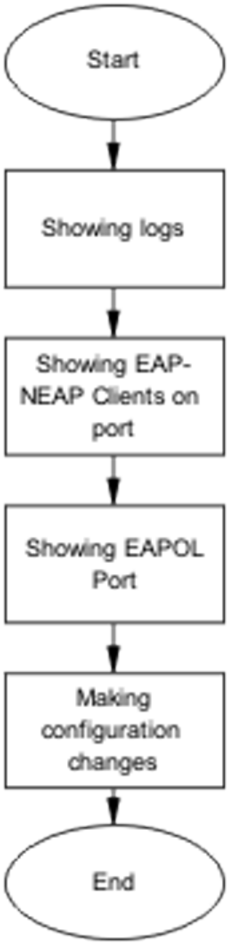

Start
Showing logs
Showing EAP-NEAP Clients on port
Showing EAPOL Port
Making configuration changes
End

Figure 62: Configure switch

Configure switch navigation:

- Showing Logs on page 133
- Showing EAP-NEAP clients on port on page 134
- Showing EAPOL port information on page 134
- Making changes on page 134

Showing Logs

Display log information for detailed 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-NEAP clients on port

Display EAP-NEAP client information about 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 detailed information 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.

Making changes

This section provides troubleshooting guidelines for changing the EAP settings. It cleans up old MACs.

1. Use the **`eap-force-unauthorised`** command to set the administrative state of the port to forced unauthorized.
2. Use the **`eapol status auto`** command to change to eap-auto to start.
3. Use the **`shut/no shut`** commands in the Interface Exec Mode.

Chapter 10: Troubleshooting Secure Network Access Solution

Secure Network Access Solution issues can interfere in the device operation and function. The following work flow contains some common authentication problems.

Troubleshooting Secure Network Access Solution work flow

The following work flow contains some typical Secure Network Access Solution (SNAS) problems. These situations are not normally dependant upon each other.

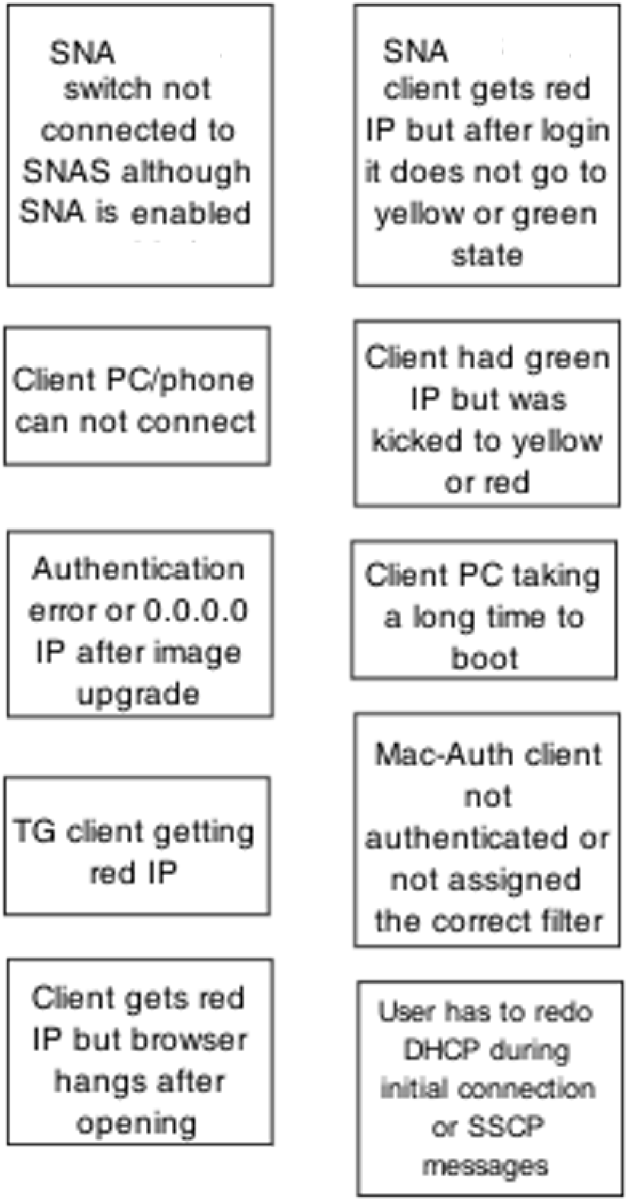

SNA switch not connected to SNAS although SNA is enabled
Client PC/phone can not connect
Authentication error or 0.0.0.0 IP after image upgrade
TG client getting red IP
Client gets red IP but browser hangs after opening
SNA client gets red IP but after login it does not go to yellow or green state
Client had green IP but was kicked to yellow or red
Client PC taking a long time to boot
Mac-Auth client not authenticated or not assigned the correct filter
User has to redo DHCP during initial connection or SSCP messages

Figure 63: Troubleshooting Secure Network Access Solution

Troubleshooting Secure Network Access Solution work flow navigation:

- NSNA switch not connected to Secure Network Access Solution although NSNA is enabled on page 137
- Client PC/phone can not connect on page 148
- Authentication error or 0.0.0.0 IP after image upgrade on page 159
- TG client getting red IP on page 163
- Client gets red IP but browser hangs after opening on page 165

- Secure Network Access client gets red IP but after login it does not go to yellow or green state on page 167
- Client had green IP but was kicked to yellow or red on page 169
- Client PC taking a long time to boot on page 172
- Mac-Auth client not authenticated or not assigned the correct filter on page 174
- Client has no DHCP information during initial connection or SSCP messages

NSNA switch not connected to Secure Network Access Solution although NSNA is enabled

Ensure the Secure Network Access Solution is displayed as connected to the ERS 5500 series device.

Work flow: Secure Network Access switch not connected to Secure Network AccessSolution although Secure Network Access is enabled

The following work flow assists you to determine the solution for an Secure Network Access (SNA) switch that does not connect to a Secure Network Access Solution.

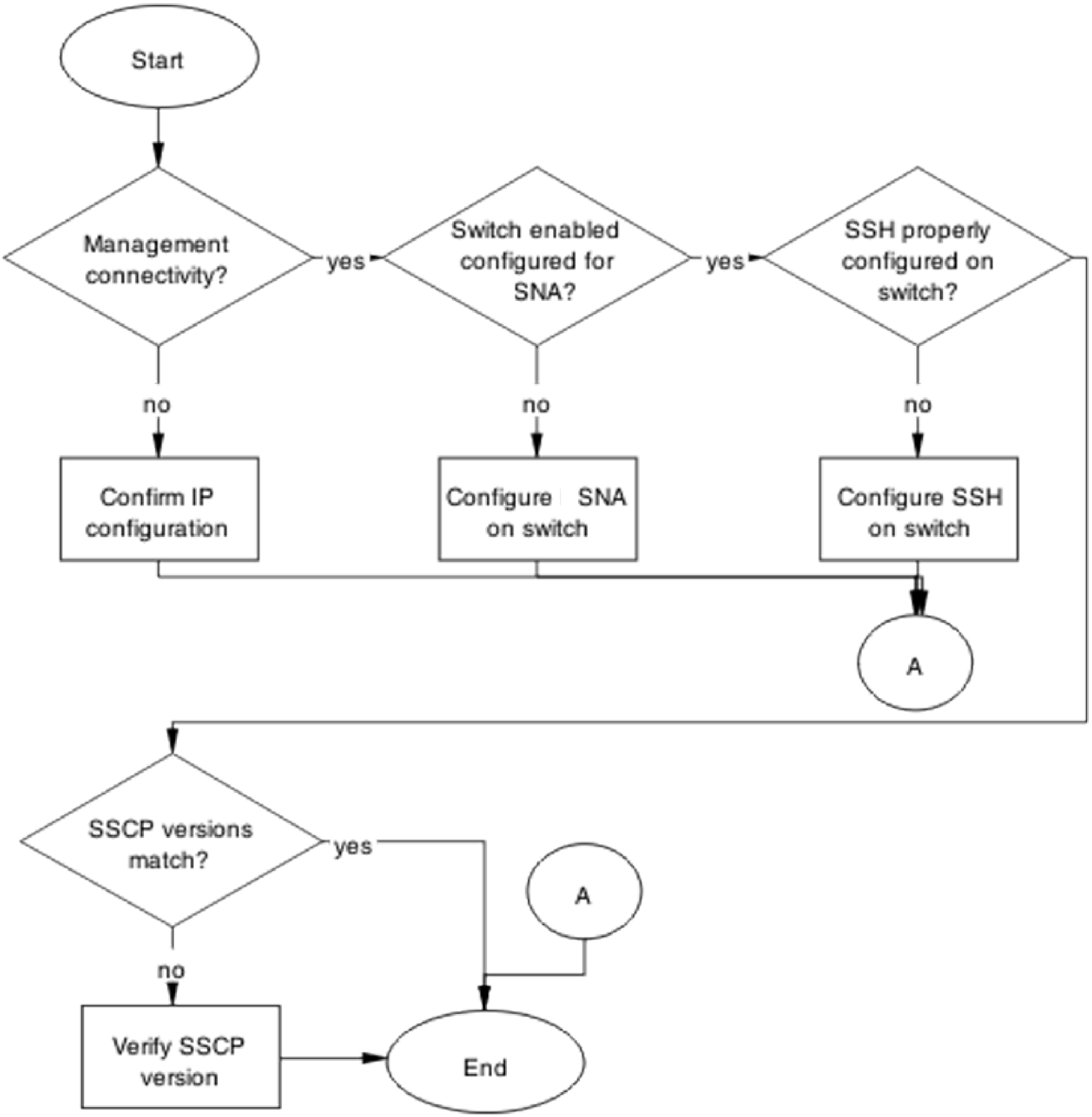


Figure 64: Secure Network Access switch not connected to Secure Network Access Solution although Secure Network Access is enabled

Secure Network Access switch not connected to Secure Network Access Solution although Secure Network Access is enabled navigation:

- Confirm IP Configuration on page 139
- Configure Secure Network Access Solution on switch on page 141

- Configure SSH on switch on page 143
- Verify SSCP version on page 146

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.

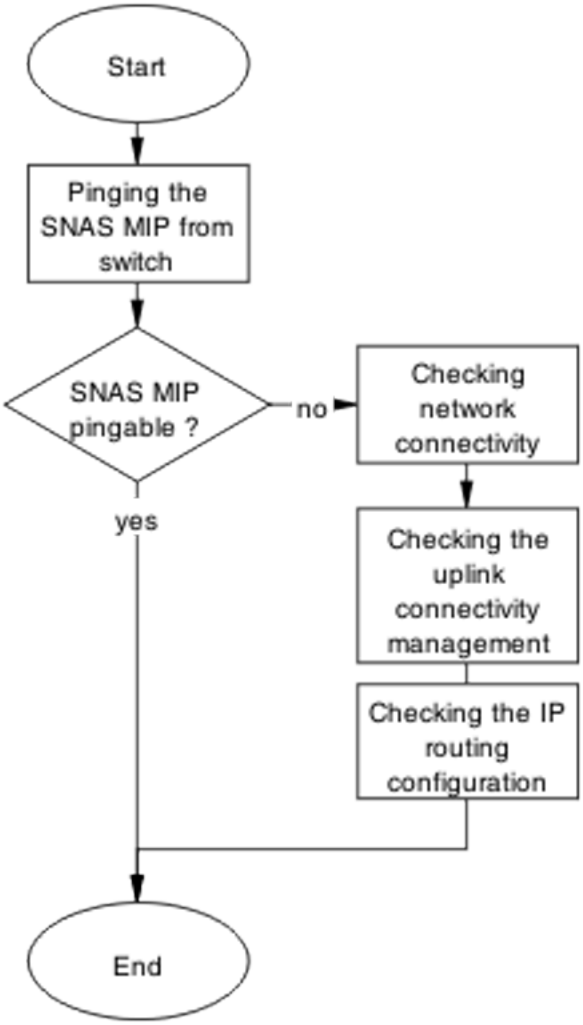

Start
Pinging the SNAS MIP from switch
SNAS MIP pingable ?
no
yes
Checking network connectivity
Checking the uplink connectivity management
Checking the IP routing configuration
End

Figure 65: Confirm IP configuration

Confirm IP configuration navigation:

- Pinging the Secure Network Access Solution MIP from switch on page 140
- Checking network connectivity from switch to router to Secure Network Access Solution on page 141
- Checking the uplink connectivity management on page 141
- Checking IP routing configuration on page 141

Pinging the Secure Network Access Solution MIP from switch

Confirm IP connectivity from the switch.

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

Checking network connectivity from switch to router to Secure Network Access Solution

Confirm network connection from the switch to Secure Network Access Solution.

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.

Checking IP routing configuration

Confirm the IP routing configuration is correct in L3 mode

1. Use the `show ip routing` command to show IP routing information.
2. Confirm L3 mode enabled.

Configure Secure Network Access Solution on switch

Configure and enable Secure Network Access Solution (SNAS) on the switch.

Task flow: Configure Secure Network Access Solution on switch

The following task flow assists you to ensure the ERS 5500 series device has Secure Network Access (SNA) enabled.

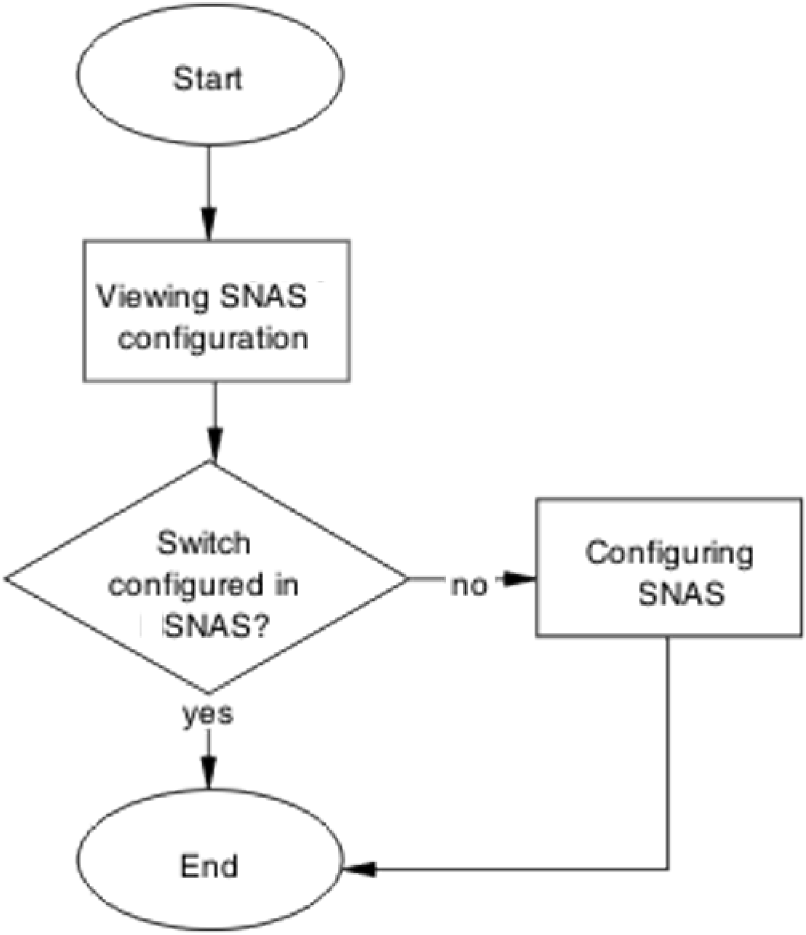


Figure 66: Configure Troubleshooting Secure Network Access on switch

Configure Secure Network Access on switch navigation:

- Checking Secure Network Access Solution configuration on page 142
- Configuring Secure Network Access on page 143

Checking Secure Network Access Solution 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 Secure Network Access Solution.

Configuring Secure Network Access

Configure the Secure Network Access (SNA) 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 **`SNA SNAs <IP>/<subnet> port <port>`** command to configure the SNAS IP address/subnet and the TCP communication port.
3. Set the created VLANs as SNA VoIP, RED, YELLOW and GREEN VLANs using the following commands:
   - **`SNA vlan 240 color voip`**
   - **`SNA vlan 210 color red filter RED`**
   - **`SNA vlan 220 color yellow filter YELLOW yellow-subnet 10.200.201.0/24`**
   - **`SNA vlan 230 color green filter GREEN`**
4. Set ports as SNA uplink and dynamic using the following commands:
   - **`interface fast Ethernet all`**
   - **`SNA port 47-48 uplink vlans 210,220,230,240`**
   - **`SNA 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 ERS 5500 series device.

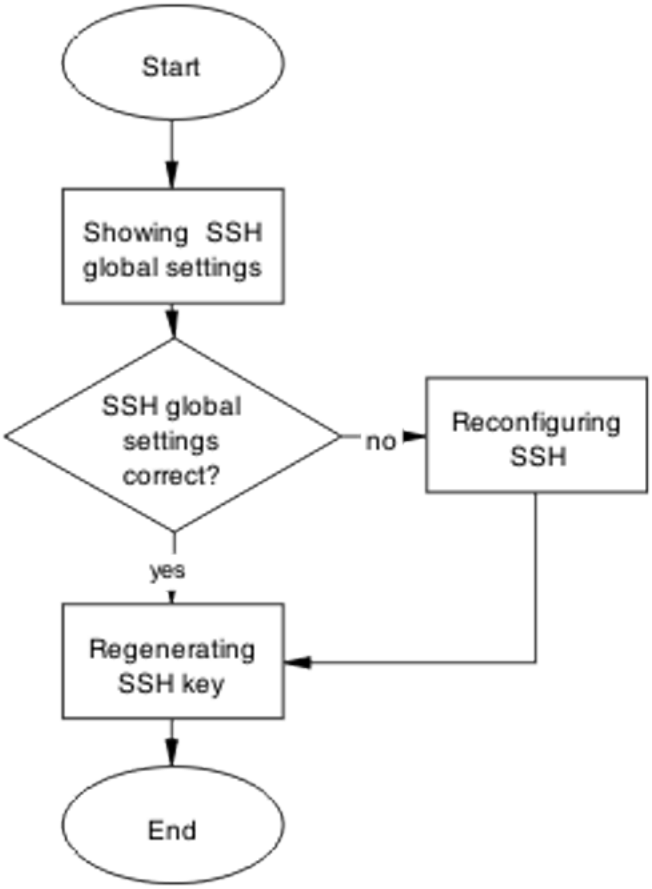


Figure 67: Configure SSH on switch

Configure SSH on switch navigation:

- Showing SSH globally on page 144
- Reconfiguring SSH on page 145
- Regenerating SSH key on page 145

Showing SSH globally

Display the SSH configuration of the switch.

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

Reconfiguring SSH

Change the SSH settings to be correct.

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

Regenerating SSH key

Regenerate the SSH Key in the case that all SSH settings are fine and the problem still exists.

1. Enter the **`no SNA`** command.
2. Enter the **`no ssh`** command.
3. Enter the **`no ssh dsa-auth-key`** command.
4. Enter the **`ssh`** command.
5. Enter the **`SNA enable`** command.
6. On SNAS 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 SNA`** 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 ERS 5500 series device.

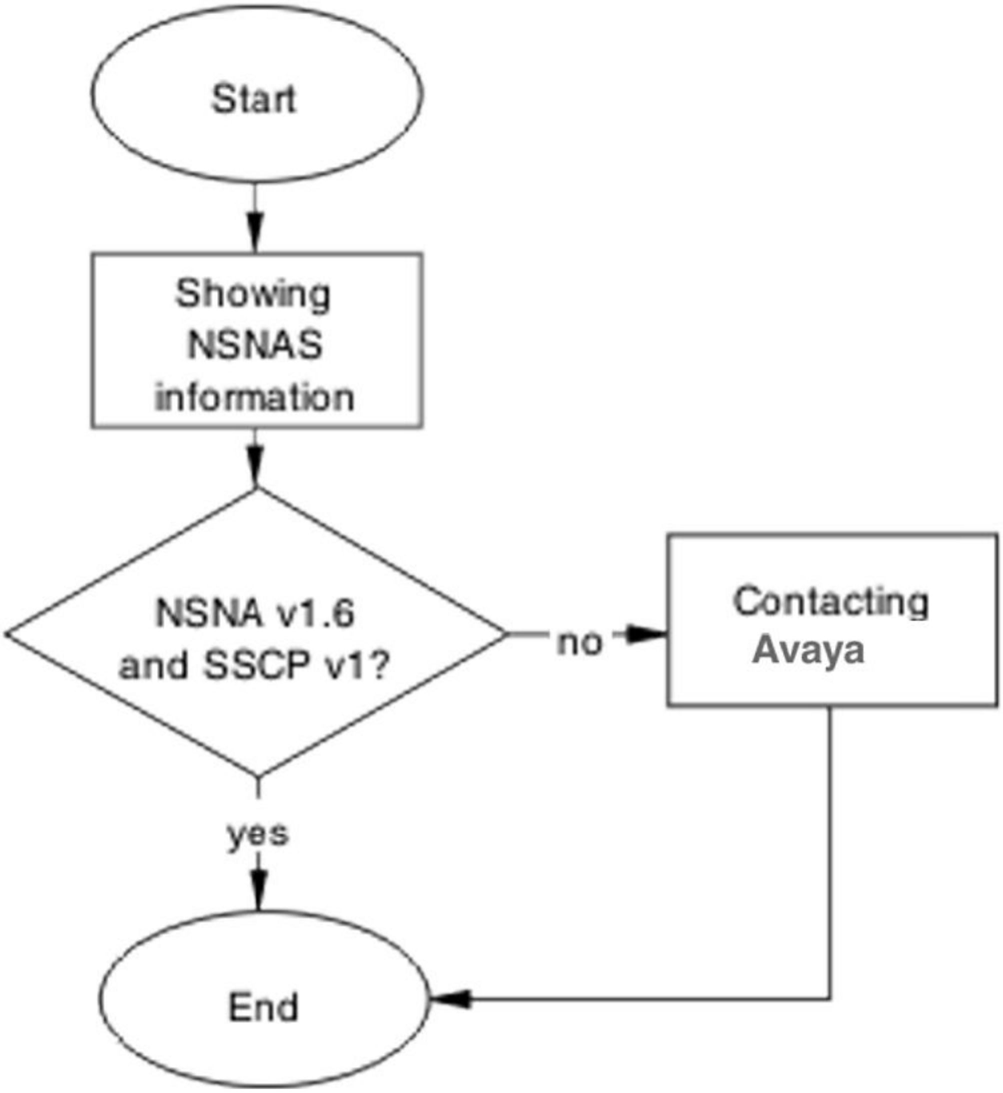


Figure 68: Verify SSCP version

Verify SSCP version navigation:

- Show Secure Network Access on page 147
- Contacting Avaya on page 148

Show Secure Network Access

Display the Secure Network Access (SNA) information for review.

1. Enter the `show SNA` command to display the configuration.
2. Enter `/info/local` command to display the software version on the Secure Network Access Solution (SNAS) side.
3. Note the following is to be on the switch:

   Secure Network Access Solution Connection Version: SSCPv1

   Higher versions are backward compatible.
4. Note the following is to be on the Secure Network Access Solution:

   Software version: 1.6.1.2

   Higher versions are be 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 can not connect

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 an client PC or phone that cannot connect.

