NORTEL

Ethernet Routing Switch 5500 Series

Troubleshooting

Release: 5.1
Document Revision: 01.01

www.nortel.com

NN47200-700 324386-A

Ethernet Routing Switch 5500 Series
Release: 5.1
Publication: NN47200-700
Document status: Standard
Document release date: 1 April 2008

Sourced in Canada

This document contains Nortel confidential and proprietary information. It is not to be copied, disclosed or distributed in any manner, in whole or in part, without Nortel’s express written authorization. While the information in this document is believed to be accurate and reliable, except as otherwise expressly agreed to in writing NORTEL PROVIDES THIS DOCUMENT "AS IS" WITHOUT WARRANTY OR CONDITION OF ANY KIND, EITHER EXPRESS OR IMPLIED. The information and/or products described in this document are subject to change without notice.

Contents

New In This Release

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

Introduction

This document :

- Describes the diagnostic tools and utilities available for troubleshooting the Nortel ERS 5500 Series products including the Nortel Networks Command Line Interface (NNCLI) and Java Device Manager (JDM)..
- 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 Nortel 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 ERS 5500 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 ERS 5500 Series network topologies. Other tools are more general in their application and can be used to diagnose and monitor ingress and egress traffic.

Troubleshooting Planning

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

First, use the *Ethernet Routing Switch 5500 Series Documentation Roadmap* to familiarize yourself with the documentation set, so you know where to get information when you need it.

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

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

- A site **network map** identifies where each device is physically located on your site, which helps locate the users and applications that are affected by a problem. You can use the map to systematically search each part of your network for problems.
- You must know how your devices are **connected** logically and physically with virtual local area networks (VLAN).
- 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. It is a good practice to keep records of your previous passwords in case you must restore a device to a previous software version. You need to use the old password that was valid for that version.
- It is a good practice 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.
- It is a good practice 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 should speed the process of isolating network problems.

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. When port mirroring is enabled, the ingress or egress packets of the mirrored (source) port are forwarded normally and a copy of the packets is sent from the mirrored port to the mirroring (destination) port. 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 *Nortel 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 on 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 may not be 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.

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

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

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

For more detail regarding stack loopback testing, please reference the *Nortel Ethernet Routing Switch 5500 Series Configuration — System Monitoring* (NN47200-505).

Time Domain Reflectometer

Beginning with Release 5.0 software, the Nortel ERS 5500 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 NNCLI or the JDM.

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. When 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)

Understand AUR to replace a failed device in the stack.

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.

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

If the hardware version of the replaced unit is different from the previous unit, the unit will be allowed to join the stack. However, the configuration of the previous unit will not be replicated in the new unit.

AUR can be enabled or disabled from the NNCLI and JDM. By default, AUR is enabled.

Nortel Knowledge and Solution Engine

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

General Diagnostic Tools

The ERS 5500 Series device has diagnostic features available with the JDM, NNCLI, 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 NNCLI to perform the majority of troubleshooting. For purposes of using this document, CLI and NNCLI are interchangeable. Refer to *Nortel ERS 5500 Series Commands Reference* (NN47200-500) for information on 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.

NNCLI command modes

Understand the NNCLI command modes and how they differ.

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

- User EXEC
- 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 EXEC mode:** The User EXEC mode (also referred to as exec mode) is the default CLI command mode. User EXEC 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:** The Privileged EXEC mode (also referred to as privExec mode) enables the user to perform basic switch-level management tasks, such as downloading software images, setting passwords, and booting the switch. privExec is an unrestricted mode that allows you to view all settings on the switch, and if you are logged in with write access, it also allows you to access all configuration modes and commands that affect operation of the switch (such as downloading images, rebooting, etc.).
- **Global configuration mode:** The Global Configuration mode (also referred to as config mode) enables the user to set and display general configurations for the switch such as IP address, SNMP parameters, Telnet access, and VLANs.
- **Interface configuration mode:**The Interface Configuration mode (also referred to as config-if mode) enables the user to configure parameters for each port or VLAN, such as speed, duplex mode, and rate-limiting.
- **Router configuration mode:**The Router Configuration mode (also referred to as config-router mode) enables the user to configure routing parameters for RIP, OSPF, and VRRP.

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

Initial Troubleshooting

The types of problems that typically occur with networks involve connectivity and performance. It is usually best to follow the OSI network architecture layers. Confirm that the physical environment, such as the cables and module connections, is operating without any failures before moving up to the network and application layers.

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

Gather information

Before contacting Nortel 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`**: When connectivity problems occur, get information on 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>`**

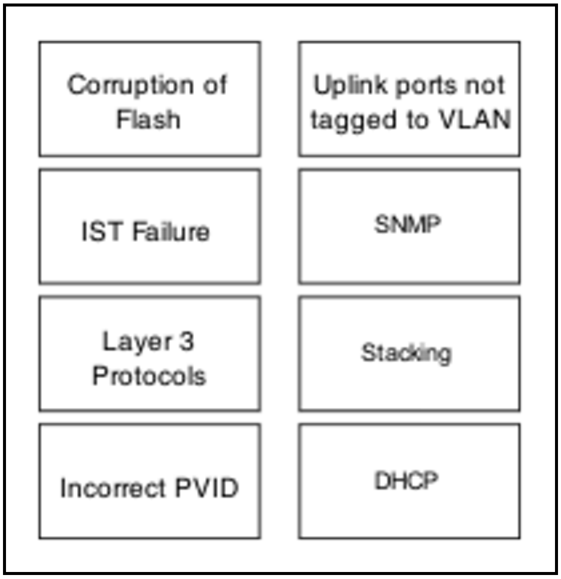
Emergency Recovery Trees

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



Corruption of Flash	Uplink ports not tagged to VLAN
IST Failure	SNMP
Layer 3 Protocols	Stacking
Incorrect PVID	DHCP

Navigation

- "Corruption of flash" (page 22)
- "IST Failure" (page 23)
- "Layer 3 protocols" (page 25)
- "Incorrect PVID" (page 26)
- "VLAN not tagged to uplink ports" (page 27)

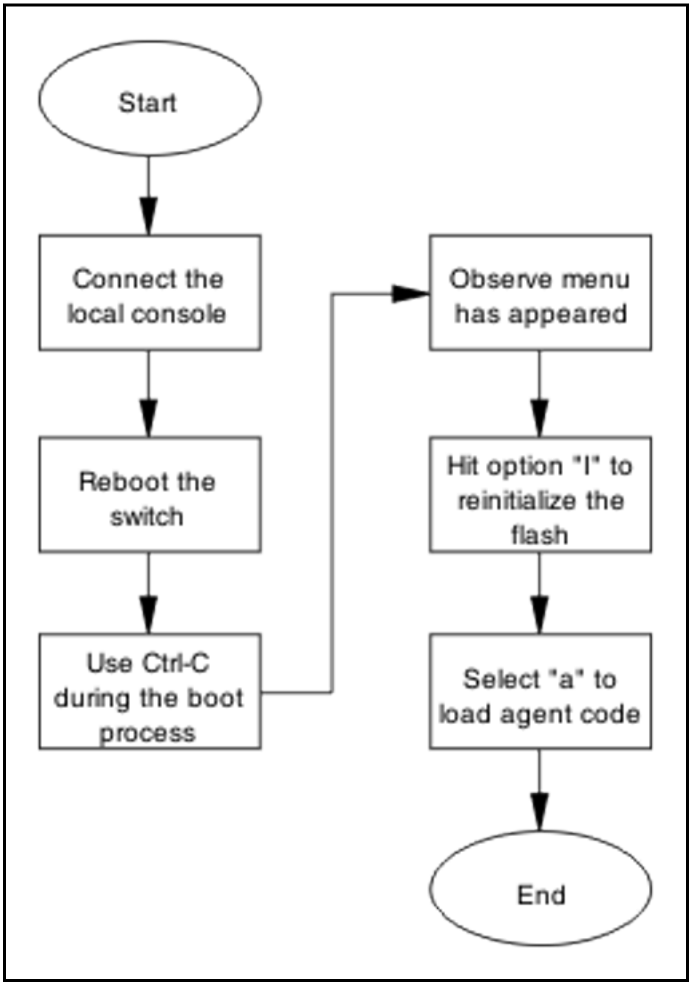
- "SNMP" (page 28)
- "Stack " (page 30)
- "Dynamic Host Configuration Protocol (DHCP)" (page 34)

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

Figure 2
Corruption of flash

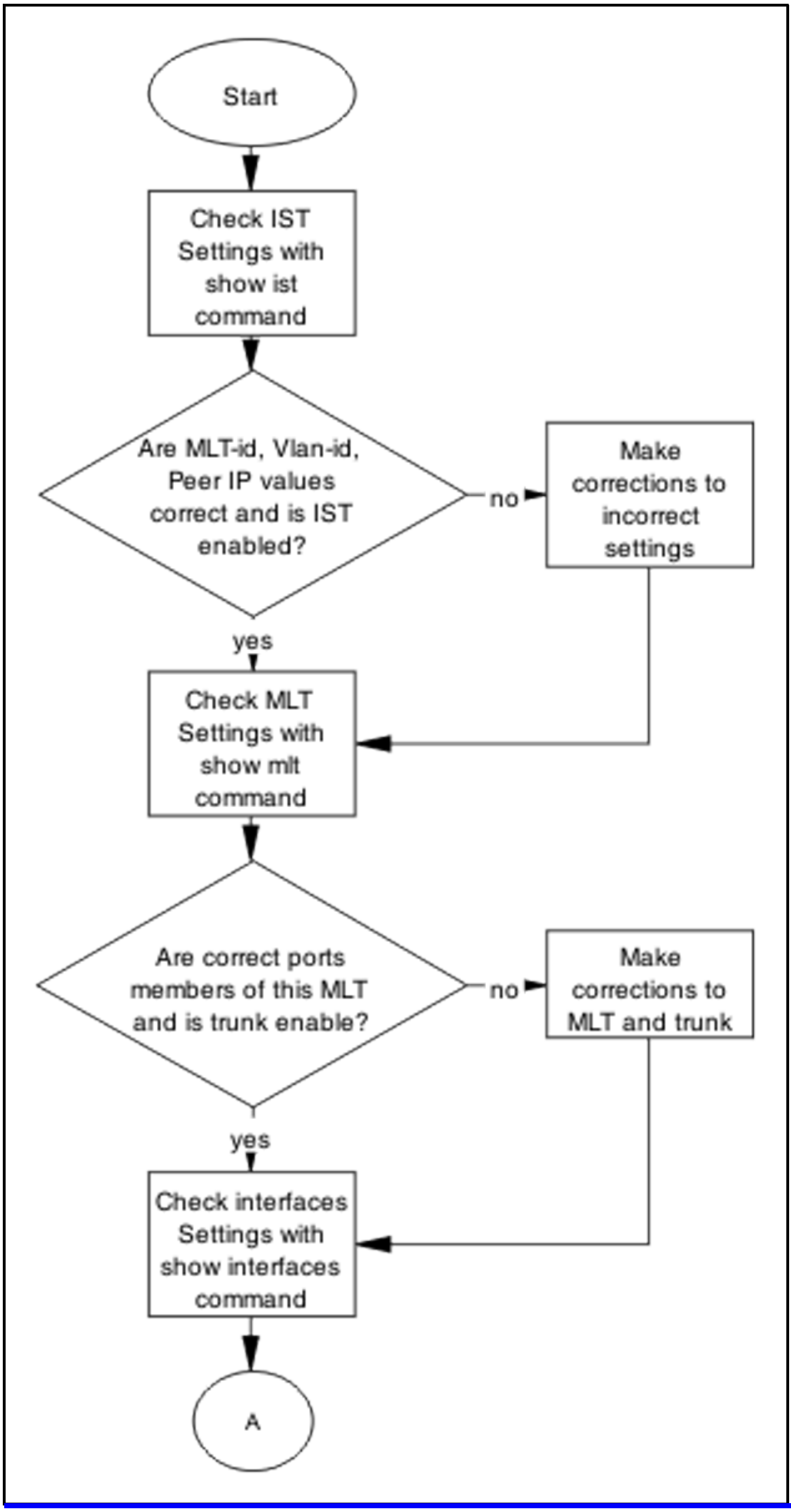

Start
Connect the local console
Reboot the switch
Use Ctrl-C during the boot process
Observe menu has appeared
Hit option "I" to reinitialize the flash
Select "a" to load agent code
End

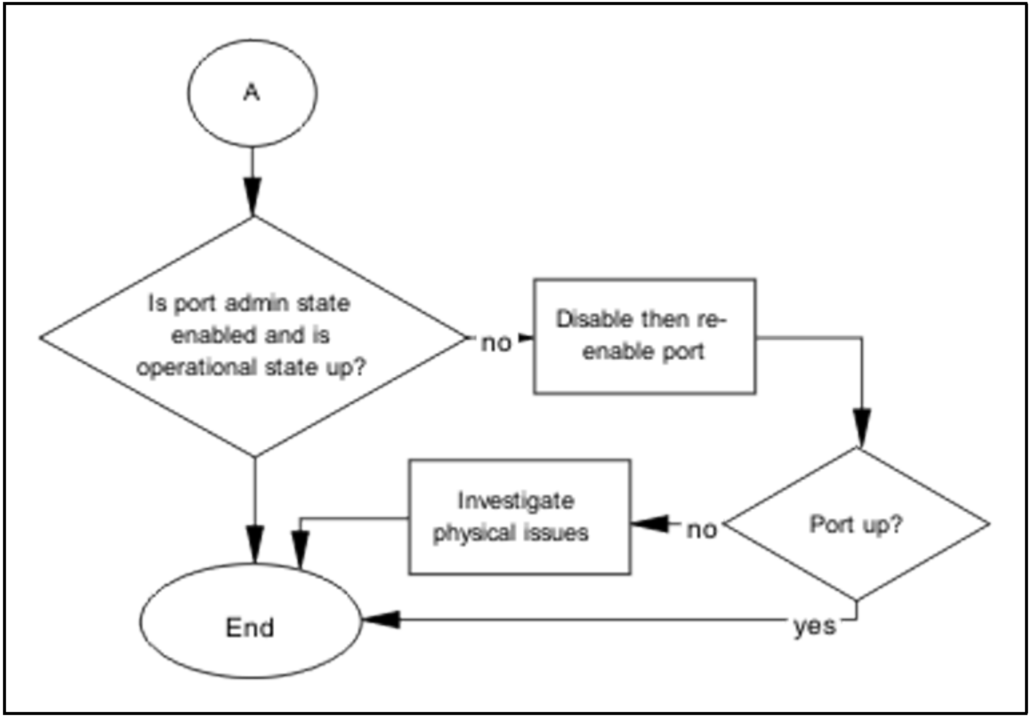
IST Failure

Two ERS 5500 series devices running IST between them may 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 in the event of IST failure, network protocol like RIP,VRRP,OSPF,VLACP start flapping and will finally cause a network outage.

IST Failure Recovery Tree

Figure 3
IST Failure


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

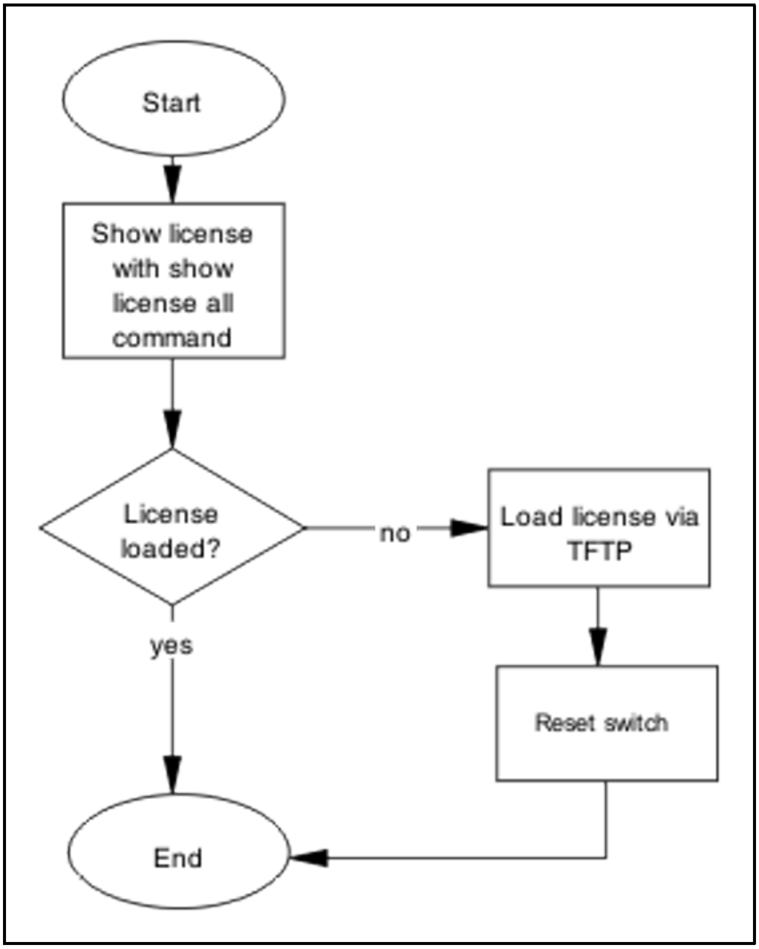

A
Is port admin state enabled and is operational state up?
no
Disable then re-enable port
Port up?
no
Investigate physical issues
yes
End

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 4
Layer 3 Protocols

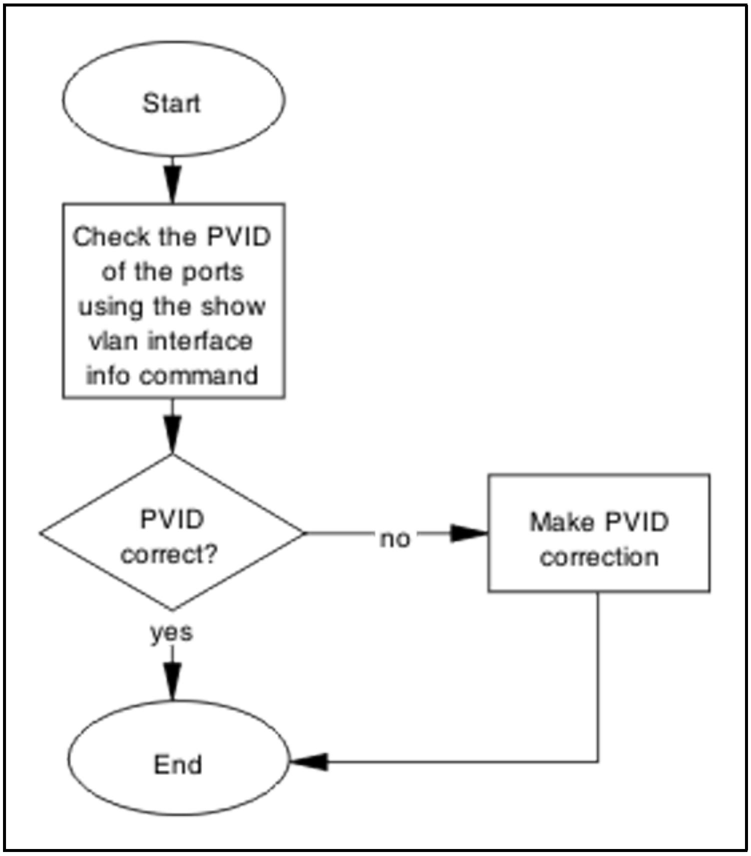


Incorrect PVID

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

Figure 5
Incorrect PVID

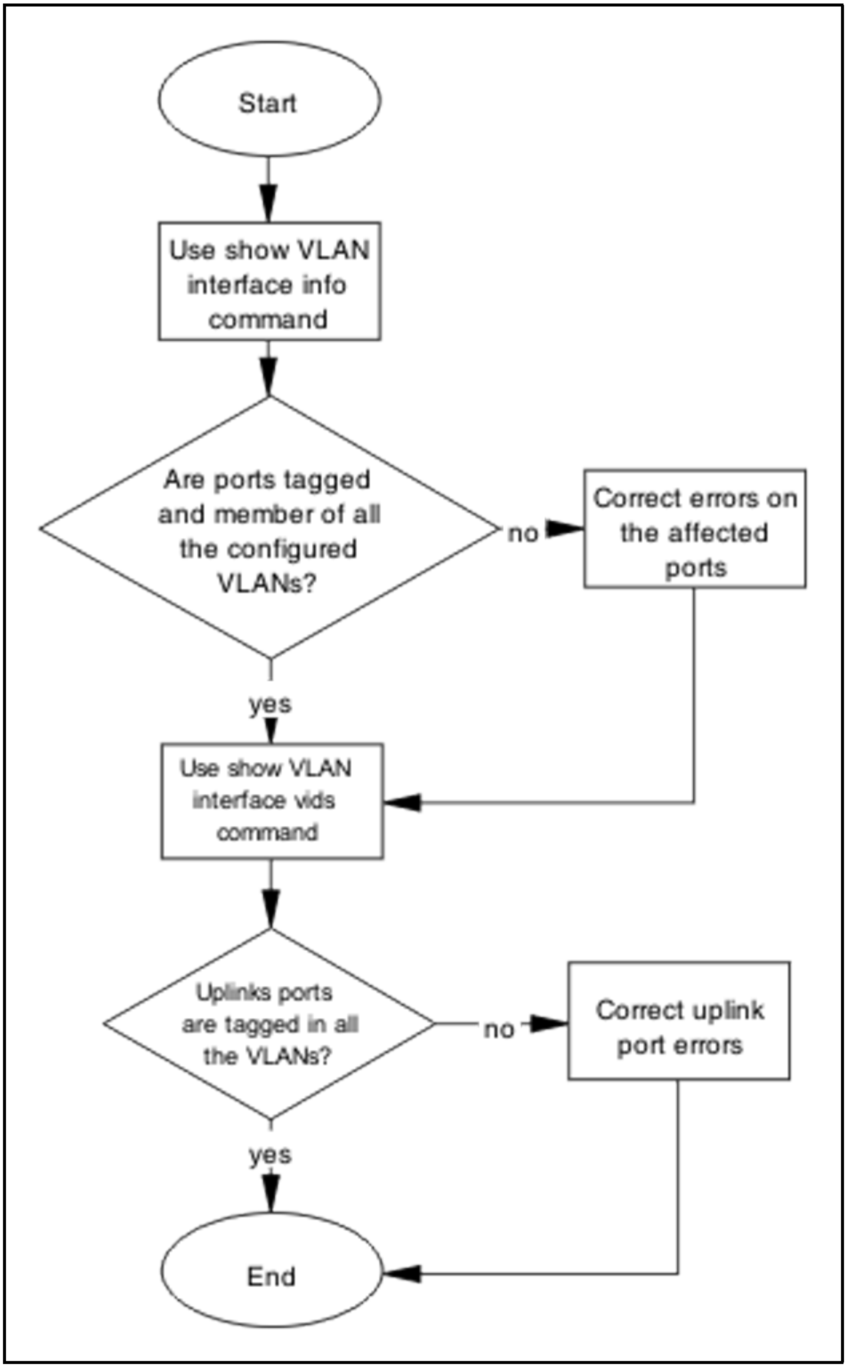

Start
Check the PVID of the ports using the show vlan interface info command
PVID correct?
no
Make PVID correction
yes
End

VLAN not tagged to uplink ports

When 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

Figure 6
VLAN not tagged to uplink ports

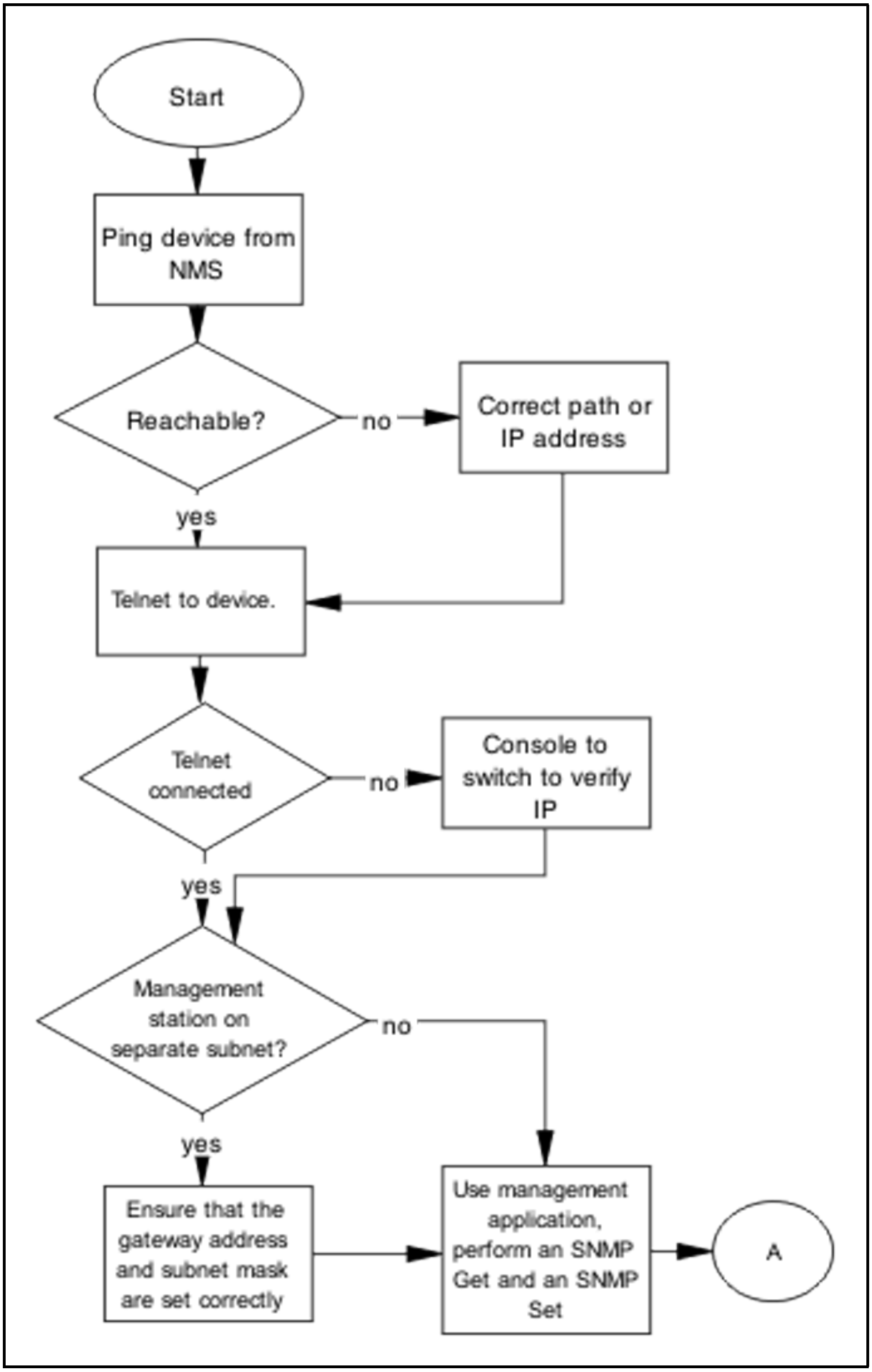

Start
Use show VLAN interface info command
Are ports tagged and member of all the configured VLANs?
no
Correct errors on the affected ports
yes
Use show VLAN interface vids command
Uplinks ports are tagged in all the VLANs?
no
Correct uplink port errors
yes
End

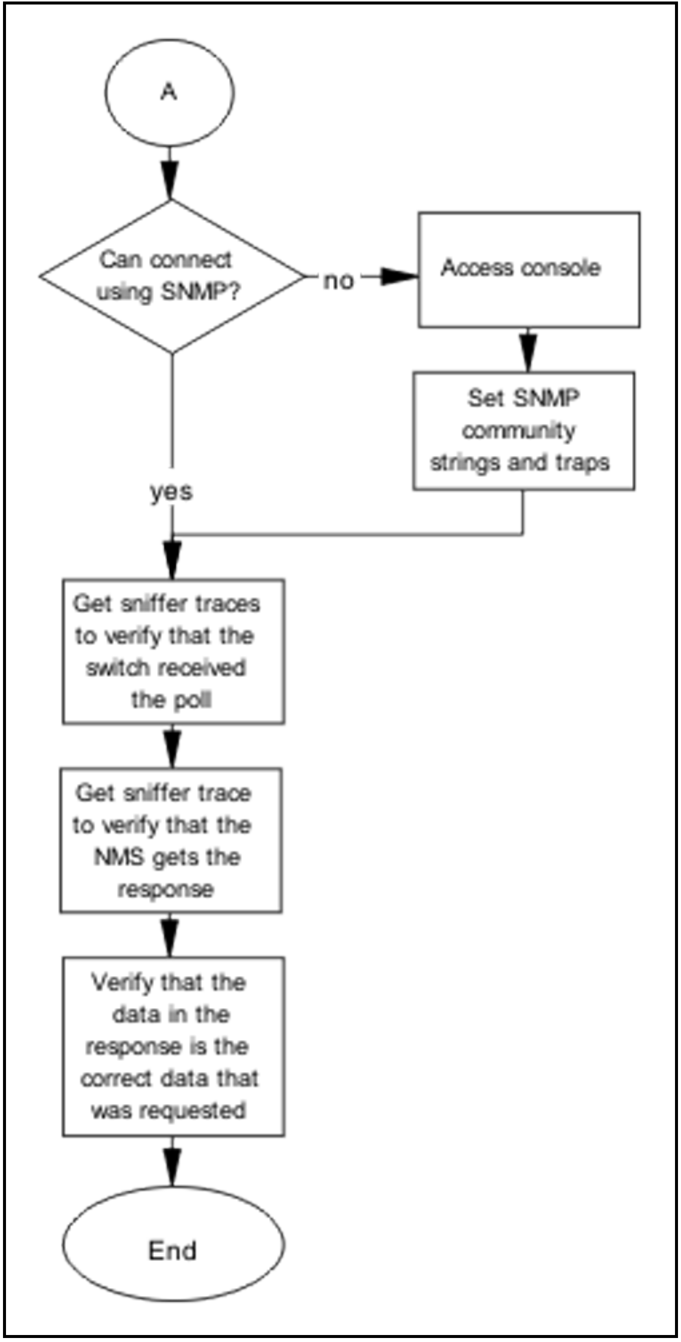
SNMP

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).

Recovery Tree

Figure 7
SNMP


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

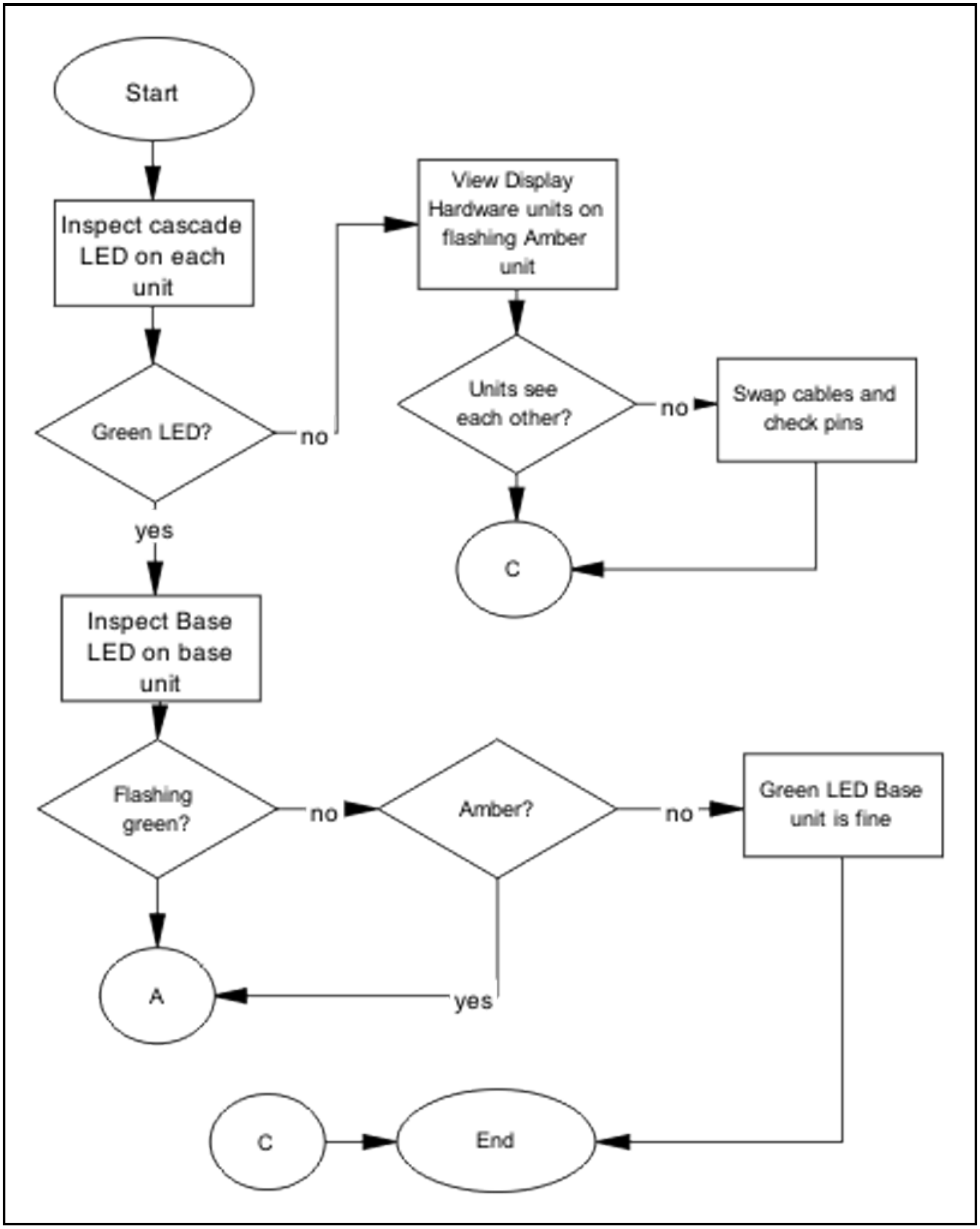

A
Can connect using SNMP?
no
Access console
Set SNMP community strings and traps
yes
Get sniffer traces to verify that the switch received the poll
Get sniffer trace to verify that the NMS gets the response
Verify that the data in the response is the correct data that was requested
End

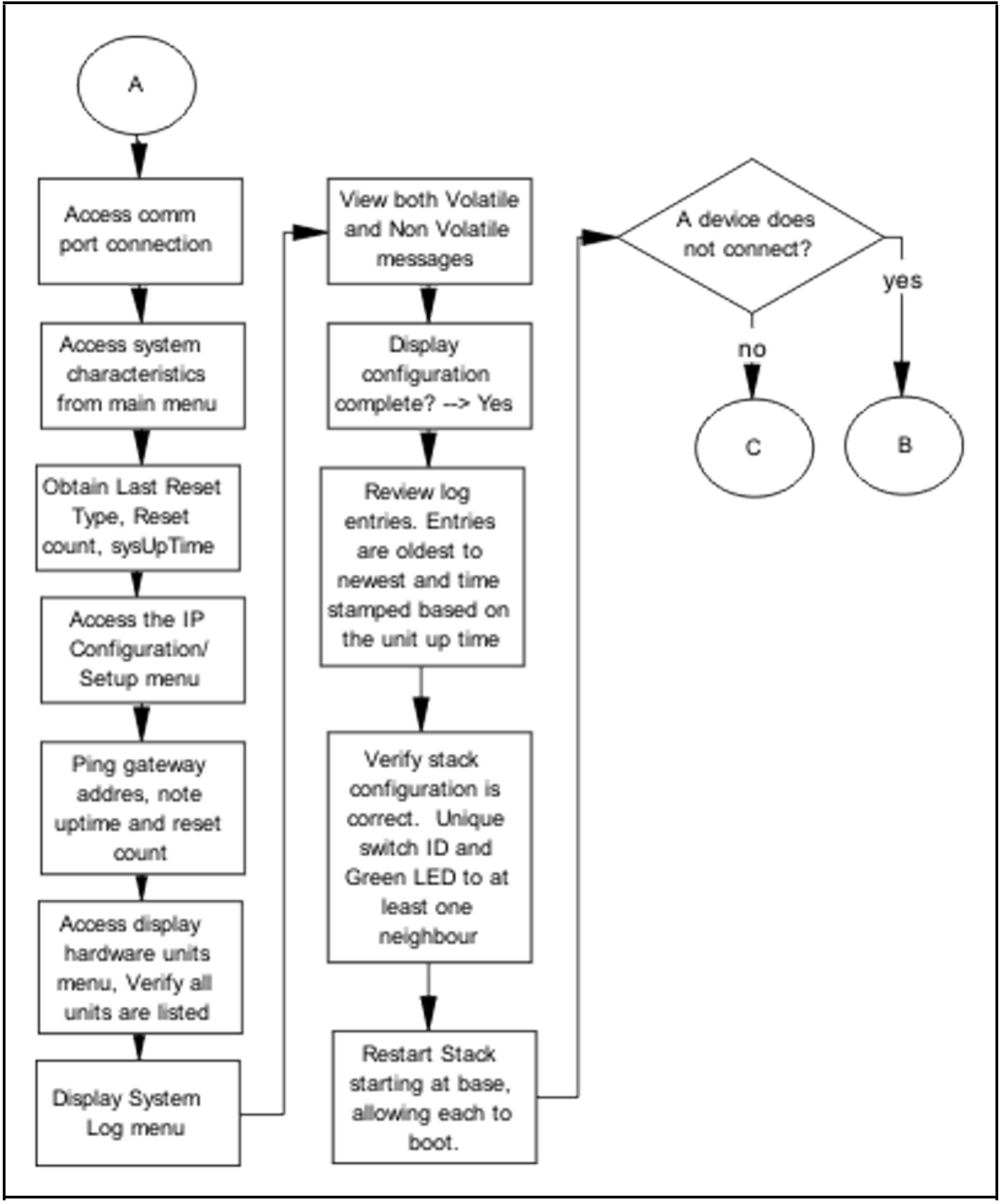
Stack

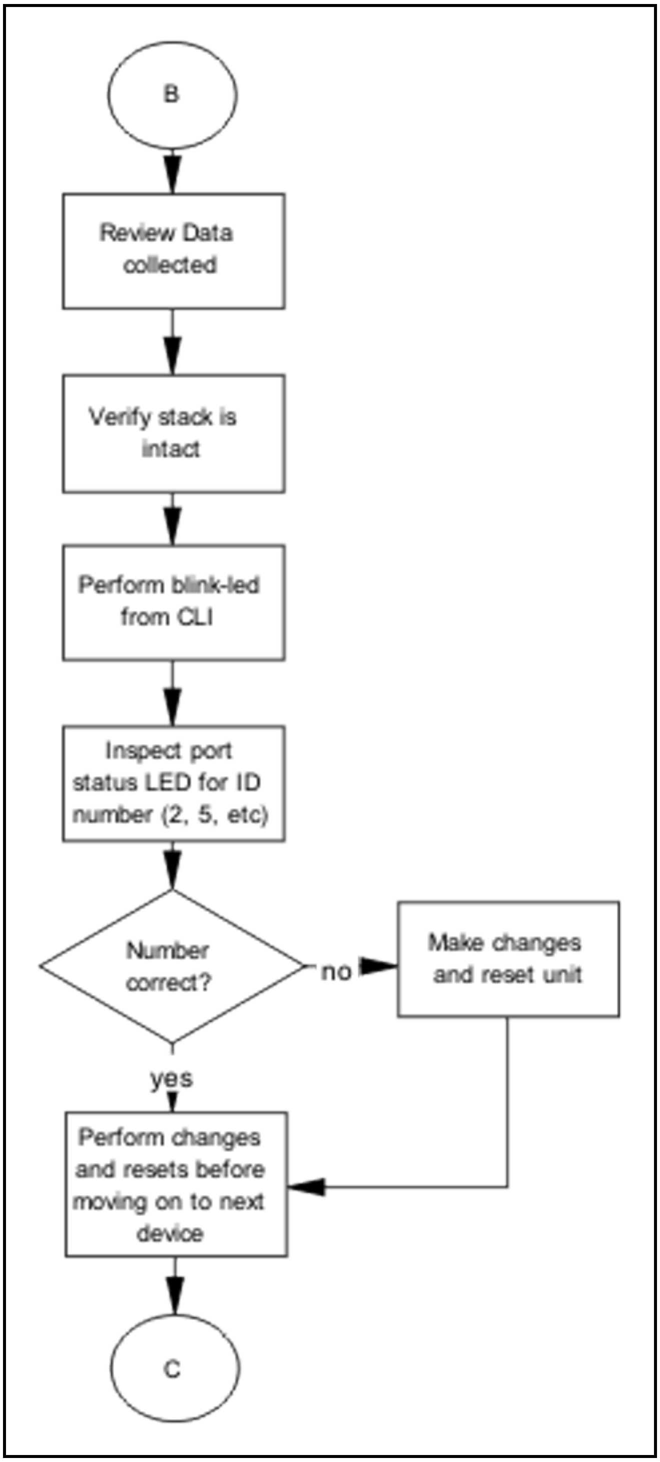
Stack failure can be the result of a communication error between the individual units due to configuration or cabling. Failures can also arise when there are multiple bases configured.

Stack Recovery Tree

Figure 8
Stack


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


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

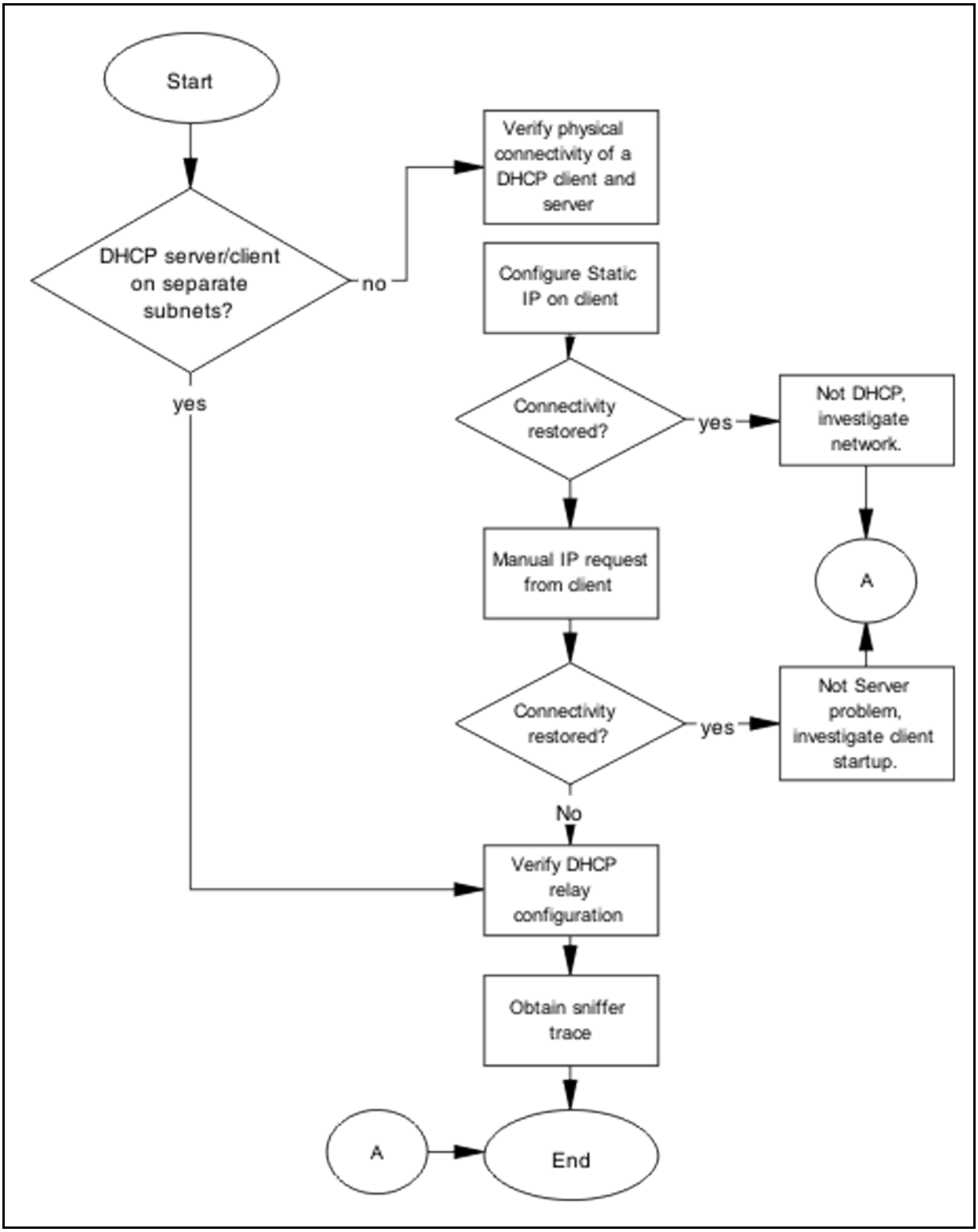

B
Review Data collected
Verify stack is intact
Perform blink-led from CLI
Inspect port status LED for ID number (2, 5, etc)
Number correct?
no
Make changes and reset unit
yes
Perform changes and resets before moving on to next device
C

Dynamic Host Configuration Protocol (DHCP)

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

DHCP Recovery Tree

Figure 9
DHCP


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.
A
Manual IP request from client
Connectivity restored?
yes
Not Server problem, investigate client startup.
No
Verify DHCP relay configuration
Obtain sniffer trace
A
End

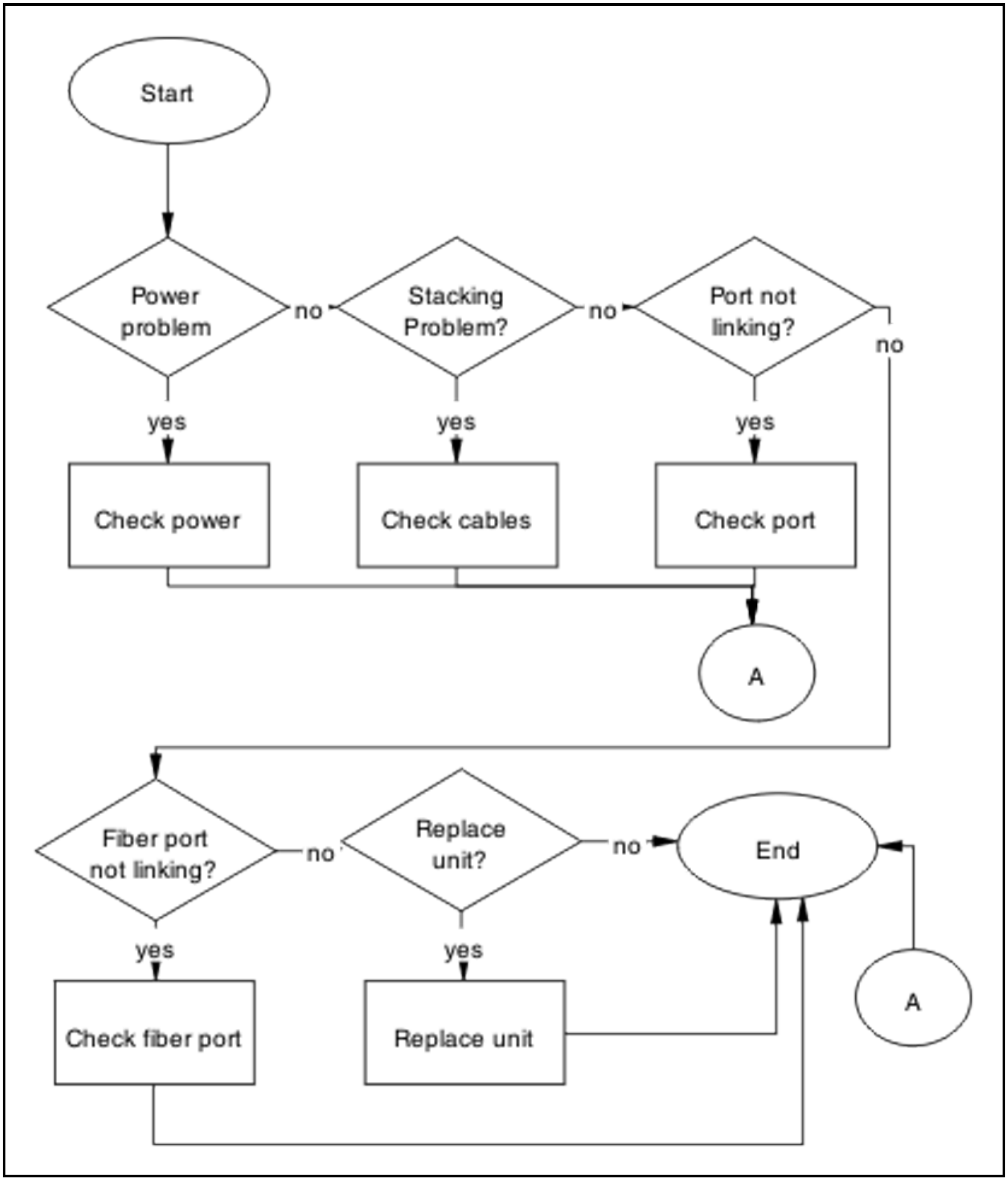
Troubleshooting Hardware

Complete hardware troubleshooting specific to the ERS 5500 series.

Work flow: Troubleshooting hardware

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

Figure 10
Troubleshooting hardware



Navigation

- "Check power" (page 39)
- "Check cables" (page 41)
- "Check port" (page 42)

- "Check fiber port" (page 45)
- "Replace unit" (page 48)

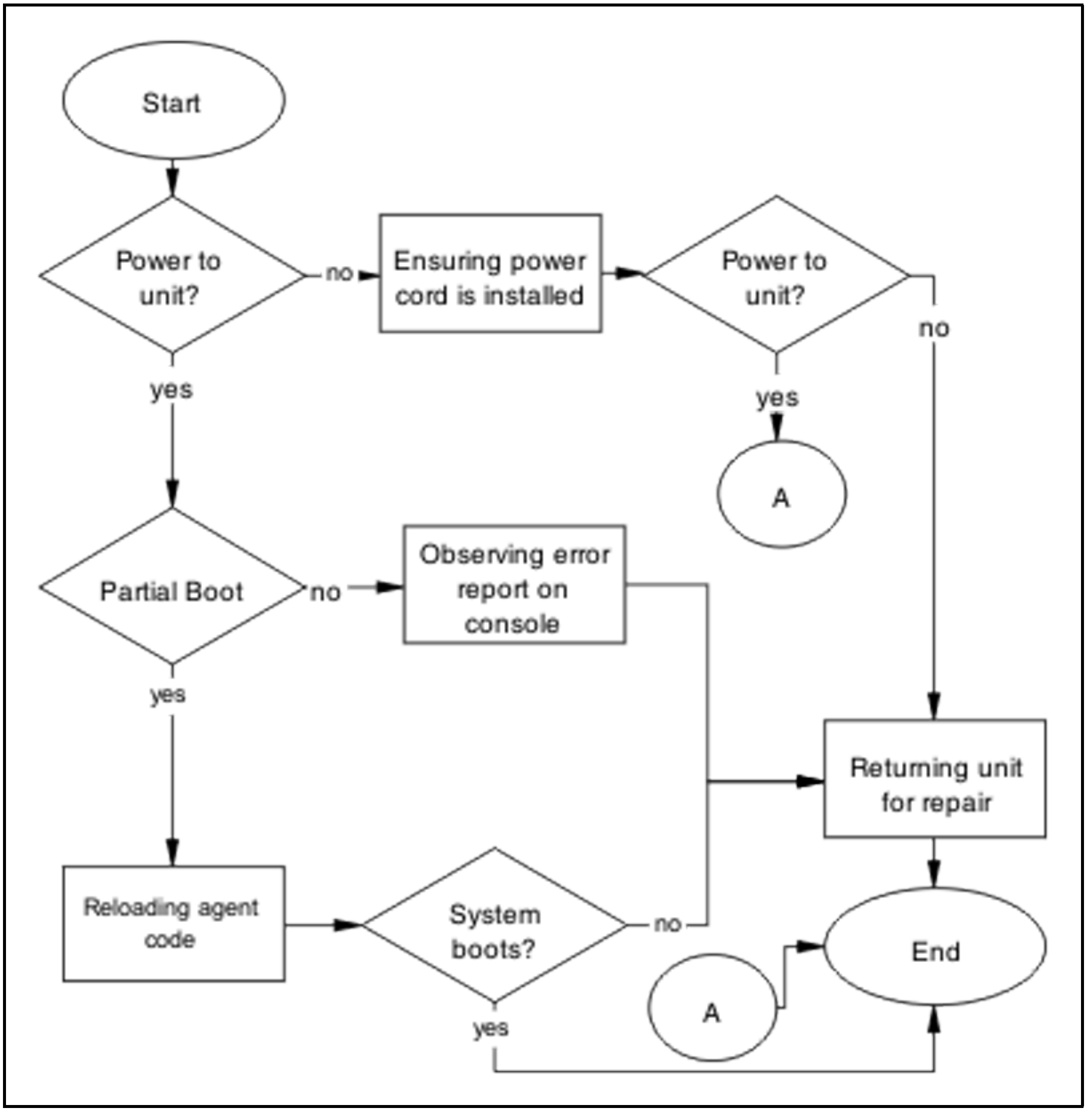
Check power

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 11
Check power



Navigation

Ensuring power cord is installed

Confirm the power cord is properly installed for the device.

Refer to *Nortel 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.

Procedure Steps

Step **Action**

1 View console information and note any 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

--End--

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 have adequate backup of your configuration prior to reloading software.
>
> Know the current version of your software before reloading it. Loading incorrect software versions may cause further complications.

Procedure Steps

Step **Action**

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

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

--End--

Returning unit for repair

Return unit to Nortel for repair

Contact Nortel for return instructions and RMA information.

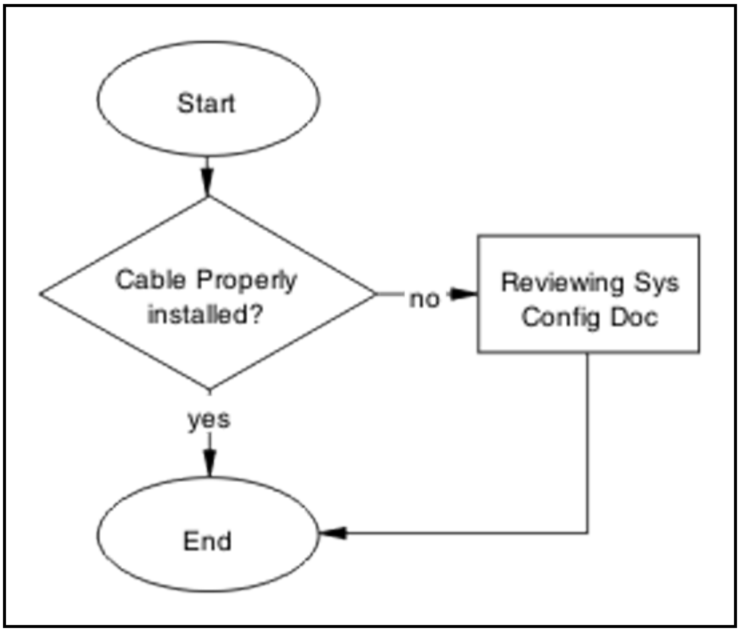
Check cables

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 12
Check cables



Navigation

- "Reviewing Sys Config Doc" (page 41)

Reviewing Sys Config Doc

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

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

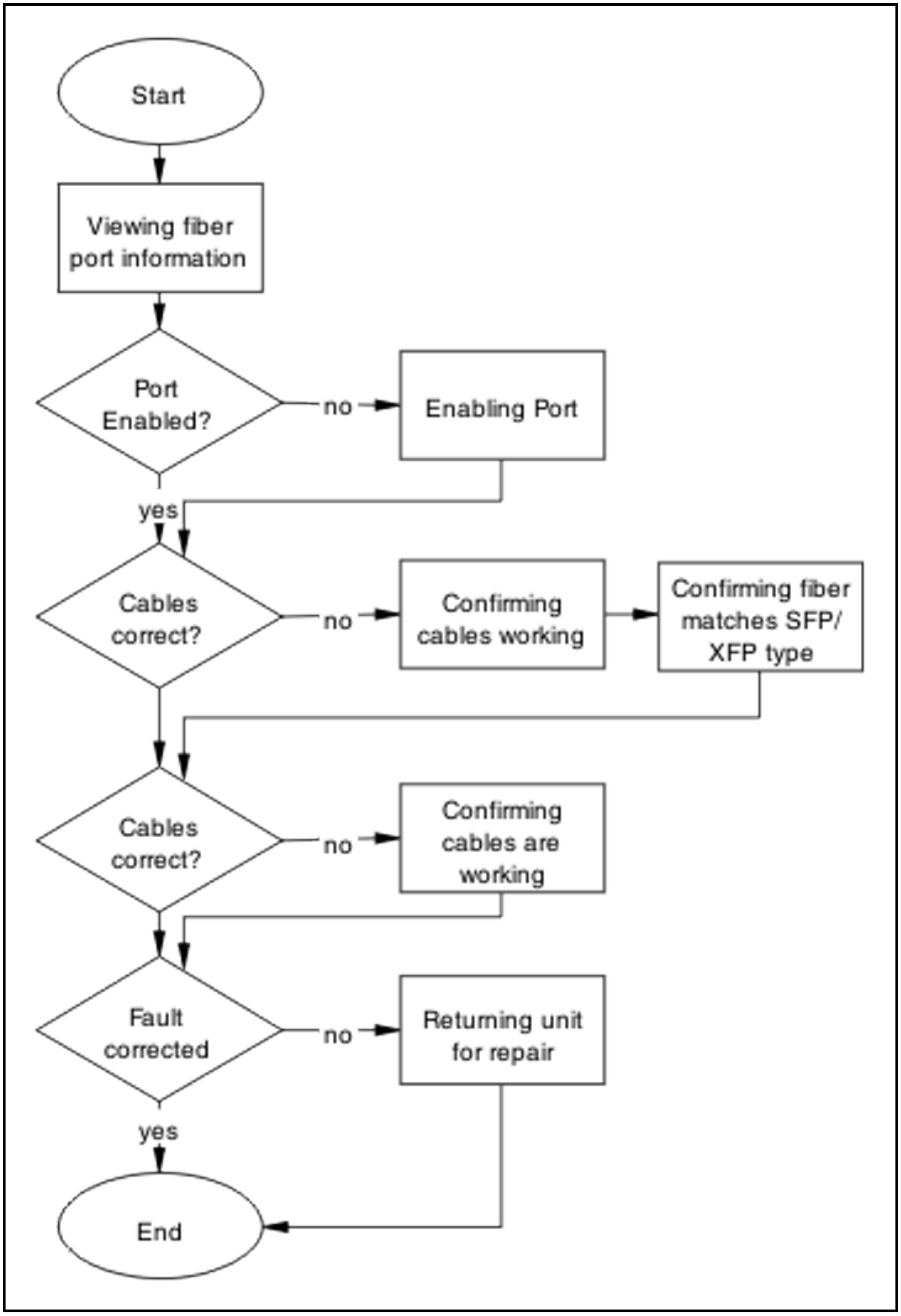
Check port

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

Task flow: Check port

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

Figure 13
Check port


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

Navigation

- "Viewing port information" (page 44)
- "Enabling the port" (page 44)
- "Confirming the cables are working" (page 44)

Viewing port information

Review the port information to ensure it is enabled.

Procedure Steps

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

--End--

Enabling the port

Enable the port.

Procedure Steps

Step	Action
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.