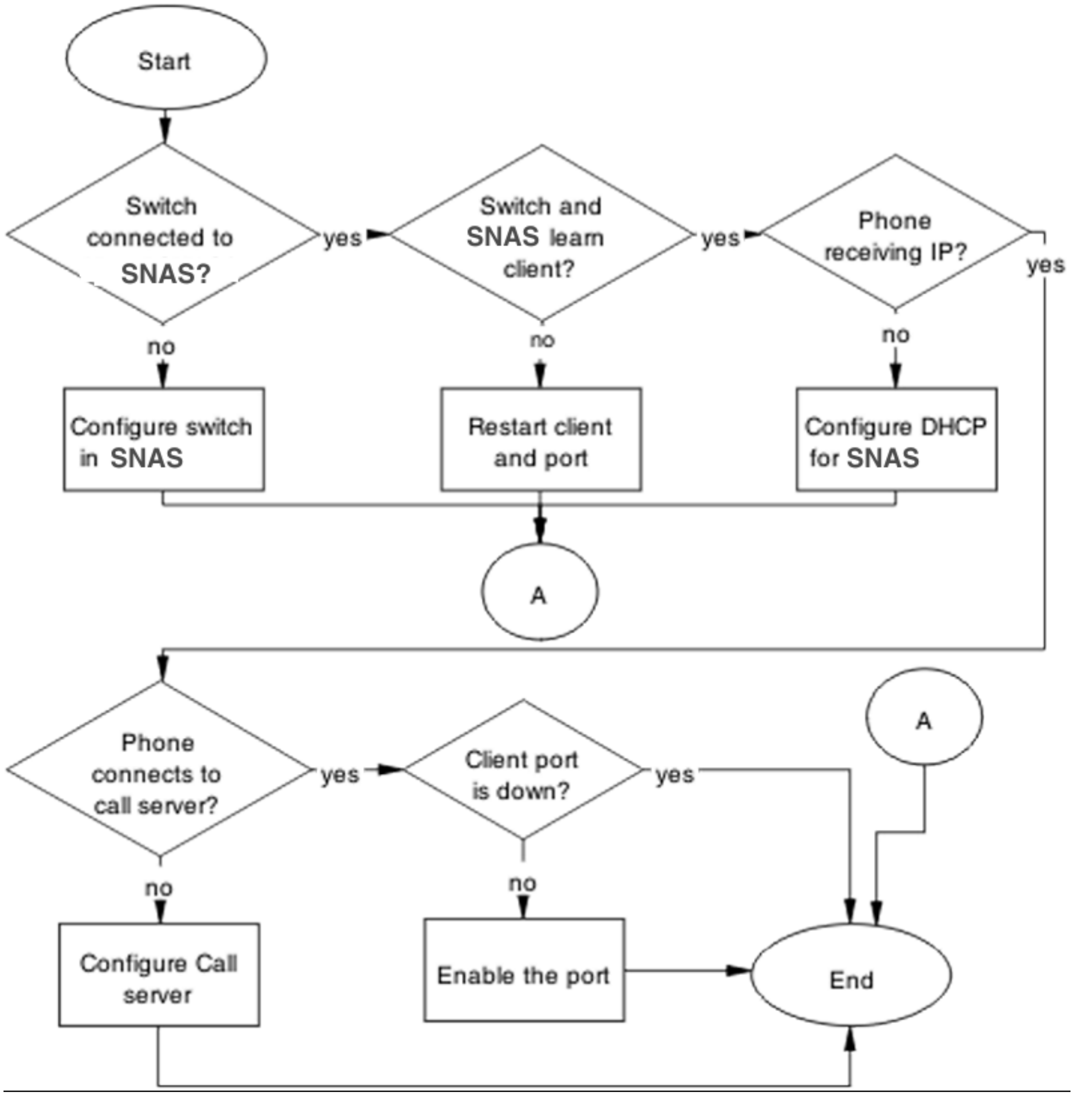


Figure 69: Client PC/phone can not connect

Client PC/phone can not connect navigation:

- Configure switch on Secure Network Access Solution on page 150
- Restart client and port on page 151
- Configure DHCP for Secure Network Access Solution on page 154
- Configure call server on page 156
- Enable the port on page 157

Configure switch on Secure Network Access Solution

Configure and enable the switch on Secure Network Access Solution (SNAS).

Task flow: Configure the switch on Secure Network Access Solution

The following task flow assists you to enable the ERS 5500 series device on Secure Network Access Solution (SNAS).

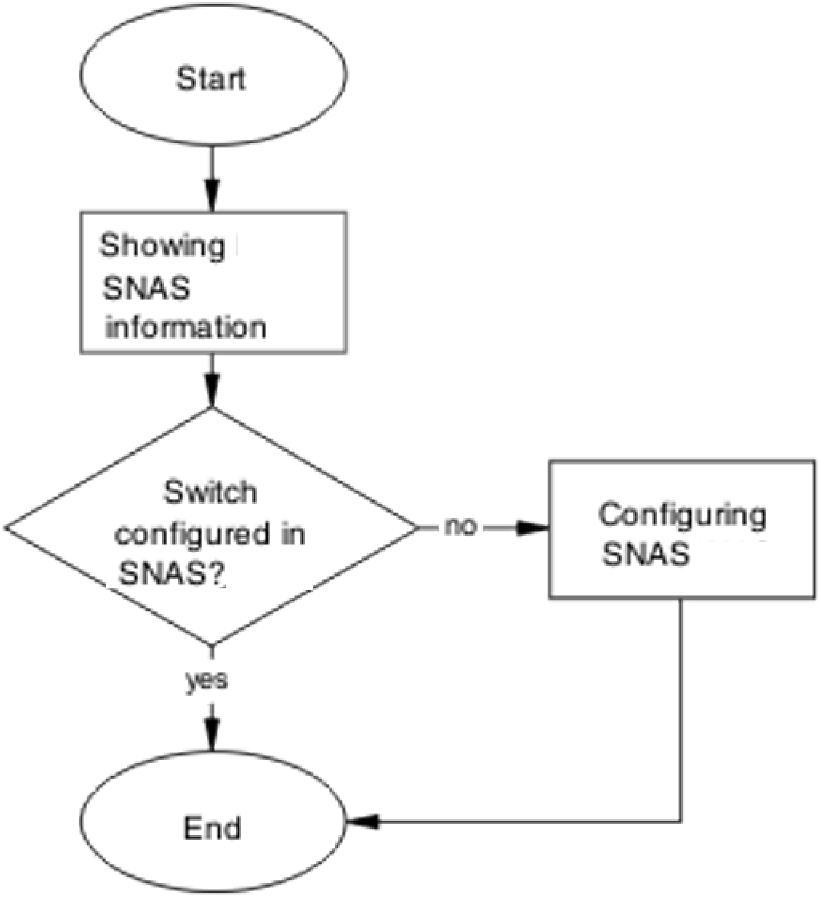


Figure 70: Configure the switch on Secure Network Access Solution

Configure the switch on Secure Network Access Solution navigation:

- Showing Secure Network Access information on page 151
- Configuring Secure Network Access Solution on page 151

Showing Secure Network Access 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 Secure Network Access Solution.

Configuring Secure Network Access Solution

Configure the Secure Network Access Solution (SNAS) with the settings for the ERS 5500 Series device.

Switch configuration on Secure Network Access Solution is in Technical_Configuration_Document _for_SNA for 1.6 release.

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.

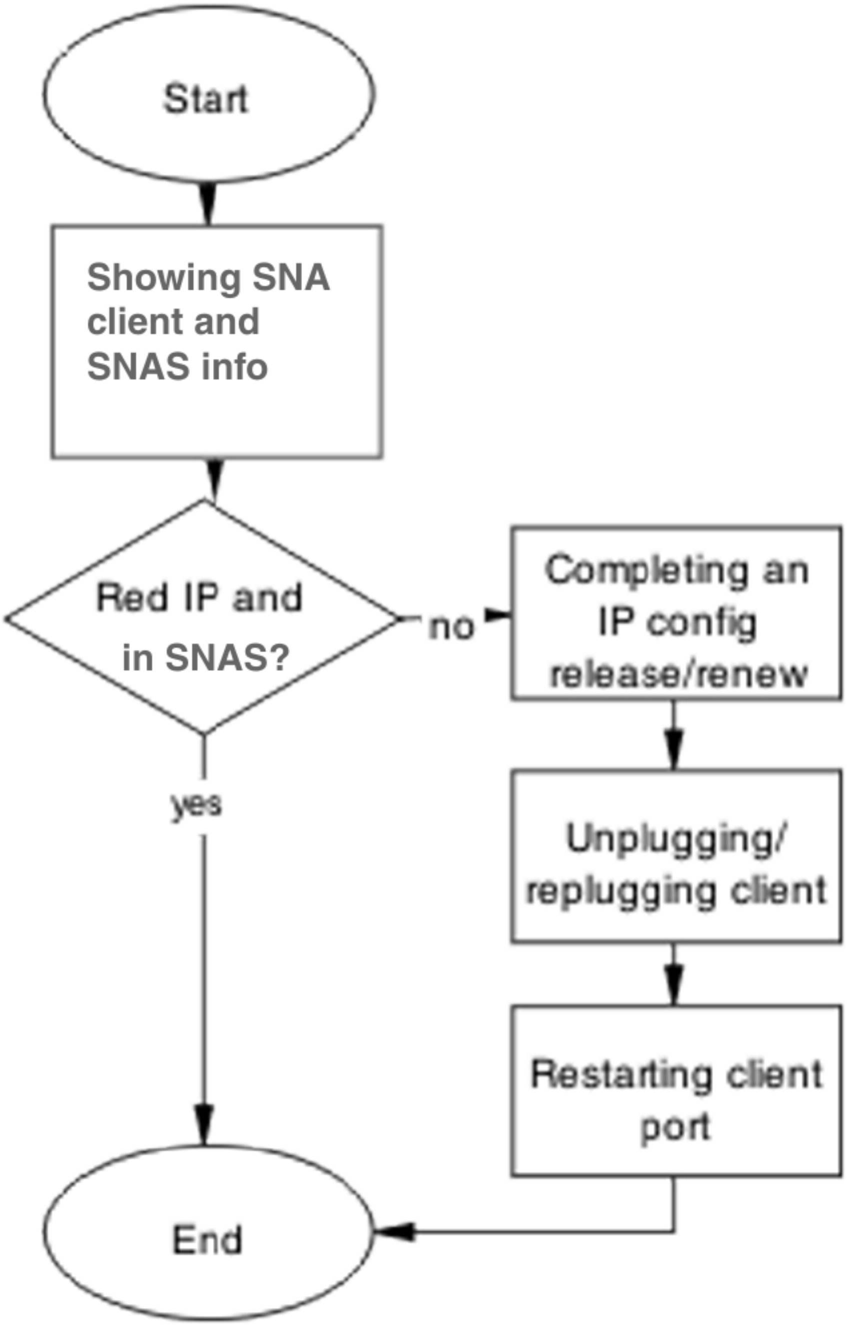

Start
Showing SNA client and SNAS info
Red IP and in SNAS?
no
yes
Completing an IP config release/renew
Unplugging/ replugging client
Restarting client port
End

Figure 71: Restart client and port

Restart client and port navigation:

- Showing Secure Network Access client and Secure Network Access Solution info on page 153
- Completing an IP config release/renew on page 153

- Unplugging/replugging client on page 153
- Restarting client port on page 153

Showing Secure Network Access client and Secure Network Access Solution info

Display the Secure Network Access client information

1. Use the **`show SNA client`** command.
2. Note the output.
3. Use the **`info/switch 1 n`** command in Secure Network Access Solution.
4. Observe both are 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 and ipconfig renew on the client PC.

Unplugging/replugging client

Physically disconnect 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 then restart it.

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

Configure DHCP for Secure Network Access Solution

Eliminate DHCP configuration issues if the phone is still not getting an IP.

Task flow: Configure DHCP for Secure Network Access

The following task flow assists you to configure the DHCP for Secure Network Access Solution (SNAS).

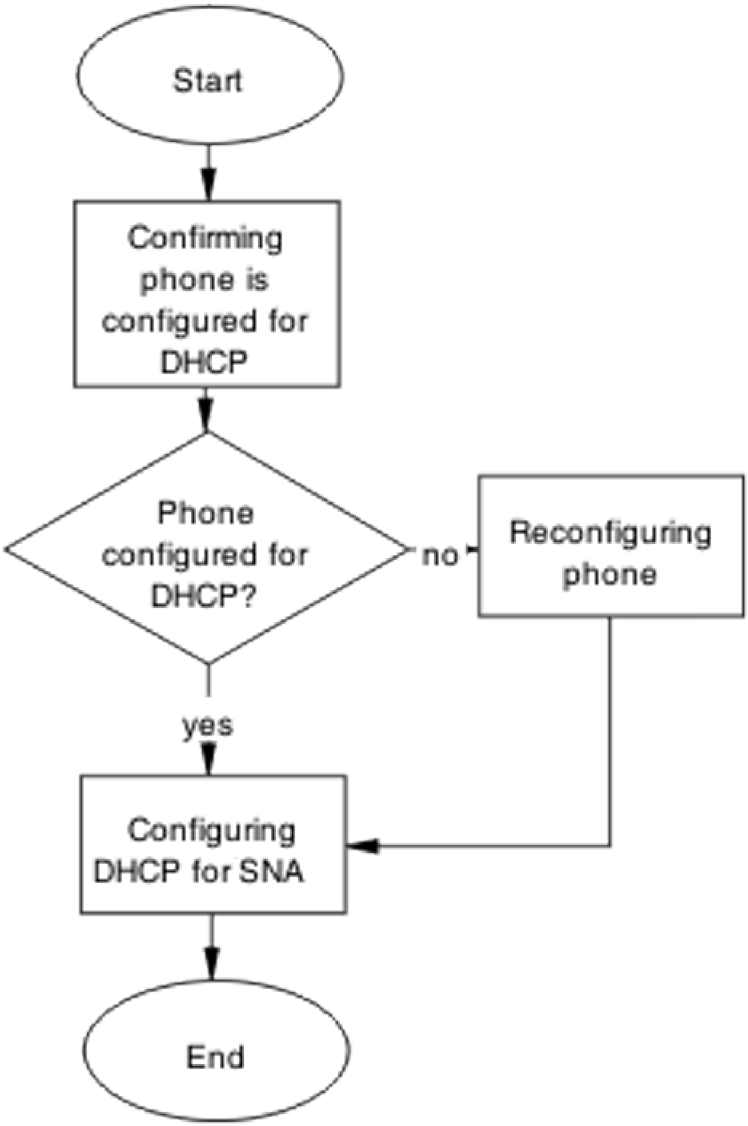

Start
Confirming phone is configured for DHCP
Phone configured for DHCP?
no
Reconfiguring phone
yes
Configuring DHCP for SNA
End

Figure 72: Configure DHCP for Secure Network Access

Configure DHCP for Secure Network Access navigation:

- Confirming phone is configured for DHCP on page 155
- Reconfiguring phone on page 156
- Configuring DHCP for Secure Network Access on page 156

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 Secure Network Access

Change DHCP server to work with Secure Network Access.

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.

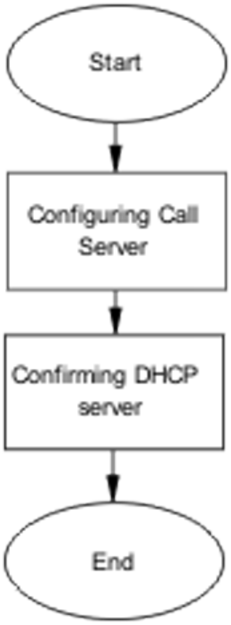


Figure 73: Configure call server.

Configure call server navigation:

- Configuring call server on page 157
- Configuring DHCP server on page 157

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 when a new client PC/Phone (behind a hub) is not able to get IP or connect OR the ERS 5500 series client port is down.

Task flow: Enable the port

The following task flow assists you to enable the port.

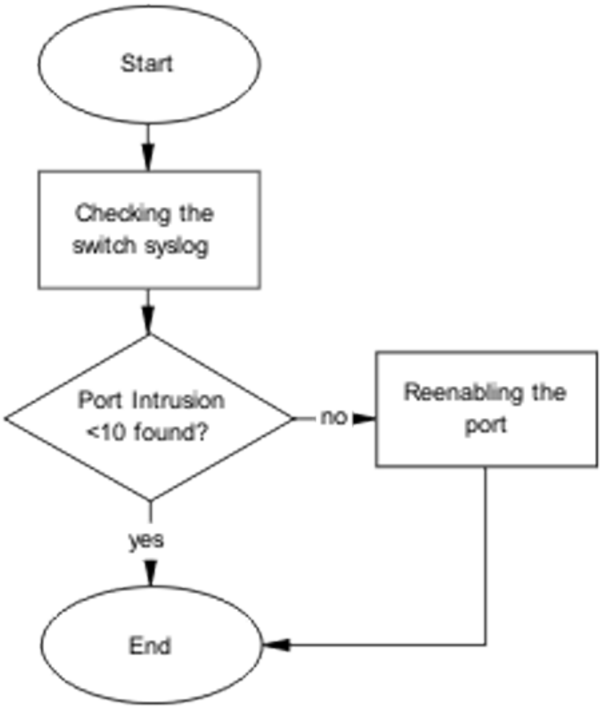


Figure 74: Enable the port

Enable the port navigation:

- Checking the switch log on page 158Checking the switch log
- Reenabling the port on page 158

Checking the switch log

Review the switch log to determine if more than 10 intruders are 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.

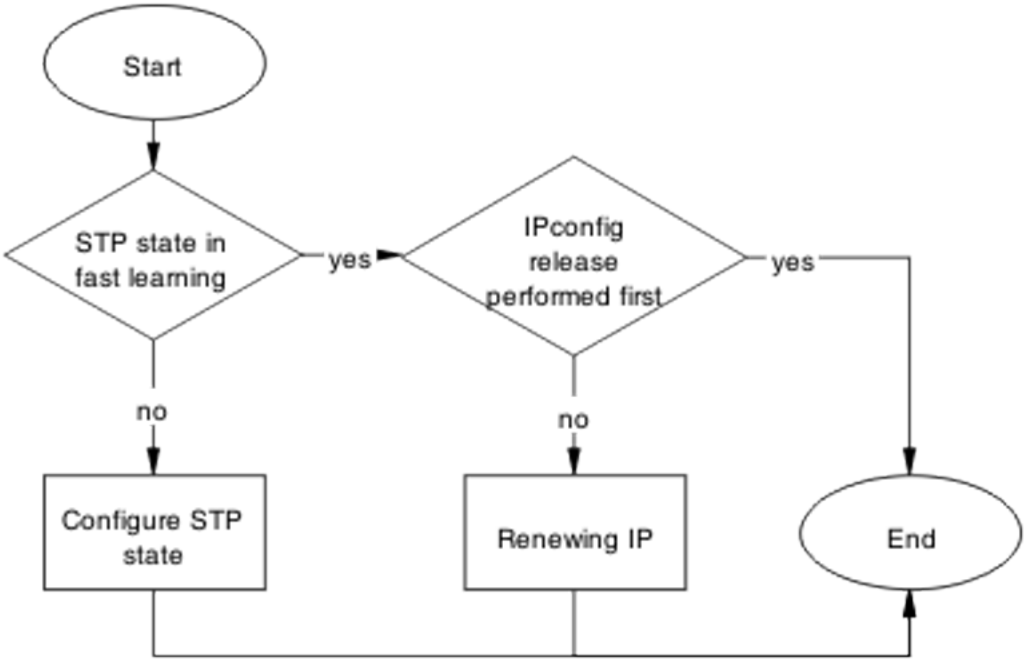


Figure 75: Authentication error or 0.0.0.0 IP after image upgrade

Authentication error or 0.0.0.0 IP after image upgrade navigation:

- Configure STP state on page 160
- Renewing IP on page 161

Configure STP state

Place the STP state in fast learning in the case the ports come up to fast.

Important:

Ensure that your 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.

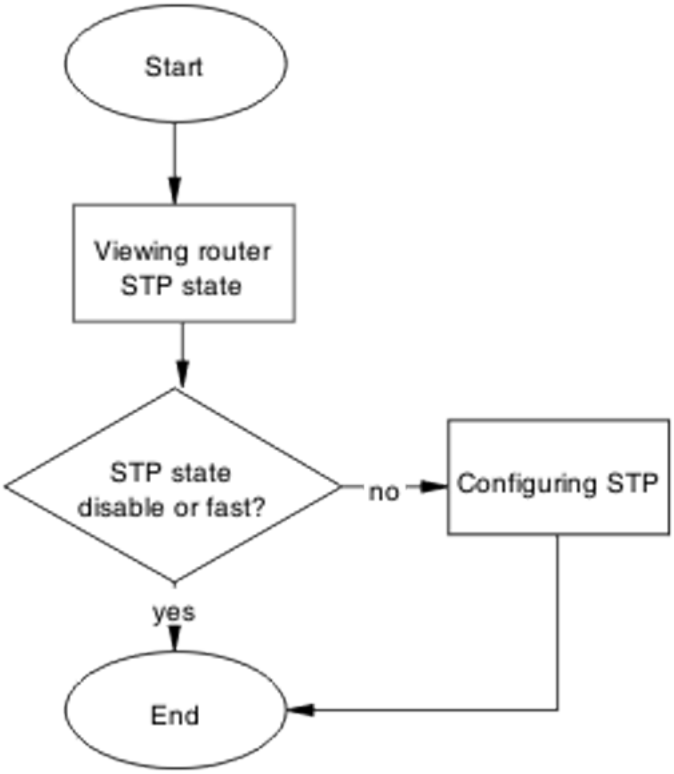


Figure 76: Configure STP state

Configure STP state task flow navigation:

- Viewing Router STP state on page 161
- Configuring STP state on page 161

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.

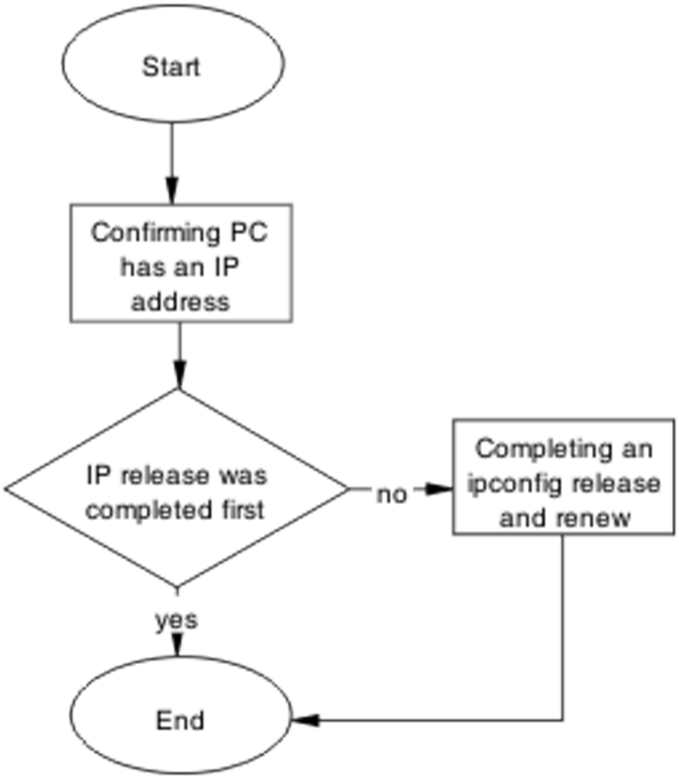

Start
Confirming PC has an IP address
IP release was completed first
no
Completing an ipconfig release and renew
yes
End

Figure 77: Renewing IP

Renewing IP navigation:

- Confirming PC has IP address on page 162
- Completing and ipconfig release and renew on page 162

Confirming PC has IP address

Confirm the PC has a proper IP.

1. Using vendor documentation, Use the **`ipconfig /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 NSAS.

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.

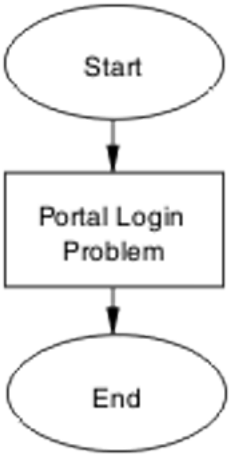


Figure 78: TG Client getting red IP

TG Client getting red IP navigation:

- Portal Login Problem on page 163

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.

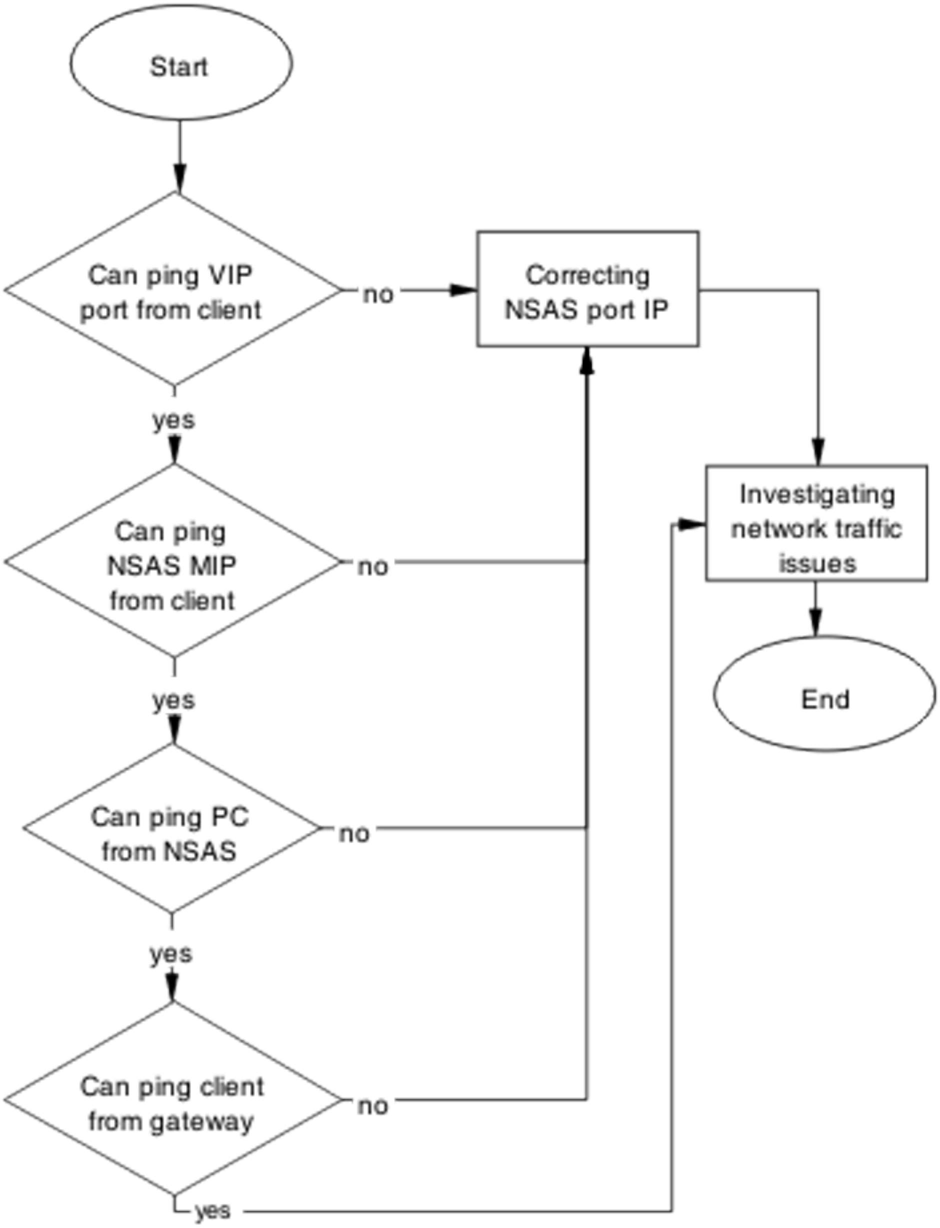

Start
Can ping VIP port from client
no
Correcting NSAS port IP
yes
Can ping NSAS MIP from client
no
Investigating network traffic issues
End
yes
Can ping PC from NSAS
no
yes
Can ping client from gateway
no
yes

Figure 79: Portal login problem

Portal login problem navigation:

- Correcting SNAS port IP on page 165
- Investigating network traffic issues on page 165

Correcting SNAS port IP

Make changes to Secure Network Access Solution (SNAS) port IP.