--End--

Confirming the cables are working

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

Procedure Steps

Step	Action
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.

--End--

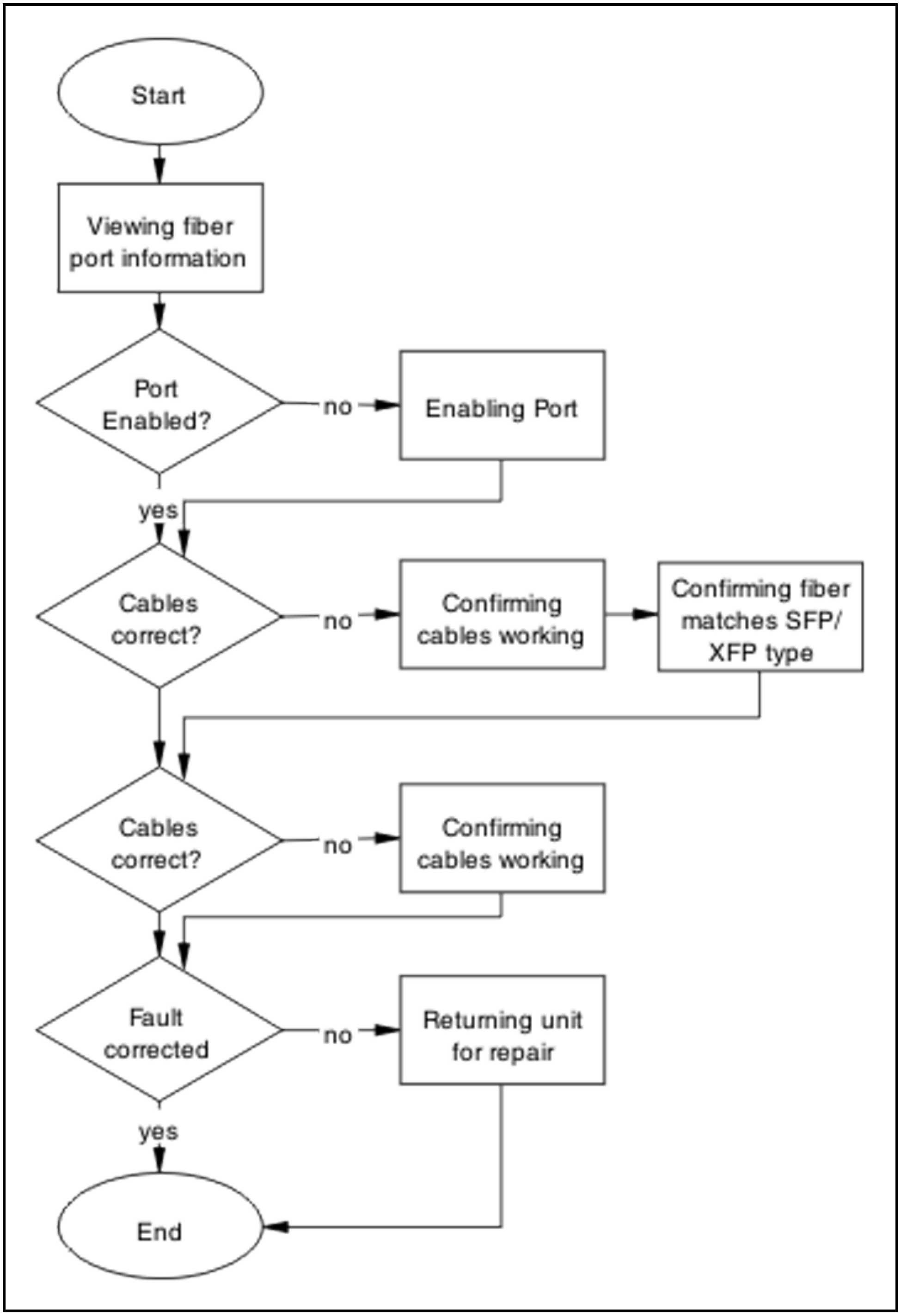
Check fiber port

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.

Figure 14
Check fiber port


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

Navigation

- "Viewing fiber port information" (page 47)
- "Enabling Port" (page 47)

- "Confirming cables working" (page 47)
- "Confirming fiber matches SFP/XFP Type" (page 48)
- "Returning unit for repair" (page 48)

Viewing fiber port information

Review the port information to ensure it is enabled.

Procedure Steps

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

--End--

Enabling Port

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

Procedure Steps

Step	Action
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.

--End--

Confirming cables working

Confirm that the cables are working on the port.

Procedure Steps

Step	Action
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.

--End--

Confirming fiber matches SFP/XFP Type

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

Procedure Steps

Step	Action
1	Inspect the fiber cables to ensure they are the correct type.
2	*Review Nortel 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.

--End--

Returning unit for repair

Return unit to Nortel for repair

Contact Nortel 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 Nortel 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.

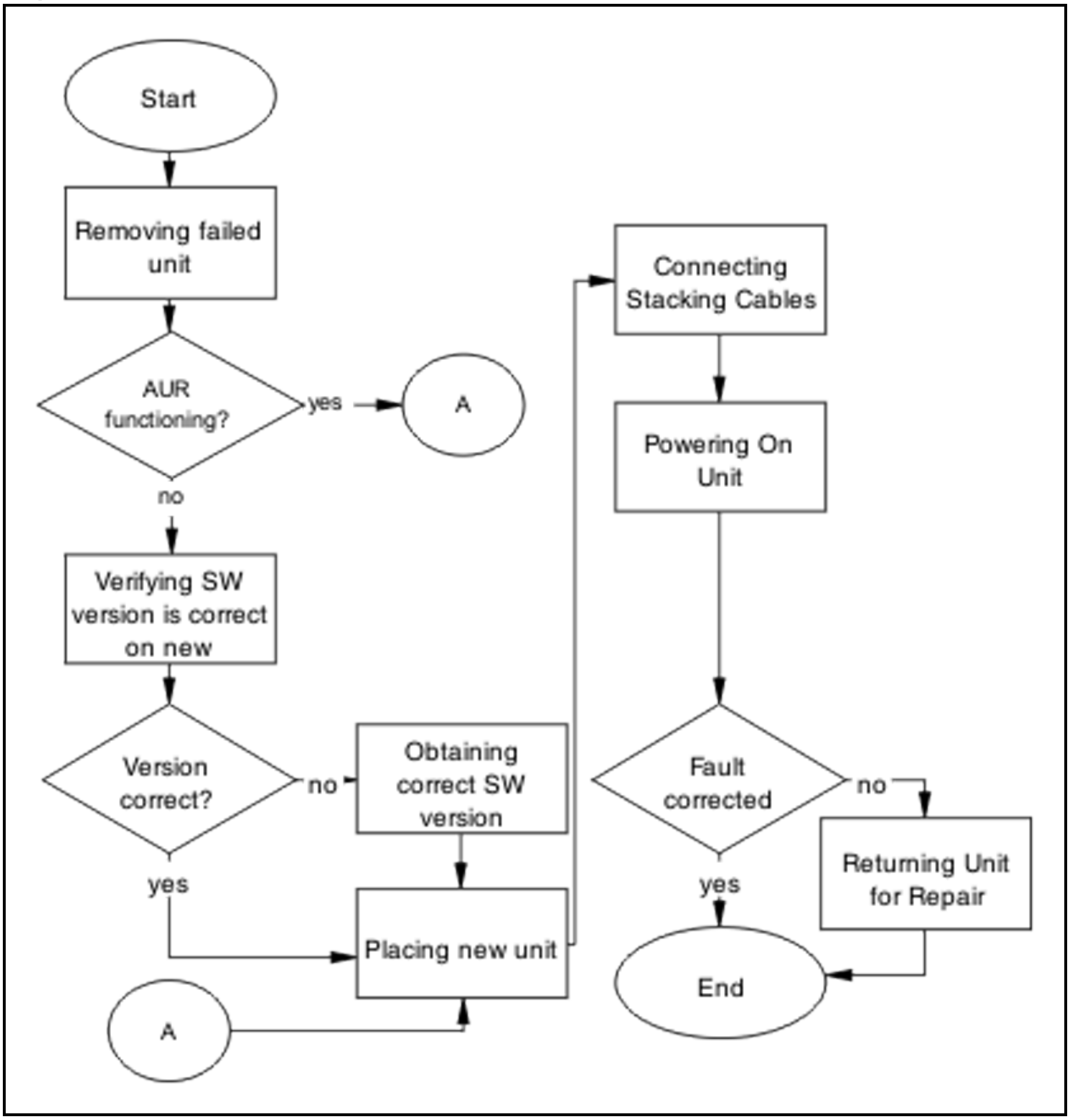
Also understand, that if you are replacing the base unit, then another unit of the stack will be designated as the temporary base unit. When the base unit is replaced, the new unit will not resume as the base unit automatically.

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), then the verify software procedures are not required.

Figure 15
Replace unit



Navigation

- "Removing failed unit" (page 50)
- "Verifying software version is correct on new device" (page 50)
- "Obtaining correct software version" (page 50)

- "Placing new unit" (page 51)
- "Connecting stacking cables" (page 51)
- "Powering on unit" (page 51)
- "Returning unit for repair" (page 52)

Removing failed unit

Remove the failed unit from the stack.

Procedure Steps

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

--End--

Verifying software version is correct on new device

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

Procedure Steps

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

--End--

Obtaining correct software version

Obtain and install correct software version

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

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

Procedure Steps

Action
Refer to the *Nortel 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 *Nortel Ethernet Routing Switch 5500 Series Installation* (NN47200-300).

Connecting stacking cables

Reconnect the stacking cables to correctly stack the device.

Procedure Steps

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

--End--

Powering on unit

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

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

Procedure Steps

Step	Action
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.

--End--

Returning unit for repair

Return unit to Nortel for repair

Contact Nortel for return instructions and RMA information.

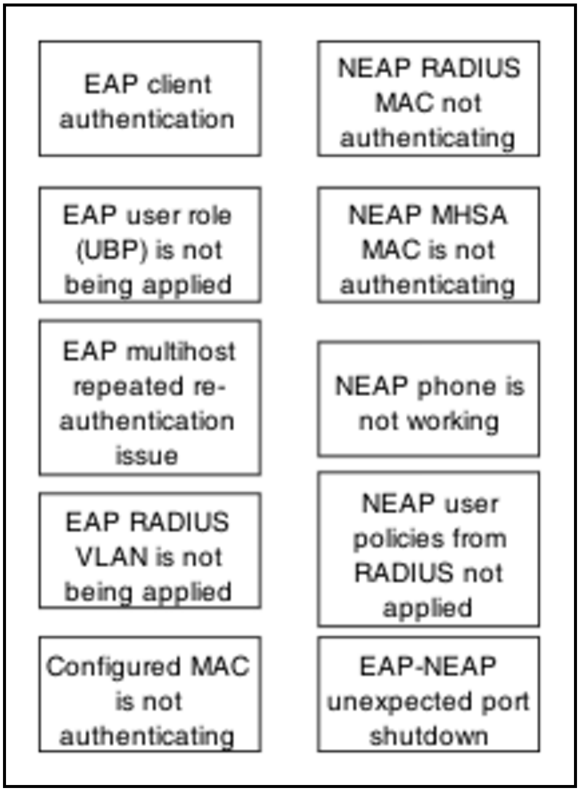
Troubleshooting Authentication

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.

Figure 16
Troubleshooting authentication


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

Navigation

- "EAP client authentication " (page 54)
- "EAP user role (UBP) is not being applied" (page 62)

- "EAP multihost repeated re-authentication issue" (page 76)
- "EAP RADIUS VLAN is not being applied " (page 80)
- "Configured MAC is not authenticating" (page 88)
- "NEAP RADIUS MAC not authenticating" (page 93)
- "NEAP MHSA MAC is not authenticating" (page 98)
- "NEAP phone is not working" (page 103)
- "NEAP user policies from RADIUS not applied" (page 110)
- "EAP-NEAP unexpected port shutdown" (page 127)

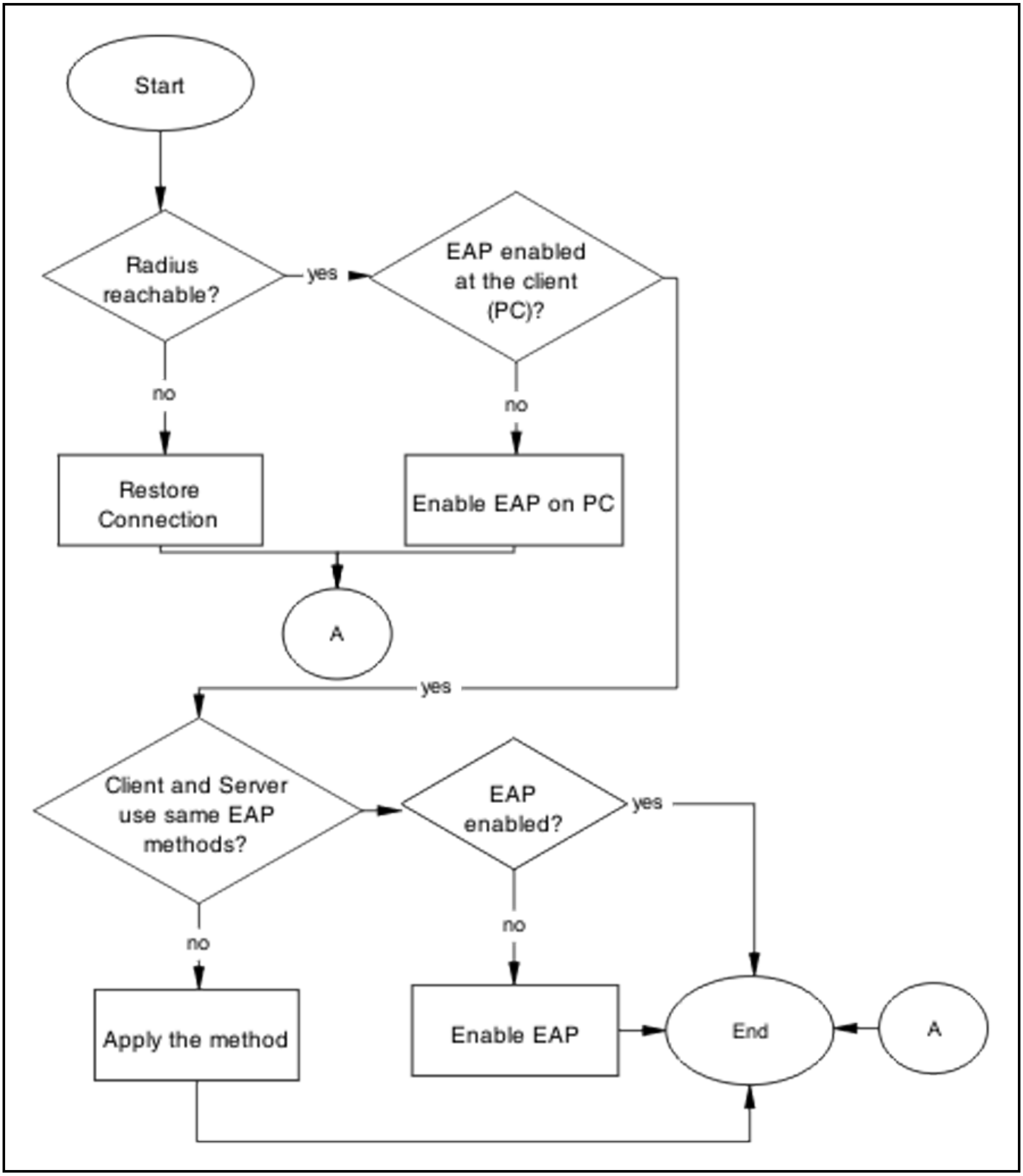
EAP client authentication

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 17
EAP client is not authenticating



Troubleshooting EAP Client is not Authenticating Navigation

- "Restore RADIUS connection" (page 56)
- "Enable EAP on The PC" (page 58)

- "Apply the method" (page 59)
- "Enable EAP globally" (page 60)

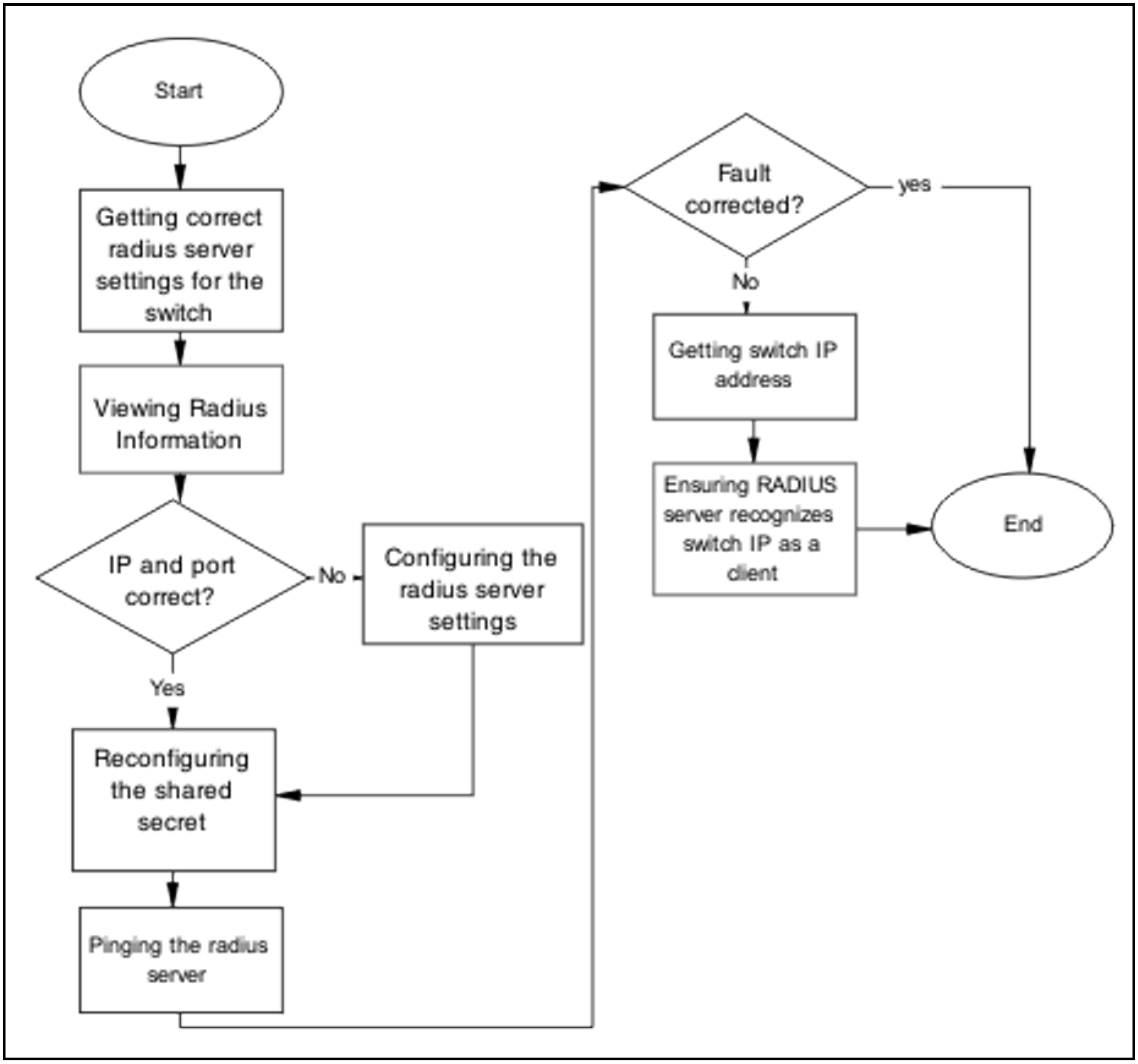
Restore RADIUS connection

Ensure that the RADIUS server has connectivity to the device

Task flow: Restore RADIUS connection

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

Figure 18
Restore RADIUS connection


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

Navigation

- "Getting correct RADIUS server settings for the switch" (page 57)
- "Viewing RADIUS information" (page 57)
- "Configuring the RADIUS server settings" (page 57)
- "Reconfiguring the shared secret" (page 58)
- "Pinging the RADIUS server" (page 58)

Getting correct RADIUS server settings for the switch

This section provides troubleshooting guidelines for obtaining the RADIUS server settings

Procedure Steps

Step	Action
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.

--End--

Viewing RADIUS information

To review the RADIUS server settings in the device.

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

Procedure Steps

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

--End--

Configuring the RADIUS server settings

The RADIUS Server settings should be set to be correct for the network.

Follow vendor documentation to set the RADIUS server settings.

Reconfiguring the shared secret

The Shared Secret should be reset in case there was any corruption

Procedure Steps

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

--End--

Pinging the RADIUS server

Ping the RADIUS server to ensure connection exists.

Procedure Steps

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

--End--

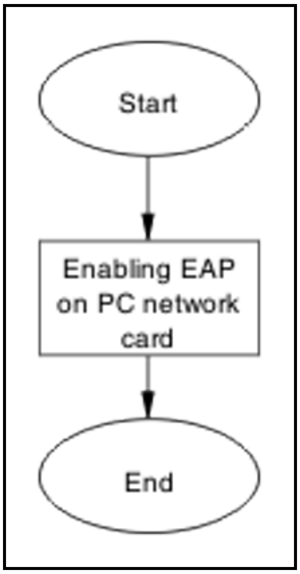
Enable EAP on The PC

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 19
Enable EAP on the PC



Navigation

- "Enabling EAP on PC network card" (page 59)

Enabling EAP on PC network card

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

Procedure Steps

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

--End--

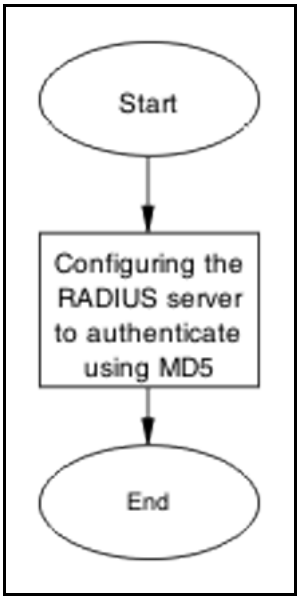
Apply the method

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 20
Apply the method



Navigation

- "Configuring the RADIUS server" (page 60)

Configuring the RADIUS server

The RADIUS server should be configured to authenticate using MD5.

Procedure Steps

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

--End--

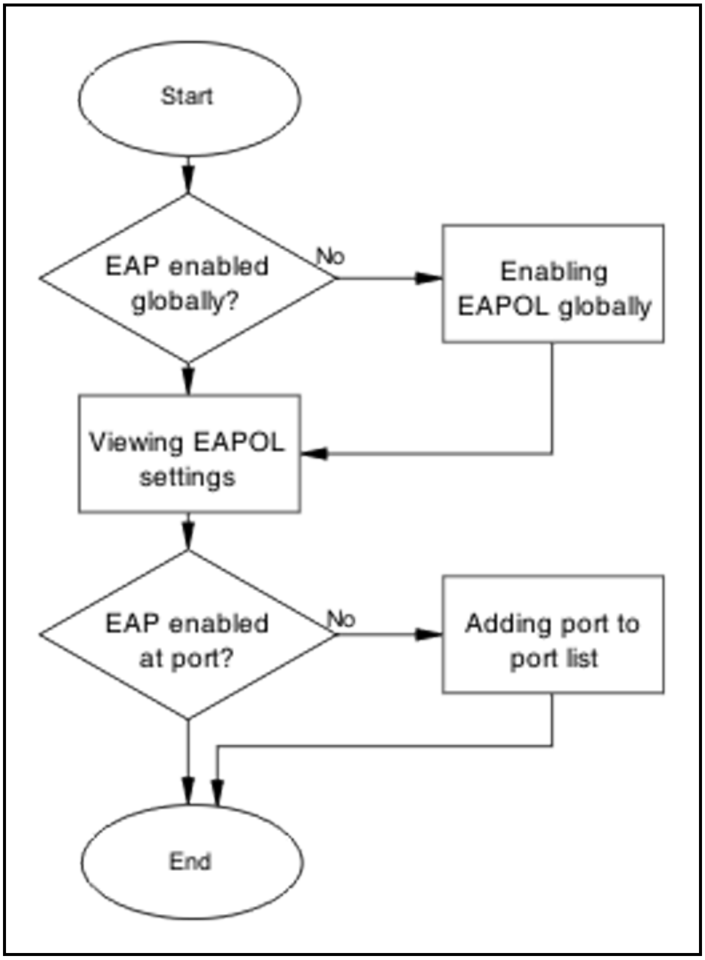
Enable EAP globally

EAP should 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 21
Enable EAP globally



Navigation

- "Enabling EAP globally" (page 61)
- "Viewing EAPOL settings" (page 62)
- "Setting EAPOL port administrative status to auto" (page 62)

Enabling EAP globally

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

Procedure Steps

Step	Action
1	Use the **`eapol enable`** command to enable EAP globally on the ERS 5500 series device.

2	Observe no errors after command execution.

--End--

Viewing EAPOL settings

The EAPOL settings should be reviewed to ensure EAP is enabled.

Procedure Steps

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

--End--

Setting EAPOL port administrative status to auto

The port should be included in the port list.

Procedure Steps

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

--End--

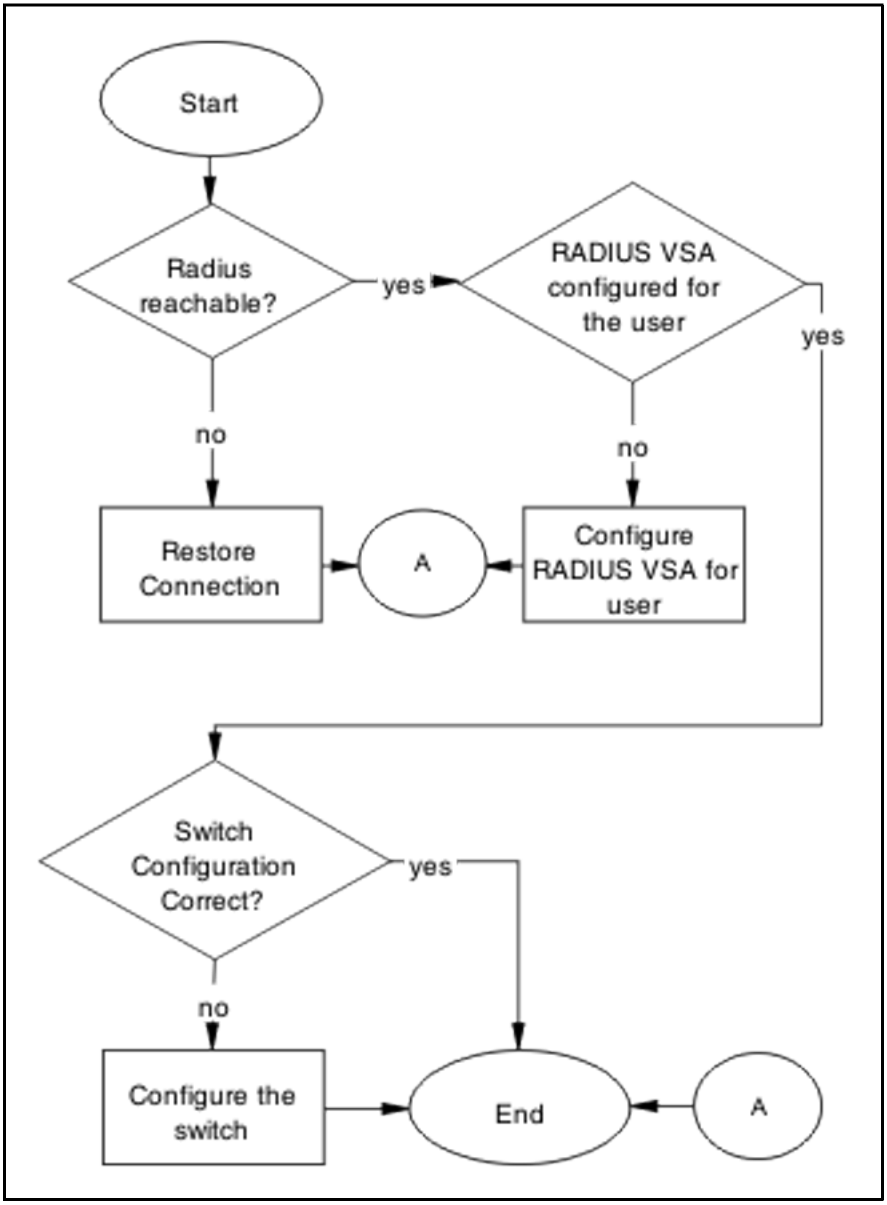
EAP user role (UBP) is not being applied

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.