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

Investigating network traffic issues

Eliminate network traffic issues that 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.

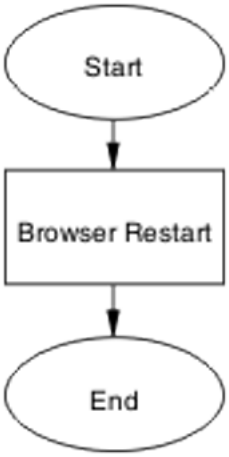


Figure 80: Client gets red IP but browser hangs after opening

Client gets red IP but browser hangs after opening navigation:

Browser restart on page 166

Browser restart

Restart the browser to regain connectivity.

Task flow: Browser restart

The following task flow assists you to restart the browser.

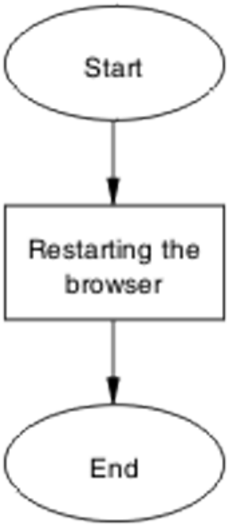


Figure 81: Browser restart

Browser restart navigation:

Restarting the browser on page 167

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.

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

Correct the client maintaining red state for too long due to Secure Network Access Solution communication failing.

Work flow: Secure Network Access client gets red IP but after loginit does not go to yellow or green state

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

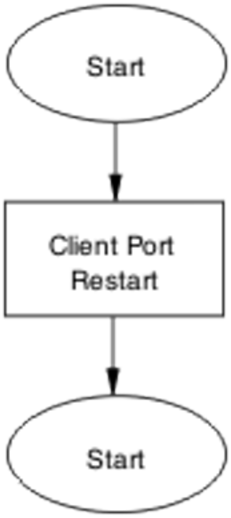


Figure 82: Secure Network Access client gets red IP but after login it does not go to yellow or green state

Secure Network Access client gets red IP but after login it does not go to yellow or green state navigation:

- Client port restart on page 168

Client port restart

Client link down and up.

Task flow: Client port restart

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

Start
Restarting client port link
End

Figure 83: Client port restart

Client port restart navigation:

- Restarting client port link on page 169

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 kicked to yellow or red

Correct the communication issue causing the IP status to change.

Work flow: Client had green IP but was kicked 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.

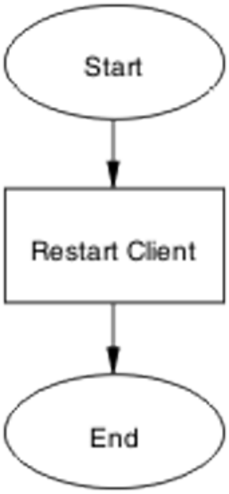


Figure 84: Client had green IP but was kicked to yellow or red

Client had green IP but was kicked to yellow or red navigation:

- Restart client on page 170

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.

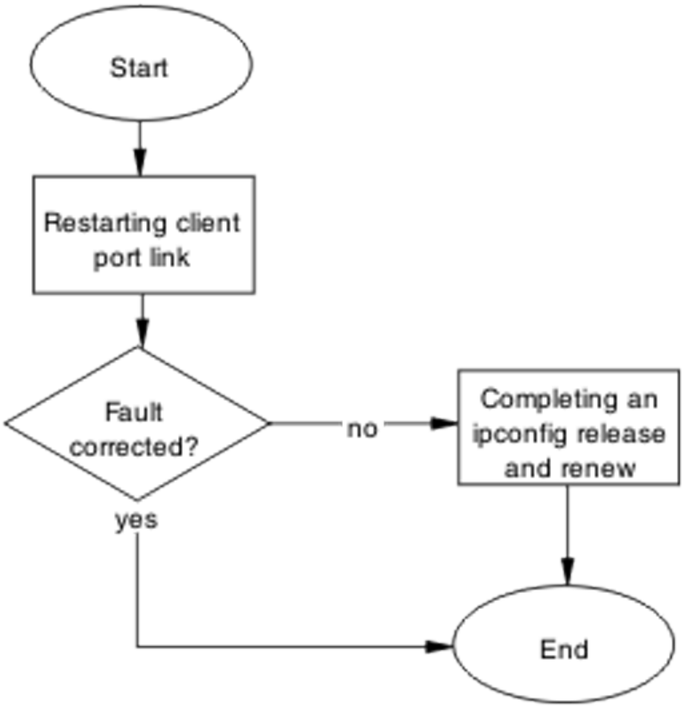

Start
Restarting client port link
Fault corrected?
no
Completing an ipconfig release and renew
yes
End

Figure 85: Restart client

Restart client navigation:

- Restarting client port link on page 171
- Completing an ipconfig release and renew on page 171

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 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.

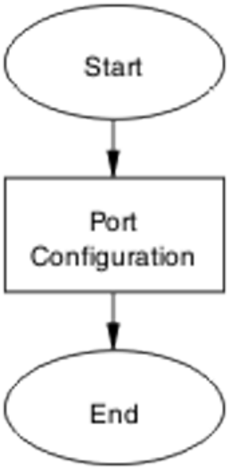


Figure 86: Client PC taking a long time to boot

Client PC taking a long time to boot navigation:

- Port configuration on page 172

Port configuration

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

Task flow: Port configuration

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

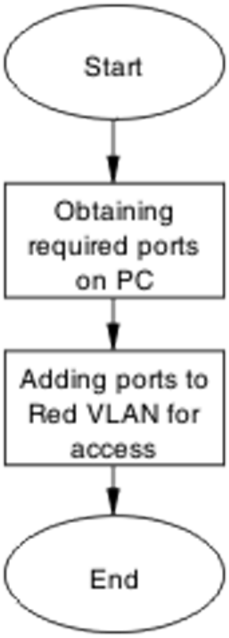

Start
Obtaining required ports on PC
Adding ports to Red VLAN for access
End

Figure 87: Port configuration

Port configuration navigation:

- Obtaining required ports on PC on page 173
- Adding ports to red VLAN for access on page 173

Obtaining required ports on PC

Identify the correct ports that 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 access.

1. Refer to the Avaya Ethernet Routing Switch 5500 Series Configuration — Quality of Service
2. Repeat previous step as required for multiple ports.

Result

Example of adding ports to a VLAN

1. Use the **`qos SNA classifier name red protocol 17 dst-port-min 427 dst-port-max 427 ethertype 0x0800 drop-action disable block RED eval-order 101`** command.
2. Use the **`qos SNA classifier name red protocol 6 dst-port-min 524 dst-port-max 524 ethertype 0x0800 drop-action disable block RED eval-order 102`** command.

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

Correct the client that is not authenticating. After not assigning the correct filter, the authentication can fail.

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.

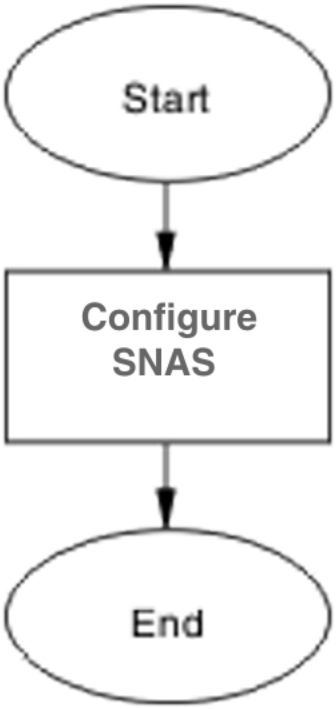


Figure 88: Mac-Auth client not authenticated or not assigned the correct filter

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

- Configure Secure Network Access Solution on page 175

Configure Secure Network Access Solution

Change the Secure Network Access Solution (SNAS) settings to ensure authentication can occur.

Task flow: Configure Secure Network Access Solution

The following task flow assists you to configure the Secure Network Access Solution (SNAS) to allow authentication.

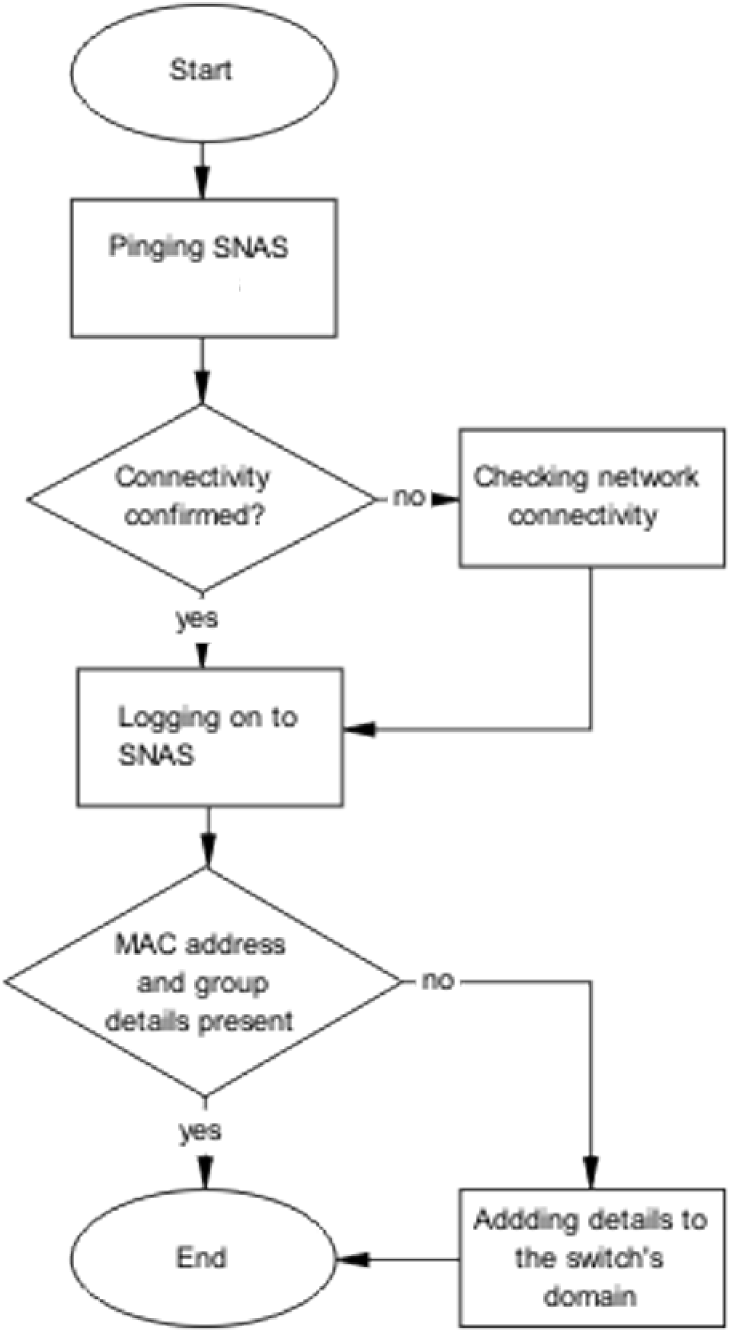

Start
Pinging SNAS
Connectivity confirmed?
no
Checking network connectivity
yes
Logging on to SNAS
MAC address and group details present
no
yes
End
Addding details to the switch's domain

Figure 89: Configure Secure Network Access Solution

Configure Secure Network Access Solution navigation:

- Pinging Secure Network Access Solution on page 177
- Checking network connectivity on page 177
- Logging on to Secure Network Access Solution on page 177
- Adding details to the switch domain on page 177

Pinging Secure Network Access Solution

Verify the network connectivity using ping.

1. Use the ping **<SNASIP>** 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 Secure Network Access Solution

Logon to Secure Network Access Solution (SNAS) to view more information.

1. Use vendor procedure to log on to the Secure Network Access Solution.
2. Observe the following:

   the macdb list for the switch's domain

Adding details to the switch domain

Add MAC address and group details to the switch domain.

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

Chapter 11: Troubleshooting layer 2 and layer 3

Layer 2 and layer 3 issues can interfere in the device operation and function. Some possible ARP, OSPF, RIP, and VRRP problems are listed.

Work flow: Troubleshooting Layer 2 and Layer 3

The following work flow contains some typical Layer 2 and Layer 3 problems. These situations are not normally dependant upon each other.

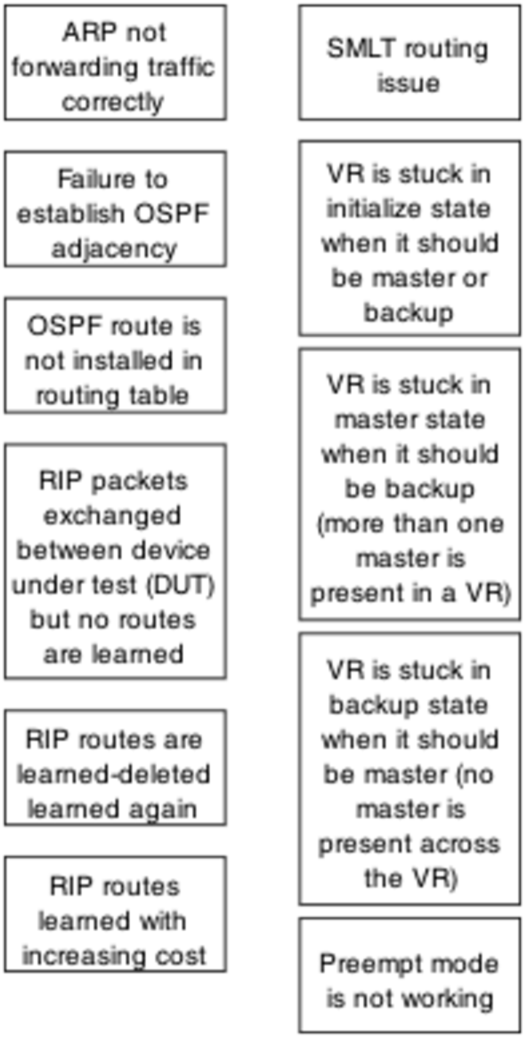

ARP not forwarding traffic correctly
Failure to establish OSPF adjacency
OSPF route is not installed in routing table
RIP packets exchanged between device under test (DUT) but no routes are learned
RIP routes are learned-deleted learned again
RIP routes learned with increasing cost
SMLT routing issue
VR is stuck in initialize state when it should be master or backup
VR is stuck in master state when it should be backup (more than one master is present in a VR)
VR is stuck in backup state when it should be master (no master is present across the VR)
Preempt mode is not working

Figure 90: Troubleshooting Layer 2 and Layer 3

Troubleshooting Layer 2 and Layer 3 navigation:

- ARP not forwarding traffic correctly on page 181
- Failure to establish OSPF adjacency on page 195
- OSPF route is not installed in routing table on page 219
- RIP packets exchanged between device under test (DUT) but no routes are learned on page 224
- RIP routes are learned-deleted learned again on page 231
- RIP routes learned with increasing cost on page 235
- SMLT routing issue on page 237
- VR is stuck in initialize state when it should be master or backup on page 247

- VR is stuck in master state when it should be backup (more than one master is present in a VR) on page 253
- VR is stuck in backup state when it should be master (no master is present across the VR) on page 255
- Preempt mode is not working on page 258

ARP not forwarding traffic correctly

Information about Address Resolution Protocol (ARP) table is used, together with that about routing table, to diagnose if Layer 3 traffic is forwarded correctly.

Work flow: Troubleshooting ARP

The following work flow assists you to determine the solution for ARP not forwarding traffic as expected.

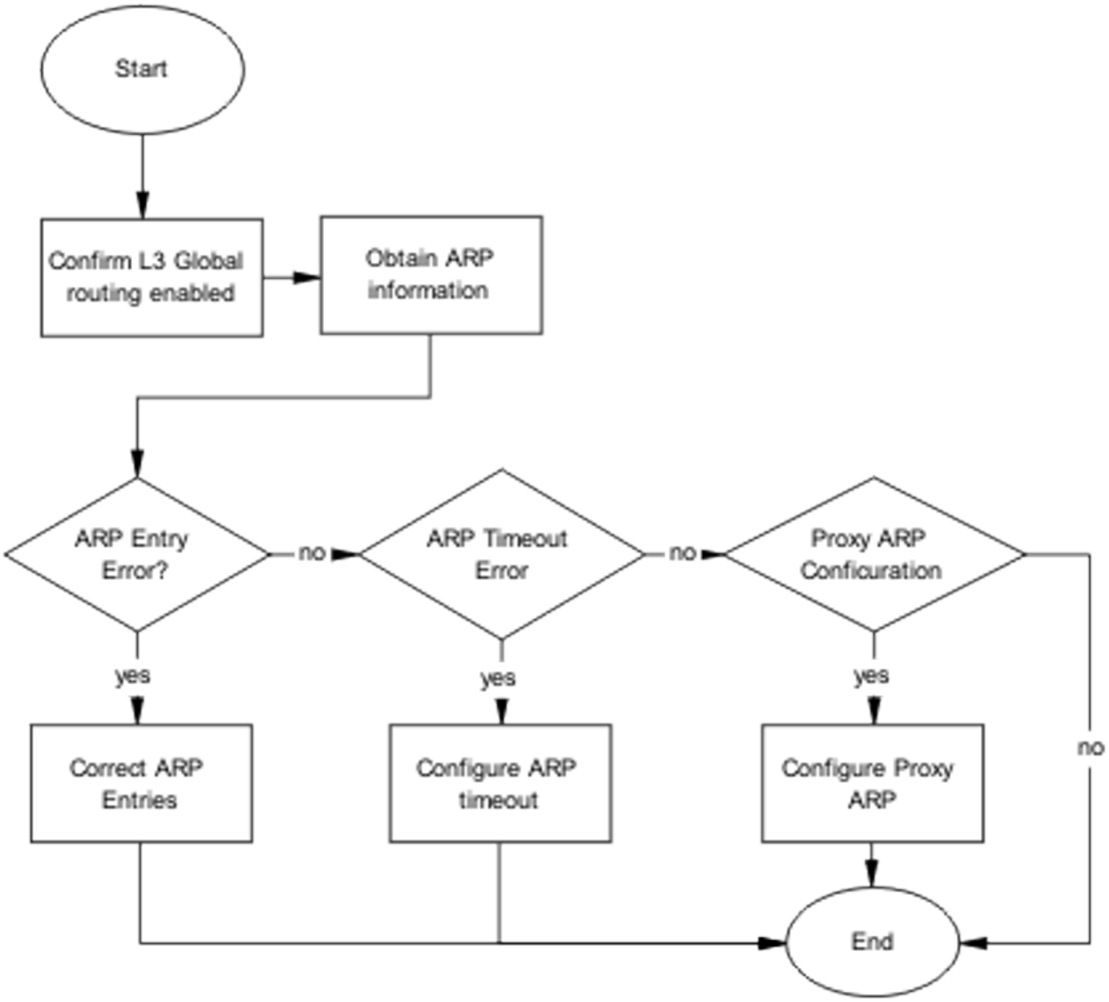


Figure 91: Troubleshooting ARP

Troubleshooting ARP navigation:

- Confirming global L3 routing enabled on page 182
- Obtain ARP information on page 184
- Correct ARP Entries on page 186
- Configure ARP timeout on page 190
- Configuring the proxy ARP on page 192

Confirming global L3 routing enabled

Confirm that the L3 global routing is enabled.

Task flow: Confirming global L3 routing

The following task flow assists you to enable L3 routing globally.

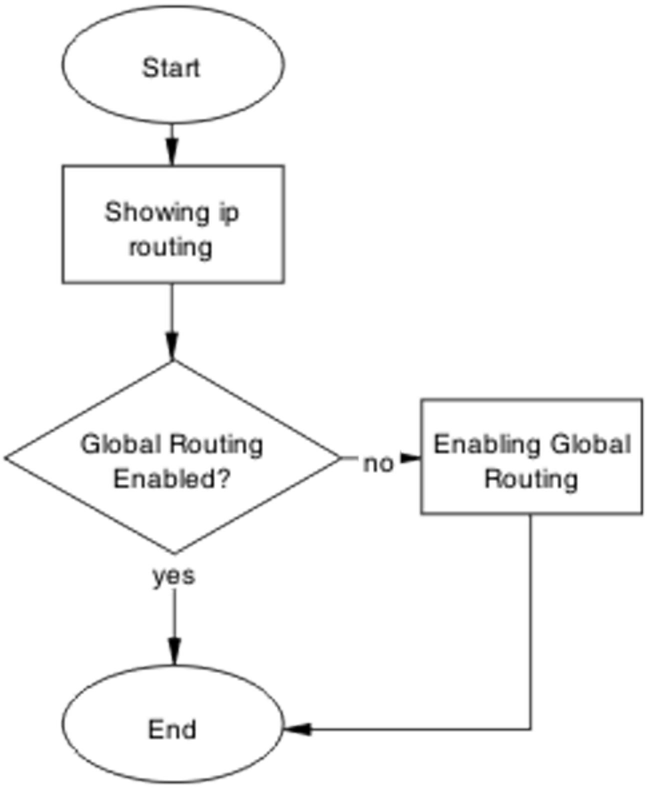


Figure 92: Confirming global L3 routing

Result

Navigation

- Showing IP Routing on page 183
- Enabling global routing on page 184

Showing IP Routing

Show the IP Routing Information of the switch to ensure it is enabled.

1. Enter the **`show ip routing`** command.
2. Observe IP Routing is enabled.

Enabling global routing

Enable the IP Routing on the switch.

1. Use the **`ip routing enable`** command to enable ip routing in the global configuration mode.
2. Observe no errors after execution.

Obtain ARP information

View the ARP information to compare the information provided by the three methods.

Task flow: Obtaining ARP information

The following task flow assists you to obtain the ARP information from CLI, DM, and SMTP.

Start
Displaying ARP table in CLI
Displaying ARP table in JDM
Completing an SNMP walk to objects
End

Figure 93: Obtaining ARP information

Obtaining ARP information navigation:

- Displaying the ARP Table in the CLI on page 185
- Displaying ARP table information in DM on page 186
- Completing an SNMP walk to objects on page 186

Displaying the ARP Table in the CLI

Use the CLI to obtain ARP table information.

Prerequisites

CLI Exec mode on base unit only

1. Enter the **`show ip arp`** command.
2. Observe ARP entries.
   In software Release 5.1, the number of ARP entries is also displayed.

Displaying ARP table information in DM

Use the DM to obtain ARP table information.

1. Open the DM for the Ethernet Routing Switch 5000 series device.
2. Connect to the Ethernet Routing Switch 5000 series device for which you wish to display the ARP information for.
3. Navigate to IP Routing, IP, ARP .
4. Observe ARP entries displayed.

Completing an SNMP walk to objects

The SNMP walk is used to assist in the diagnosis of the ARP situation.

1. Enter the **`SNMP walk`** command on the ipNetToMediaIfIndex object.
2. Enter the **`SNMP walk`** command on the ipNetToMediaPhysAddress object.
3. Enter the **`SNMP walk`** command on the ipNetToMediaNetAddress object.
4. Emter the **`SNMP walk`** command on the ipNetToMediaType object.

Correct ARP Entries

The ARP Entries can be corrected by using CLI, DM, or SNMP.

Task flow: Correct ARP entries

The following task flow assists you to correct the ARP entries using either CLI, DM, or SNMP.

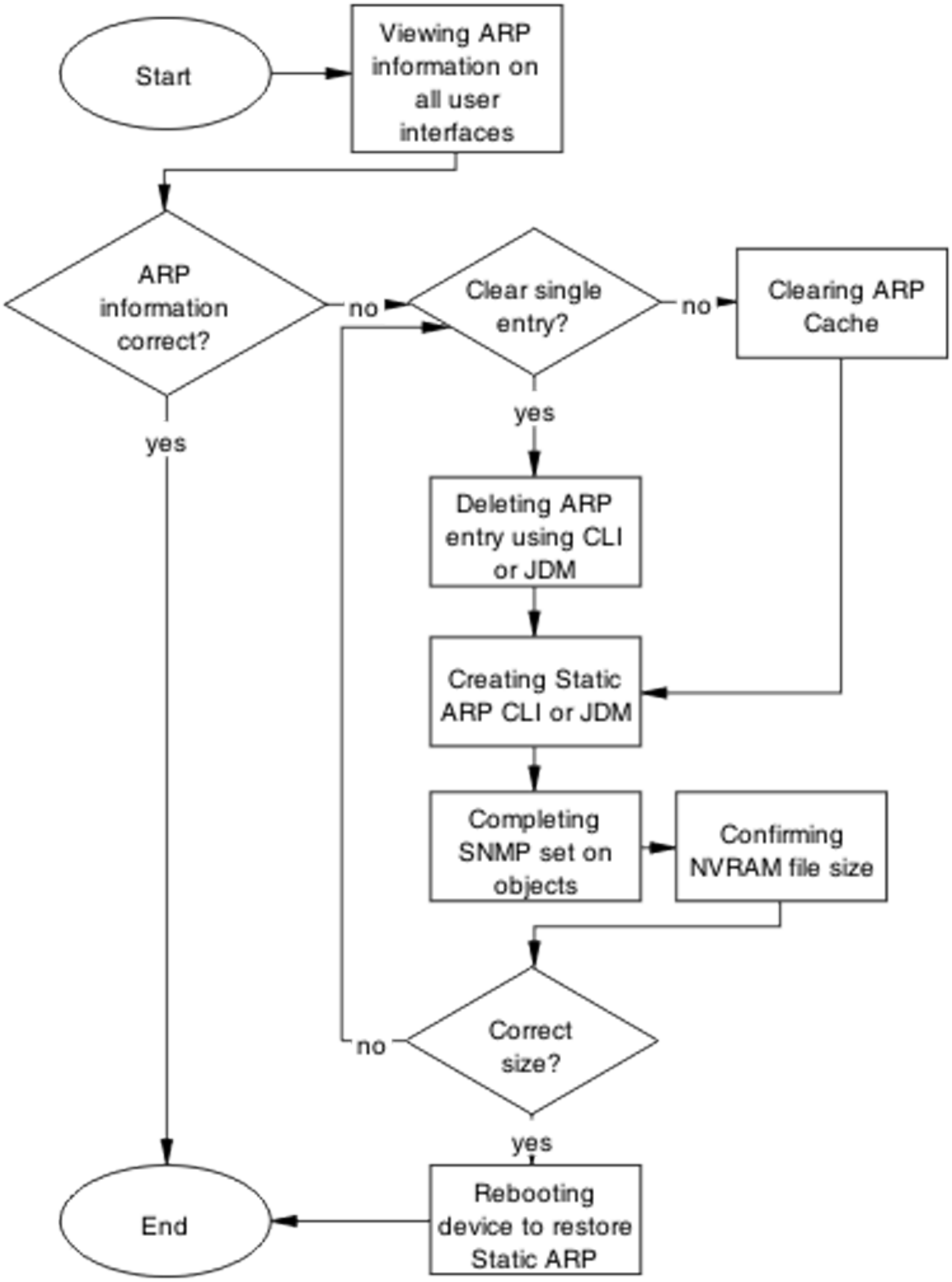

Start
Viewing ARP information on all user interfaces
ARP information correct?
no
Clear single entry?
no
Clearing ARP Cache
yes
yes
Deleting ARP entry using CLI or JDM
Creating Static ARP CLI or JDM
Completing SNMP set on objects
Confirming NVRAM file size
no
Correct size?
yes
End
Rebooting device to restore Static ARP

Figure 94: Correct ARP entries

Correct ARP entries:

- Confirming ARP entries are correct on page 188
- Clearing ARP cache on page 188
- Deleting ARP entry in CLI or DM on page 188

- Creating Static ARP entries in CLI or DM on page 189
- Setting objects with SNMP on page 189
- Confirming NVRAM file size on page 190
- Rebooting the device to restore static ARP on page 190

Confirming ARP entries are correct

Comparing ARP entries to ensure they are correct.

1. Review the CLI, DM, and SNMP data.
2. Compare entries to determine if discrepancies exist.

Clearing ARP cache

The ARP cache can be completely cleared.

1. Enter CLI Exec mode.
2. Enter the `clear arp-cache` command to clear the static and dynamic entries.

Deleting ARP entry in CLI or DM

Individual ARP entries can be deleted in the CLI and DM.

Procedure for CLI

1. Enter the CLI Exec mode.
2. Enter the `no ip arp <a.b.c.d>` command to delete the entry.

Procedure for DM

1. Navigate to DM ARP table IP Routing, IP, ARP, select and delete the entry.
2. Select the entry to be deleted.
3. Delete the entry by selecting the delete button.

Creating Static ARP entries in CLI or DM

Use the CLI or DM to create the static ARP entries.

Creating static ARP entries using the CLI

1. Enter Global configuration mode.
2. Use the command **`ip arp <a.b.c.d> <h.h.h> <unit/port> <vid>`** to create the static ARP entry.

Creating static ARP entries using the DM

1. Select **IP Routing, IP, ARP** in the DM.
2. Enter the values required and press the **Insert** button.

Deleting ARP entry using SNMP

Individual ARP entries removed using SNMP.

1. Set the corresponding ipNetToMediaType to value “2” .
2. Observe the change.

Setting objects with SNMP

SNMP objects can be set.

1. Use the **`SNMP set`** command on the ipNetToMediaIfIndex object.
2. Use the **`SNMP set`** command on the ipNetToMediaPhysAddress object.
3. Use the **`SNMP set`** command on the ipNetToMediaNetAddress object.
4. Use the **`SNMP set`** command on the ipNetToMediaType object.

Confirming NVRAM file size

The NVRAM file size is to conform to parameters.

Prerequisites:

- File NVRAM:/APPS/staticarp.cfg is stored
- File size is as follows:
  - 8 byte header.
  - 20 byte record for each ARP.

1. Enter the **`dbg enable`** command.
2. Enter the **`dbg ll APPS`** command.

Rebooting the device to restore static ARP

Restore static ARP entries on device after reboot.

1. Reboot ERS 5500 Series device.
2. Ensure device has rebooted correctly.

Configure ARP timeout

Change the ARP timeout value.

Task flow: Configure ARP timeout

The following task flow assists you to change the ARP timeout value.

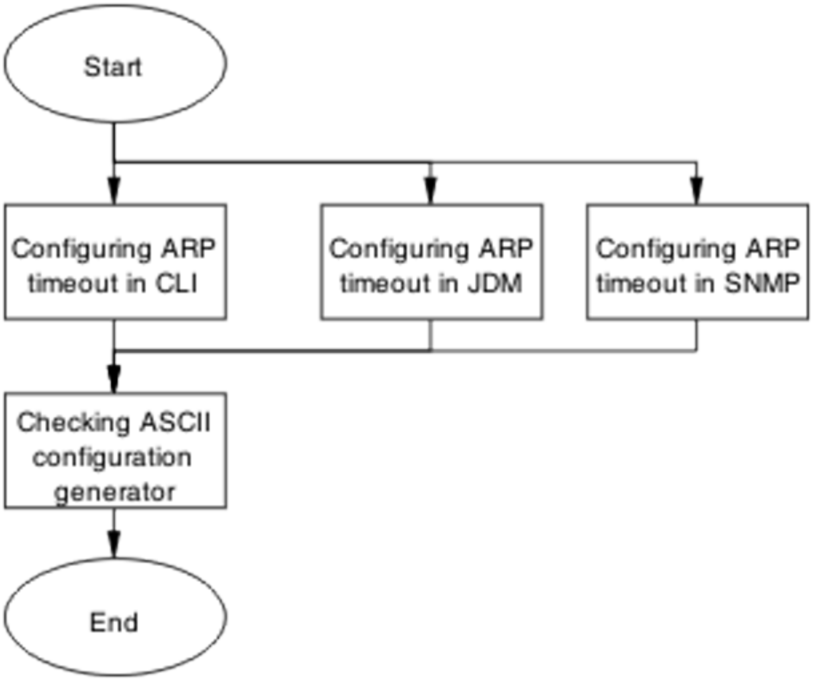

Start
Configuring ARP timeout in CLI
Configuring ARP timeout in JDM
Configuring ARP timeout in SNMP
Checking ASCII configuration generator
End

Figure 95: Configure ARP timeout

Configure ARP timeout navigation:

- Configuring ARP timeout using CLI on page 191
- Configuring ARP timeout using DM on page 192
- Configuring ARP timeout using SNMP on page 192
- Checking ASCII configuration generator on page 192

Configuring ARP timeout using CLI

The CLI can be used to set the ARP timeout.

1. Enter CLI global configuration mode.
2. Enter the **`ip arp timeout <value>`** command.

Configuring ARP timeout using DM

The DM can be used to set the ARP timeout.

1. Navigate to the Globals tab.
2. Change the timeout value.
3. Select the Apply button.

Configuring ARP timeout using SNMP

The SNMP can be used to set the ARP timeout.

1. Use the **`snmp set`** command on the rcArpExtLifeTime object.
2. Use the **`snmp get`** command on the rcArpExtLifeTime object to verify the value.

Checking ASCII configuration generator

Use the ASCII Configuration Generator to display the static ARPs and for the ARP timeout.

1. Use the **`show running-config`** command .
2. Review details under the L3 section.

Configuring the proxy ARP

The Proxy ARP can be enabled or disabled.

Task flow: Configuring the proxy ARP

The following task flow assists you to enable or disabel the Proxy ARP.

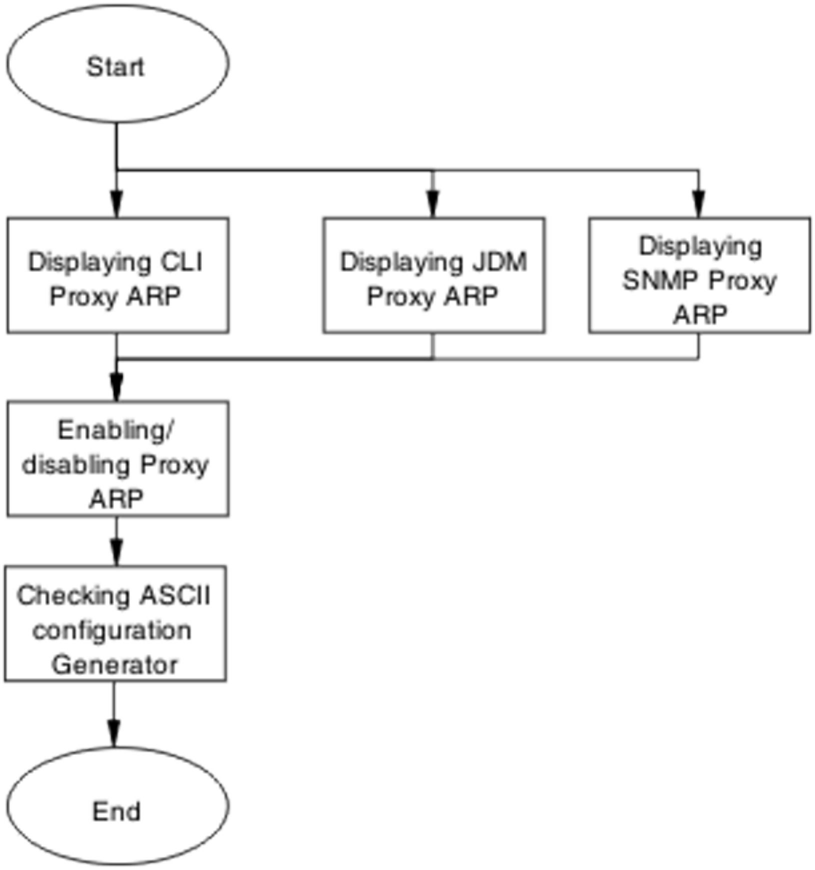

Start
Displaying CLI Proxy ARP
Displaying JDM Proxy ARP
Displaying SNMP Proxy ARP
Enabling/ disabling Proxy ARP
Checking ASCII configuration Generator
End

Figure 96: Configuring the proxy ARP

Configuring the proxy ARP navigation:

- Displaying CLI proxy ARP on page 193
- Displaying DM Proxy ARP on page 194
- Displaying SNMP proxy ARP on page 194
- Enabling/disabling Proxy ARP on page 194
- Checking ASCII configuration Generator on page 195

Displaying CLI proxy ARP

The CLI can be used to set the Proxy ARP.

1. Enter CLI Exec mode.
2. Enter the **`show ip arp-proxy interface`** command.
3. Enter the **`show ip arp-proxy interface [vlan <vid>]`**command.

4. Enter IP VLAN configuration mode.
5. Enter the **`ip arp proxy [enable]`** command.
6. Enter the **`no ip arp proxy [enable]`** command.
7. Enter the **`default ip arp proxy [enable]`** command.

Displaying DM Proxy ARP

The DM can be used to set the proxy ARP.

1. Navigate to IP Routing->IP>ARP Interfaces .
2. Select an interface.
3. Set desired value in DoProxy field.

Displaying SNMP proxy ARP

The SNMP can be used to view the proxy ARP.

1. Use the **`snmp walk`** command on the rcArpExtEntDoProxy object.
2. Observe the no errors after execution.

Enabling/disabling Proxy ARP

The Proxy ARP can be enabled or disabled. By default, ARP is disabled.

Enabling/disabling Proxy ARP using CLI

1. Use the **`ip arp proxy enable`** command to enable the proxy ARP.
2. Use the **`no ip arp proxy [enable]`** command to set the IP ARP proxy.
3. Use the **`default ip arp proxy [enable]`** command to set the IP ARP proxy.
4. Review details under the L3 section.

Enabling/disabling Proxy ARP using DM

1. Navigate to **IP Routing, IP, ARP Interface**.
2. Select an interface from the list.
3. Set the desired value in the DoProxy field.

Enabling/disabling Proxy ARP using SNMP

1. Do an SNMP set on the rcArpExtEntDoProxy object. .
2. Observe no errors after execution.

Checking ASCII configuration Generator

The ASCII configuration generator is a tool to check the Proxy ARP configuration.

1. Enter the command `show running-config`.
2. Review output under "L3 Protocols" and "Proxy ARP" sub sections.

Failure to establish OSPF adjacency

Correct the OSPF parameters to ensure that adjacencies are established.

Work flow: Failure to establish an OSPF adjacency

The following work flow assists you to determine the solution for adjancies that do not form.

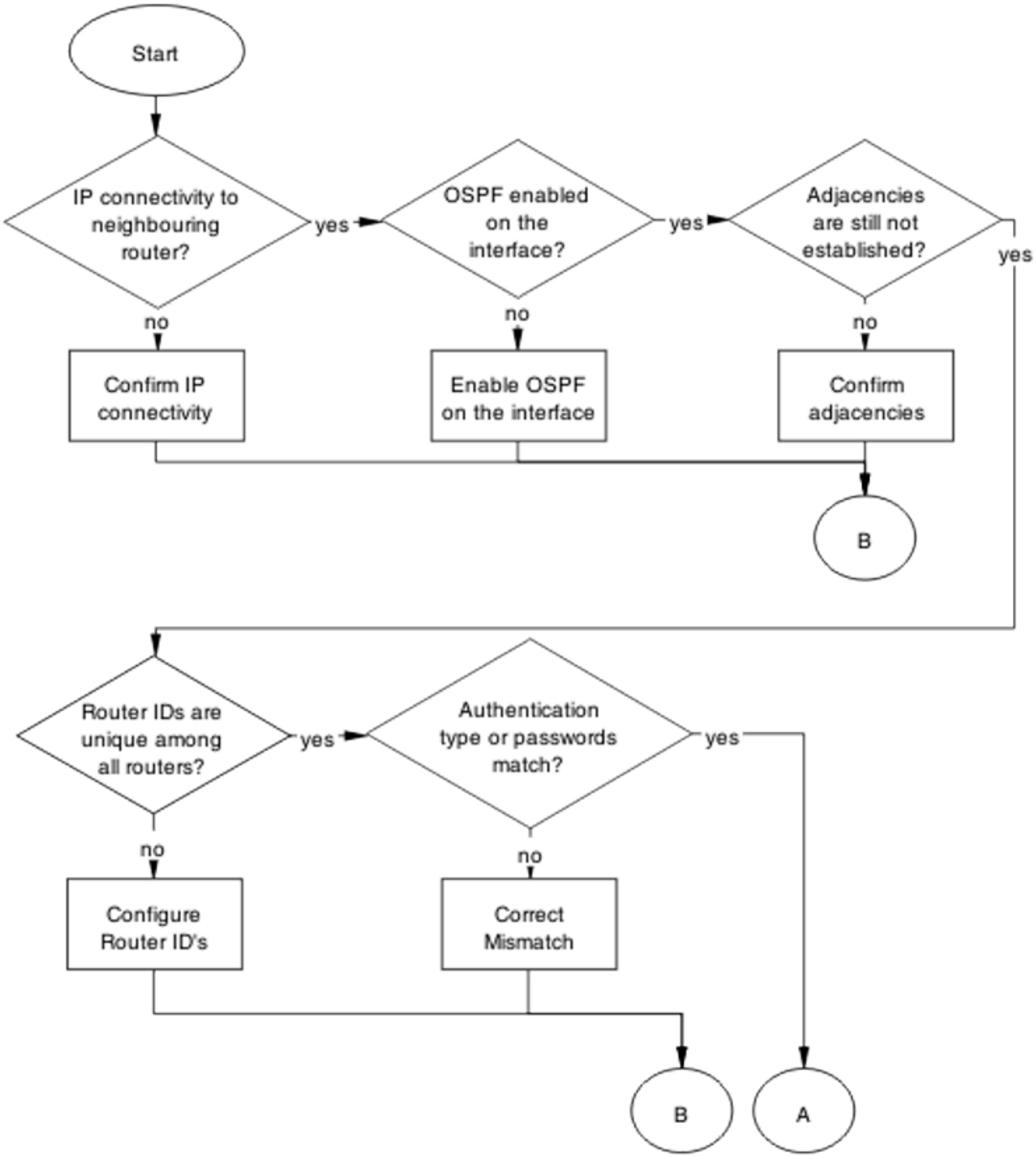

Start
IP connectivity to neighbouring router?
yes
OSPF enabled on the interface?
yes
Adjacencies are still not established?
yes
no
Confirm IP connectivity
no
Enable OSPF on the interface
no
Confirm adjacencies
B
Router IDs are unique among all routers?
yes
Authentication type or passwords match?
yes
no
Configure Router ID's
no
Correct Mismatch
B
A

Figure 97: Failure to Establish an OSPF adjacency part 1

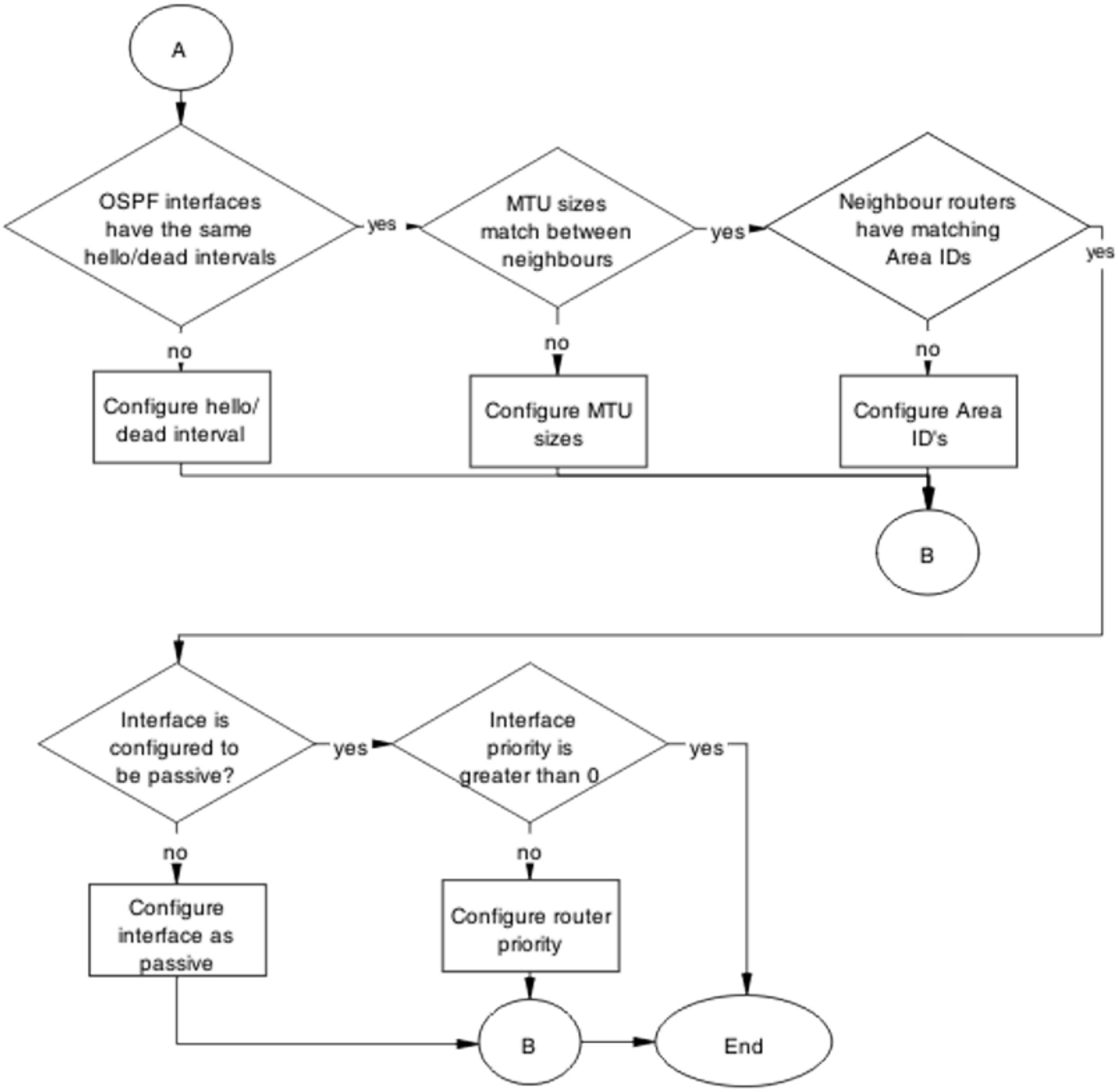

A
OSPF interfaces have the same hello/dead intervals
yes
MTU sizes match between neighbours
yes
Neighbour routers have matching Area IDs
yes
no
Configure hello/ dead interval
no
Configure MTU sizes
no
Configure Area ID's
B
Interface is configured to be passive?
yes
Interface priority is greater than 0
yes
no
Configure interface as passive
no
Configure router priority
B
End

Figure 98: Failure to Establish an OSPF adjacency part 2

Failure to Establish an OSPF adjacency navigation:

- Confirm IP connectivity on page 198
- Enable OSPF on interface on page 199
- Confirm Adjacencies on page 202
- Configure router IDs on page 204
- Correct mismatch on page 206
- Configure hello/dead interval on page 209
- Configure MTU sizes on page 212
- Configure area IDs on page 213

- Configure an interface to not be passive on page 215
- Configure router priority on page 217

Confirm IP connectivity

Isolate the IP connectivity for the devices.

Task flow: Confirm IP connectivity

The following task flow assists you to confirm IP connectivity on the network.