Figure 22
EAP user role not being applied


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

Navigation

- "Restore RADIUS Connection" (page 63)
- "Configure RADIUS VSA for User" (page 66)
- "Configure the switch" (page 67)

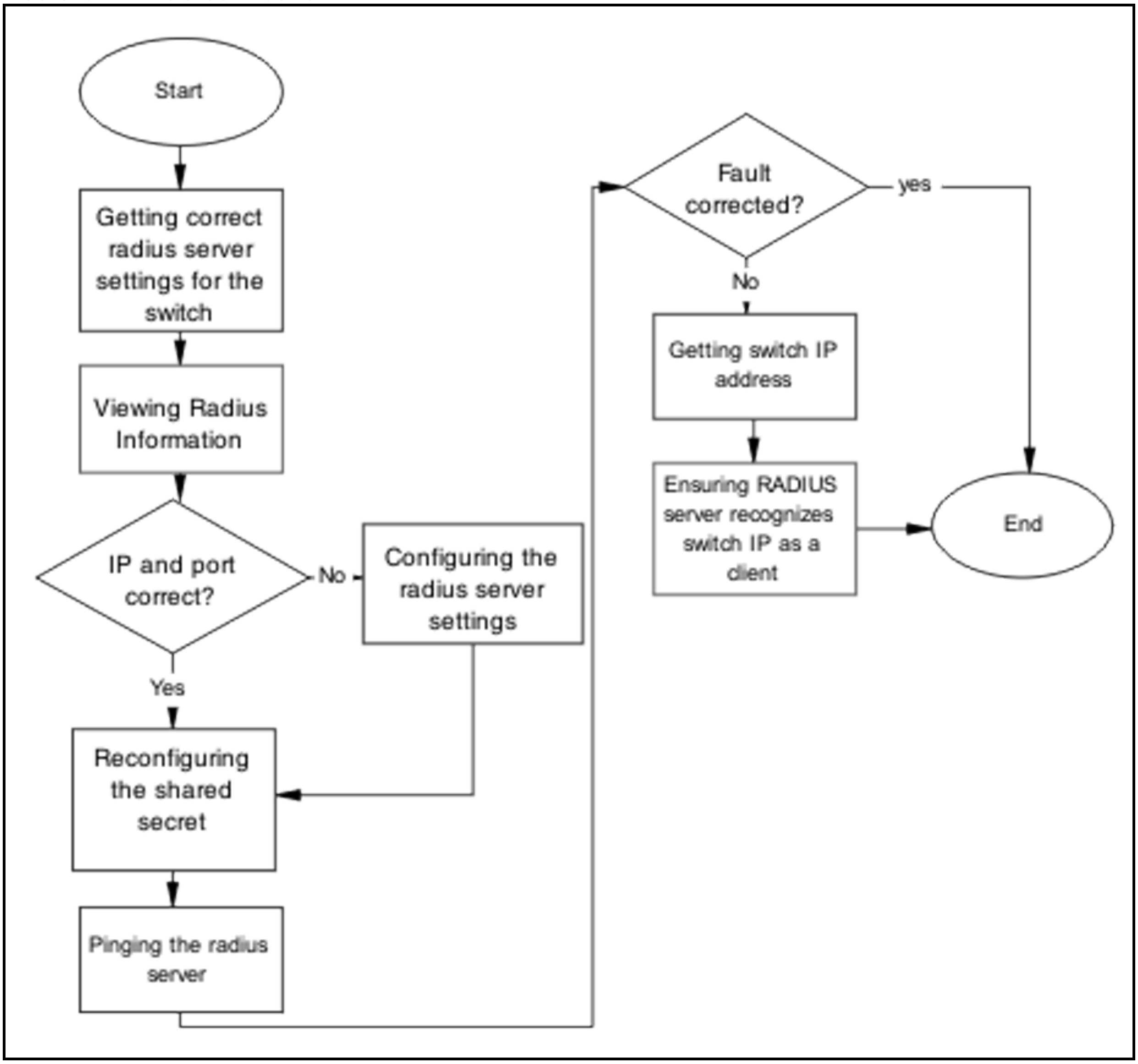
Restore RADIUS Connection

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.

Figure 23
Restore RADIUS connection


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

Navigation

- "Getting correct radius server settings for the switch" (page 65)
- "Viewing Radius Information" (page 65)
- "Configuring the RADIUS server settings" (page 65)
- "Reconfiguring the shared secret" (page 65)
- "Pinging the radius server" (page 66)

Getting correct radius server settings for the switch

Obtain the Radius server settings.

Procedure Steps

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

--End--

Viewing Radius Information

To review the Radius server settings in the device.

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

Procedure Steps

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

--End--

Configuring the RADIUS server settings

The RADIUS server settings should be set to be correct for the network.

Follow vendor documentation to set the RADIUS server.

Reconfiguring the shared secret

The Shared Secret should be reset in case there was any corruption

Procedure Steps

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

--End--

Pinging the radius server

Ping the Radius Server to ensure connection exists

Procedure Steps

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

--End--

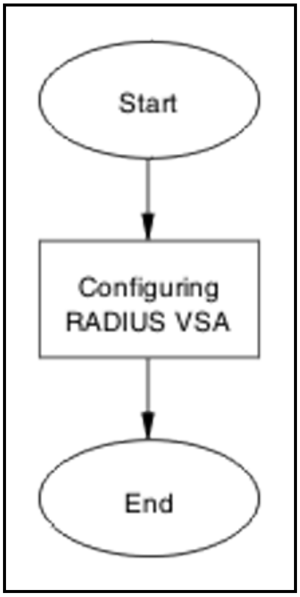
Configure RADIUS VSA for User

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 24
Configure RADIUS VSA for user



Navigation

- "Configuring RADIUS VSA for User" (page 66)

Configuring RADIUS VSA for User

Configure the RADIUS VSA for the user.

Procedure Steps

Step	Action
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 should be declared.

--End--

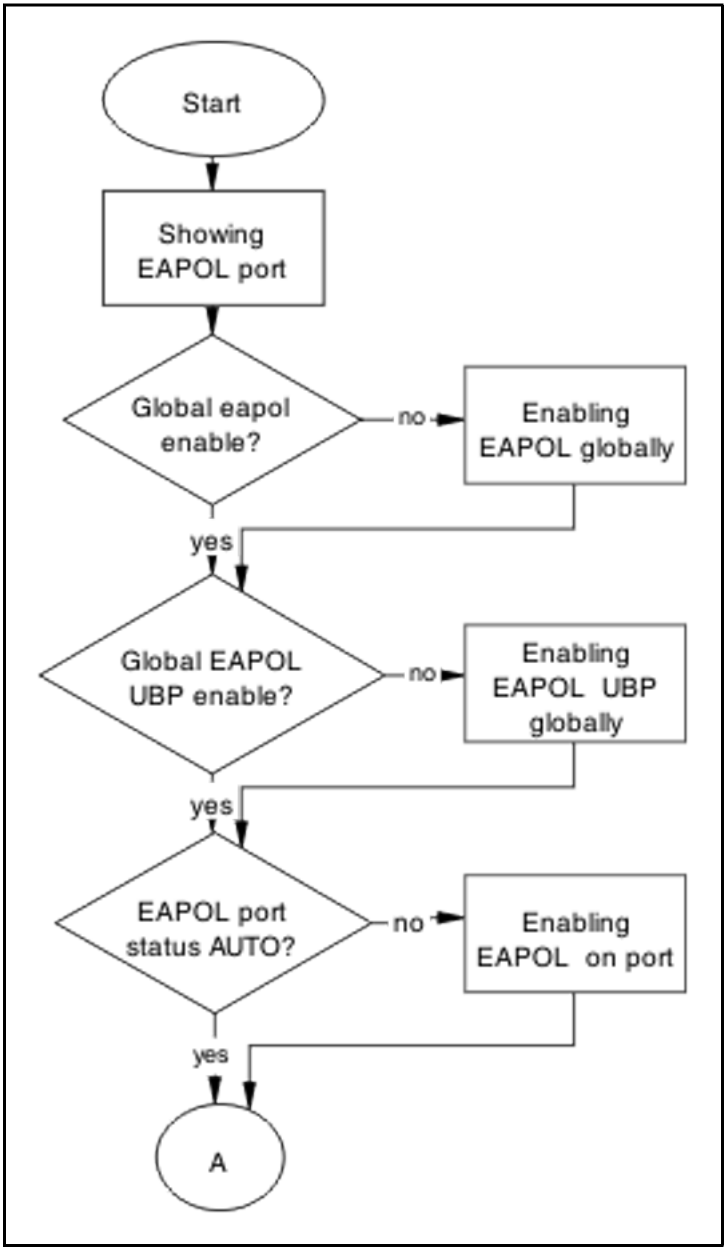
Configure the switch

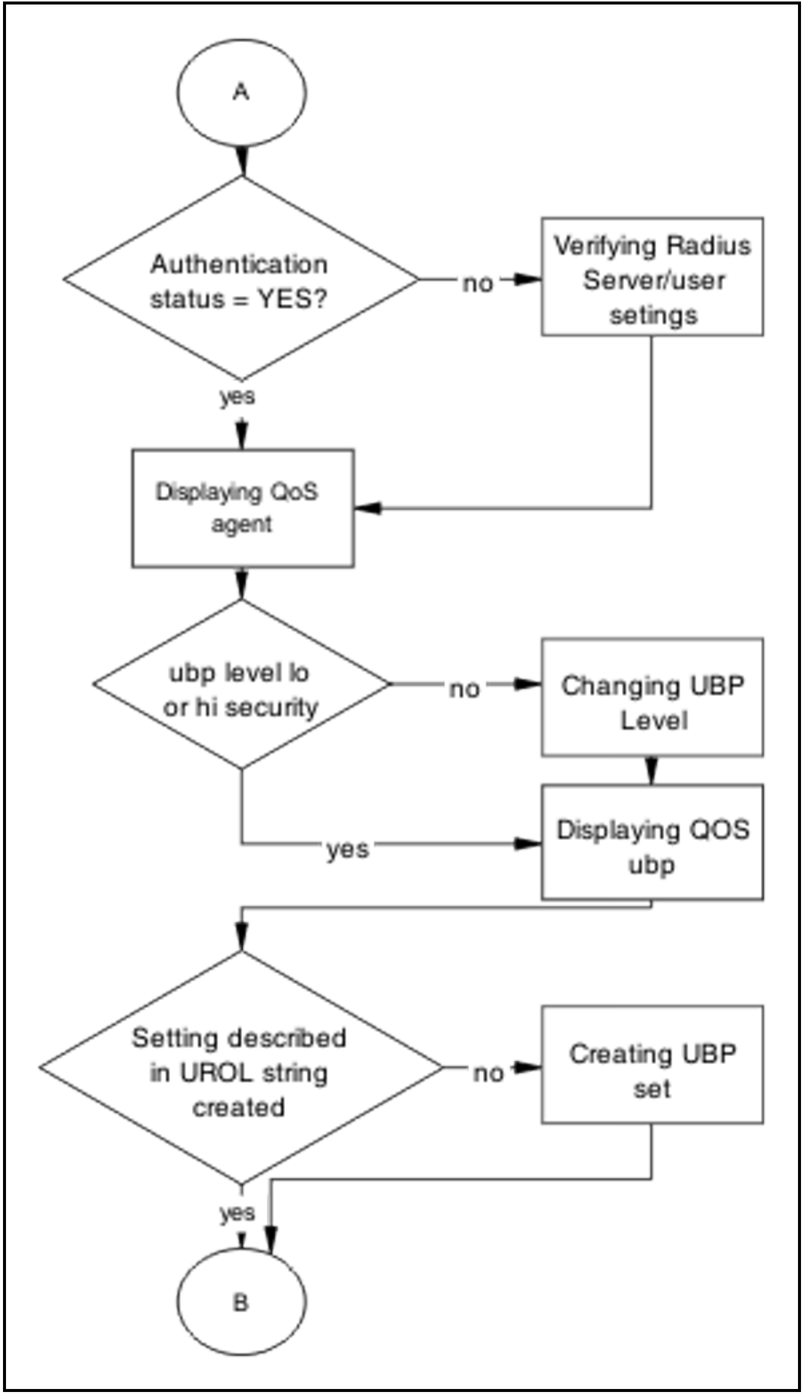
Configure the switch for UBP globally.

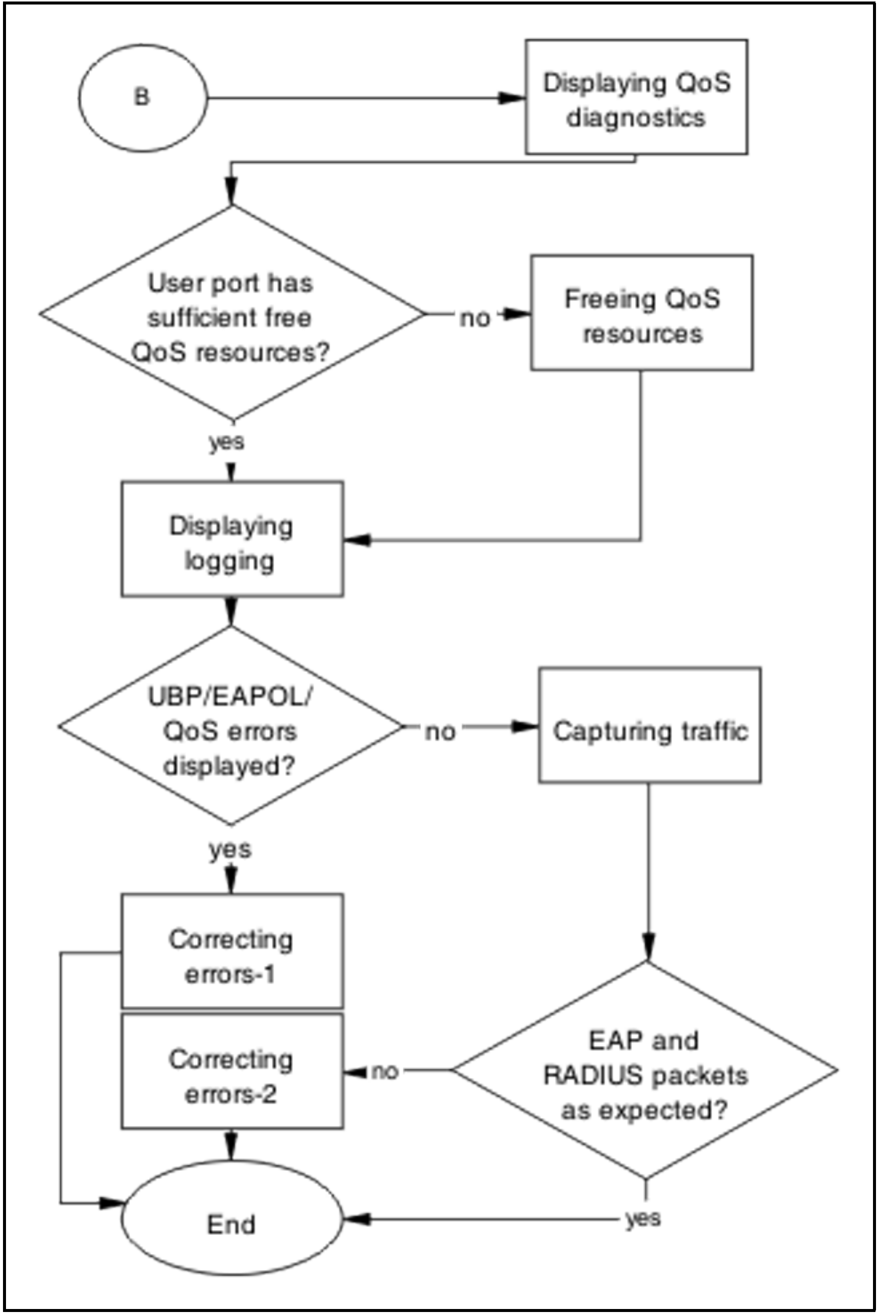
Task flow: Configure the switch

The following task flow assists you to enable UBP globally on the device.

Figure 25
Configure the switch




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


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?
End
yes

Navigation

- "Displaying EAPOL Port" (page 71)
- "Enabling EAPOL globally" (page 71)
- "Enabling EAPOL UBP globally" (page 71)
- "Enabling EAPOL on port" (page 72)
- "Verifying Radius Server/User settings " (page 73)
- "Showing QoS Agent" (page 73)

- "Changing UBP Level" (page 73)
- "Displaying QoS UBP" (page 73)
- "Creating UBP Set" (page 74)
- "Displaying QoS Diag" (page 74)
- "Freeing QoS resources" (page 74)
- "Displaying logging" (page 75)
- "Correcting errors-1" (page 75)
- "Capturing traffic " (page 75)
- "Correcting errors-2 " (page 76)

Displaying EAPOL Port

Obtain details of the EAPOL port configuration

Procedure Steps

Step	Action
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.

--End--

Enabling EAPOL globally

Enable EAPOL Globally for the switch.

Procedure Steps

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

--End--

Enabling EAPOL UBP globally

Enable EAPOL UBP globally for the switch.

Procedure Steps

Step	Action
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.

--End--

Enabling EAPOL on port

Enable EAPOL on the user port.

Procedure Steps

Step	Action
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.

--End--

Enabling EAPOL on port

Enable EAPOL on the user port.

Procedure Steps

Step	Action
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.

--End--

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.

Procedure Steps

Action

Use vendor procedures to verify the information.

Showing QoS Agent

Obtain details of the QOS Agent.

Procedure Steps

Step **Action**

1 Use the **`qos agent`** command to display the QOS agent information.

2 Verify that ubp level is low or high security.

--End--

Changing UBP Level

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

Procedure Steps

Step **Action**

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.

--End--

Displaying QoS UBP

Obtain details of QoS agent settings.

Procedure Steps

Step **Action**

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 should be UROL student).

--End--

Creating UBP Set

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

Procedure Steps

Step	Action
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.

--End--

Displaying QoS Diag

Obtain details of QoS resources usage.

Procedure Steps

Step	Action
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)).

--End--

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.

Procedure Steps

Step	Action
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)).

--End--

Displaying logging

Obtain log messages for the device.

Procedure Steps

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

--End--

Correcting errors-1

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

Procedure Steps

Step	Action
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.

--End--

Capturing traffic

Capture traffic between user PC and DUT and also between DUT and radius server.

Procedure Steps

Step	Action
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.

--End--

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.

Procedure Steps

Step	Action
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.

--End--

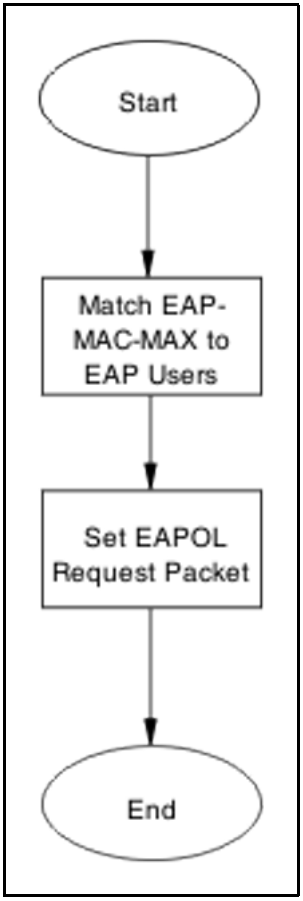
EAP multihost repeated re-authentication issue

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 26
EAP Multihost repeated re-authentication issue



Navigation

- "Match EAP-MAC-MAX to EAP users" (page 77)
- "Set EAPOL request packet" (page 79)

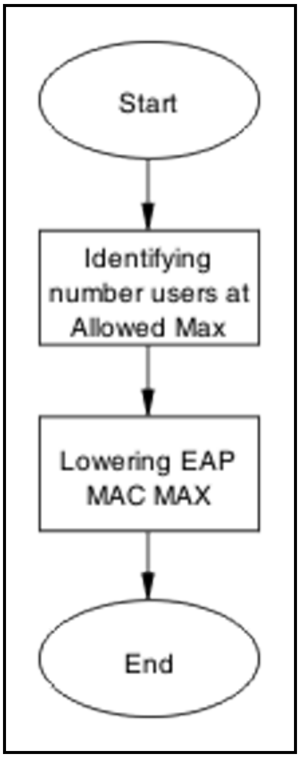
Match EAP-MAC-MAX to EAP users

Lower the eap-mac-max to the exact number of EAP users that may soon enter when the number of authenticated users reaches the allowed maximum in order 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 27
Match EAP-MAC-MAX to EAP users



Navigation

- "Identifying number users at allowed max" (page 78)
- "Lowering EAP max MAC" (page 78)

Identifying number users at allowed max

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

Procedure Steps

Action
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.

Procedure Steps

Step	Action
1	Use the **`eapol multihost eap-mac-max`** command to set the mac-max value.

2	Observe no errors after execution.

--End--

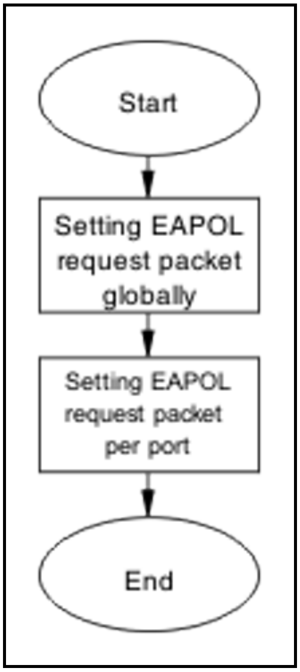
Set EAPOL request packet

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.

Figure 28
Set EAPOL request packet


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

Navigation

- "Setting EAPOL request packet globally" (page 79)
- "Setting EAPOL request packet per port" (page 80)

Setting EAPOL request packet globally

Globally change the EAPOL request packet from multicast to unicast.

Procedure Steps

Step	Action
1	Use the `eapol multihost eap-packet-mode unicast` command to set the EAPOL request packet to unicast.

2 Observe no errors after execution.

--End--

Setting EAPOL request packet per port

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

Procedure Steps

Step	Action
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.

--End--

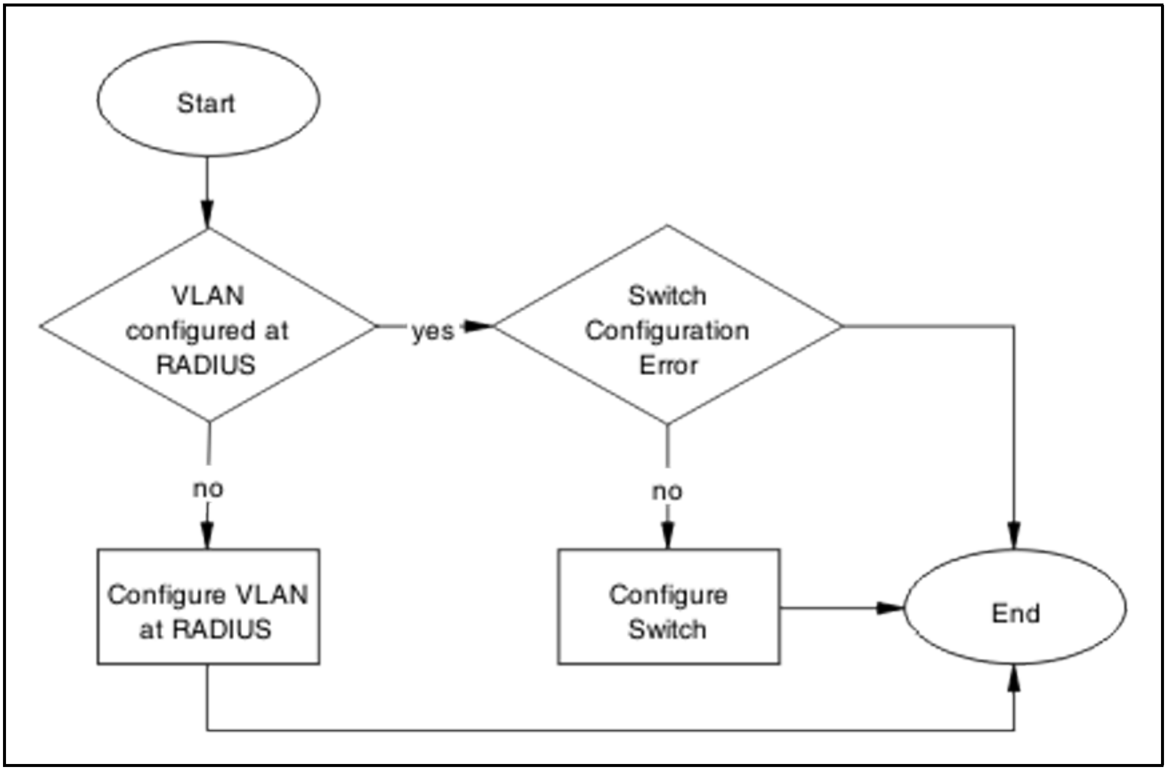
EAP RADIUS VLAN is not being applied

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 29
EAP Radius VLAN is not being applied



Navigation

- "Configure VLAN at RADIUS " (page 81)
- "Configure Switch" (page 83)

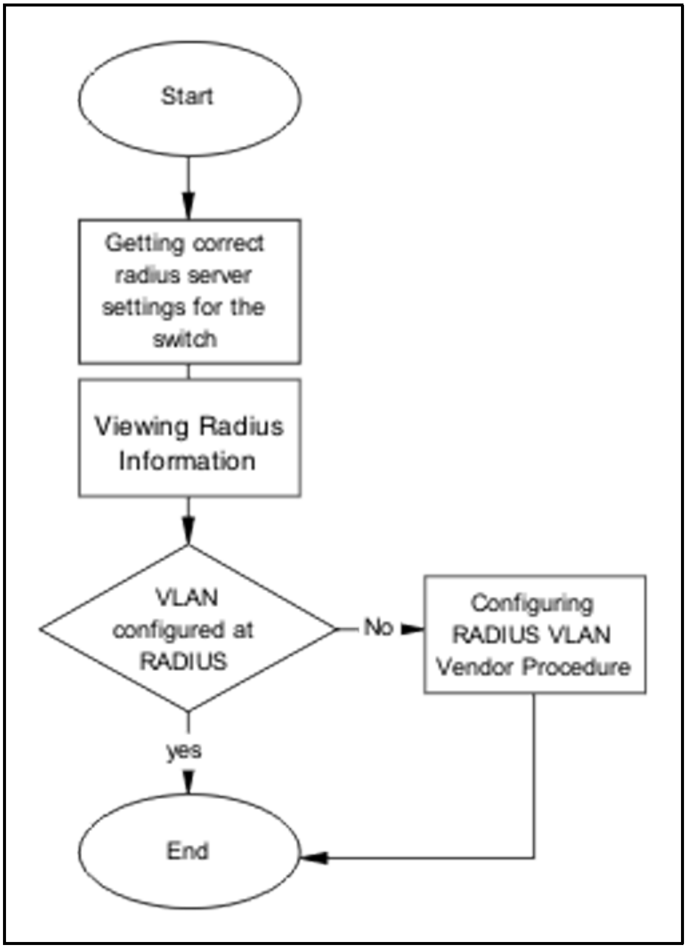
Configure VLAN at RADIUS

Correct any 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.

Figure 30
Configure VLAN at RADIUS


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

Navigation

- "Getting correct RADIUS server settings" (page 82)
- "Viewing RADIUS information" (page 83)
- "Configuring RADIUS" (page 83)

Getting correct RADIUS server settings

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

Procedure Steps

Step	Action
1	Obtain network information from Planning and Engineering documentation locate server information

2 Obtain network information for RADIUS server.

--End--

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

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

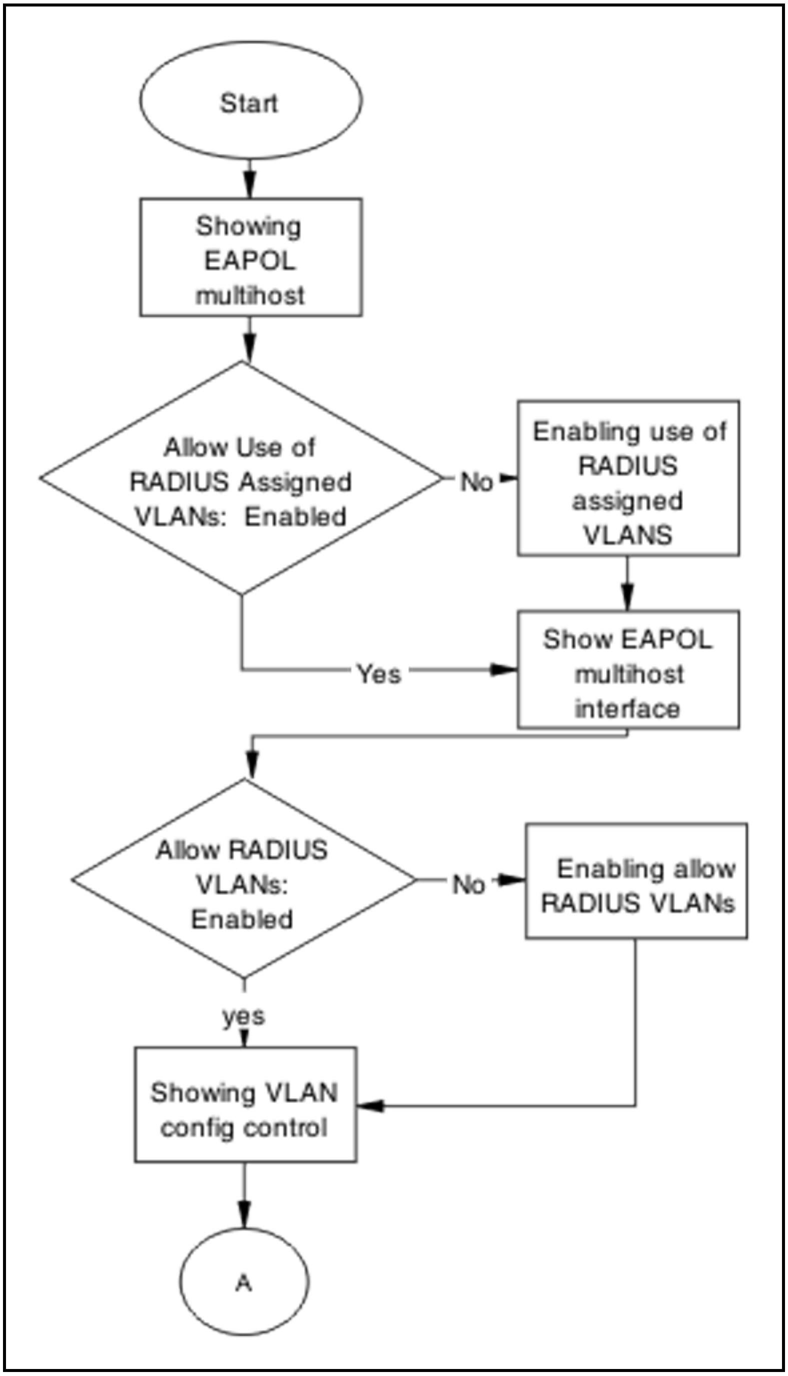
Configure Switch

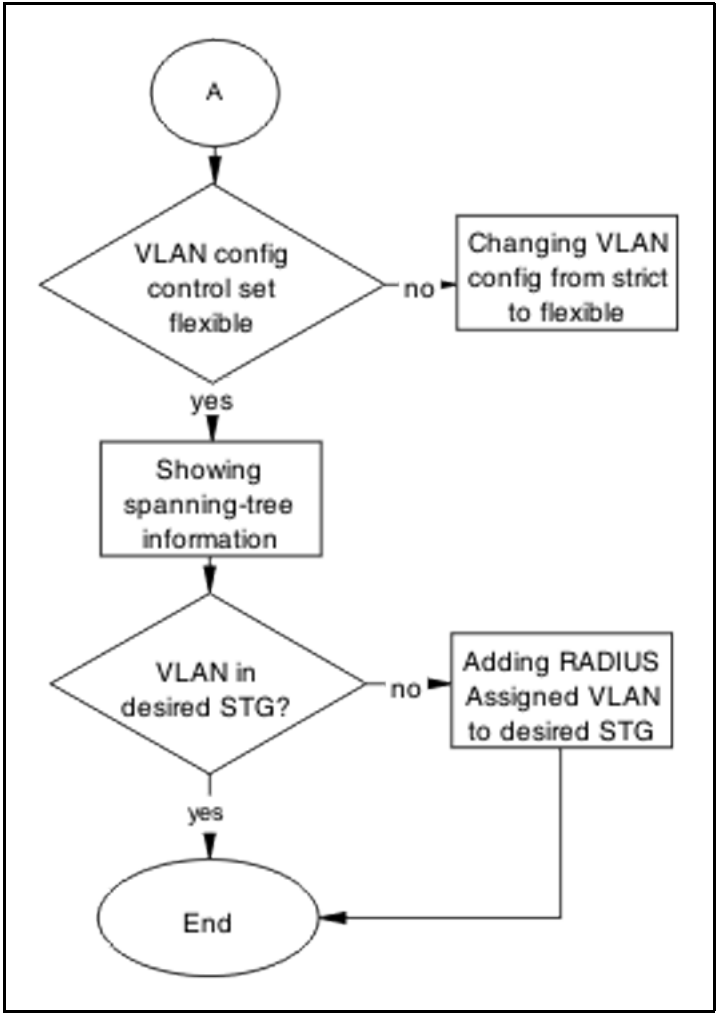
The VLAN has to be configured correctly on the ERS 5500 series device.

Task flow: Configure switch

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

Figure 31
Configure switch task


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


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

Navigation

- "Showing EAPOL Multihost" (page 85)
- "Enabling allow RADIUS VLANs" (page 86)
- "Showing EAPOL multihost interface" (page 86)
- "Enabling allow RADIUS VLANs" (page 86)
- "Showing VLAN config control" (page 86)
- "Changing VLAN config from strict to flexible" (page 87)
- "Showing Spanning Tree" (page 87)
- "Adding RADIUS assigned VLAN to desired STG" (page 87)

Showing EAPOL Multihost

Identify the EAPOL multihost information.

Procedure Steps

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

--End--

Enabling allow RADIUS VLANs

Change the allow RADIUS assigned VLAN to enable.

Procedure Steps

Step	Action
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.

--End--

Showing EAPOL multihost interface

Display the EAPOL Interface.

Procedure Steps

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

--End--

Showing VLAN config control

Display the VLAN config control information.

Procedure Steps

Step	Action
1	Use the **`show vlan config control`** command to display the information.

2	Identify if config control is set to strict.

--End--

Changing VLAN config from strict to flexible

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

Procedure Steps

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

--End--

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.

Procedure Steps

Step	Action
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.

--End--

Adding RADIUS assigned VLAN to desired STG

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

Procedure Steps

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

2 Review output to identify that the change was made.

--End--

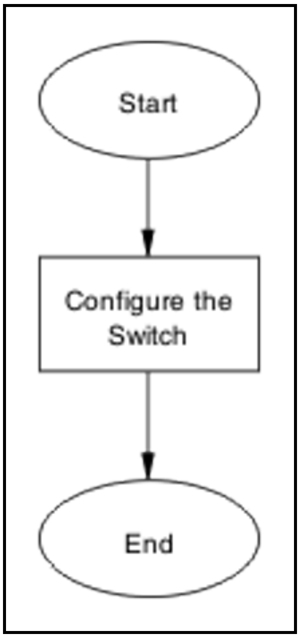
Configured MAC is not authenticating

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 32
Configured MAC is not authenticating



Navigation

- "Configure the switch" (page 88)

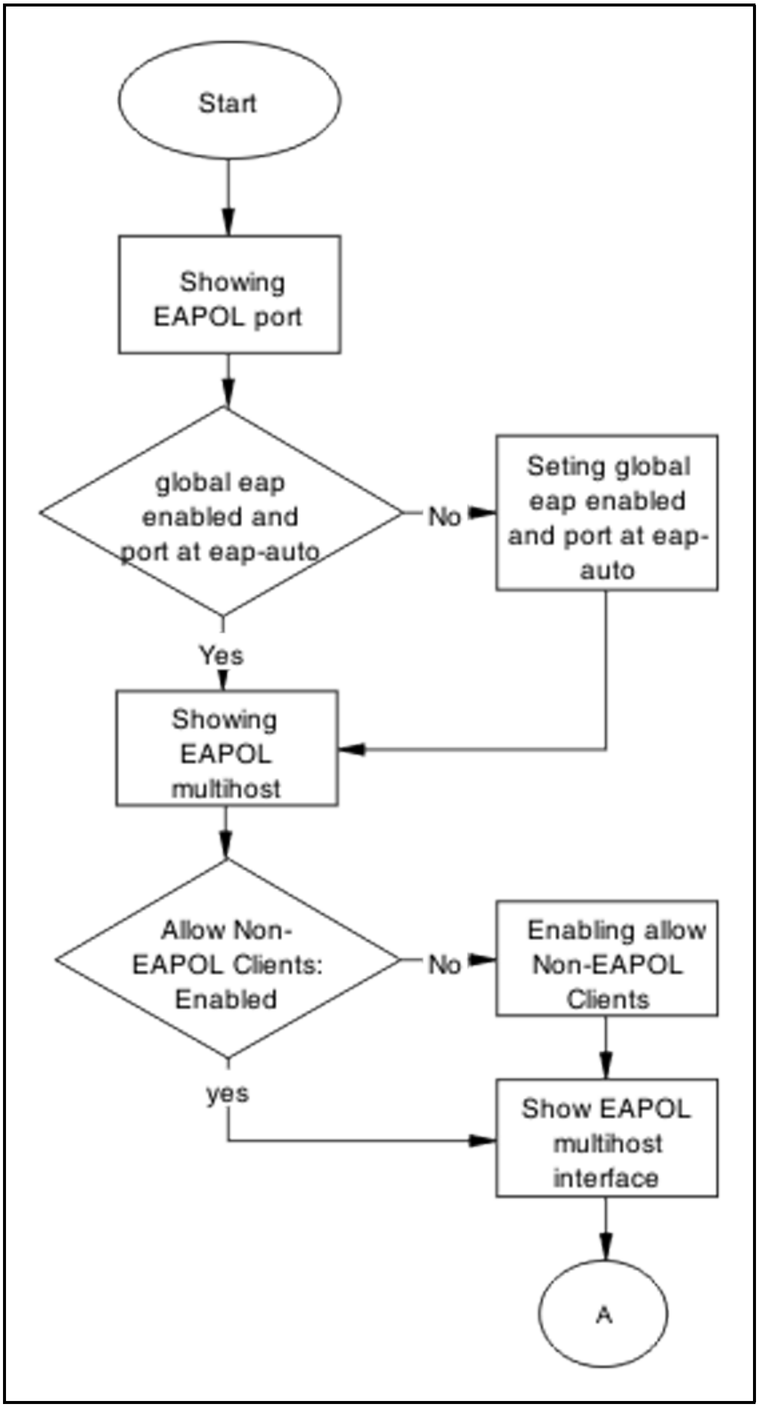
Configure the switch

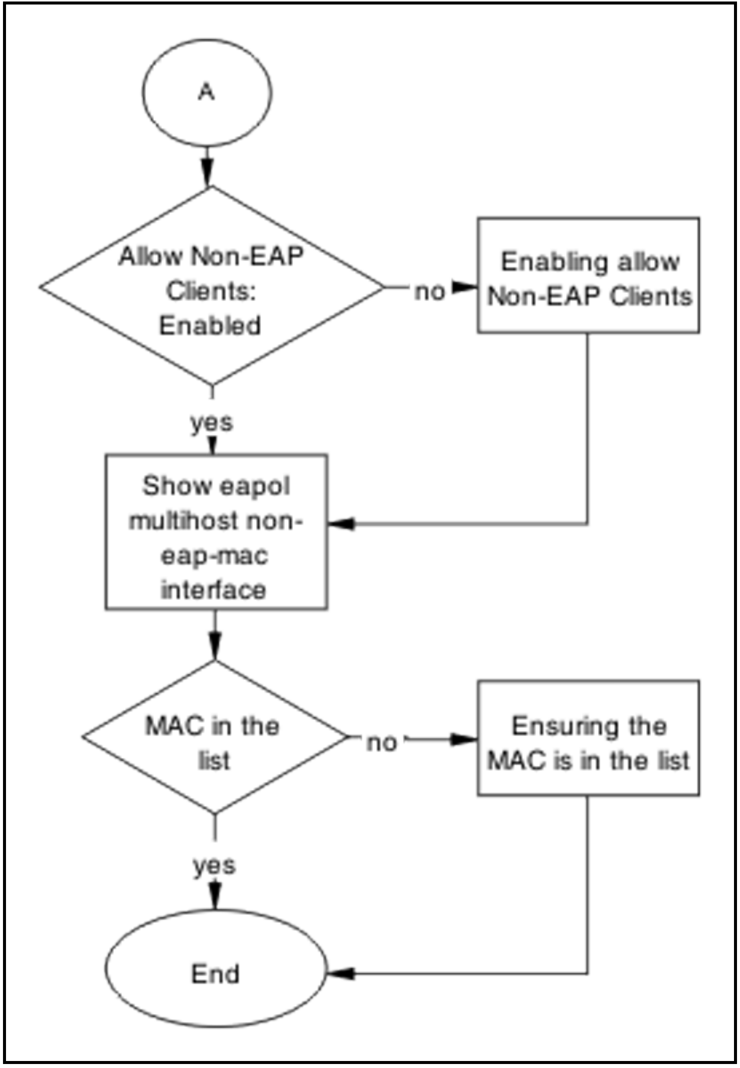
Configure the switch to ensure the correct settings are set to ensure the MAC is authenticating.

Task flow: Configure the switch

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

Figure 33
Configure the switch


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


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

Navigation

- "Showing EAPOL port" (page 90)
- "Setting global EAP enabled and port at eap-auto" (page 91)
- "Showing EAPOL multihost" (page 91)
- "Enabling Allow Non-EAPOL Clients" (page 91)
- "Showing EAPOL multihost interface " (page 92)
- "Enabling multihost status and allow non-EAPOL clients " (page 92)
- "Showing EAPOL multihost non-eap-mac interface " (page 92)
- "Ensuring MAC in the list" (page 93)

Showing EAPOL port

Display the EAPOL port information

Procedure Steps

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

--End--

Setting global EAP enabled and port at eap-auto

Make the corrections to ensure the settings as required.

Procedure Steps

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

--End--

Showing EAPOL multihost

Display the EAPOL multihost information.

Procedure Steps

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

--End--

Enabling Allow Non-EAPOL Clients

Correct the Non-EAPOL client attribute.

Procedure Steps

Step	Action
1	Use the **`eapol multihost allow-non-eap-enable`** command to enable.

2	Observe no errors after execution.

--End--

Showing EAPOL multihost interface

Display the EAPOL multihost interface information.

Procedure Steps

Step	Action
1	Enter the `show eapol multihost interface <port#>` command to display the information.
2	Note that Allow Non-EAPOL clients is enabled.
3	Note that Multihost status is enabled.

--End--

Enabling multihost status and allow non-EAPOL clients

Correct the Non-EAP client attribute.

Procedure Steps

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

--End--

Showing EAPOL multihost non-eap-mac interface

Display the EAPOL multihost interface information.

Procedure Steps

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

--End--

Ensuring MAC in the list

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

Procedure Steps

Step	Action
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.

--End--

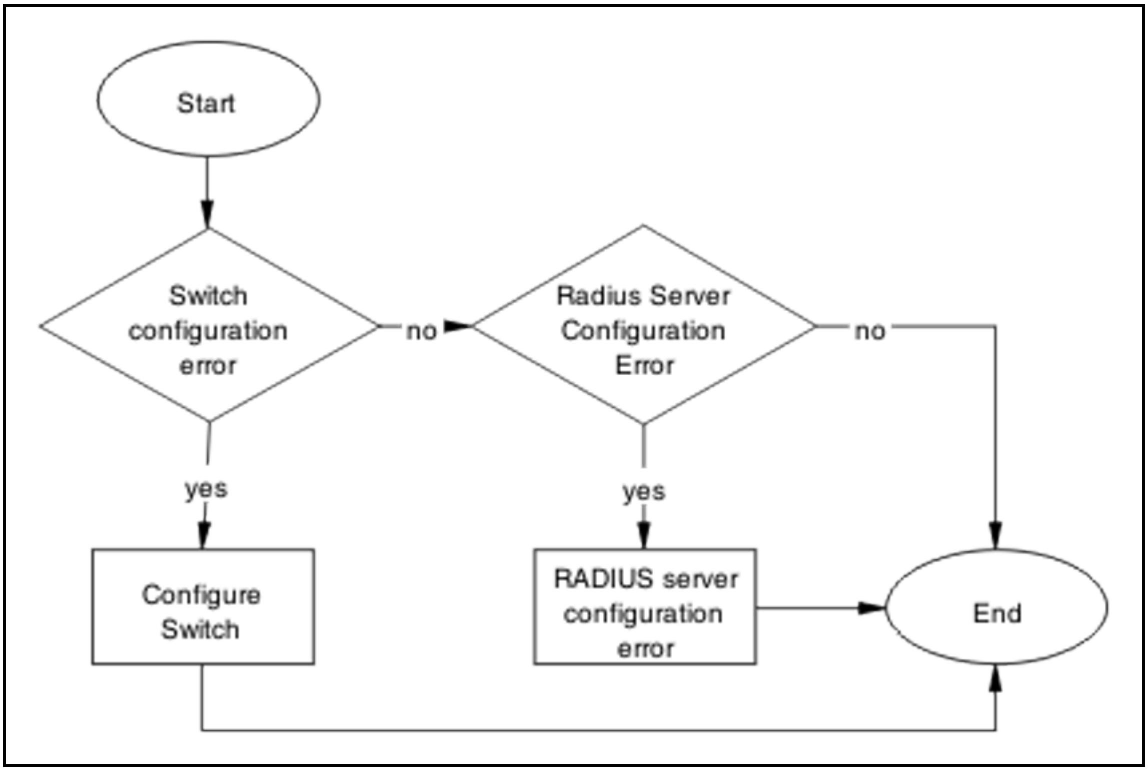
NEAP RADIUS MAC not authenticating

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.

Figure 34
NEAP RADIUS MAC not authenticating


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

Navigation

- "Configure Switch" (page 94)
- "RADIUS server configuration error" (page 97)

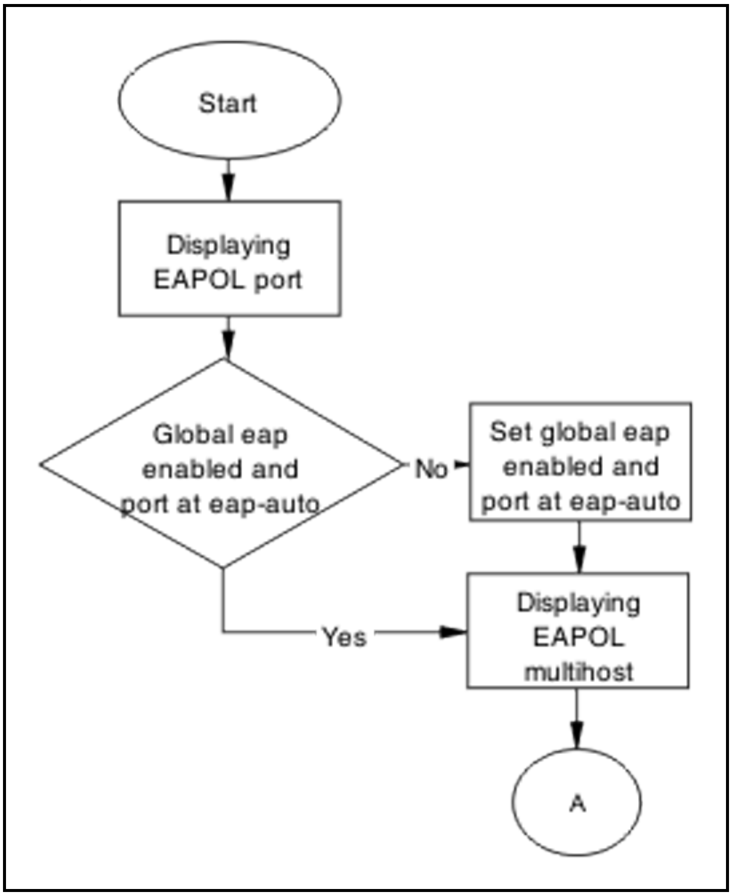
Configure Switch

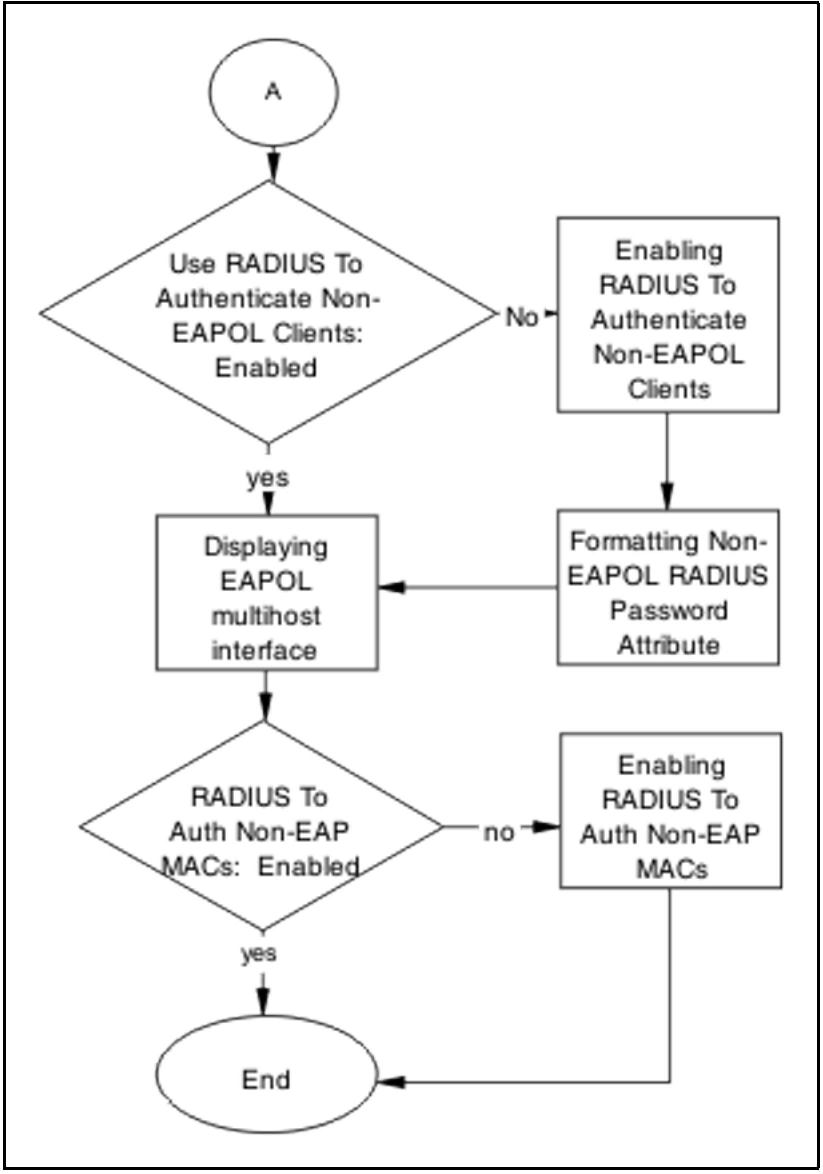
Correct switch configuration to correct issue with RADIUS MAC.

Task flow: Configure switch

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

Figure 35
Configure switch


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


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

Navigation

- "Displaying EAPOL port" (page 95)
- "Setting global eap enabled and port at eap-auto" (page 96)
- "Displaying EAPOL multihost" (page 96)
- "Enabling RADIUS to authenticate non-EAPOL clients" (page 96)
- "Formatting non-EAPOL RADIUS password attribute" (page 97)
- "Displaying EAPOL multihost interface" (page 97)
- "Enabling RADIUS To Auth Non-EAP MACs" (page 97)

Displaying EAPOL port

Display the EAPOL port information for review.

Procedure Steps

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

--End--

Setting global eap enabled and port at eap-auto

Make the required changes to ensure the settings are correct.

Procedure Steps

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

--End--

Displaying EAPOL multihost

Display the EAPOL Multihost information for review.

Procedure Steps

Step	Action
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**

--End--

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 have the format changed to **IpAddr.MACAddr.PortNumber**.

Displaying EAPOL multihost interface

Display the EAPOL Multihost information for review.

Procedure Steps

Step	Action
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

--End--

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.

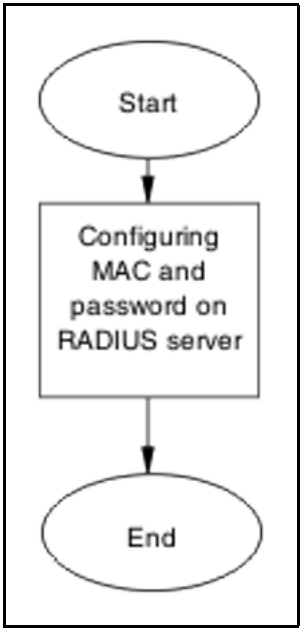
RADIUS server configuration error

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.

Figure 36
RADIUS server configuration error



Navigation

- "Configuring MAC and password on RADIUS server" (page 98)

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 may not authenticate.

Reference the vendor documentation for the RADIUS server

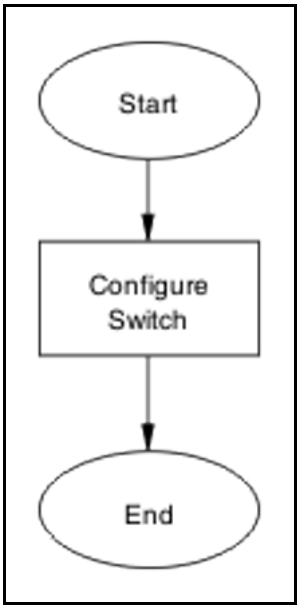
NEAP MHSA MAC is not authenticating

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 37
NEAP MHSA MAC is not authenticating



Navigation

- "Configure switch " (page 99)

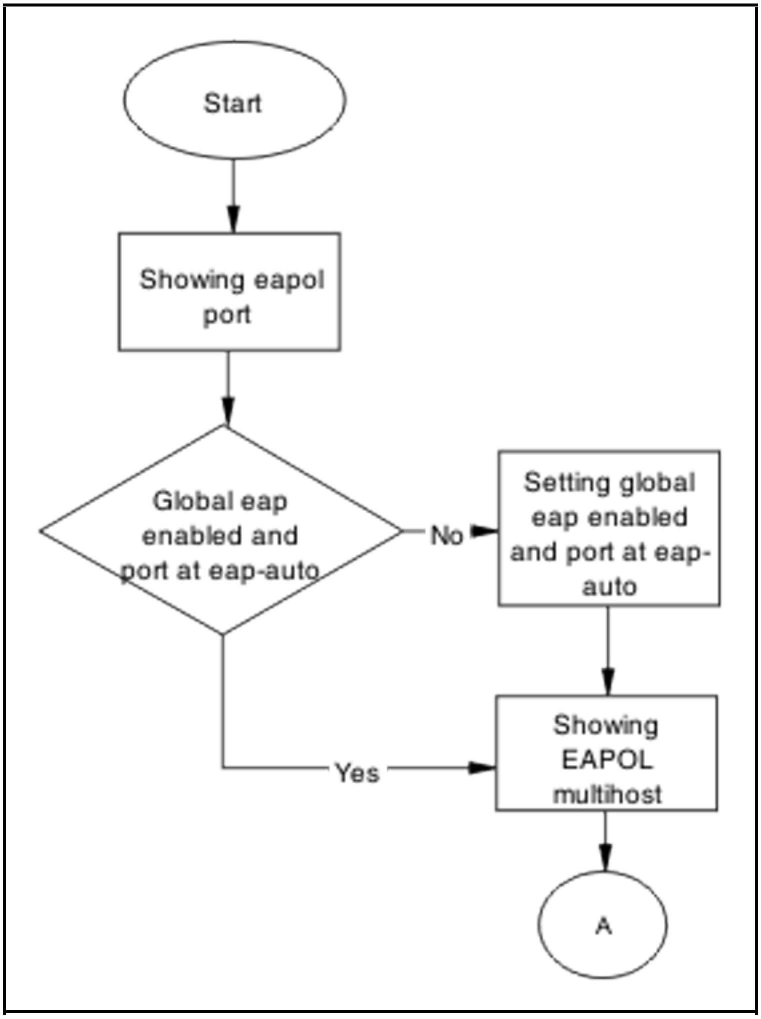
Configure switch

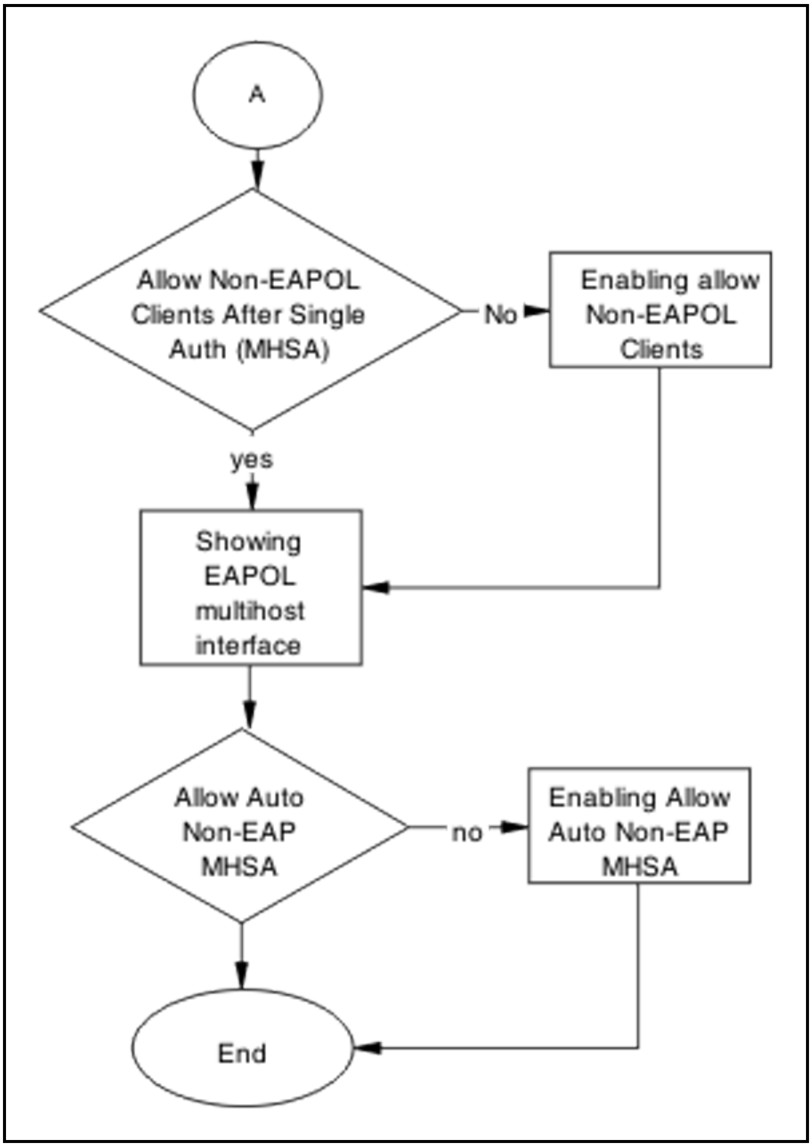
Configure the switch to enable MHSA.

Task flow: Configure switch

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

Figure 38
Configure switch


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


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

Navigation

- "Showing EAPOL port" (page 101)
- "Setting global EAP enabled and port at eap-auto" (page 102)
- "Showing EAPOL multihost" (page 102)
- "Formatting non-EAPOL RADIUS password attribute" (page 102)
- "Showing EAPOL multihost interface" (page 103)
- "Enabling RADIUS to auth Non-EAP MACs" (page 103)

Showing EAPOL port

Display the EAPOL port information for review.

Procedure Steps

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

--End--

Setting global EAP enabled and port at eap-auto

Make the required changes to ensure the settings are correct.

Procedure Steps

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

--End--

Showing EAPOL multihost

Display the EAPOL Multihost information for review.

Procedure Steps

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

--End--

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.

Procedure Steps

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

--End--

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.