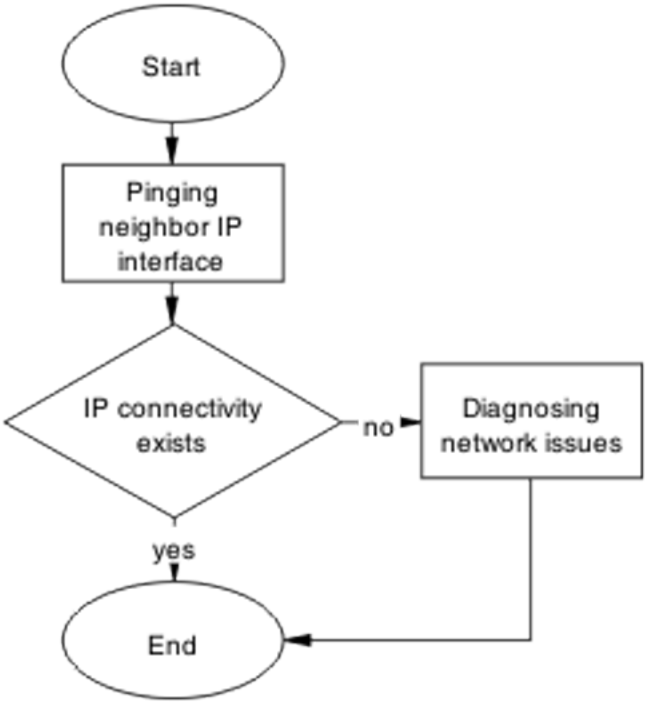


Figure 99: Confirm IP connectivity

Confirm IP connectivity navigation:

- Pinging IP Interface of neighbor on page 198
- Diagnosing network issues on page 199

Pinging IP Interface of neighbor

Identify IP connectivity to neighbor.

1. Enter the `ping <neighbor interface IP>` to ping the interface.
2. Observe the output during the ping execution to confirm connectivity.

Diagnosing network issues

Fundamental networking issues are to be resolved.

Follow local and vendor procedures to reestablish connectivity between devices.

Enable OSPF on interface

Enable OSPF on interface level to establish an adjacency.

Task flow: Enable the OSPF on interface

The following task flow assists you to enable OSPF on an interface.

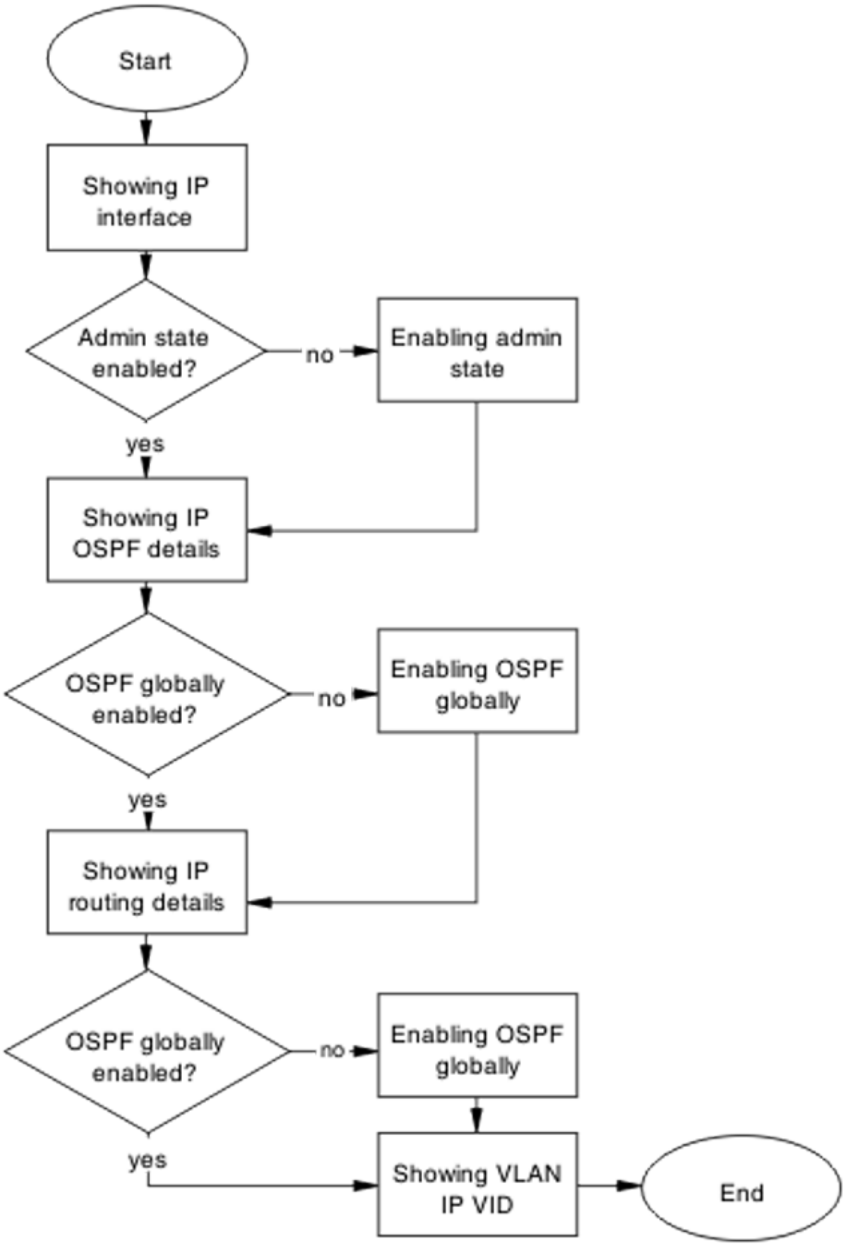


Figure 100: Enable OSPF on interface

Enable the OSPF on interface navigation:

- Showing IP Interface on page 201
- Enabling admin state on page 201
- Showing IP OSPF on page 201
- Enabling OSPF globally on page 201
- Showing IP routing on page 202

- Enabling OSPF globally on page 201
- Showing VLAN IP VID on page 202

Showing IP Interface

Display the IP interface information.

1. Use the **`show ip ospf interface vlan`** command.
2. Verify the admin state.

Enabling admin state

Enable the admin state of the switch.

1. Use the **`ip ospf interface vlan`** command to change the admin state.
2. Observe that no errors occur after execution.

Showing IP OSPF

Identify if OSPF is globally enabled.

1. Use the **`show ip ospf interface vlan <vid>`** command.
2. Verify if the OSPF is globally enabled.

Enabling OSPF globally

Enable the OSPF globally for the device.

1. Use the**`ip ospf interface vlan <vid>`** command.
2. Verify the change was made.

Showing IP routing

Display the IP routing information to verify that ip routing is enabled.

1. Use the **`show ip routing`** command to display the information.
2. Verify that IP routing is enabled.

Showing VLAN IP VID

Verify that the IP routing is enabled on the interface.

1. Use the **`show vlan ip vid <vid>`** command to display the interface IP status.
2. Observe the information displayed.

Confirm Adjacencies

Adjacencies between neighbor routers is to be formed in order for OSPF to function correctly.

Task flow: Confirm adjacencies

The following task flow assists you to verify the adjacencies between neighbor routers.

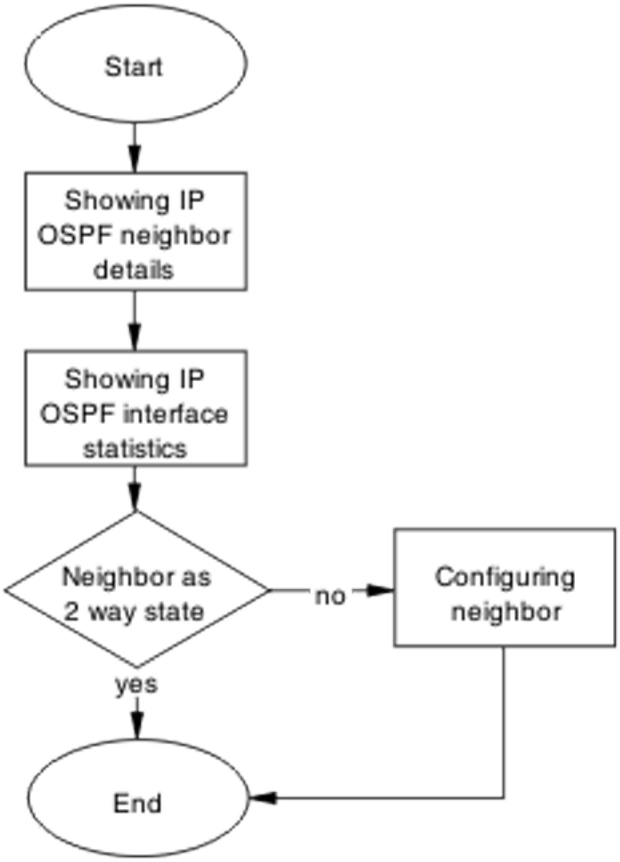

Start
Showing IP OSPF neighbor details
Showing IP OSPF interface statistics
Neighbor as 2 way state
no
Configuring neighbor
yes
End

Figure 101: Confirm adjacencies

Confirm adjacencies navigation:

- Showing IP OSPF neighbor on page 203
- Showing IP OSPF IP stats on page 204
- Configuring neighbor on page 204

Showing IP OSPF neighbor

Display the IP OSPF neighbor information.

1. Use the **`show ip ospf neighbor`** command.
2. Verify displayed information.

Showing IP OSPF IP stats

Display the IP OSPF neighbor information.

1. Use the **`show ip ospf ifstats`** command.
2. Note displayed information.

Configuring neighbor

Configure the neighbor device properly.

1. Follow vendor documentation to ensure the neighbor is configured correctly.
2. Verify displayed information.

Configure router IDs

Change the router ID as appropriate to ensure it is unique.

Task flow: Configure router IDs

The following task flow assists you to configure router IDs to ensure they are unique.

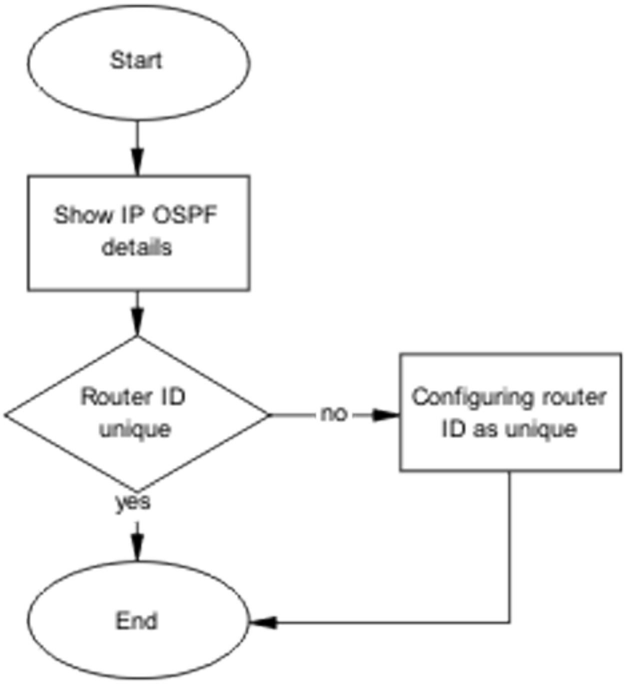


Figure 102: Configure router IDs

Configure router IDs navigation:

- Showing IP OSPF on page 205
- Configuring router ID as unique on page 205

Showing IP OSPF

Verify that the router ID is not the same for two routers within the OSPF domain. By default, router ID is derived from last 4 bytes of the base unit's MAC address. You are allowed to change this value at time.

1. Use the **`show ip ospf`** command.
2. Verify the Router ID. `Router ID: 0.0.0.1 .`

Configuring router ID as unique

Change the Router ID to ensure it is unique.

1. Use the **`enable`** command to enter userEXEC mode.
2. Use the **`configure terminal`** command to enter Privileged Executive mode.
3. Enter the configuration commands, one for each line,**`router ospf`** command.
    a. Use the **`router ospf`** command to enter the router OSPF configuration.
    b. Use the **`router-ID <A.B.C.D>`** command to assign the router ID.
4. Enter `Control-Z` to exit the configuration.

Correct mismatch

Correct mismatched authentication type settings, mismatched passwords, or message-digest settings.

Task flow: Correct mismatch

The following task flow assists you to correct mismatched authentication type, passwords, or message-digest settings.

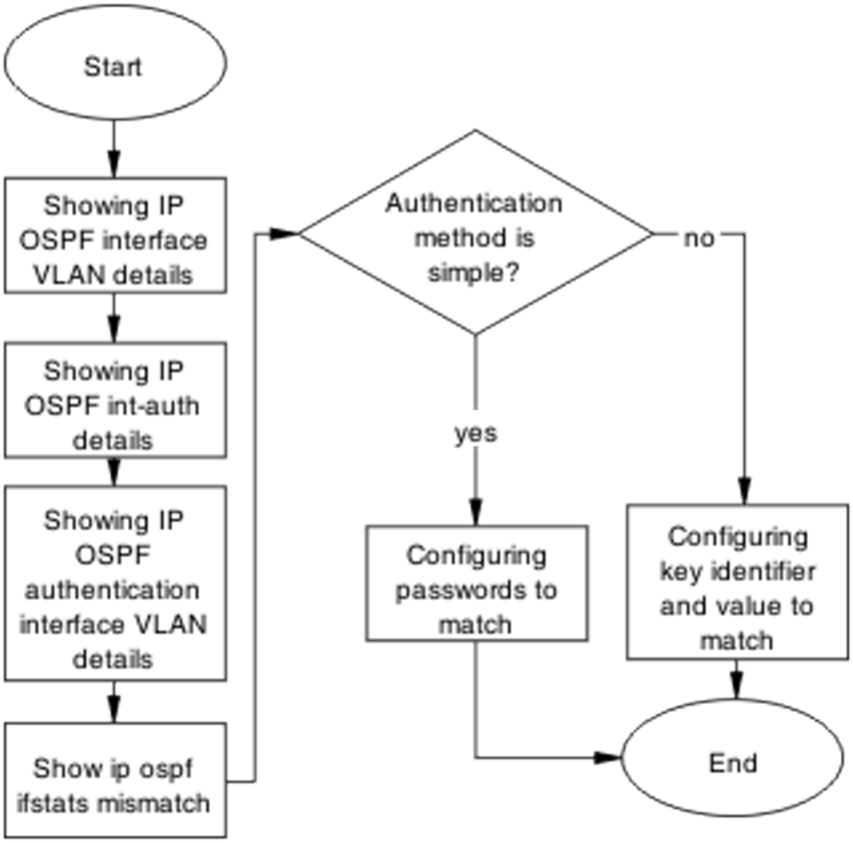

Start
Showing IP OSPF interface VLAN details
Showing IP OSPF int-auth details
Showing IP OSPF authentication interface VLAN details
Show ip ospf ifstats mismatch
Authentication method is simple?
no
yes
Configuring passwords to match
Configuring key identifier and value to match
End

Figure 103: Correct mismatch

Correct mismatch navigation:

- Showing IP OSPF interface VLAN on page 207
- Showing IP ospf int-auth on page 208
- Showing IP OSPF authentication interface VLAN on page 208
- Showing IP OSPF IFSTATS mismatch on page 208
- Configuring key identifier and value on page 208
- Configuring passwords to match on page 209

Showing IP OSPF interface VLAN

Display OSPF information for each VLAN interface.

1. Use the **`show ip ospf interface vlan <vid>`** command to display the authentication type.
2. Verify the authentication type: `Authentication Type: None` ..

Showing IP ospf int-auth

Display the authentication methods for all interfaces.

1. Use the **`show ip ospf int-auth`** command to display the authentication method.
2. Verify the displayed information.

Showing IP OSPF authentication interface VLAN

Displays the assigned MD5 IDs and keys.

1. Use the **`sho ip ospf authentication interface vlan <vid>`** command to display the IDs and keys.
2. Verify the displayed information.

Showing IP OSPF IFSTATS mismatch

Display statistics for mismatched OSPF parameters.

1. Use the **`show ip ospf ifstats mismatch`** command to display the mismatch counters.
2. Verify the mismatch counters type and fail.

Configuring key identifier and value

Both the key identifier and value must be matched.

1. Use the **enable** command to enter userEXEC mode.
2. Use the **configure terminal** command to enter Privileged Executive mode.
3. Enter the configuration commands:
    a. Use the **int vlan 2** command to enter the interface configuration.
    b. Use the **ip ospf message-digest-key <MD5 Key ID> md5 <password>** command to set the key.
    c. Use the **ip ospf authentication-type message-digest** command to set the authentication type.
4. Enter `Control-Z` on the keyboard to exit the configuration.

Configuring passwords to match

Passwords must match on both endpoints.

1. Use the **enable** command to enter userEXEC mode.
2. Use the **configure terminal** command to enter Privileged Executive mode.
3. Enter the configuration commands:
    a. Use the **int vlan 2** command to enter the interface configuration.
    b. Use the **ip ospf authentication-type simple** command to set the authentication type to simple.
    c. Use the **ip ospf authentication-key <password>** command to set the authentication key password.
4. Enter `Control-Z` on the keyboard to exit the configuration.

Configure hello/dead interval

Configure interfaces to use the same hello time and dead intervals on both OSPF endpoints. By default hello interval is 10 seconds and the dead interval is 40 seconds.

Task flow: Configure hello/dead interval

The following task flow assists you to use the same hello time and dead intervals.

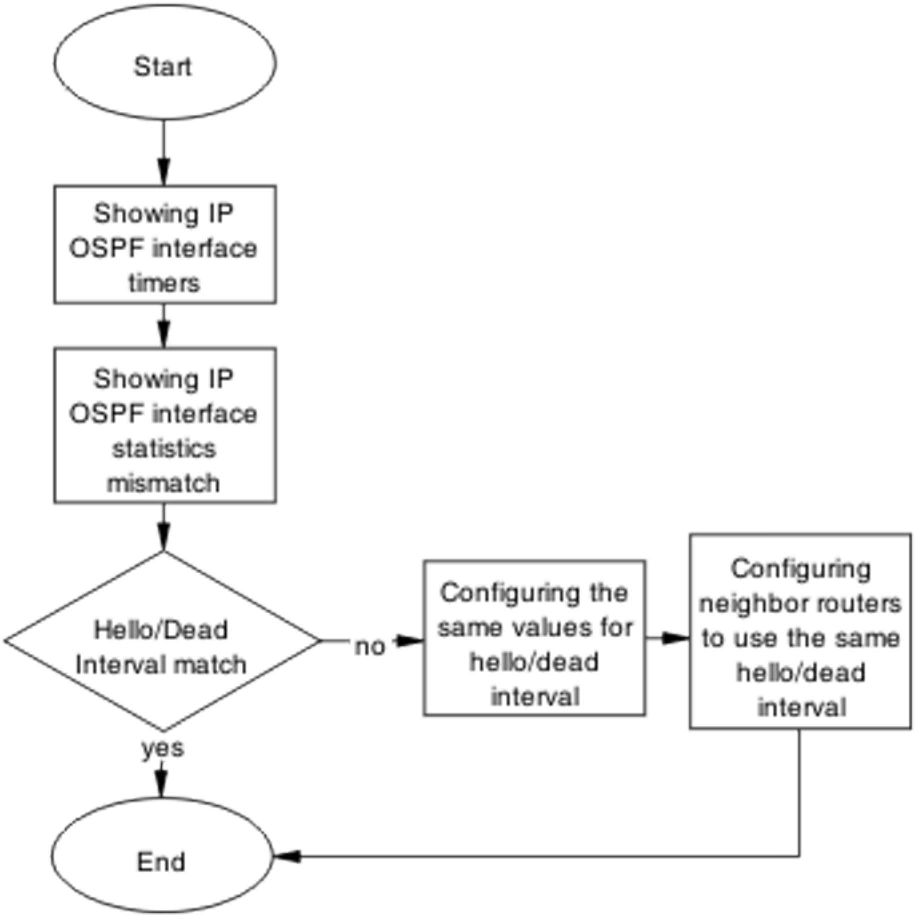

Start
Showing IP OSPF interface timers
Showing IP OSPF interface statistics mismatch
Hello/Dead Interval match
no
Configuring the same values for hello/dead interval
Configuring neighbor routers to use the same hello/dead interval
yes
End

Figure 104: Configure hello/dead interval

Configure hello/dead interval navigation:

- Showing IP OSPF interface timers on page 210
- Showing IP OSPF ifstats mismatch on page 211
- Configuring the same values for hello/dead interval on page 211
- Configuring neighbor routers to use the same hello/dead interval on page 211

Showing IP OSPF interface timers

Display OSPF timers for each interface.

1. Use the **`show ip ospf int-timers`** command to display the interface timer information.
2. Verify the displayed information.

Showing IP OSPF ifstats mismatch

Display statistics of each OSPF interface.

1. Use the **`show ip ospf ifstats mismatch`** command.
2. Verify the displayed information displayed.

Configuring the same values for hello/dead interval

Configure the same hello and dead-Intervals between neighbor routers.

1. Use the **`int vlan 50`** command to enter the configuration mode of the VLAN.
2. Use the **`ip ospf hello-interval 10`** command to configure the hello interval to 10.
3. Use the **`ip ospf dead-interval 40`** command to configure the dead interval to 40.
4. Following the vendor documentation, configure the neighbor router with the same parameters from steps 1 to 3.

Configuring neighbor routers to use the same hello/dead interval

Configure neighbor routers to use the same hello/dead interval values as configured on Avaya routers.

1. Reference vendor documentation to properly configure the neighbor routers.
2. Ensure the parameters are set as follows:
   - Hello interval is 10
   - Dead interval is 40

Configure MTU sizes

Match MTU sizes between neighboring routers so the neighbors will not remain in ExStart/ Exchange state.

Task flow: Configure MTU sizes

The following task flow assists you to configure the MTU sizes to match between neighboring routers.

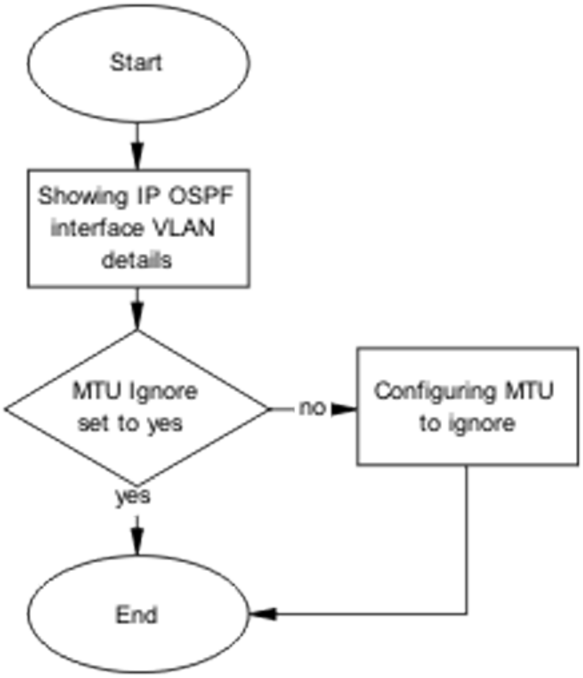

Start
Showing IP OSPF interface VLAN details
MTU Ignore set to yes
no
Configuring MTU to ignore
yes
End

Figure 105: Configure MTU sizes

Configure MTU sizes navigation:

- Showing IP OSPF interface VLAN on page 212
- Configuring MTU To ignore on page 213

Showing IP OSPF interface VLAN

This section provides troubleshooting guidelines for the displaying of the VLAN configuration for each interface OSPF configuration.

1. Use the **`show ip ospf interface vlan <vid>`** command.
2. Verify that MTU is set to Ignore: `MTU Ignore: Yes` .

Configuring MTU To ignore

Configure the receiving interface to accept incoming LSUs regardless of the packet's MTU size.

1. Use the **`enable`** command to enter userEXEC mode.
2. Use the **`configure terminal`** command to enter Privileged Executive mode.
3. Enter the configuration commands:
   1. Use the **`int vlan 2`** command to enter the interface configuration.
   2. Use the **`ip ospf mtu-ignore enable`** command to set the interface to ignore the MTU size.
4. Enter `Control-Z` on the keyboard to exit the configuration.

Configure area IDs

Configure neighboring routers to use matching area ID.

Task flow: Configure area ID

The following task flow assists you to match the area IDs between neighboring routers.

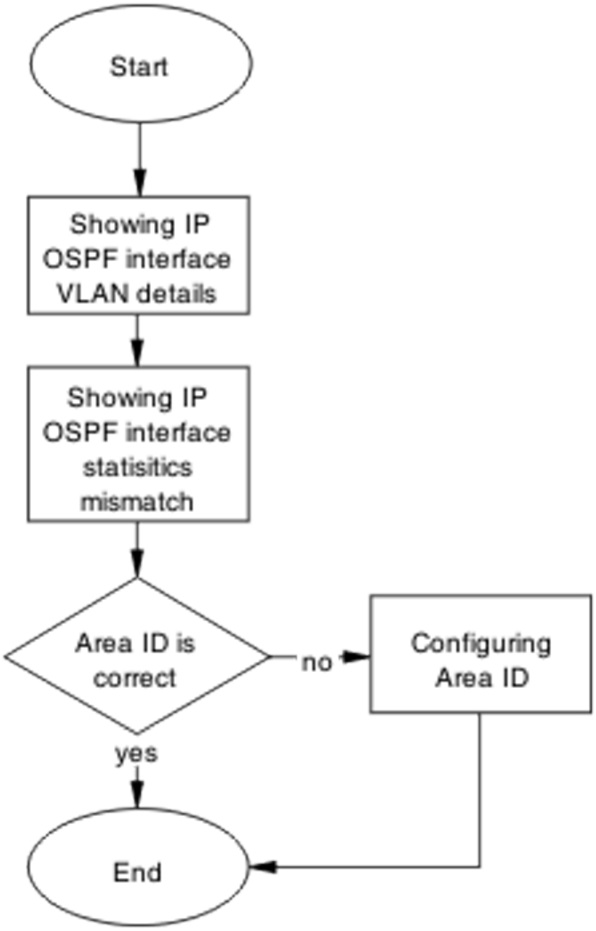

Start
Showing IP OSPF interface VLAN details
Showing IP OSPF interface statisitics mismatch
Area ID is correct
no
Configuring Area ID
yes
End

Figure 106: Configure area ID

Configure area ID navigation:

- Showing IP OSPF interface VLAN on page 214
- Showing IP OSPF IFSTATS mismatch on page 215
- Configuring Area IDs on page 215

Showing IP OSPF interface VLAN

Display configuration of each interface OSPF.

1. Use the **show ip ospf interface vlan <vid>** command.
2. Verify the Area ID.

Showing IP OSPF IFSTATS mismatch

Display the statistics for mismatched OSPF parameters.

1. Use the **`show ip ospf ifstats mismatch`** command.
2. Observe the mismatch OSPF parameters.

Configuring Area IDs

Configure the Area IDs to match.

1. Use the **`show ip ospf ifstats`** command to identify which area has an incorrect area attached.
2. Use the **`enable`** command to enter userEXEC mode.
3. Use the **`configure terminal`** command to enter Privileged Executive mode.
4. Enter the configuration commands:
    a. Use the **`router ospf`** command to enter the OSPF configuration.
    b. Use the **`network <ip> area <A.B.C.D>`** command to set the area ID.
5. Enter `Control-Z` on the keyboard to exit the configuration.

Configure an interface to not be passive

Configure an interface not to be passive. In this mode it does not send hello to its connected neighbors, or process hello from connected neighbors. By default, OSPF interfaces are type BROADCAST (not PASSIVE).

Task flow: Configure an interface to not be passive

The following task flow assists you to configure an interface to not be passive.

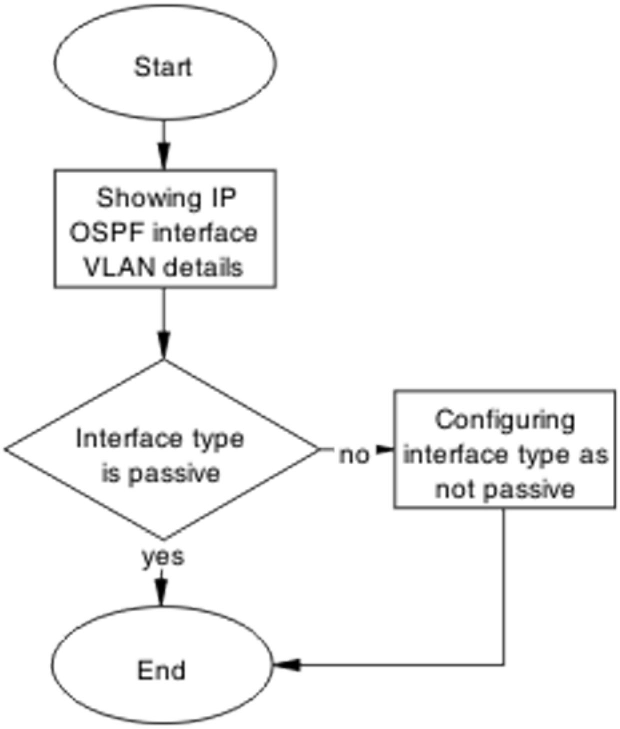

Start
Showing IP OSPF interface VLAN details
Interface type is passive
no
Configuring interface type as not passive
yes
End

Figure 107: Configure an interface to not be passive

Configure an interface to not be passive navigation:

- Showing IP OSPF interface VLAN on page 216
- Configuring interface type as not passive on page 216

Showing IP OSPF interface VLAN

Display the OSPF interface VLAN information.

1. Use the **`show ip ospf interface vlan <vid>`** command.
2. Verify `Type: Passive` .

Configuring interface type as not passive

Configure an interface not to be passive. In this mode it does not send Hello to its connected neighbors, or process Hello from connected neighbors. By default, OSPF interfaces are type BROADCAST (not PASSIVE).

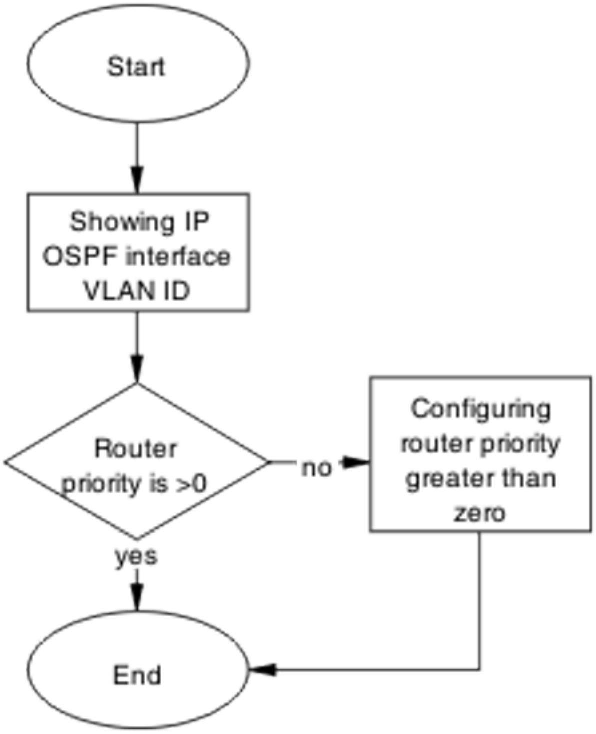
1. Use the **`show ip ospf interface vlan 2`** command to verify OSPF is not enabled on the interface on which you are planning to modify.
2. Use the **`int vlan 2`** command to enter the VLAN interface configuration.
3. Use the **`ip ospf network broadcast`** command to change the type to broadcast.
4. Use the **`ip ospf enable`** command to enable OSPF.

Configure router priority

Verify that the interfaces of all routers do not use a router priority of 0. At least one router must use a router priority of 1 or greater so that it can become the Designated Router (DR) for the network.

Task flow: Configure router priority

The following task flow assists you to change the router priority so that at least one has a priority higher than zero.


Start
Showing IP OSPF interface VLAN ID
Router priority is >0
no
Configuring router priority greater than zero
yes
End

Configure router priority navigation:

- Showing IP OSPF interface VLAN on page 218
- Configuring router priority greater than zero on page 218

Showing IP OSPF interface VLAN

Display the OSPF interface VLAN information

1. Use the **`show ip ospf interface vlan <vid>`** command.
2. Verify `Priority: 1 .`

Configuring router priority greater than zero

Configure the router so the priority is greater than zero.

1. Use the **`configure terminal`** command to enter Privileged Executive mode.
2. Enter the configuration commands:
    a. Use the **`int vlan 2`** command to enter the interface configuration.

   b. Use the **`ip ospf priority 1`** command to change the priority.

3. Enter `Control-Z` on the keyboard to exit the configuration.

OSPF route is not installed in routing table

Ensure that the OSPF route is properly in the routing table.

Work flow: OSPF route is not installed in routing table

The following work flow assists you to determine the solution for an OSPF route that is not installed in the routing table.

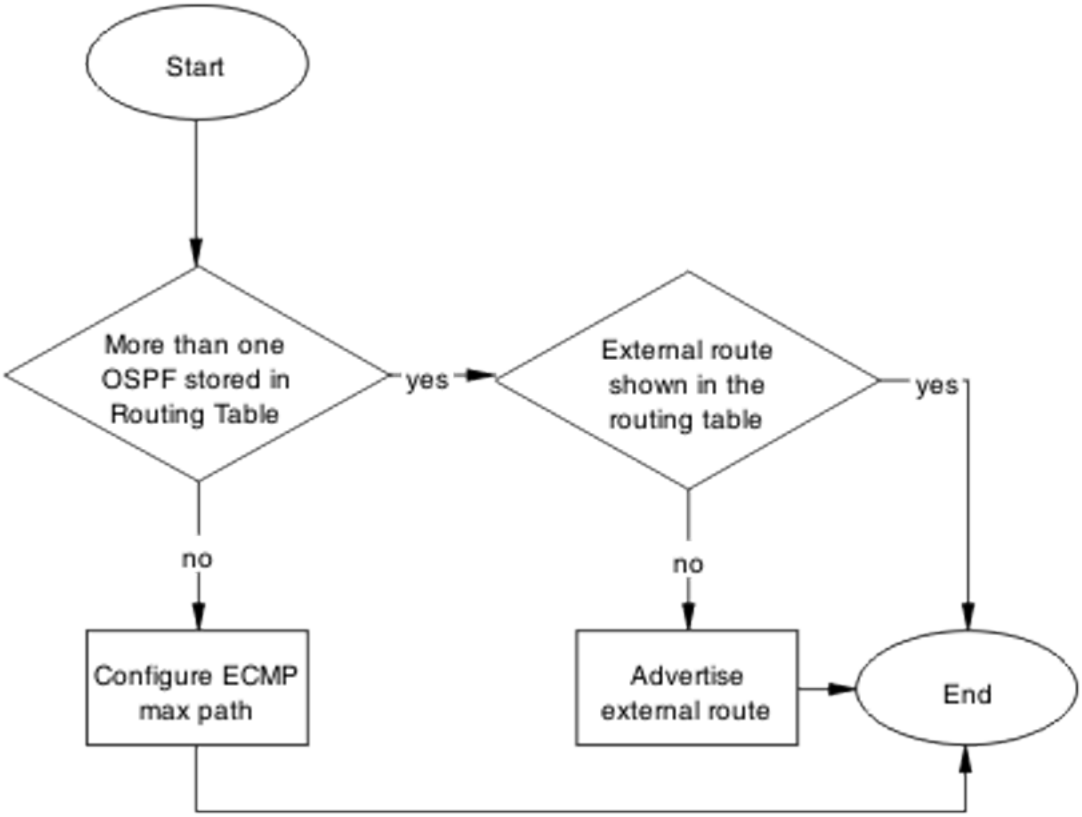

Start
More than one OSPF stored in Routing Table
yes
no
External route shown in the routing table
yes
no
Configure ECMP max path
Advertise external route
End

Figure 108: OSPF route is not installed in routing table

OSPF route is not installed in routing table navigation:

- Confirm ECMP max path on page 220
- Advertise external route on page 222

Confirm ECMP max path

Only one OSPF route is added into routing table for a reachable destination.

Task flow: Confirm ECMP max path

The following task flow assists you to ensure only one OSPF route is added to the routing table.

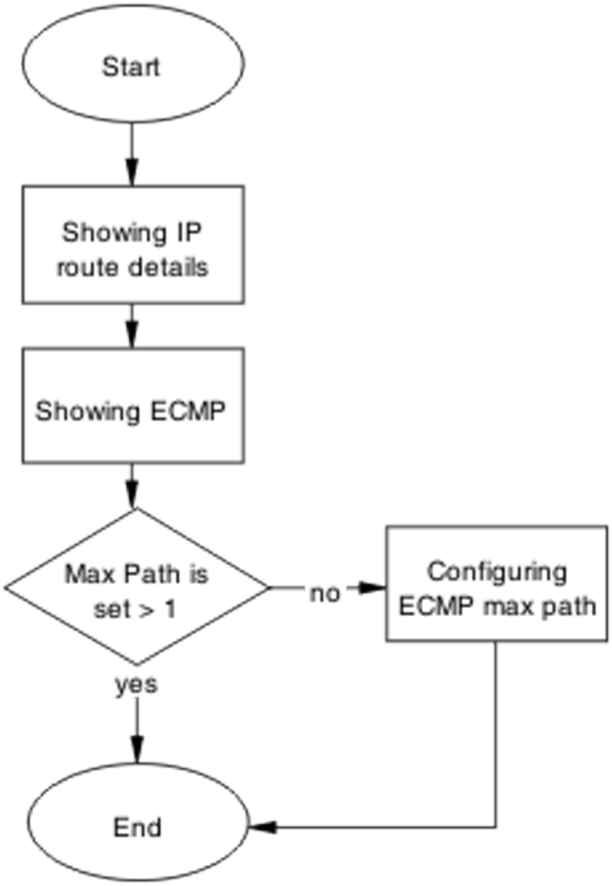


Figure 109: Confirm ECMP max path

Confirm ECMP max path navigation:

- Showing IP Route on page 221
- Showing ECMP on page 222
- Configuring ECMP on page 222

Showing IP Route

Display the routing table information.

Setting ECMP to allow multiple routes can be done on the ERS 5520/5530.

1. Enter the **`show ip route`** to display the routing information.
2. Use the **`show ip ospf redistribute`** command to view the redistribution policy.

Showing ECMP

Display the number of equal cost paths that will be installed in the routing table for the same destination. Supported protocols are Static, RIP and OSPF.

1. Enter the **`show ecmp`** to display the routing information.
2. Observe the displayed ECMP information.

Configuring ECMP

To use more routes (max 4) to the same destination with the same cost learned by RIP, you are to enable the ECMP.

An ECMP license is required to enable this feature.

1. Use the **`enable`** command to enter UserEXEC mode.
2. Use the **`configure terminal`** command to enter Privileged Executive mode.
3. Use the **`rip maximum-path <number)`** command to configure the maximum number of ECMP paths.
4. Use the **`show ecmp`** command to show the new ECMP settings.

Advertise external route

Ensure that the external route is advertised by Autonomous System Border Router (ASBR) as Link-State Advertisement (LSA) type-5 or type-7.

Task flow: Advertise external route

The following task flow assists you to ensure that the external route is advertised.

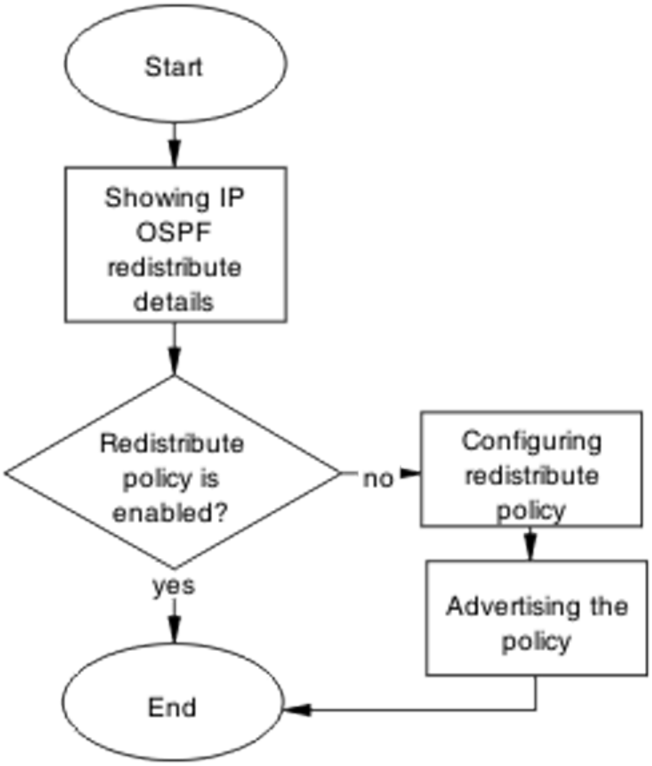

Start
Showing IP OSPF redistribute details
Redistribute policy is enabled?
no
Configuring redistribute policy
Advertising the policy
yes
End

Figure 110: Advertise external route

Advertise external route navigation:

- Showing IP OSPF redistribute on page 223
- Configuring Redistribute Policy on page 223

Showing IP OSPF redistribute

Display the routing table information.

Setting ECMP to allow multiple routes can be done on 5520/5530.

1. Enter the **`show ip ospf redistribute`**.
2. Review the policy displayed.

Configuring Redistribute Policy

Redistribute external routes into OSPF network.

1. Enter the **`router ospf`** to modify the redistribution policy.
2. Use the **`as-boundary-router enable`** command to command to make the router ASBR.
3. Use the **`redistribute rip/direct/static enable`** command to enable external route redistribution into the OSPF domain.
4. Use the **`ip ospf apply redistribute`** command to apply the changes.

RIP packets exchanged between device under test (DUT) but no routes are learned

Ensure that routes are learned between devices under test.

Work flow: RIP packets exchanged between device under test (DUT) but no routes are learned

The following work flow assists you to determine the solution for routes not being learned between devices under test while RIP packets are being exchanged.

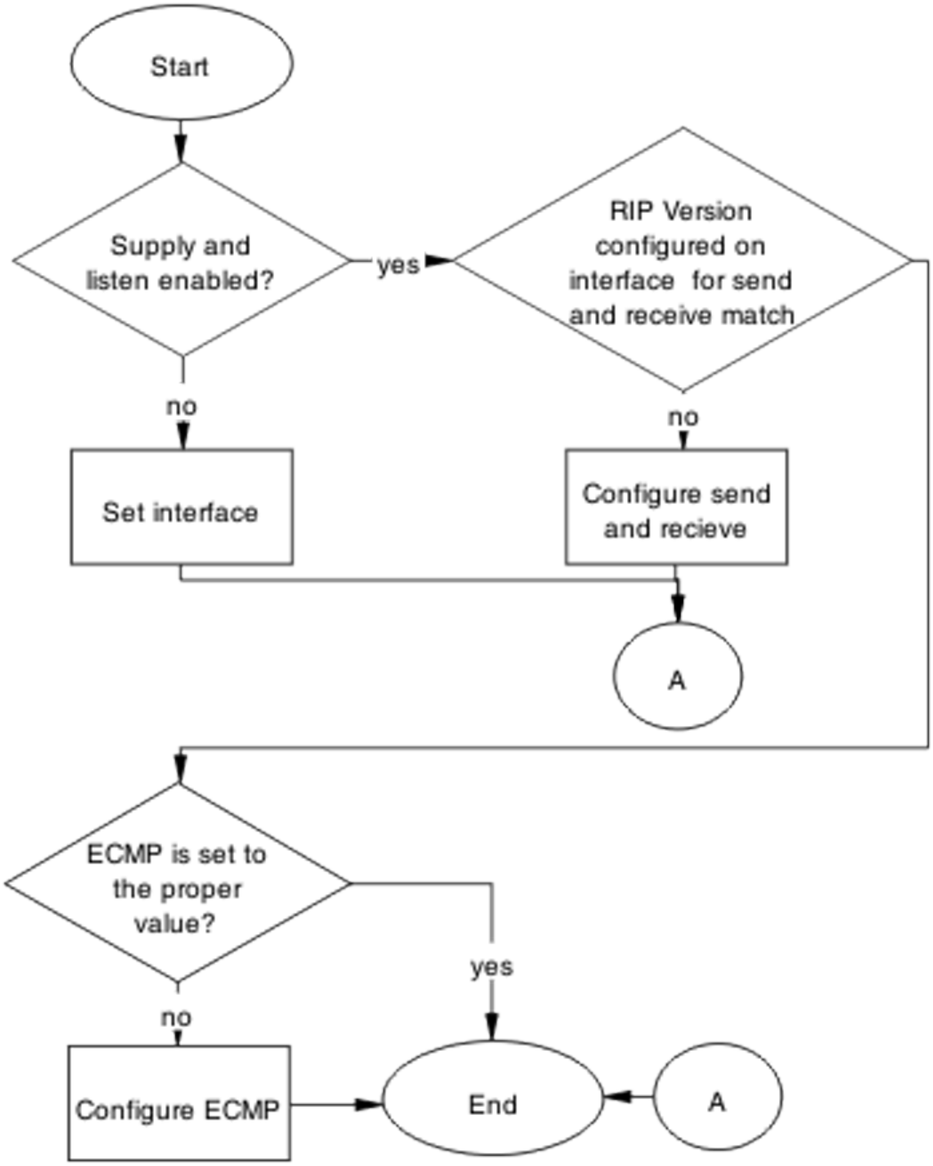

Start
Supply and listen enabled?
yes
no
RIP Version configured on interface for send and receive match
no
Set interface
Configure send and recieve
A
ECMP is set to the proper value?
yes
no
Configure ECMP
End
A

Figure 111: RIP Packets exchanged between device under test (DUT) but no routes are learned

RIP Packets exchanged between device under test (DUT) but no routes are learned navigation:

- Set interface on page 226
- Configure send and receive on page 227
- Configure ECMP on page 229

Set interface

Set the interface to verify the RIP interfaces are configured to both supply and listen to RIP updates.

Task flow: Set interface

The following task flow assists you to configure interfaces for supply and listen to RIP updates.

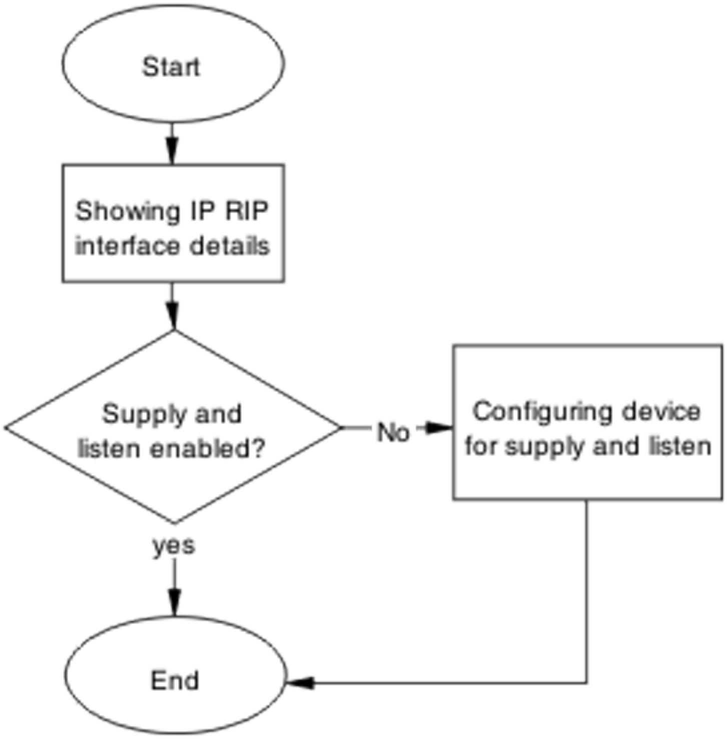

Start
Showing IP RIP interface details
Supply and listen enabled?
No
Configuring device for supply and listen
yes
End

Figure 112: Set interface

Set interface navigation:

- Showing RIP IP interface on page 226
- Configuring device for supply and listen on page 227

Showing RIP IP interface

Display the RIP interface information.

1. Enter the **`show ip rip interface`** command.
2. Review displayed information to verify if the RIP version configured on interface for receive and send match each other.

Configuring device for supply and listen

Verify the ports expected to send/receive RIP updates are not in STP blocking state.

1. Use the **`show ip rip interface`** command to display the information.
2. Ensure the supply/listen options are enabled. If not, use the following commands in sequence:
    a. The **`enable`** command to enter userEXEC mode.
    b. The **`configure terminal`** command to enter Privileged Executive mode.
    c. The **`interface vlan <1-4094>`** command to enter the interface VLAN.
    d. The **`ip rip supply/listen enable`** command to enable the supply/listen.
    e. The **`exit`** command to exit the configuration.

Configure send and receive

Verify the RIP version configured on both sending and receiving interfaces match.

Task flow: Configure send and receive

The following task flow assists you to ensure the RIP versions match on the sending and receiving interfaces.

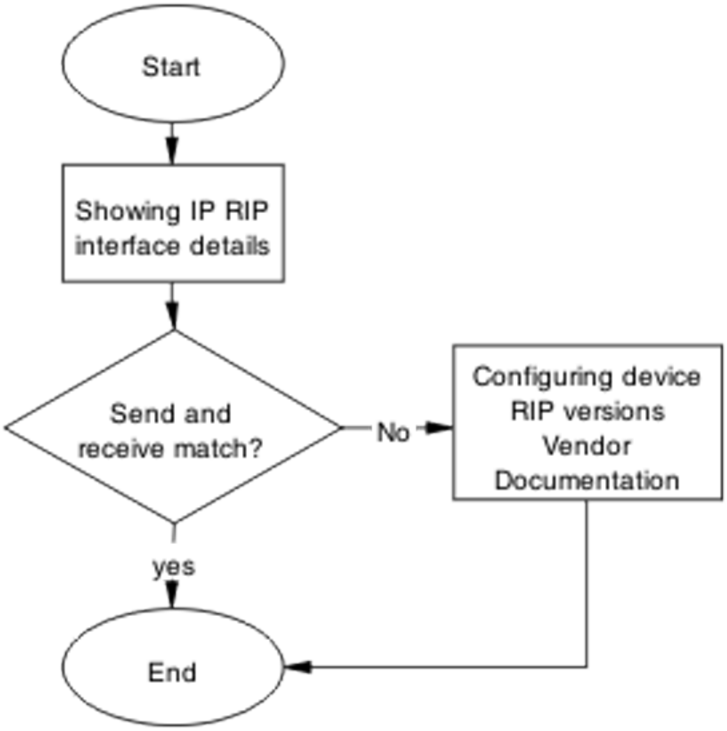

Start
Showing IP RIP interface details
Send and receive match?
No
Configuring device RIP versions Vendor Documentation
yes
End

Figure 113: Configure send and receive

Configure send and receive navigation:

- Showing RIP IP interface on page 228
- Configuring device RIP versions on page 228

Showing RIP IP interface

Display the RIP interface information

1. Enter the **`show ip rip interface`** command.
2. Review displayed information to verify if the RIP version configured on interface for receive and send match each other.