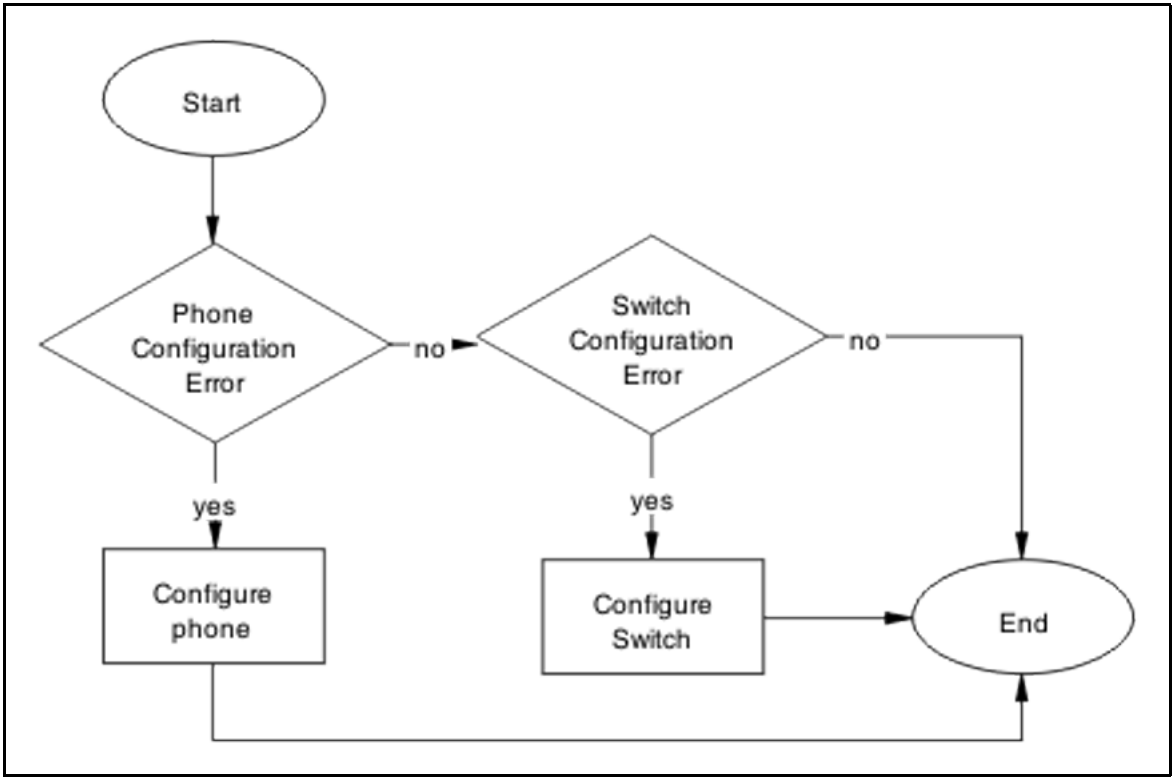
NEAP phone is not working

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 39
NEAP phone is not working



Navigation

- "Configure phone" (page 104)
- "Configure the switch" (page 105)

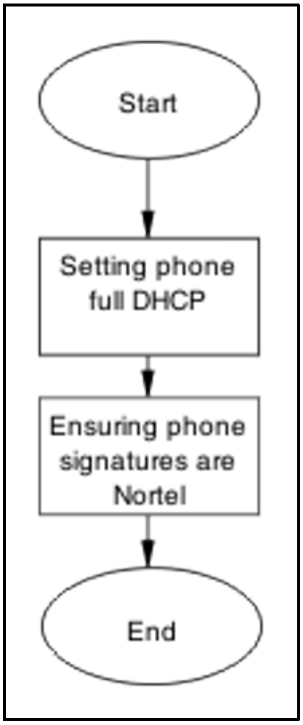
Configure phone

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 40
Configure phone



Navigation

- "Setting Phone full DHCP" (page 105)
- "Ensuring phone signatures are Nortel" (page 105)

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 Nortel

Configure the phone with Nortel signatures.

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

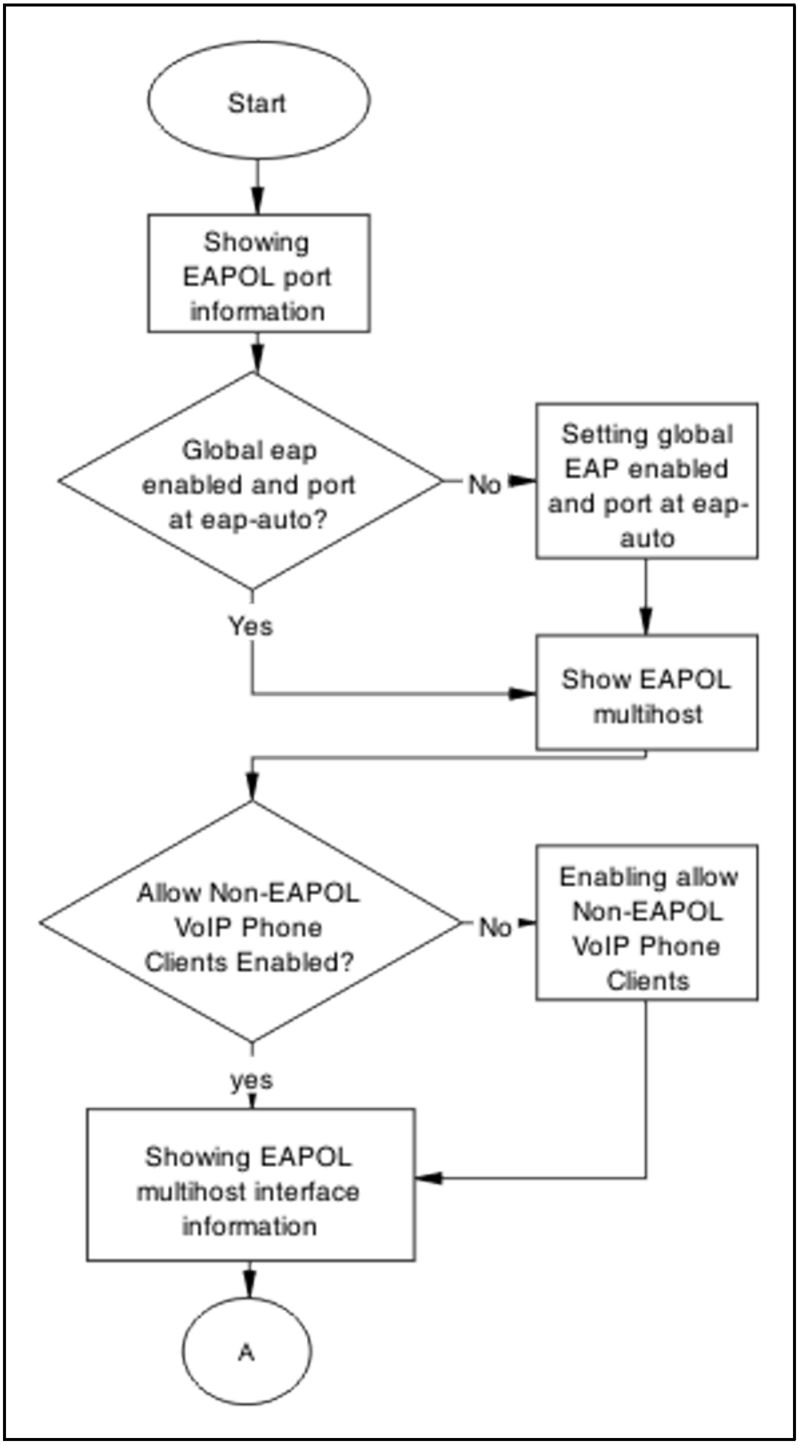
Configure the switch

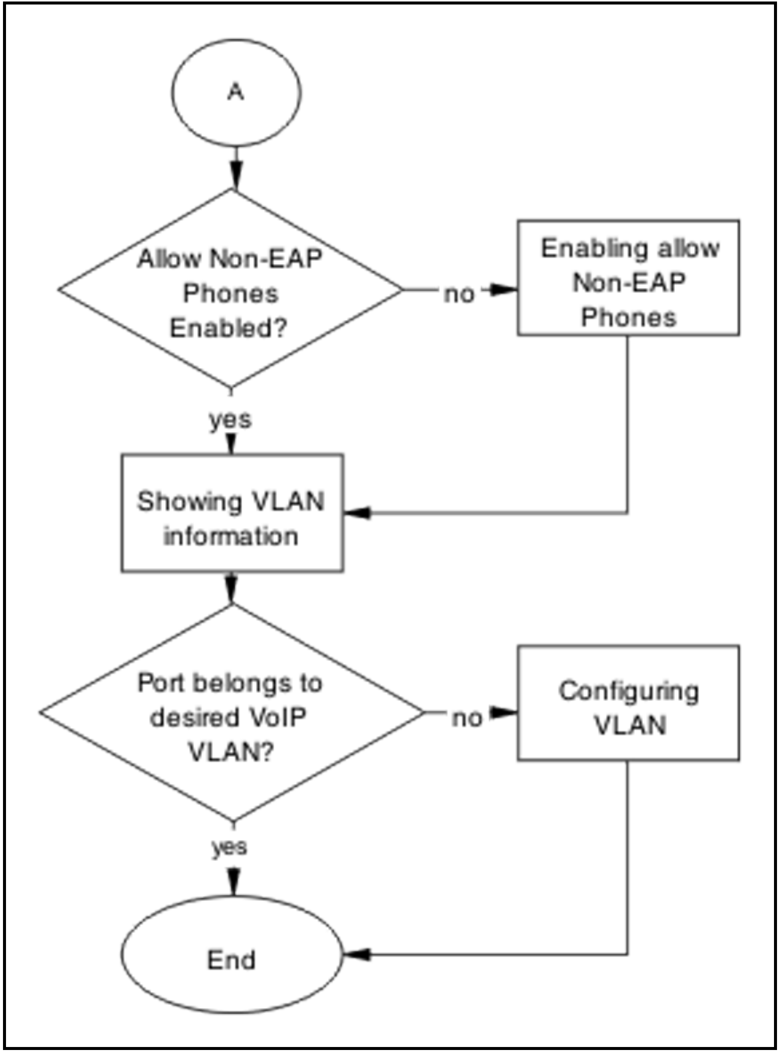
The switch has to be configured to support the phone correctly.

Task flow: Configure the switch

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

Figure 41
Configure the switch


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


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

Navigation

- "Showing EAPOL port" (page 107)
- "Setting global eap enabled and port at eap-auto" (page 108)
- "Showing EAPOL multihost" (page 108)
- "Enabling allow non-EAPOL VoIP phone clients" (page 108)
- "Showing EAPOL multihost interface" (page 109)
- "Enabling allow Non-EAP phones" (page 109)
- "Showing VLAN information" (page 109)
- "Configuring VLAN" (page 110)

Showing EAPOL port

Display the EAPOL port information for review.

Procedure Steps

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

--End--

Setting global eap enabled and port at eap-auto

Make the required changes to ensure the settings are correct.

Procedure Steps

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

--End--

Showing EAPOL multihost

Display the EAPOL Multihost information for review.

Procedure Steps

Step	Action
1	Enter the show **`eapol port multihost`** command to display the information.
2	Note the following: • Allow Non-EAPOL VoIP Phone Clients: Enabled

--End--

Enabling allow non-EAPOL VoIP phone clients

Display the EAPOL Multihost information for review.

Procedure Steps

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

--End--

Showing EAPOL multihost interface

Display the EAPOL Multihost information for review.

Procedure Steps

Step	Action
1	Enter the **`show eapol multihost interface <port#>`** command to display the information.
2	Note the following: • Allow Non-EAP Phones: Enabled

--End--

Enabling allow Non-EAP phones

Change the multihost setting to allow non-EAP phones.

Procedure Steps

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

--End--

Showing VLAN information

Display the VLAN information for review.

Procedure Steps

Step	Action
1	Enter the **`show vlan`** command to display the information.

2	Verify the following: - Ensure port belongs to desired Voip VLAN.

--End--

Configuring VLAN

Change the VLAN setting to use the correct port.

Procedure Steps

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

--End--

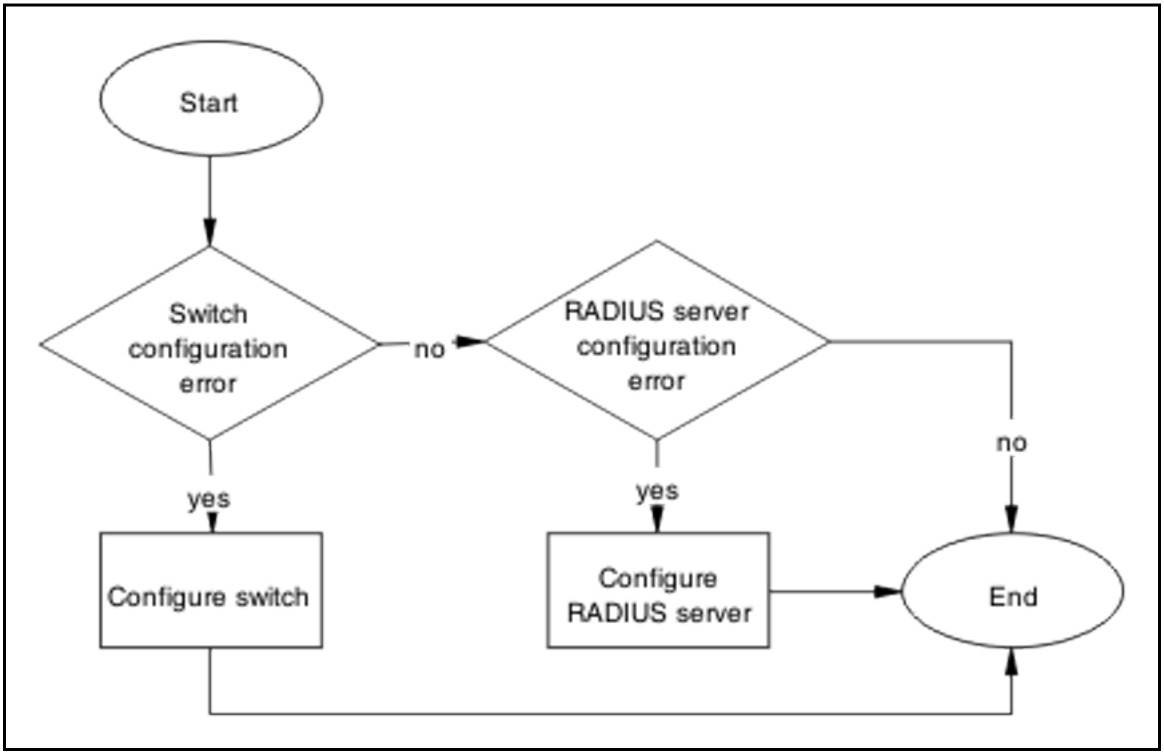
NEAP user policies from RADIUS not applied

Correct possible faults that would cause 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 42
NEAP user policies from RADIUS not applied



Navigation

- "Configure Switch" (page 111)
- "RADIUS Server Configuration" (page 126)

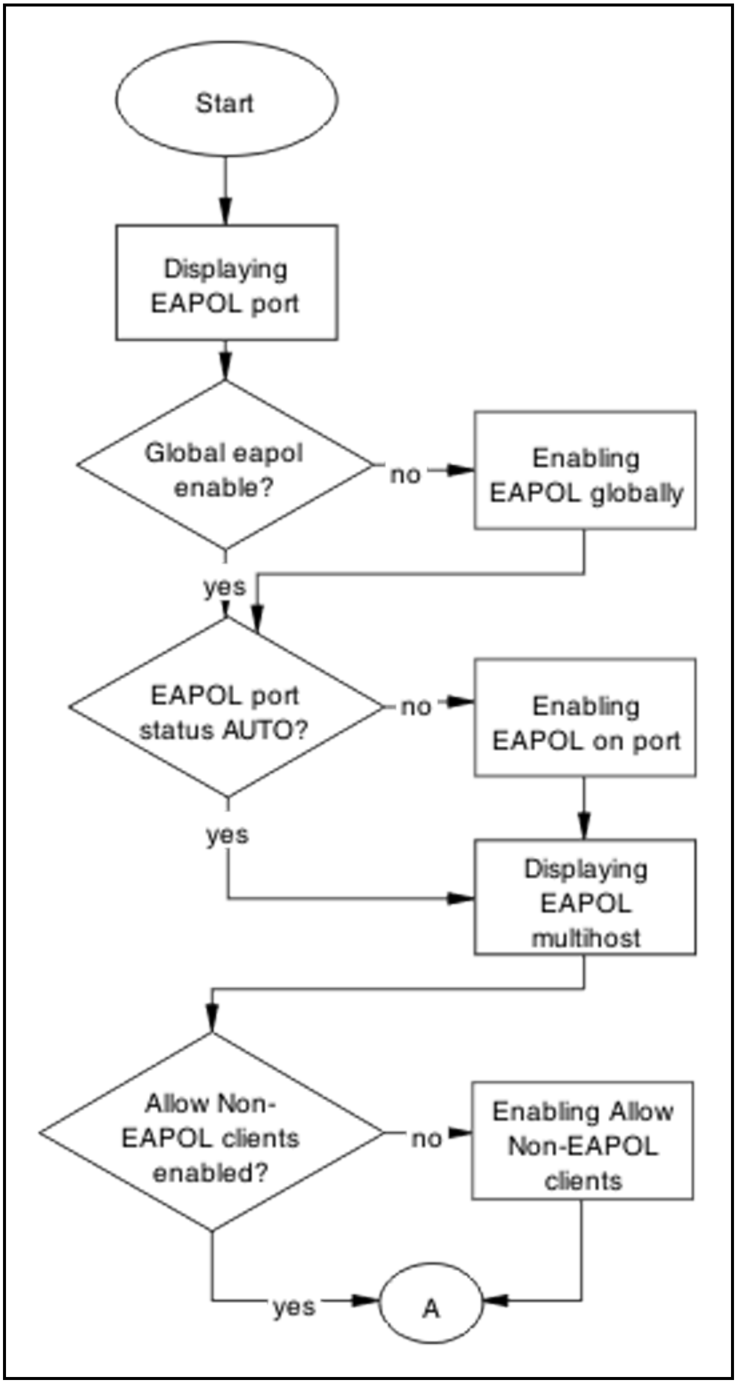
Configure Switch

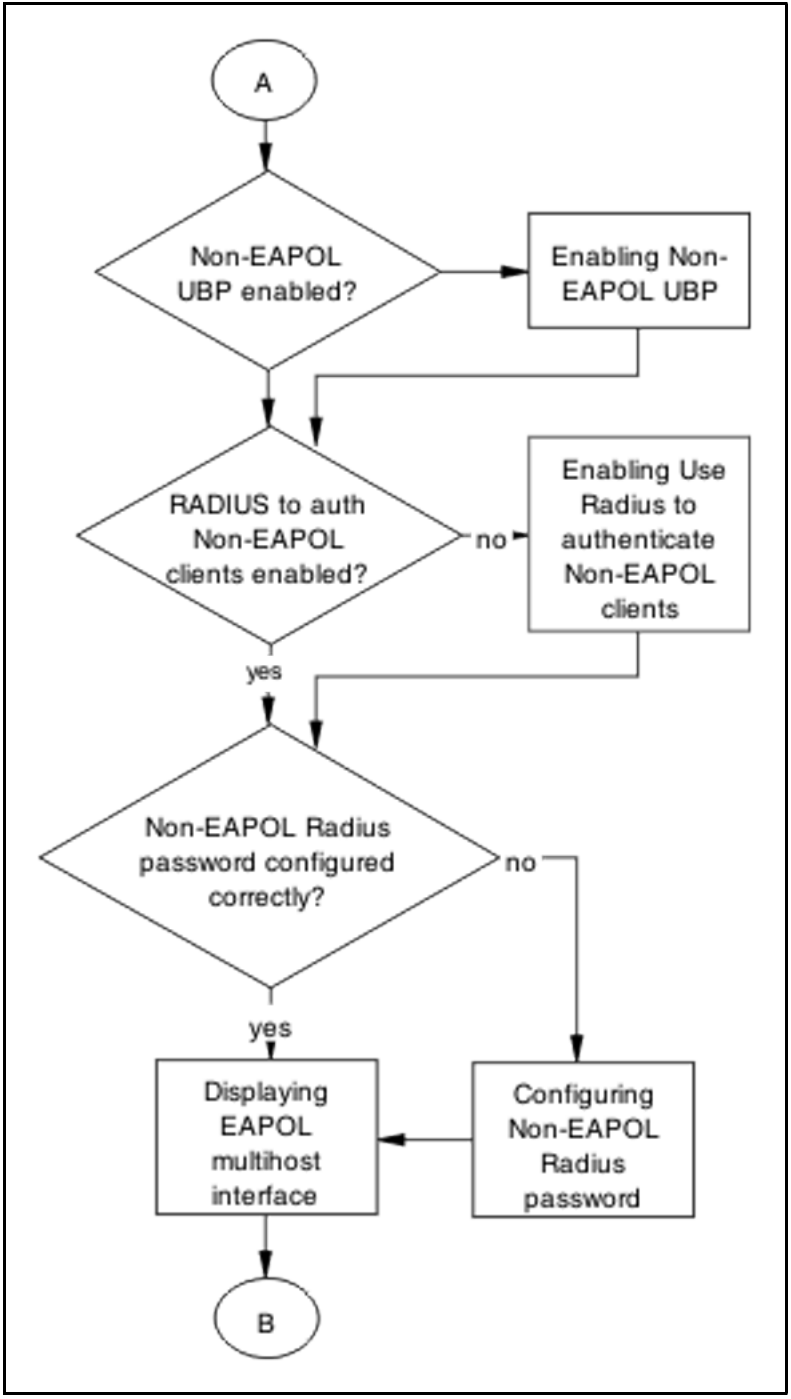
Switch configuration is configured to ensure policies are correct.

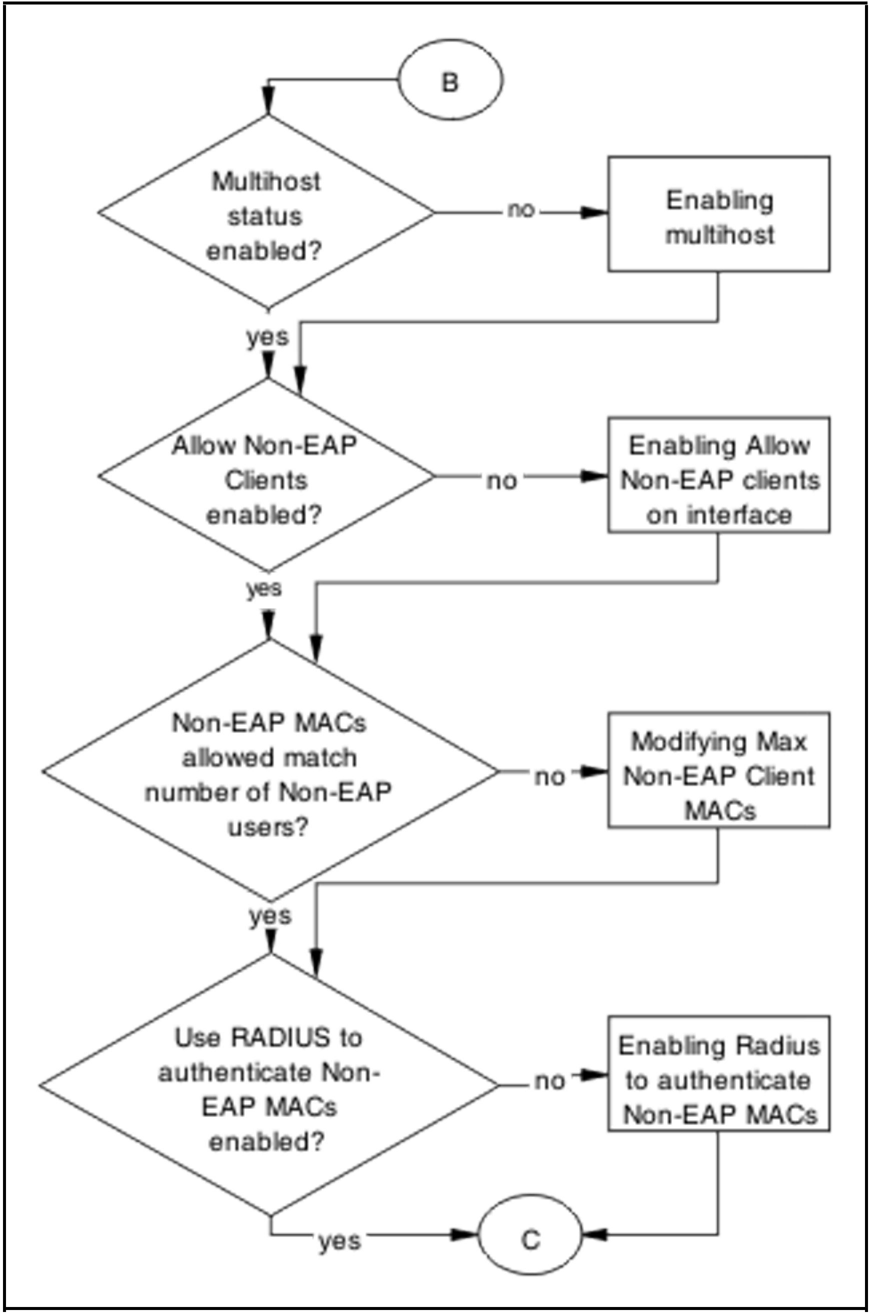
Task flow: Configure switch

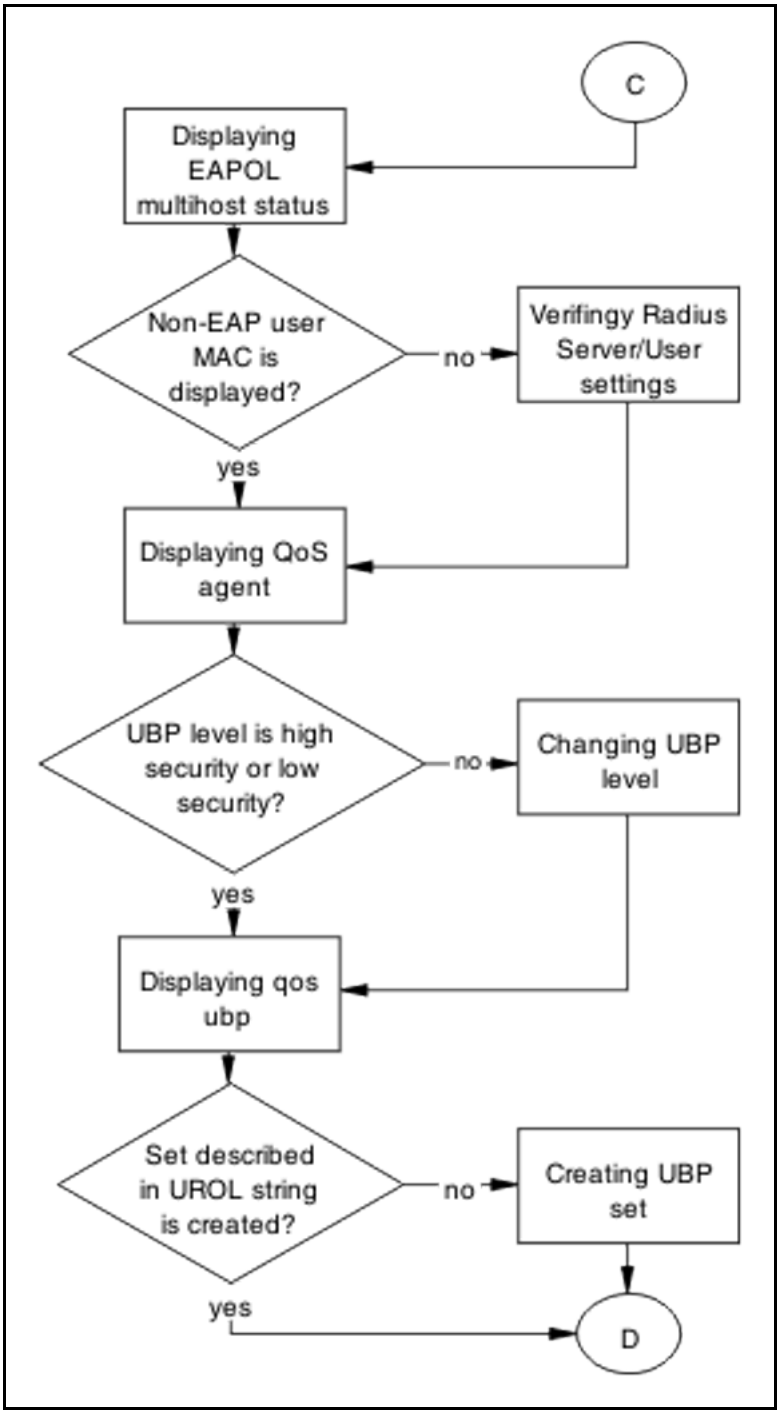
The following task flow assists you to configure the ERS 5500 series device with the correct policies.