Configuring device RIP versions

Configure the device to send and receive RIP packets.

1. Use the **`show ip rip interface`** command to display the interface information.
2. Ensure the send/receive options of the sending/receiving interfaces match. If not, use the following commands in sequence:
    a. The **`enable`** command to enter userEXEC mode.
    b. The **`configure terminal`** command to enter Privileged Executive mode.
    c. The **`interface vlan <1-4096>`** command to enter the interface.
    d. **`ip rip send version notsend/rip1/rip1comp/rip2`**.
    e. **`ip rip receive version rip1/rip1orrip2/rip2`**.

Configure ECMP

Set ECMP to proper value.

Task flow: Configure ECMP

The following task flow assists you to set the value of ECMP.

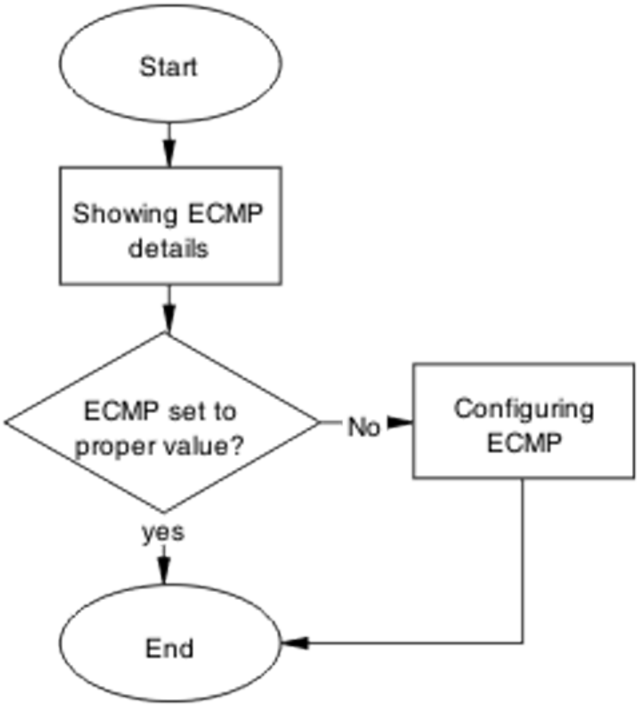


Figure 114: Configure ECMP

Configure ECMP navigation:

- Showing ECMP details on page 230
- Configuring ECMP on page 230

Showing ECMP details

Ensure that ECMP is set to the proper value the ports with ECMP paths are not STP blocked.

1. Enter the **`show ecmp`** command to display the ECMP information.
2. Review the displayed ECMP information.

Configuring ECMP

To use more routes (max 4) to the same destination with the same cost learned by RIP, you are to enable the ECMP.

Prerequisites:

An ECMP license is required to enable this feature.

1. Use the **enable** command to enter UserEXEC mode.
2. Use the **configure terminal** command to enter Privileged Executive mode.
3. Use the **rip maximum-path 4** command to configure the maximum number of ECMP paths.
4. Use the **show ecmp** command to show the new ECMP settings.

RIP routes are learned-deleted learned again

Timeout interval on the bouncing DUT must not be smaller than update interval on the peer DUT.

Task flow: RIP routes are learned-deleted learned again

The following task flow assists you to change the timeout interval to stop the RIP routed from being deleted after being learned.

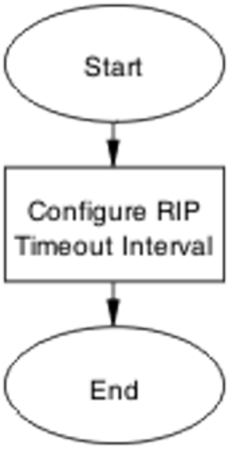


Figure 115: RIP routes are learned-deleted learned again

RIP routes are learned-deleted learned again navigation:

- Configuring RIP timeout interval on page 232

Configuring RIP timeout interval

Configure the timeout interval on the bouncing DUT must not be smaller than update interval on the peer DUT.

Task flow: Configure RIP timeout interval

The following task flow assists you to ensure the timeout and update intervals are appropriate for DUTs.

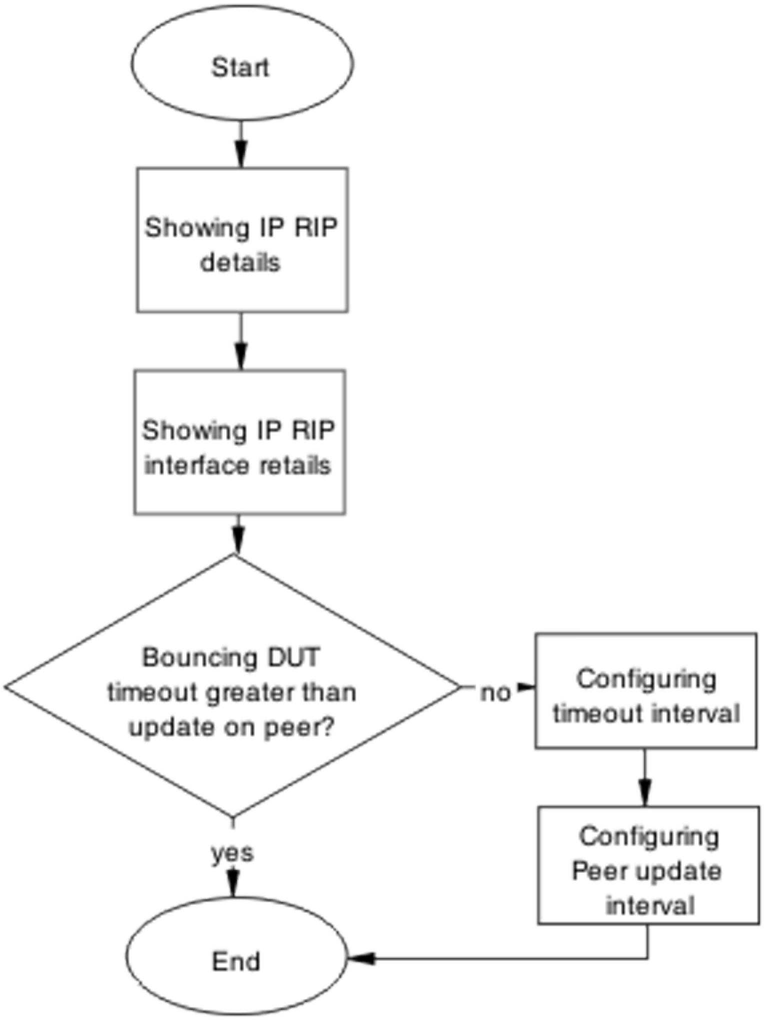

Start
Showing IP RIP details
Showing IP RIP interface retails
Bouncing DUT timeout greater than update on peer?
no
Configuring timeout interval
Configuring Peer update interval
yes
End

Figure 116: Configure RIP timeout interval

Configure RIP timeout interval navigation:

- Showing IP RIP on page 233
- Showing RIP IP interface on page 234
- Configuring timeout Interval on page 234
- Configuring peer update interval on page 234

Showing IP RIP

Display the IP RIP information to observe the timeout intervals.

1. Use the show ip rip command to display the RIP information.
2. Observe the timeout intervals.

Showing RIP IP interface

Display the IP RIP interface information to observe the timeout intervals.

1. Enter the **`show ip rip interface`** .
2. Observe the timeout intervals.

Configuring timeout Interval

Configure the timeout interval to correct the learning and relearning behavior.

1. Use the **`enable`** command to enter User Executive mode.
2. Use the **`configure terminal`** command to Privileged Executive mode.
3. Use the **`router rip`** command to enter router configuration mode.
4. Use the **`timers basic timeout 30`** command to change the timeout settings.
5. Use the **`exit`** command to leave the current mode.
6. Use the **`show ip rip`** command to review the current settings.

Configuring peer update interval

Configure the peer update timeout interval.

1. Use the **`enable`** command to enter User Executive mode.
2. Use the **`configure terminal`** command to Privileged Executive mode.
3. Use the **`router rip`** command to enter router configuration mode.
4. Use the **`timers basic update 10`** command to change the update settings.

5. Use the **`exit`** command to leave the current mode.
6. Use the **`show ip rip`** command to review the current settings.

RIP routes learned with increasing cost

In some unstable networks with potential loops, routes are learned with increasing cost (until 16) even though the actual route is gone.

Work flow: RIP routes learned with increasing cost

The following work flow assists you to determine the solution for RIP routes that continue to be learned with an increasing cost.

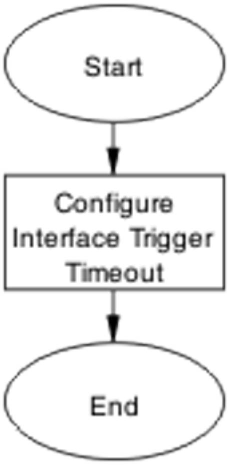


Figure 117: RIP routes learned with increasing cost

RIP routes learned with increasing cost navigation:

- Configure interface trigger timeout on page 235

Configure interface trigger timeout

Configure triggered updates to force the DUT to send RIP updates immediately after a RIP interface goes down, announcing the rest of the network.

Task flow: Configure interface trigger timeout

The following task flow assists you to configure the interface trigger timeout to send RIP updates after a device goes down.

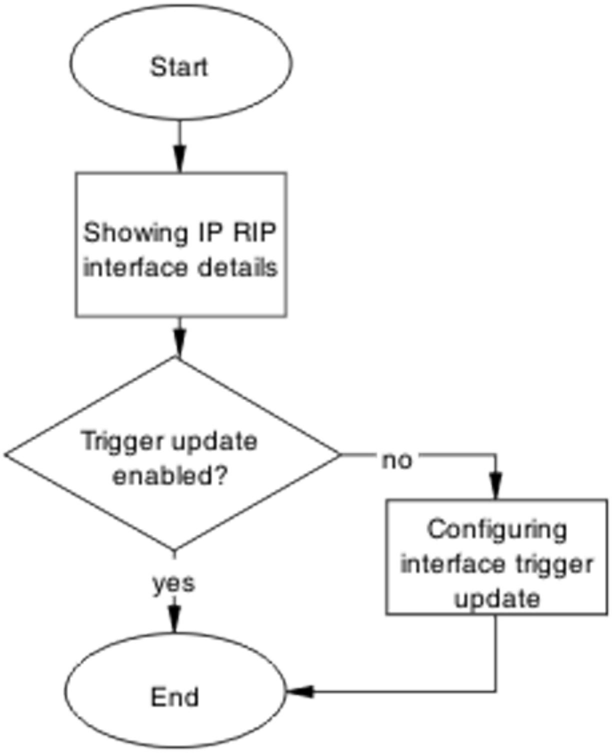

Start
Showing IP RIP interface details
Trigger update enabled?
no
Configuring interface trigger update
yes
End

Figure 118: Configure interface trigger timeout

Configure interface trigger timeout navigation:

- Showing IP RIP interface on page 236
- Configuring interface trigger update on page 237

Showing IP RIP interface

Display the IP RIP interface information for the ERS 5500 series device.

1. Use the **`show ip rip interface`** command to display the RIP interface information.
2. Observe the trigger update.

Configuring interface trigger update

Change the trigger update to enabled.

1. Use the **`enable`** command to enter User Executive mode.
2. Use the **`configure terminal`** command to Privileged Executive mode.
3. Use the **`interface vlan x`** command to enter VLAN Interface configuration mode.
4. Use the **`ip rip triggered enable`** command to change the update settings.

SMLT routing issue

Ensure that the SMLT is routing packets properly.

Work flow: SMLT routing issue

The following work flow assists you to determine the solution for routing issues under SMLT.

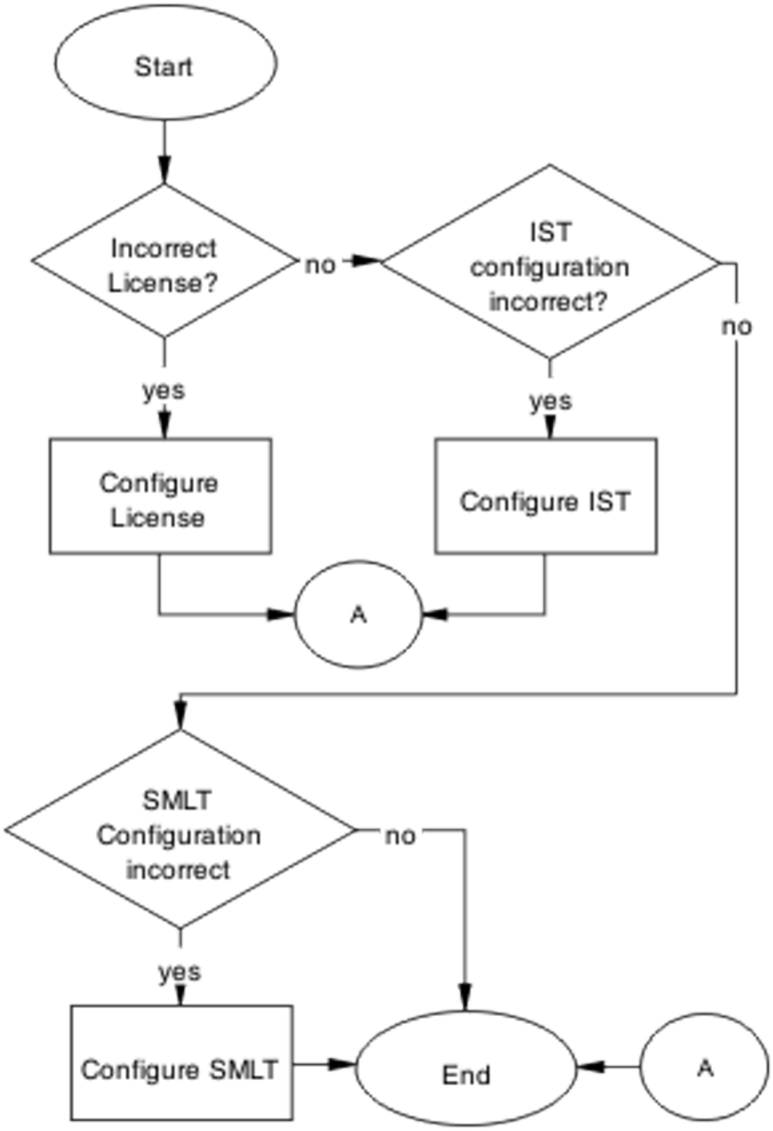


Figure 119: SMLT routing issue

SMLT routing issue navigation:

- Configure License on page 238
- Configure IST on page 240
- Configure SMLT on page 245

Configure License

Ensure the SMLT license is present in order in to operate correctly.

Task flow: Configure license

The following task flow assists you to configure the license for SMLT.

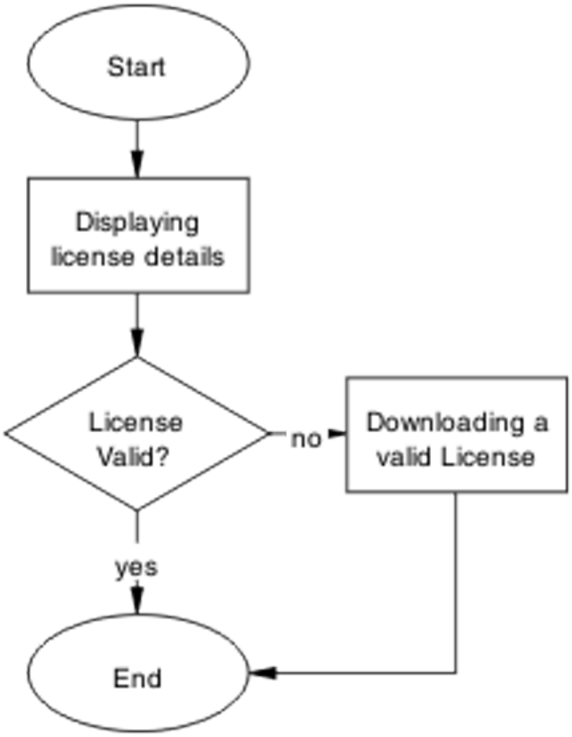


Figure 120: Configure license

Configure license navigation:

- Displaying license details on page 239
- Downloading a valid license on page 240

Displaying license details

View license information about the edge and aggregation devices.

1. Use the **`show license all`** command to display the status of the license installed on the device.
2. Observe the displayed information.

Downloading a valid license

Download the valid license to the switch.

Refer to document *Avaya Ethernet Routing Switch 5500 Series Configuration — System* (NN47200-500) for license download instructions.

Configure IST

Set IST to ensure routing is correctly configured.

Task flow: Configure IST

The following task flow assists you to configure IST to ensure the routing is correctly configured.

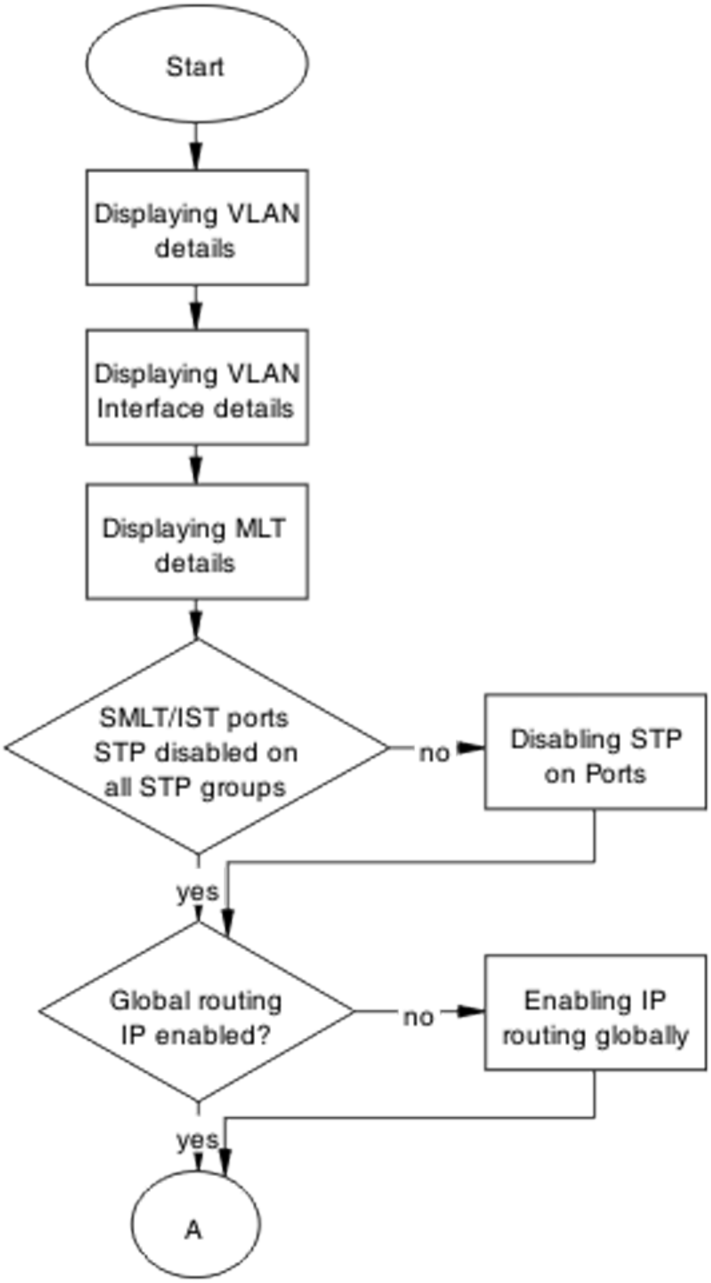

Start
Displaying VLAN details
Displaying VLAN Interface details
Displaying MLT details
SMLT/IST ports STP disabled on all STP groups
no
Disabling STP on Ports
yes
Global routing IP enabled?
no
Enabling IP routing globally
yes
A

Figure 121: Configure IST part 1

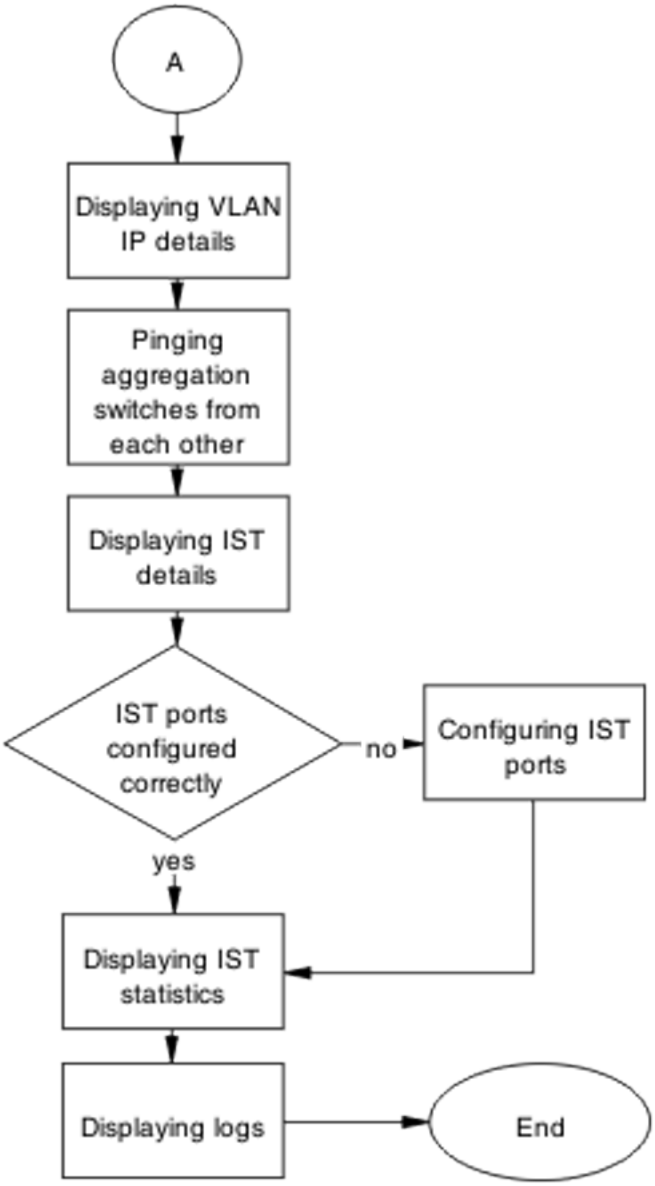

A
Displaying VLAN IP details
Pinging aggregation switches from each other
Displaying IST details
IST ports configured correctly
no
Configuring IST ports
yes
Displaying IST statistics
Displaying logs
End

Figure 122: Configure IST part 2

Configure IST navigation:

- Displaying VLAN details on page 243
- Displaying VLAN interface details on page 243
- Displaying MLT details on page 243
- Disabling STP on ports on page 243
- Enabling IP routing globally on page 244
- Displaying VLAN IP details on page 244

- Pinging aggregation switches from each other on page 244
- Configuring IST ports on page 244
- Displaying IST statistics on page 245
- Displaying logs on page 245

Displaying VLAN details

View the information to ensure the same VLAN configured on both ends of the IST. The IST owner VLAN is to contain only the IST ports.

1. Use the **`show vlan`** command to display the VLAN ports membership for the VLANs.
2. Observe the displayed information.

Displaying VLAN interface details

Ensure that the port members in the IST owner VLAN are tagged.

1. Use the **`show vlan interface info`** command to display the vlan operation for IST ports.
2. Observe the displayed information.

Displaying MLT details

Show the MLT information to ensure the IST is an MLT.

1. Use the **`show mlt`** command to display the MLT configuration.
2. Confirm that the EDGE device links to aggregation devices are forming a MLT.

Disabling STP on ports

View the spanning tree port to disable spanning-tree participation for the IST and SMLT ports connected to the EDGE.

1. Use the **`show spanning-tree port`** command to display the spanning-tree participation for ports.
2. Observe the displayed information.

Enabling IP routing globally

View the IP routing information

1. Use the **`ip routing`** command to display the status of IP routing.
2. Enable the IP routing.

Displaying VLAN IP details

Display the VLAN IP information.

1. Enter the **`show vlan ip`** to show the IP.
2. Observe the displayed information.

Pinging aggregation switches from each other

Test the IP connection between two switches.