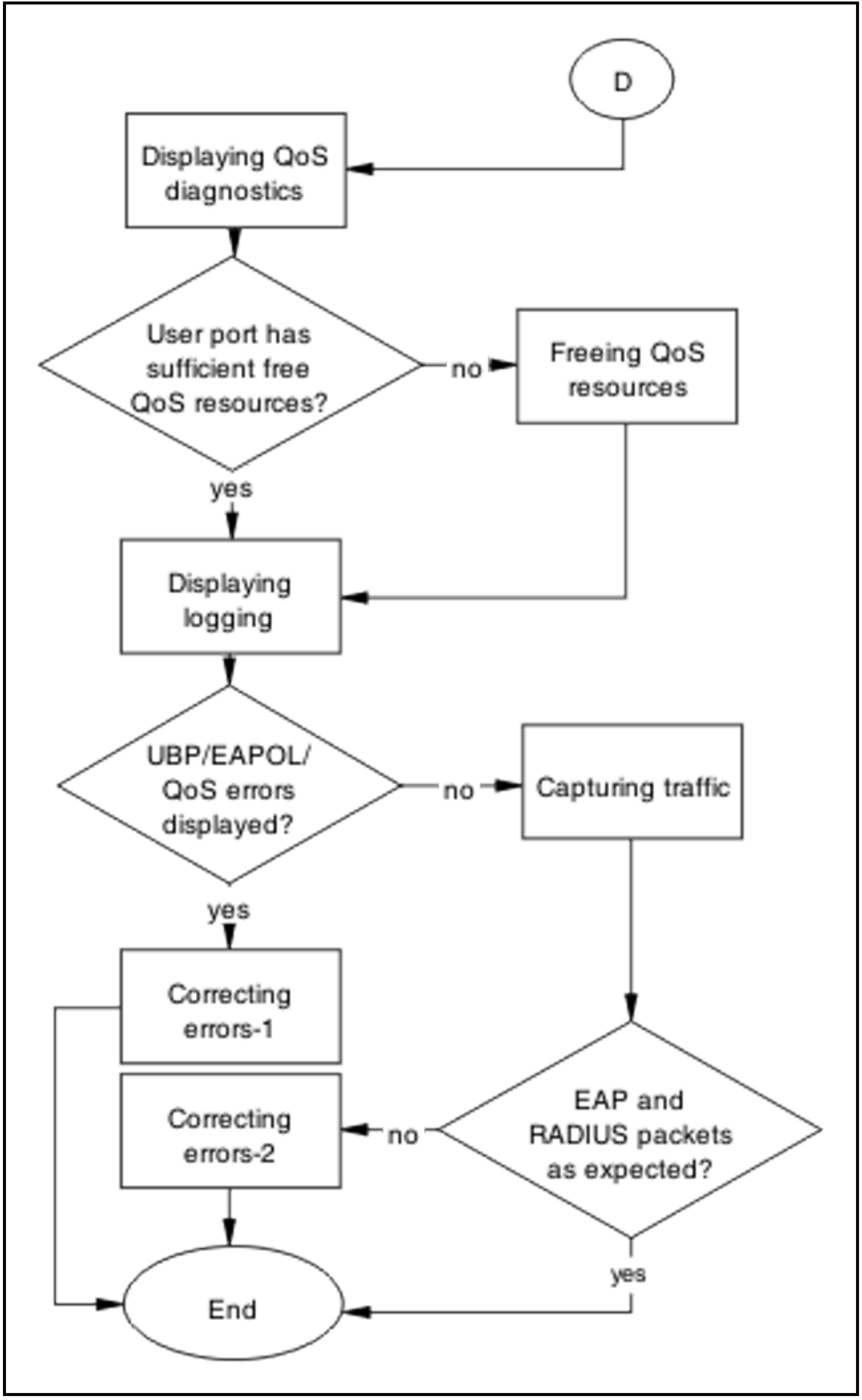
Figure 43
Configure switch




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


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


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


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

Navigation

- "Displaying EAPOL port " (page 117)
- "Enabling EAPOL globally" (page 118)
- "Enabling EAPOL UBP globally" (page 118)
- "Enabling EAPOL on port" (page 118)

Displaying EAPOL port

Obtain details of the EAPOL port configuration.

Procedure Steps

Step	Action
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

--End--

Enabling EAPOL globally

Enable EAPOL globally for the switch.

Procedure Steps

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

--End--

Enabling EAPOL UBP globally

Enable EAPOL UBP globally for the switch.

Procedure Steps

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

--End--

Enabling EAPOL on port

Enable EAPOL on the user port.

Procedure Steps

Step	Action
1	Use the **`eapol port <port>`** command to enable EAPOL on port.

2 Check that no error or warning message is displayed.

--End--

Displaying EAPOL multihost

Obtain the details for EAPOL multihost global settings.

Procedure Steps

Step Action

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

--End--

Enabling allow Non-EAPOL clients

Enable processing for non-eapol clients.

Procedure Steps

Step Action

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.

--End--

Enabling Non-EAP UBP

Enable Non-EAP UBP.

Procedure Steps

Step	Action
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.

--End--

Enabling use RADIUS to authenticate Non-EAPOL clients

Enable authentication using Radius Server for Non-EAP clients.

Procedure Steps

Step	Action
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.

--End--

Configuring Non-EAPOL RADIUS password

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

Procedure Steps

Step	Action
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.

--End--

Displaying EAPOL multihost interface

Obtain the details for EAPOL multihost interface settings.

Procedure Steps

Step Action

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

--End--

Enabling multihost on interface

Enable processing for multihost on the specified interface.

Procedure Steps

Step Action

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.

--End--

Enabling allow non-EAP clients

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

Procedure Steps

Step Action

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.

--End--

Modifying max non-EAP client MACs

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

Procedure Steps

Step	Action
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.

--End--

Displaying EAPOL multihost status

Obtain the status for EAPOL multihost interface.

Procedure Steps

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

--End--

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.

Procedure Steps

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

--End--

Changing UBP Level

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

Procedure Steps

Step	Action
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.

--End--

Displaying QoS UBP

Obtain details of QoS agent settings.

Procedure Steps

Step	Action
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 should be UROLstudent) .

--End--

Creating UBP Set

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

Procedure Steps

Step	Action
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.

--End--

Displaying QoS Diag

Obtain details of QoS resources usage.

Procedure Steps

Step	Action
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)).

--End--

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.

Procedure Steps

Step	Action
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)).

--End--

Displaying logging

Obtain log messages for the device.

Procedure Steps

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

--End--

Correcting errors-1

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

Procedure Steps

Step	Action
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.

--End--

Capturing traffic

Capture traffic between user PC and DUT and also between DUT and radius server.

Procedure Steps

Step	Action
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.

--End--

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.

Procedure Steps

Step	Action
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.

--End--

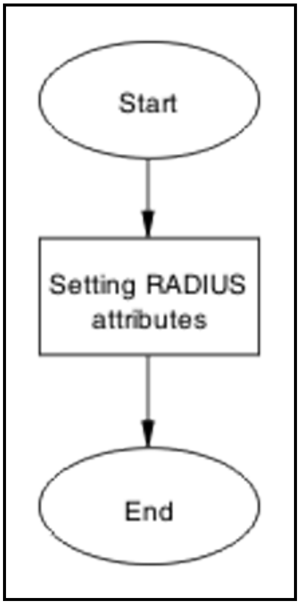
RADIUS Server Configuration

Correct the RADIUS server configuration.

Task flow: RADIUS server configuration

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

Figure 44
RADIUS server configuration



Navigation

- "Setting RADIUS attributes" (page 127)

Setting RADIUS attributes

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

Procedure Steps

Action

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

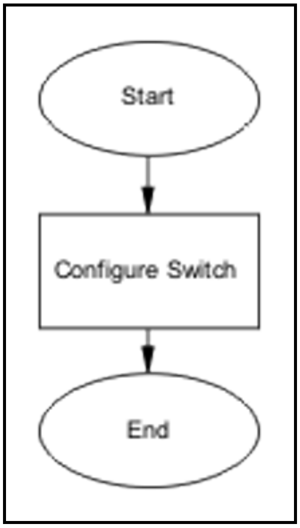
EAP-NEAP unexpected port shutdown

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 45
EAP-NEAP unexpected port shutdown



Navigation

- "Configure Switch" (page 127)

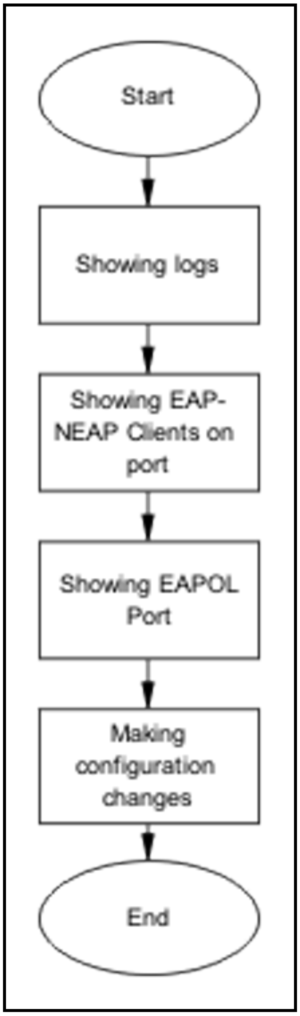
Configure Switch

Configure ports to allow more unauthorized clients.

Task flow: Configure switch

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

Figure 46
Configure switch


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

Navigation

- "Showing Logs" (page 128)
- "Showing EAP-NEAP clients on port" (page 129)
- "Showing EAPOL port information" (page 129)
- "Making changes" (page 129)

Showing Logs

Display log information for detailed information to provide any additional information.

Procedure Steps

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

--End--

Showing EAP-NEAP clients on port

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

Procedure Steps

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

--End--

Showing EAPOL port information

Display EAPOL port information for detailed information to provide any additional information.

Procedure Steps

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

--End--

Making changes

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

Procedure Steps

Step	Action
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.

--End--

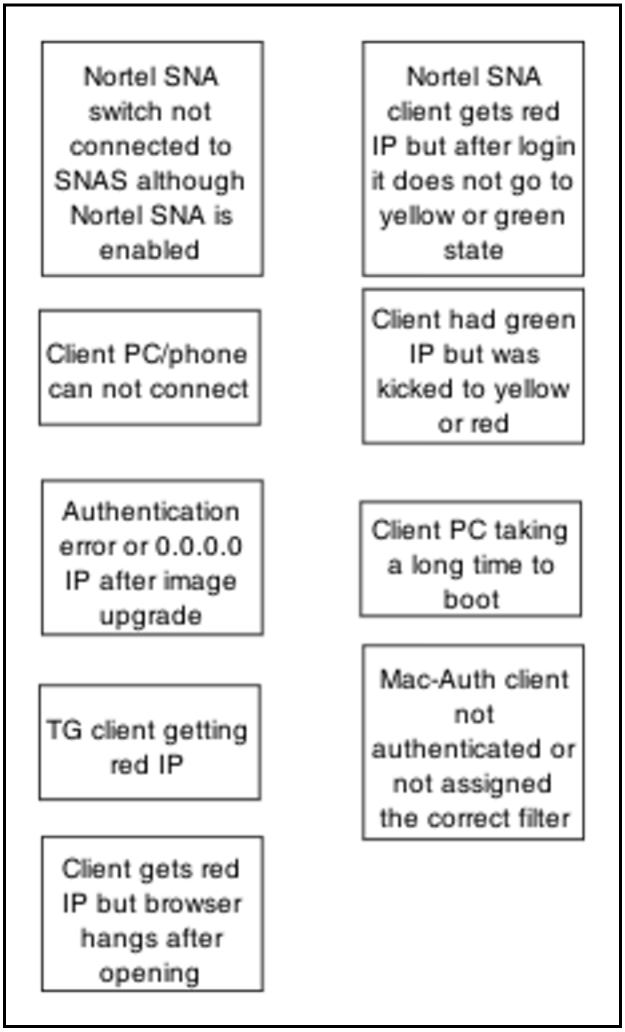
Troubleshooting Nortel SNAS

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

Troubleshooting Nortel SNAS work flow

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

Figure 47
Troubleshooting Nortel SNAS


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

Navigation

- "Nortel SNA switch not connected to Nortel SNAS although Nortel SNA is enabled" (page 133)
- "Client PC/phone can not connect" (page 142)
- "Authentication error or 0.0.0.0 IP after image upgrade" (page 151)
- "TG client getting red IP" (page 155)
- "Client gets red IP but browser hangs after opening" (page 158)
- "Nortel SNA client gets red IP but after login it does not go to yellow or green state" (page 159)
- "Client had green IP but was kicked to yellow or red" (page 161)

- "Client PC taking a long time to boot" (page 164)
- "Mac-Auth client not authenticated or not assigned the correct filter" (page 166)

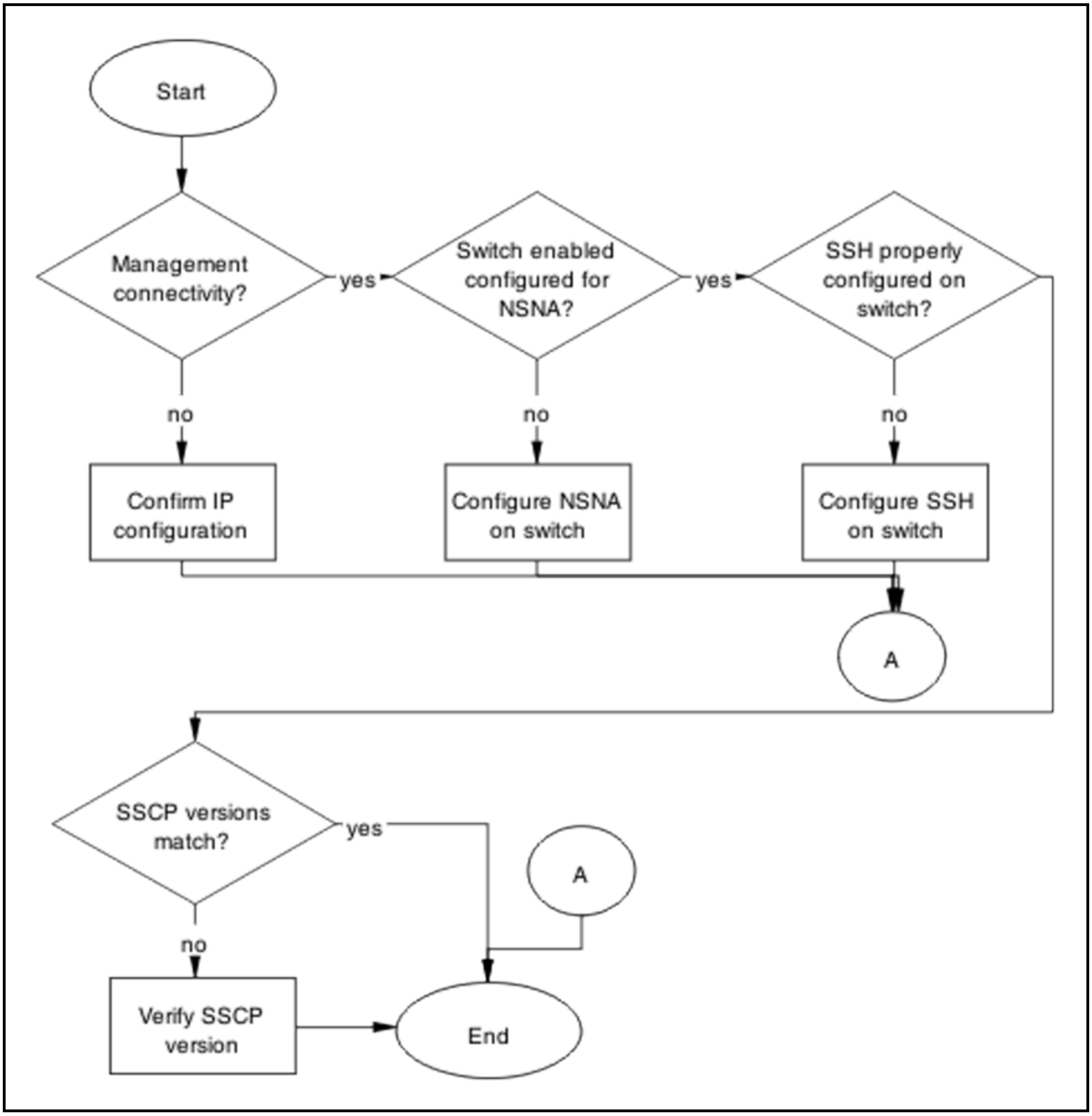
Nortel SNA switch not connected to Nortel SNAS although Nortel SNA is enabled

Ensure the Nortel SNAS is displayed as connected to the ERS 5500 series device.

Work flow: Nortel SNA switch not connected to Nortel SNAS although Nortel SNA is enabled

The following work flow assists you to determine the solution for an Nortel SNA switch that does not connect to a Nortel SNAS.

Figure 48
Nortel SNA switch not connected to Nortel SNAS although Nortel SNA is enabled



Navigation

- "Confirm IP Configuration" (page 134)
- "Configure Nortel SNA on switch" (page 137)
- "Configure SSH on switch" (page 139)
- "Verify SSCP version " (page 141)

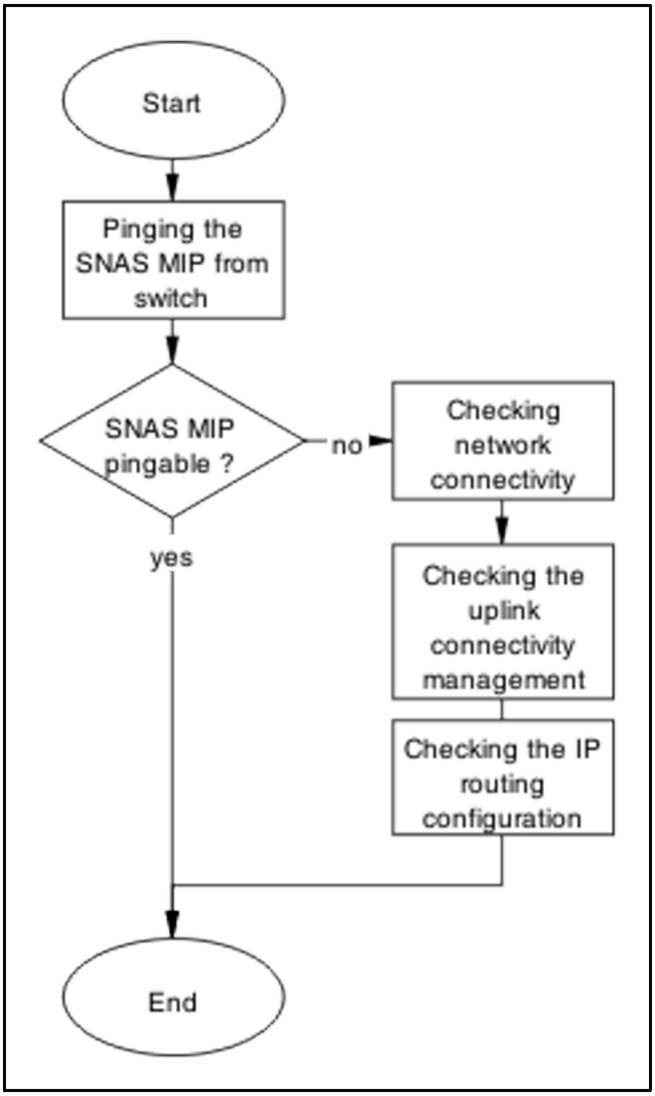
Confirm IP Configuration

Correct IP connectivity to restore management connectivity.

Task flow: Confirm IP configuration

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

Figure 49
Confirm IP configuration


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

Navigation

- "Pinging the Nortel SNAS MIP from switch" (page 136)
- "Checking network connectivity from switch to router to SNAS" (page 136)
- "Checking the uplink connectivity management" (page 136)
- "Checking IP routing configuration" (page 136)

Pinging the Nortel SNAS MIP from switch

Confirm there is IP connectivity from the switch.

Procedure Steps

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

--End--

Checking network connectivity from switch to router to SNAS

Confirm there is network connection from the switch to SNAS

Procedure Steps

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

--End--

Checking the uplink connectivity management

Procedure Steps

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

--End--

Checking IP routing configuration

Confirm the IP routing configuration is correct in L3 mode

Procedure Steps

Step	Action
1	Use the `show ip routing` command to show IP routing information.

2 Confirm L3 mode enabled.

--End--

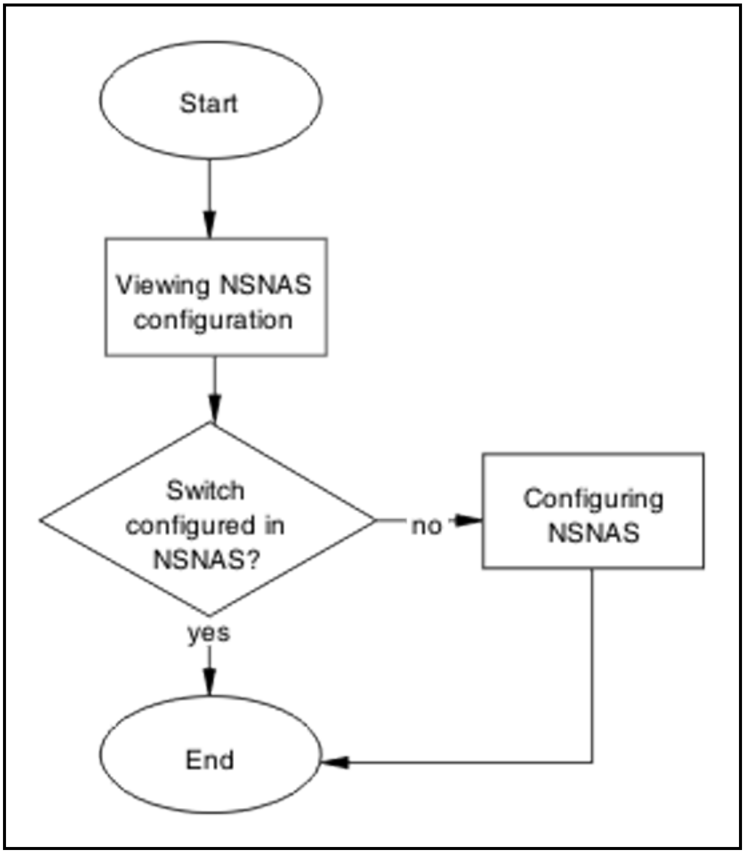
Configure Nortel SNA on switch

Configure and enable Nortel SNA on the switch.

Task flow: Configure Nortel SNA on switch

The following task flow assists you to ensure the ERS 5500 series device has Nortel SNA enabled.

Figure 50
Configure Nortel SNA on switch



Navigation

- "Checking Nortel SNAS configuration" (page 137)
- "Configuring Nortel SNA" (page 138)

Checking Nortel SNAS configuration

Verify the current configuration

Procedure Steps

Step **Action**

1 Use the `cfg/domain 1/switch Y` command followed by "cur" .

2 Note if the switch is configured in Nortel SNAS.

--End--

Configuring Nortel SNA

Configure the Nortel SNA for the switch

Procedure Steps

Step **Action**

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 `Nortel SNA Nortel SNAs <IP>/<subnet> port <port>` command to configure the Nortel SNAS IP address/subnet and the TCP communication port.

3 Set the created VLANs as Nortel SNA VoIP, RED, YELLOW and GREEN VLANs using the following commands:

- `Nortel SNA vlan 240 color voip`
- `Nortel SNA vlan 210 color red filter RED`
- `Nortel SNA vlan 220 color yellow filter YELLOW yellow-subnet 10.200.201.0/24`
- `Nortel SNA vlan 230 color green filter GREEN`

4 Set ports as Nortel SNA uplink and dynamic using the following commands:

- `interface fast Ethernet all`
- `Nortel SNA port 47-48 uplink vlans 210,220,230, 240`
- `Nortel SNA port 1-46 dynamic voip-vlans 240`

--End--

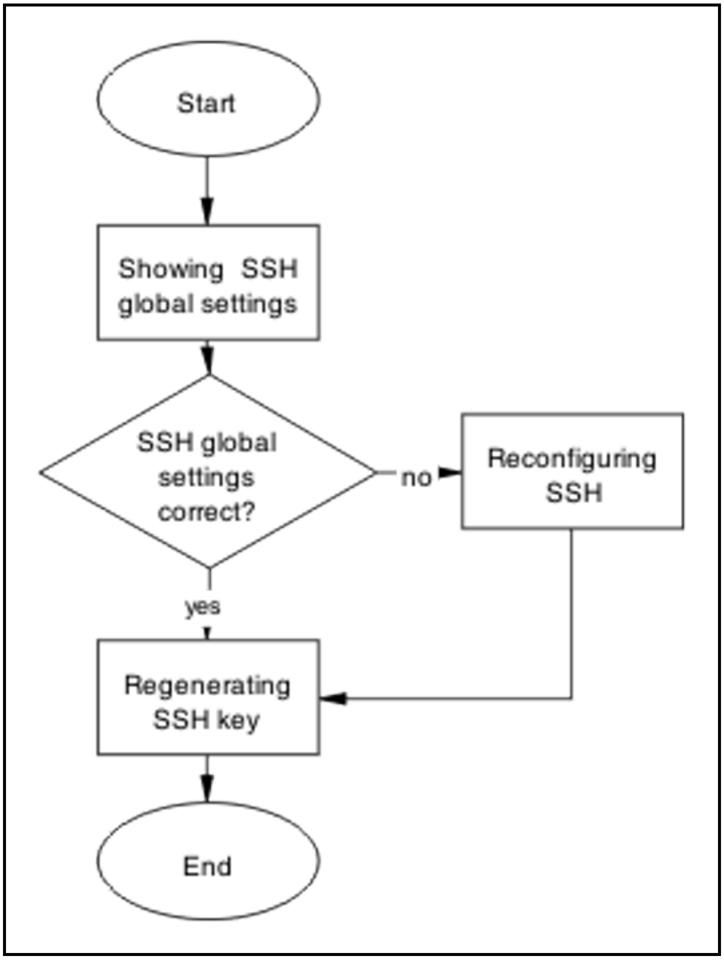
Configure SSH on switch

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 51
Configure SSH on switch



Navigation

- "Showing SSH globally" (page 139)
- "Reconfiguring SSH" (page 140)
- "Regenerating SSH key" (page 140)

Showing SSH globally

Display the SSH configuration of the switch.

Procedure Steps

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

--End--

Reconfiguring SSH

Change the SSH settings to be correct.

Procedure Steps

Step	Action
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 Nortel SNAS public key.
3	Use the **`ssh`** command to enable SSH globally.

--End--

Regenerating SSH key

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

Procedure Steps

Step	Action
1	Enter the **`no Nortel 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 **`Nortel SNA enable`** command.
6	On Nortel 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 Nortel SNA`** command to review the changes.

--End--

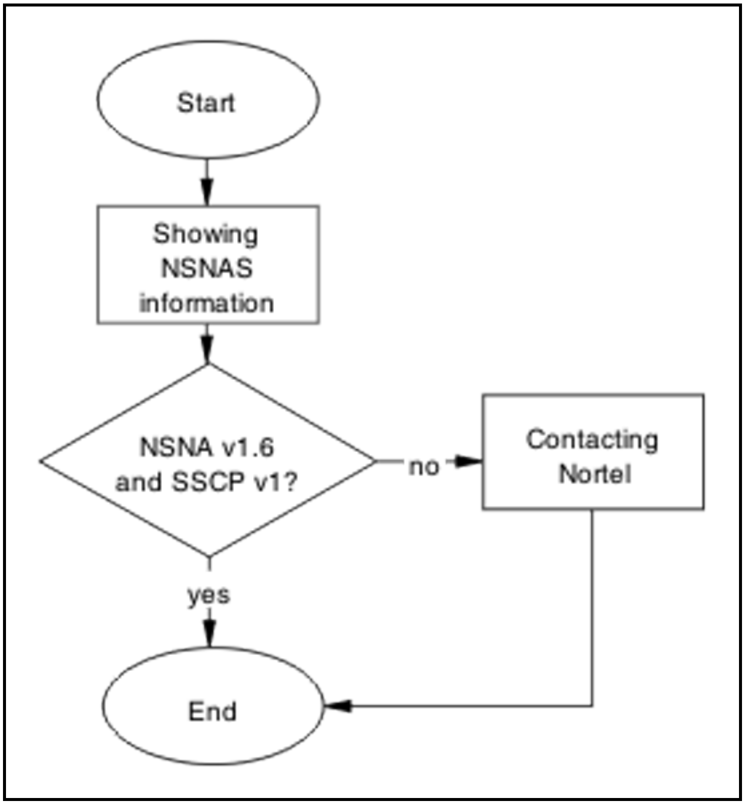
Verify SSCP version

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 52
Verify SSCP version



Navigation

- "Show Nortel SNA" (page 141)
- "Contacting Nortel" (page 142)

Show Nortel SNA

Display the Nortel SNA information for review.

Procedure Steps

Step	Action
1	Enter the `show Nortel SNA` command to display the configuration.
2	Enter `/info/local` command to display the software version on the Nortel SNAS side.
3	Note the following should be on the switch: • Nortel SNAS Connection Version: SSCPv1 Higher versions should be backward compatible.
4	Note the following should be on the SNAS: • Software version: 1.6.1.2 Higher versions should be backward compatible.

--End--

Contacting Nortel

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

Follow the Nortel customer service procedures at your convenience.