1. Use the **`ping <switch2>`** from the first switch.
2. Use the **`ping <switch1>`** from the second switch.

Configuring IST ports

View the IST configuration and operational mode.

1. Enter the **`show ist`** command to display the IST configuration and operational mode.
2. Observe the displayed information.

Displaying IST statistics

Check the counters between two aggregate switches for messages.

1. Enter the **`show ist stat`** command to show the status of the IST protocol.
2. Observe the displayed information.

Displaying logs

Check the logging to see possible messages related to IST.

1. Enter the **`show logging`** command to review the log messages.
2. Observe the displayed information.

Configure SMLT

Configure SMLT to ensure it is functioning correctly.

Task flow: Configure SMLT

The following task flow assists you to properly configure SMLT.

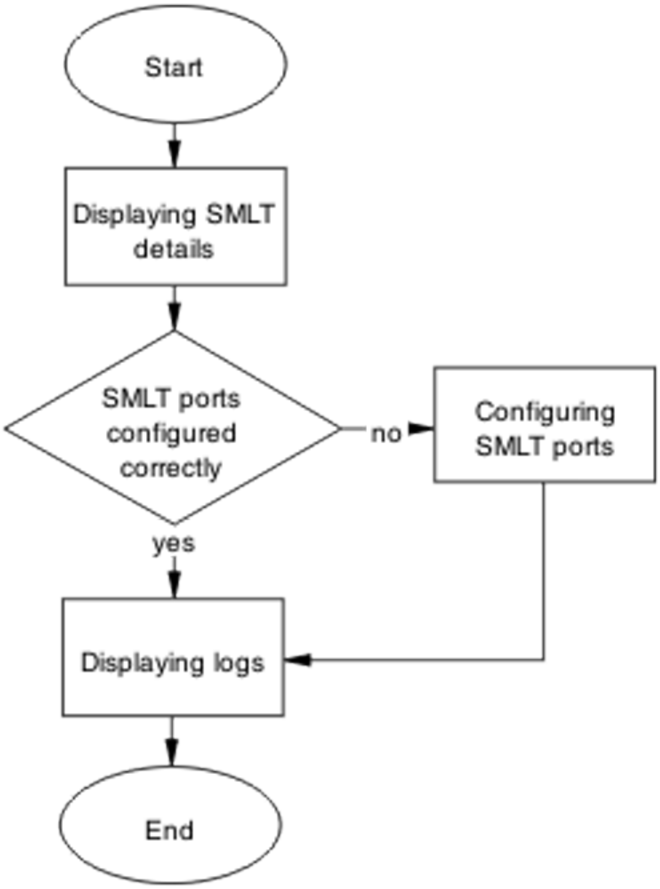


Figure 123: Configure SMLT

Configure SMLT navigation:

- Displaying SMLT details on page 246
- Configuring SMLT ports on page 247
- Displaying logs on page 247

Displaying SMLT details

View the SMLT configuration to make sure that links from EDGE device to both aggregation devices are up.

1. Enter the **`show smlt`** command to display the SMLT configuration and operational mode.
2. Observe the displayed information.

Configuring SMLT ports

Configure the SMLT on the ports.

1. Enter the **`smlt port <portlist> <1-512>`** command to change the SMLT configuration.
2. Observe no errors after program execution.

Displaying logs

Check the logging to see possible messages related to SMLT.

1. Use the **`show logging`** command to review log messages.
2. Observe the displayed information.

VR is stuck in initialize state when it should be master or backup

Correct a Virtual Rack to be master or backup.

VR is stuck in initialize state when it should be master or backup work flow

The following work flow assists you to determine the solution for VR is stuck in initialize state when it should be master or backup.

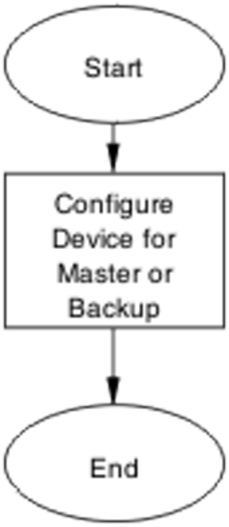


Figure 124: VR is stuck in initialize state when it should be master or backup

VR is stuck in initialize state when it should be master or backup work flow navigation:

- Configure device for master or backup on page 248

Configure device for master or backup

Set the device for master or backup under VRRP.

Task flow: Configure device for master or backup

The following task flow assists you to configure the device as master or backup.

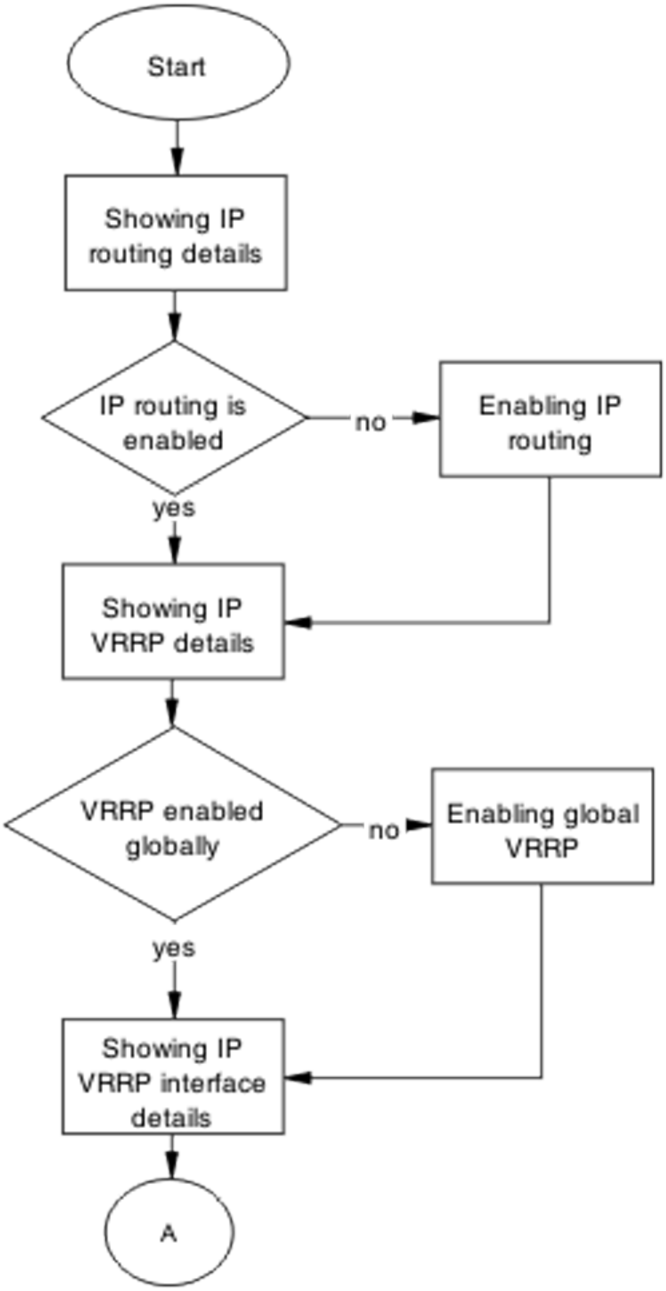


Figure 125: Configure device for master or backup part 1

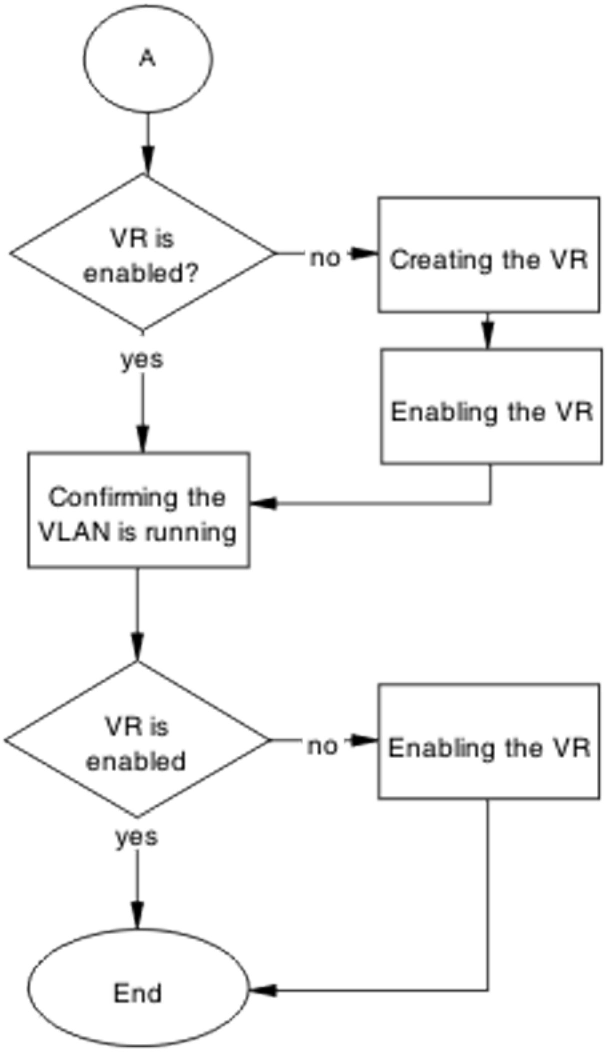


Figure 126: Configure device for master or backup part 2

Configure device for master or backup navigation:

- Showing IP routing details on page 251
- Enabling IP routing on page 251
- Showing IP VRRP details on page 251
- Enabling global VRRP on page 251
- Showing IP VRRP interface details on page 252
- Creating the VR on page 252
- Enabling the VR on page 252
- Confirming VLAN is running on page 252

Showing IP routing details

Verify that IP routing is enabled.

1. Use the command **`show ip routing`**.
2. Observe the displayed information.

Enabling IP routing

IP routing is to be globally enabled on the switch.

1. Use **`ip routing`** global configuration mode command to enable ip routing globally on switch.
2. Observe no errors after execution.

Showing IP VRRP details

Verify that VRRP is enabled globally.

1. Use the command **`show IP VRRP`**.
2. Observe the displayed information.

Enabling global VRRP

This procedure assists you to enable VRRP globally.

1. Use **`router vrrp enable`** global configuration mode command to enable VRRP globally on the ERS 5500 Series device.
2. Observe no errors after execution.

Showing IP VRRP interface details

Verify that the VR itself is enabled.

1. Use the command **`show ip vrrp interface`**.
2. Verify that the admin state is `UP` .

Creating the VR

The following procedure assists you to create a VR.

1. Use the **`ip vrrp address <VR ID=1-255> <vr ip address A.B.C.D>`** command to create the VR router for the specified ID on the respective VLAN.
2. Observe no errors after execution.

Enabling the VR

The following procedure assists to enable the VR that was created.

1. Use the **`ip vrrp <1-255> enable`** VLAN interface configuration mode command to enable the VR on the respective VLAN.
2. Observe no errors after execution.

Confirming VLAN is running

Verify that the VR itself is enabled.

1. Use the command **`ip vrrp`**.
2. Confirm at least one active link.

VR is stuck in master state when it should be backup (more than one master is present in a VR)

Correct a device that is stuck in a master state although it should be backup.

Work flow: VR stuck in master state when it should be backup (more than one master is present in a VR)

The following workflow assists you to determine the solution for a VR being stuck in the master state when it should be a backup.

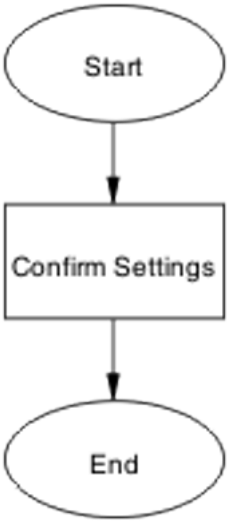


Figure 127: VR stuck in master state when it should be backup (more than one master is present in a VR)

VR stuck in master state when it should be backup (more than one master is present in a VR) navigation:

- Confirm settings on page 253

Confirm settings

Confirm the VRRP settings that are configured on the device.

Task flow: Confirm settings

The following task flow assists you to verify the settings that are configured on the ERS 5500 series device.

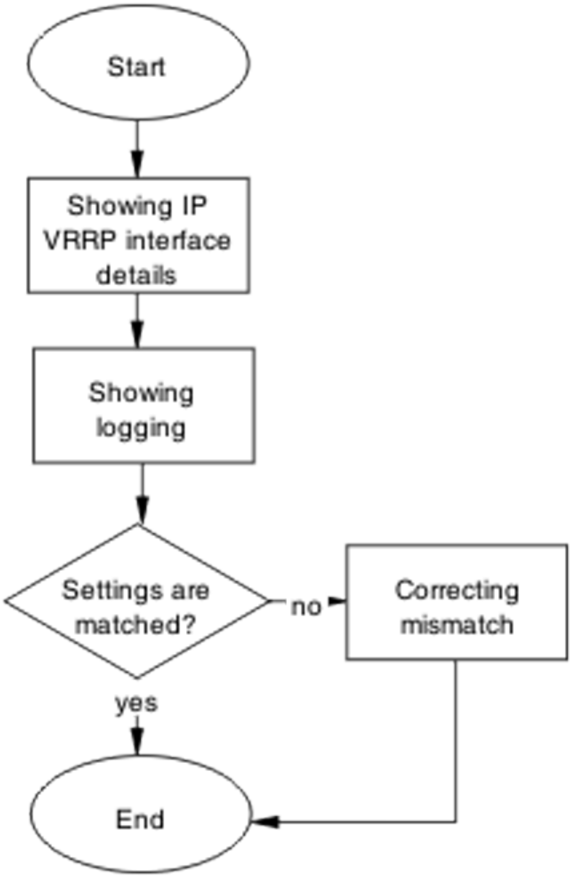


Figure 128: Confirm settings

Confirm settings navigation:

- Showing IP VRRP interface details on page 254
- Showing logging on page 255
- Correcting mismatch on page 255

Showing IP VRRP interface details

Verify critical information for the VRRP interface.

1. Use the command **`show ip vrrp interface verbose`**.
2. Verify VR is not in holddown state.
3. Verify that the corresponding VLAN is up for the critical IP feature is enabled and the critical IP address is set to one of the local L3 VLANs IP.

Showing logging

Obtain log messages for the device.

1. Use the **`show logging`** command to display device log messages.
2. Search log messages mismatch information.

Correcting mismatch

Configure the VRRP interface eliminate the mismatch.

1. Use the command **`ip vrrp interface`** to configure the interface.
2. Observe no errors after execution.

VR is stuck in backup state when it should be master (no master is present across the VR)

Configure a device to be the master when it is stuck in backup state.

Work flow: VR is stuck in master state when it should be backup (no master is present in a VR)

The following work flow assists you to determine the solution for a VR that is stuck in master state when it should be backup and no master is present in the VR

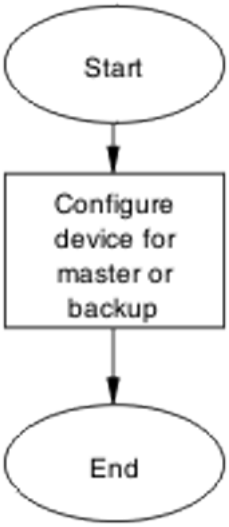


Figure 129: VR is stuck in master state when it should be backup (no master is present in a VR)

VR is stuck in master state when it should be backup (no master is present in a VR) navigation:

- Configure device for master or backup on page 256

Configure device for master or backup

Set the device to be the master or backup.

Task flow: Configure device for master or backup

The following task flow assists you to configure the device as a master or backup.

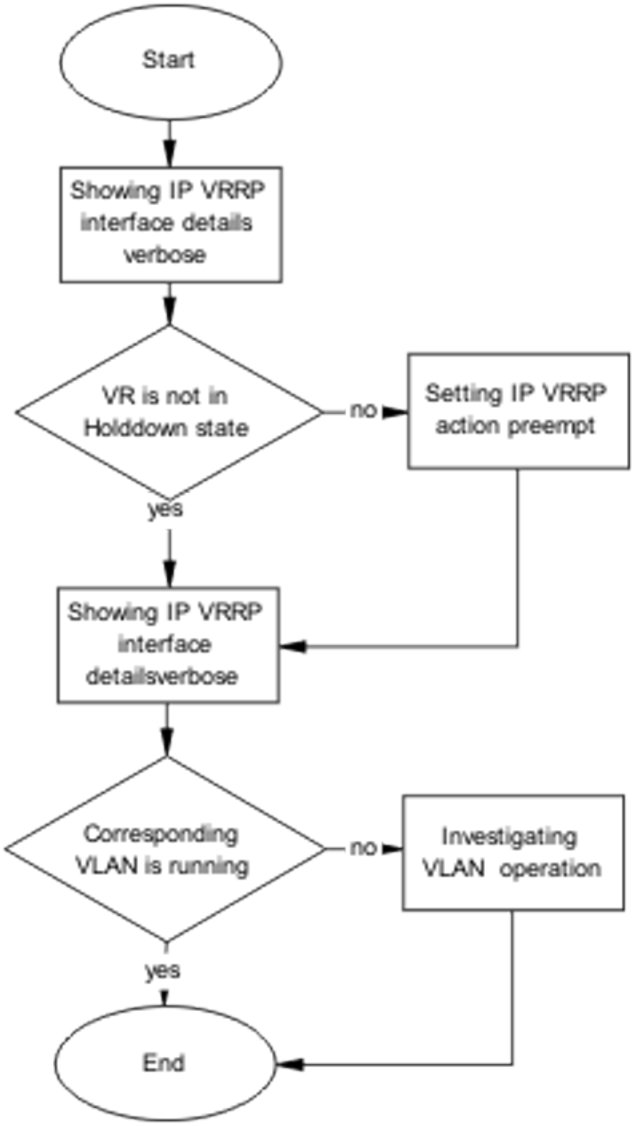

Start
Showing IP VRRP interface details verbose
VR is not in Holddown state
no
Setting IP VRRP action preempt
yes
Showing IP VRRP interface detailsverbose
Corresponding VLAN is running
no
Investigating VLAN operation
yes
End

Figure 130: Configure device for master or backup

Configure device for master or backup navigation:

- Showing IP VRRP interface details verbose on page 257
- Setting IP VRRP action preempt on page 258
- Investigating VLAN operation on page 258

Showing IP VRRP interface details verbose

Verify critical information for the VRRP interface.

1. Use the command **`show ip vrrp interface verbose`**.
2. Verify VR is not in holddown state.
3. Verify that the corresponding VLAN is up for the critical IP feature is enabled and the critical IP address is set to one of the local L3 VLANs IP.

Setting IP VRRP action preempt

Configure the IP VRRP action to manually holddown the preempt state.

1. Enter the command **`ip vrrp <VRID> action preempt`** to make manually preempt the holddown state.
2. Observe no errors after execution.

Investigating VLAN operation

If the critical IP feature is enabled and the critical IP address is set to one of the local L3 VLANs IP, verify that the corresponding VLAN is up.

1. Enter the command **`show vlan`** to view VLAN information.
2. Observe the VLAN in question is up.

Preempt mode is not working

The ‘preempt mode’ setting as directed in RFC 3768 is not supported. The device will always work with the default preempt behavior, which is ‘True’ (meaning an existing Master will always be preempted by a new, higher priority/IP address router).

Work flow: Preempt mode is not working

The following work flow assists you to determine the solution for preempt mode that does not function.

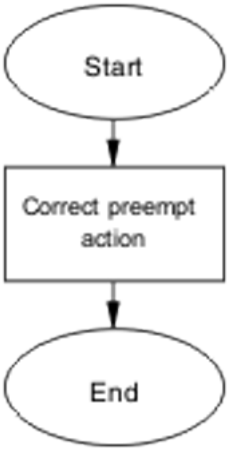


Figure 131: Preempt mode is not working

Preempt mode is not working navigation:

- Preempt mode is not working on page 258

Configure preempt action

The ‘preempt action’ setting is a trigger designed to manually terminate the active hold down state of a VR.

Task flow: Configure preempt action

The following task flow assists you to set the preempt action.

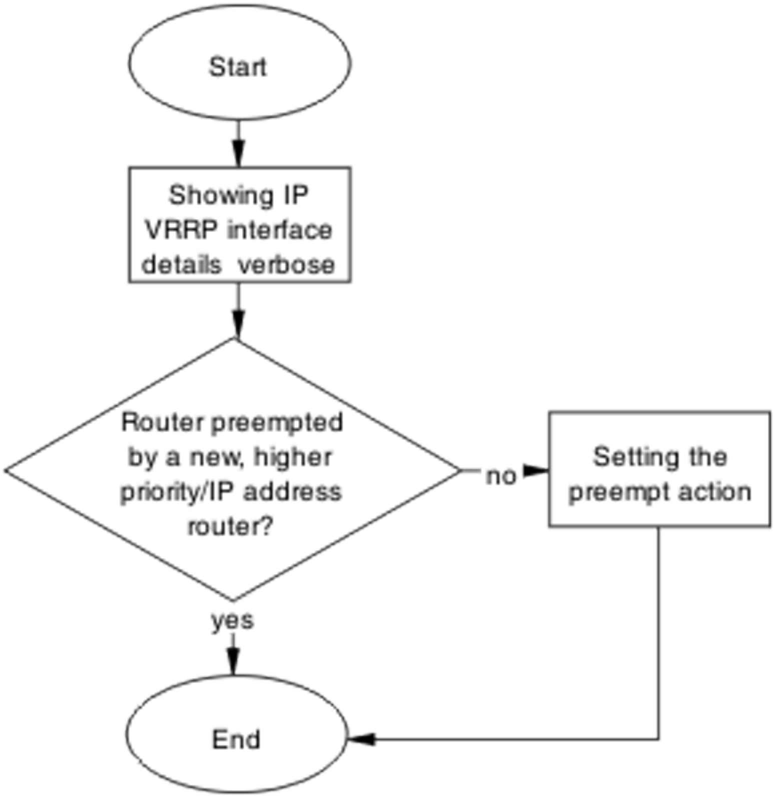

Start
Showing IP VRRP interface details verbose
Router preempted by a new, higher priority/IP address router?
no
Setting the preempt action
yes
End

Figure 132: Configure preempt action

Configure preempt action navigation:

- Showing IP VRRP interface verbose on page 260
- Setting the preempt action on page 260

Showing IP VRRP interface verbose

Verify critical information for the VRRP interface.

1. Use the command **`show ip vrrp interface verbose`**.
2. Verify VR is not in holddown state.
3. Verify that the corresponding VLAN is up for the critical IP feature is enabled and the critical IP address is set to one of the local L3 VLANs IP.

Setting the preempt action

Configure the preempt for manual operation.

1. Enter the **`ip vrrp <1-255> action preempt`** command to configure the preempt.
2. Observe no errors after execution.

Chapter 12: Common procedures

You must use the Global Configuration mode to move to another mode. The following rules apply when moving between command modes.

You can move from User Executive mode to Privileged EXEC mode by using the enable command at the command prompt. If you are currently in Privileged EXEC mode, it is possible to move into Global Configuration mode using the configure command. You enter the Interface Configuration by entering the **`interface fastethernet <port number>`** command to configure a port, or **`interface vlan <vlan number>`** command to configure a VLAN.

- **`router rip`**
- **`router ospf`**
- **`router vrrp`**

User Executive Mode

User Executive mode is the default command mode for the CLI. The command prompt will look similar to: `ERS5000>` .

1. This mode is the default command mode and does not require an entrance command.
2. To exit the CLI, type the **`exit`** or **`logout`** command.

Privileged Exec Mode

Privileged Exec mode prompt will look similar to: `ERS5000#` .

1. To enter the this command mode from User Executive mode, type the **enable** command.
2. To exit the CLI, type the **exit** or **logout** command.
3. The exit the ACLI completely, type the **logout** command.

Global Configuration Mode

Global configuration mode will look similar to: `ERS5000(config)# .`

1. To enter this command mode, from Privileged EXEC mode type the **configure** command.
2. To exit the CLI completely type the **logout** command. To return to Privileged Exec mode enter the **end** or **exit** command.
3. The exit the ACLI completely, type the **logout** command.

Interface Configuration Mode

Interface configuration mode prompt will look similar to: `ERS5000(config-if)# .`

1. Entry into this command mode is dependant on the type of interface being configured. For example, use the **interface fastethernet <port number>** command to enter this mode and configure a port.
2. To exit the CLI completely type the **logout** command.
3. To return to Global Configuration mode enter the **exit** command.
4. To return to Privileged Exec mode enter the **end** command.
5. The exit the ACLI completely, type the **logout** command.

Router Configuration Mode

Router configuration mode prompt will look similar to: `ERS5000(config-router)#` .

1. To configure router OSPF, type the **`router ospf`**command.
2. To configure router RIP, type the **`router rip`** command.
3. To configure router VRRP, type the **`router vrrp`** command.
4. To return to Global Configuration mode enter the **`exit`** command.
5. To return to Privileged Exec mode enter the **`end`** command.
6. The exit the ACLI completely, type the **`logout`** command.