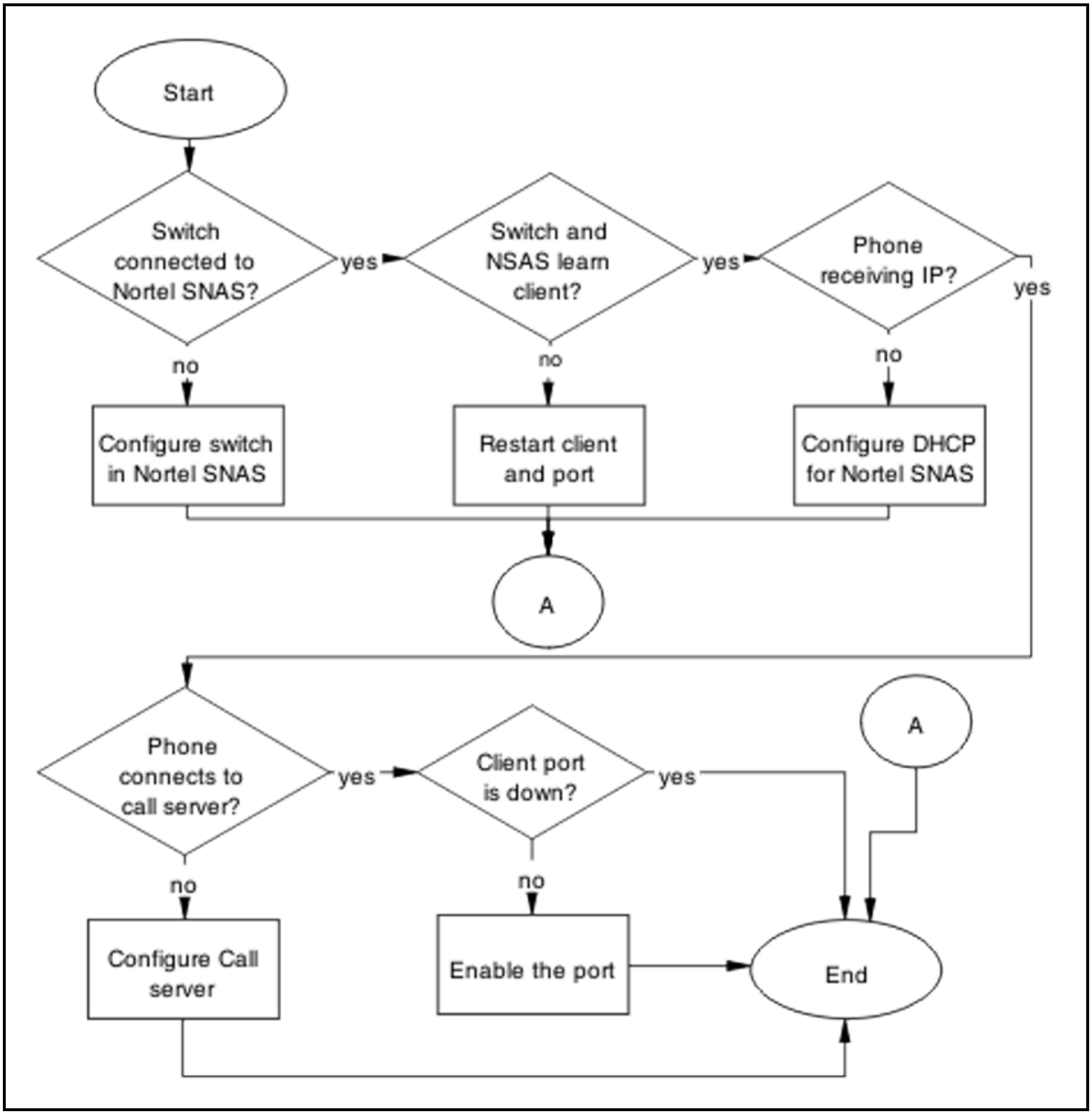
Client PC/phone can not connect

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 53
Client PC/phone can not connect


Start
Switch connected to Nortel SNAS?
yes
Switch and NSAS learn client?
yes
Phone receiving IP?
yes
no
no
no
Configure switch in Nortel SNAS
Restart client and port
Configure DHCP for Nortel SNAS
A
Phone connects to call server?
yes
Client port is down?
yes
A
no
no
Configure Call server
Enable the port
End

Navigation

- "Configure switch on Nortel SNAS" (page 143)
- "Restart client and port" (page 145)
- "Configure DHCP for Nortel SNAS" (page 147)
- "Configure call server" (page 149)
- "Enable the port" (page 150)

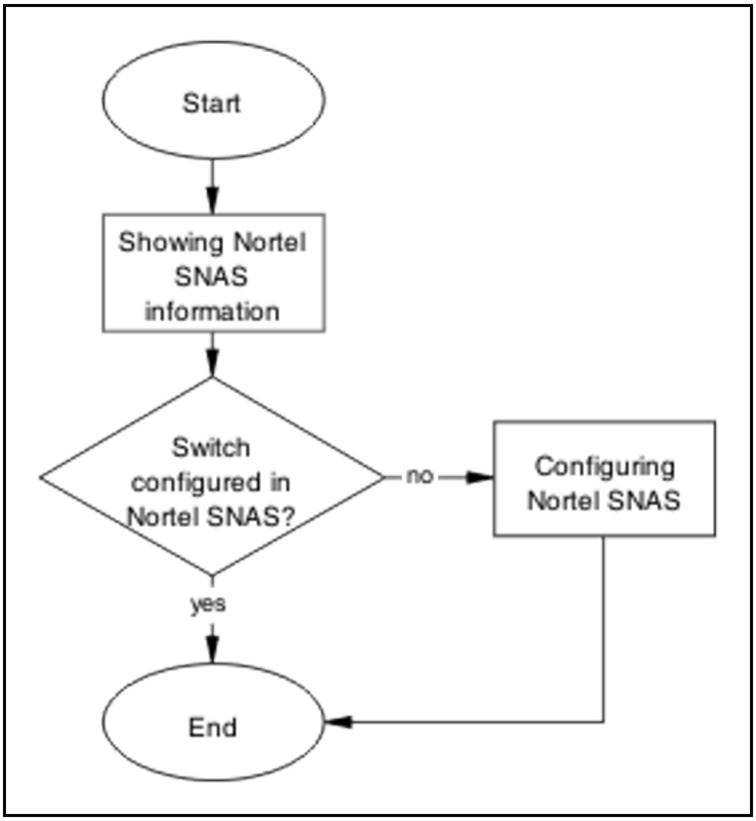
Configure switch on Nortel SNAS

Configure and enable the switch on Nortel SNAS.

Task flow: Configure the switch on Nortel SNAS

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

Figure 54
Configure the switch on Nortel SNAS


Start
Showing Nortel SNAS information
Switch configured in Nortel SNAS?
no
Configuring Nortel SNAS
yes
End

Navigation

- "Showing Nortel SNA information" (page 144)
- "Configuring Nortel SNAS" (page 145)

Showing Nortel SNA information

Verify the current configuration

Procedure Steps

Step	Action
1	Use the `cfg/domain 1/switch Y` command followed by "cur".
2	Note if the switch is configured in Nortel SNAS.

--End--

Configuring Nortel SNAS

Configure the Nortel SNAS with the settings for the ERS 5500 Series device.

Procedure Steps

Action

Switch configuration on Nortel SNAS can be found in Technical_Configuration_Document _for_Nortel SNA for 1.6 release.

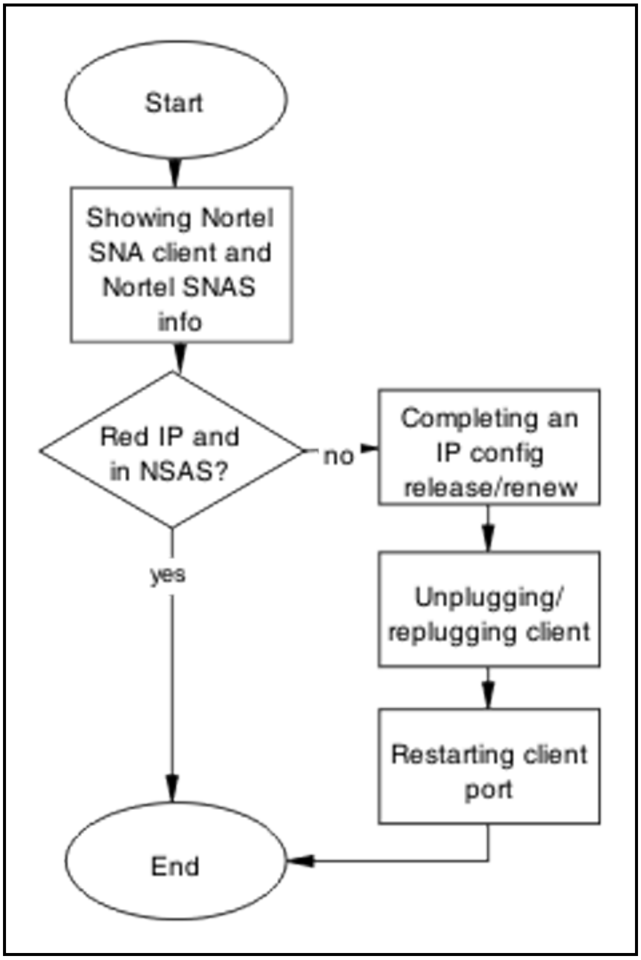
Restart client and port

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.

Figure 55
Restart client and port


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

Navigation

- "Showing Nortel SNA client and Nortel SNAS info" (page 146)
- "Completing an IP config release/renew" (page 146)
- "Unplugging/replugging client" (page 146)
- "Restarting client port" (page 147)

Showing Nortel SNA client and Nortel SNAS info

Display the Nortel SNA client information

Procedure Steps

Step	Action
1	Use the **`show Nortel SNA client`** command.
2	Note the output.
3	Use the **`info/switch 1 n`** command in Nortel SNAS.
4	Note that both are showing a consistent status.

--End--

Completing an IP config release/renew

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

Procedure Steps

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

--End--

Unplugging/replugging client

Physically disconnect client from the network.

Procedure Steps

Step	Action
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.

--End--

Restarting client port

Shut down the client port then restart it.

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

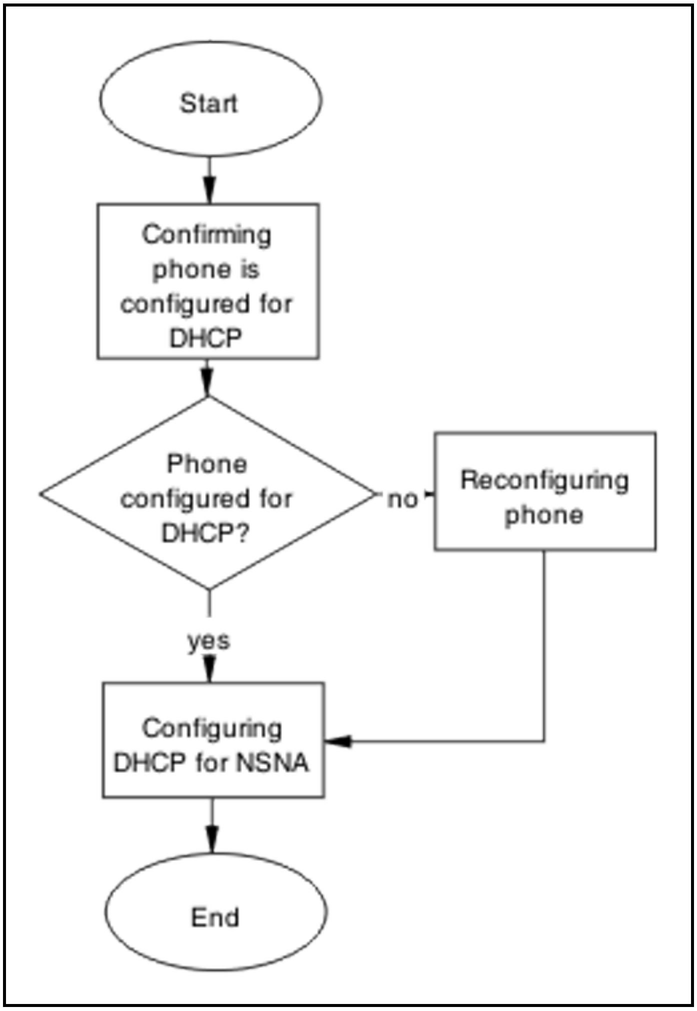
Configure DHCP for Nortel SNAS

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

Task flow: Configure DHCP for Nortel SNA

The following task flow assists you to configure the DHCP for Nortel SNAS.

Figure 56
Configure DHCP for Nortel SNA


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

Navigation

- "Confirming phone is configured for DHCP" (page 148)
- "Reconfiguring phone" (page 148)
- "Configuring DHCP for Nortel SNA" (page 149)

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 Nortel SNA

Change DHCP server to work with Nortel SNA.

Review vendor documentation to change settings of the DHCP server.

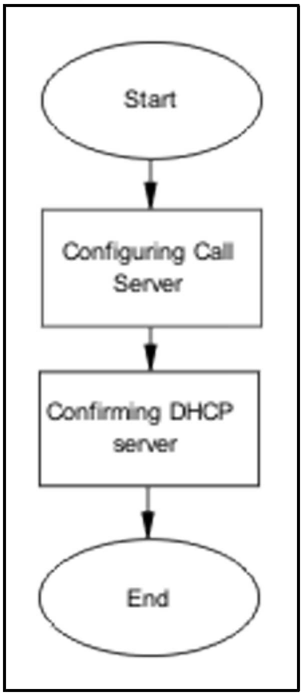
Configure call server

Ensure the call server is properly configured.

Task flow: Configure call server

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

Figure 57
Configure call server.



Navigation

- "Configuring call server" (page 149)
- "Configuring DHCP server" (page 150)

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.

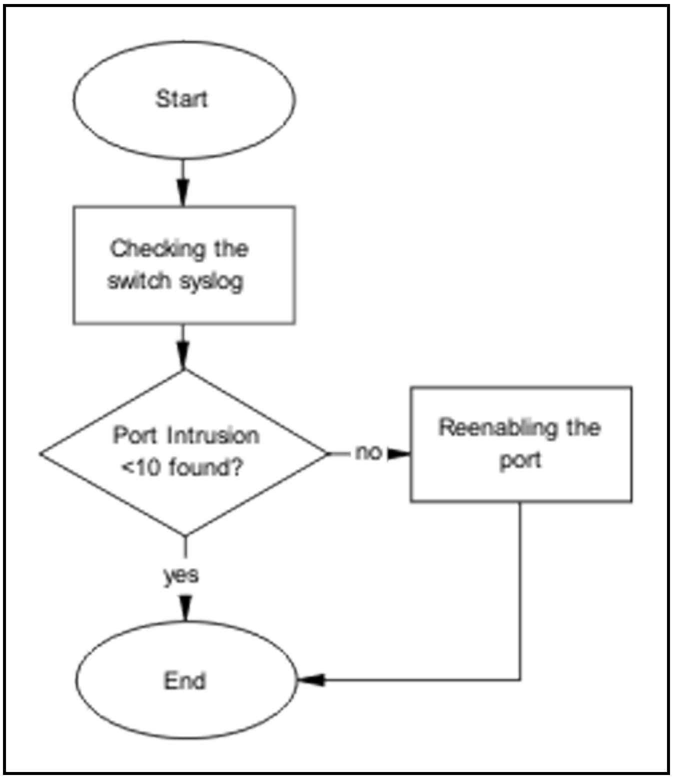
Enable the port

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 58
Enable the port



Navigation

- "Checking the switch log" (page 150)Checking the switch log
- "Reenabling the port" (page 151)

Checking the switch log

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

Procedure Steps

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

--End--

Reenabling the port

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

Procedure Steps

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

--End--

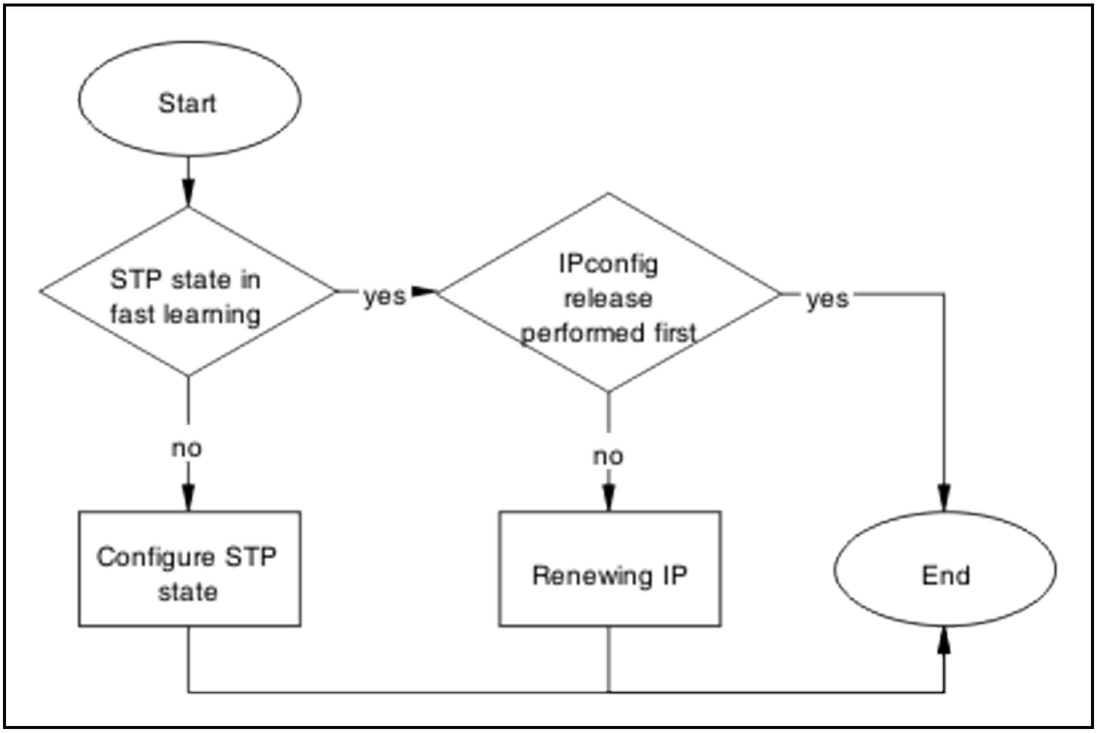
Authentication error or 0.0.0.0 IP after image upgrade

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 59
Authentication error or 0.0.0.0 IP after image upgrade



Navigation

- "Configure STP state" (page 152)
- "Renewing IP" (page 154)

Configure STP state

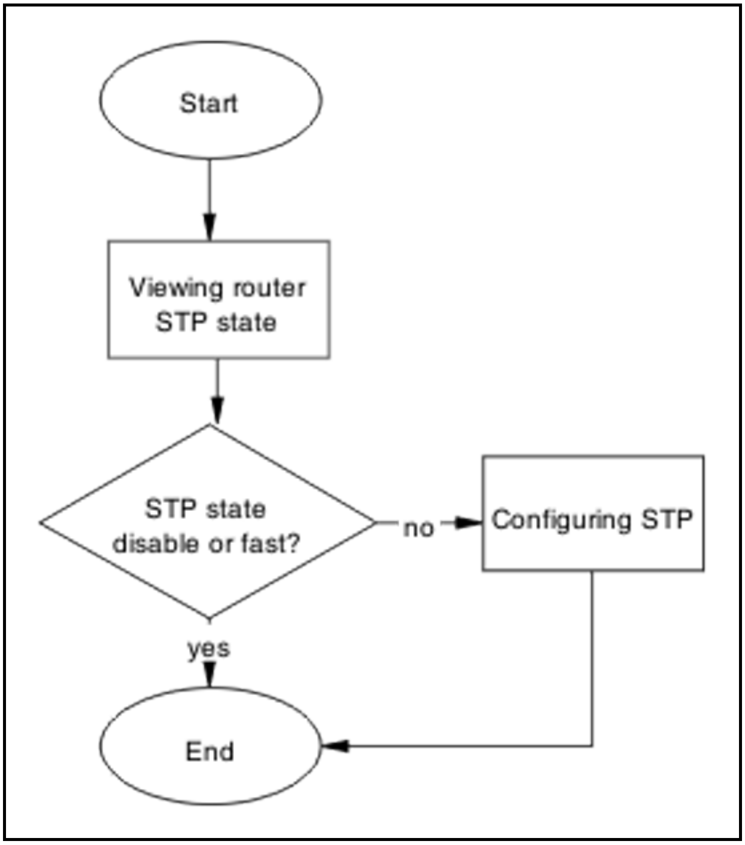
Place the STP state in fast learning in the case the ports come up to fast.

Attention: Ensure that your clearly understand the consequences of performing this action on an uplink in order to prevent loops.

Task flow: Configure STP state task flow

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

Figure 60
Configure STP state



Navigation

- "Viewing Router STP state" (page 153)
- "Configuring STP state" (page 154)

Viewing Router STP state

Identify what the STP state is on the router.

Procedure Steps

Step	Action
1	Use the `show spanning-tree port` command to show the router STP state.
2	Note the following: • STP State is disable or fast

--End--

Configuring STP state

Set the STP state to fast learning.

Procedure Steps

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

--End--

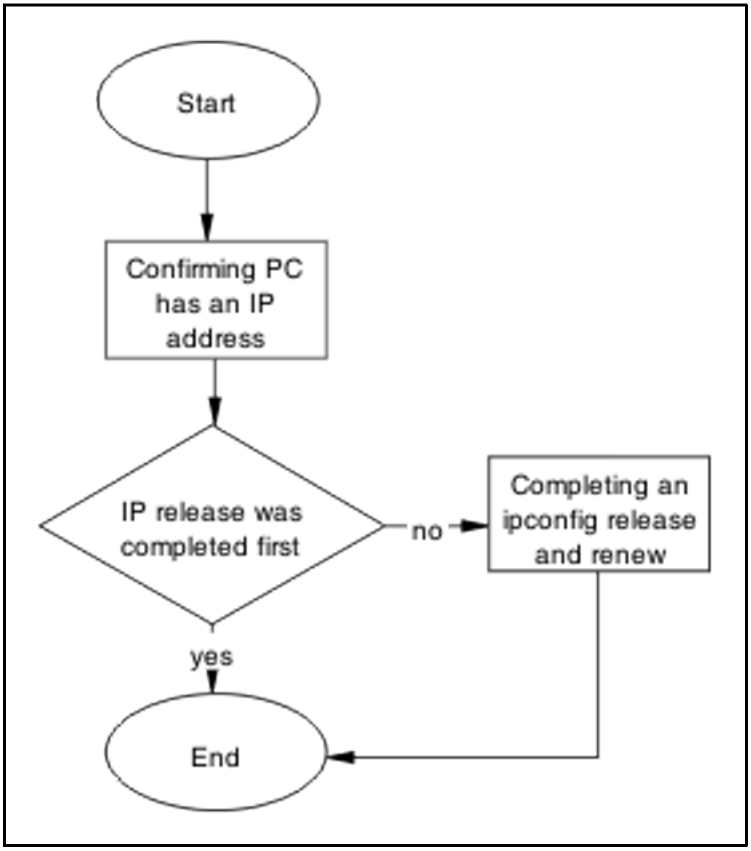
Renewing IP

Renew the IP properly to restore the connection.

Task flow: Renewing IP

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

Figure 61
Renewing IP


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

Navigation

- "Confirming PC has IP address" (page 155)
- "Completing and ipconfig release and renew" (page 155)

Confirming PC has IP address

Confirm the PC has a proper IP.

Procedure Steps

Step	Action
1	Using vendor documentation, Use the `ipconfg /all` command to view the IP information of the PC.
2	Note the IP address and any other IP information.

--End--

Completing and ipconfig release and renew

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

Procedure Steps

Step	Action
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.

--End--

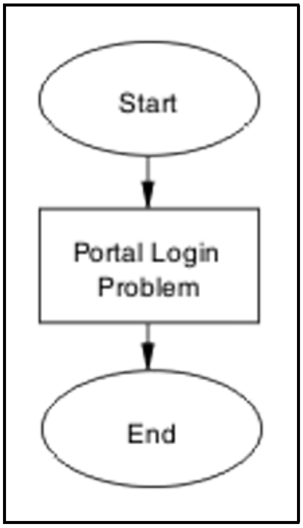
TG client getting red IP

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 62
TG Client getting red IP



Navigation

- "Portal Login Problem" (page 156)

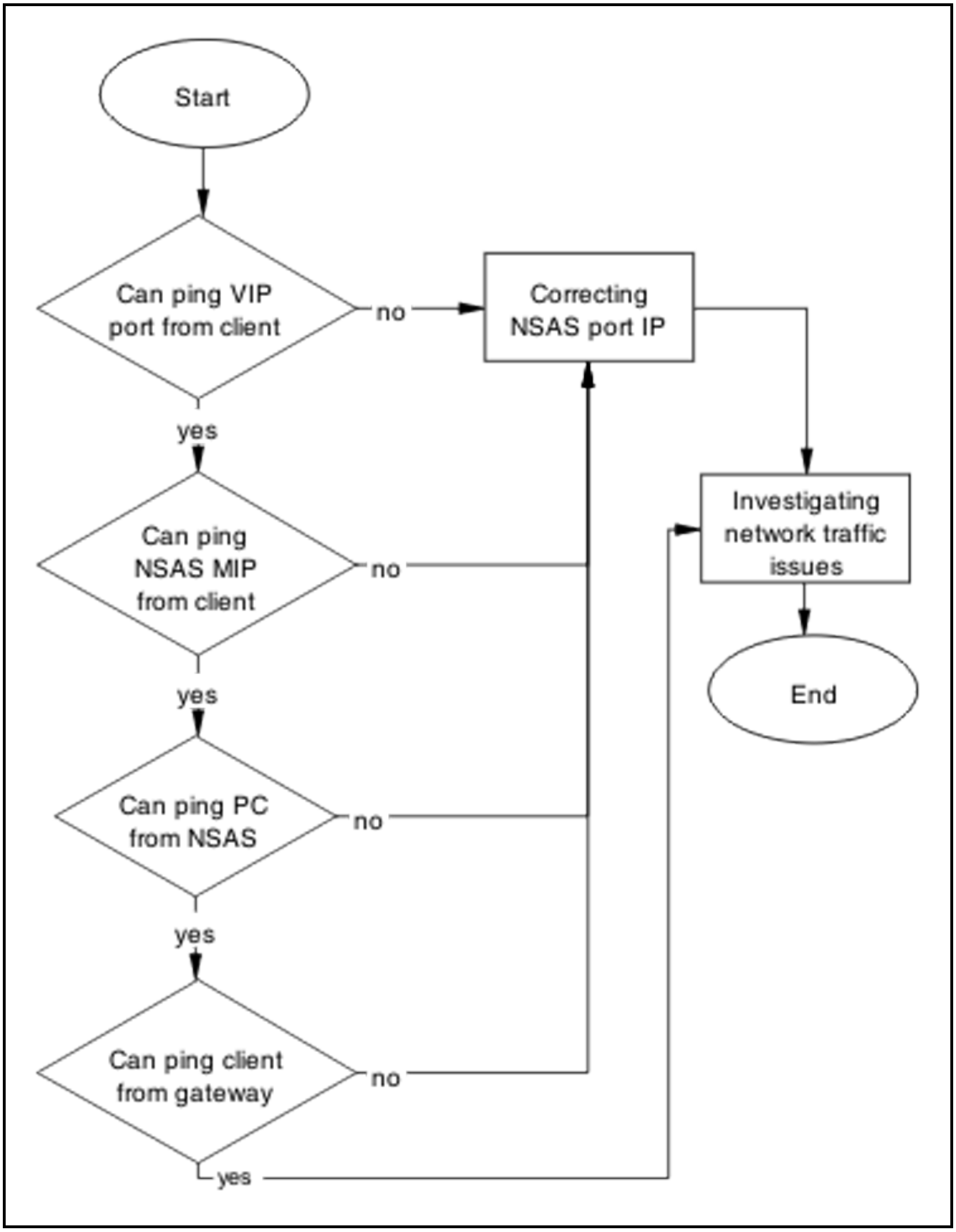
Portal Login Problem

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

Task flow: Portal login problem

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

Figure 63
Portal login problem


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

Navigation

- "Correcting NSAS port IP" (page 157)
- "Investigating network traffic issues" (page 158)

Correcting NSAS port IP

Make changes to NSAS port IP.

Procedure Steps

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

--End--

Investigating network traffic issues

Eliminate network traffic issues that may impede the browser.

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

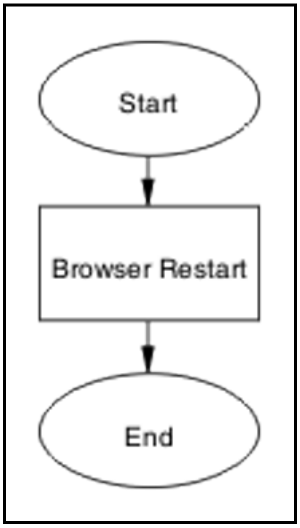
Client gets red IP but browser hangs after opening

Restart the browser to correct a browser hanging issue.

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

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

Figure 64
Client gets red IP but browser hangs after opening



Navigation

- "Browser restart" (page 158)

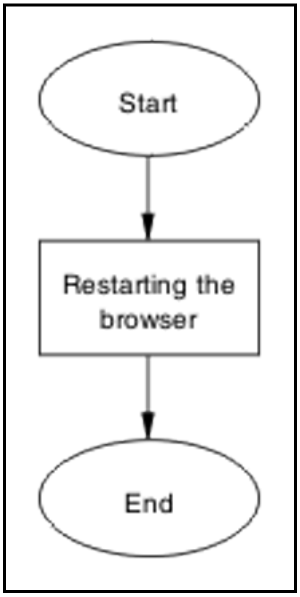
Browser restart

Restart the browser to regain connectivity.

Task flow: Browser restart

The following task flow assists you to restart the browser.

Figure 65
Browser restart



Navigation

- "Restarting the browser" (page 159)

Restarting the browser

Fully close and restart a browser.

Procedure Steps

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

--End--

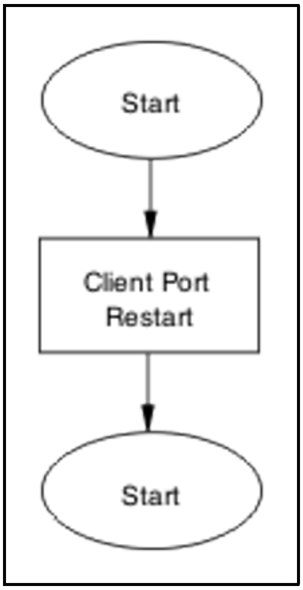
Nortel SNA client gets red IP but after login it does not go to yellow or green state

Correct the client maintaining red state for too long due to NSAS communication failing.

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

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

Figure 66
Nortel SNA client gets red IP but after login it does not go to yellow or green state



Navigation

- "Client port restart" (page 160)

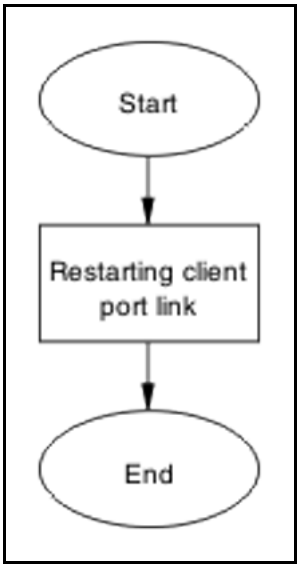
Client port restart

Client link down and up.

Task flow: Client port restart

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

Figure 67
Client port restart



Navigation

- "Restarting client port link" (page 161)

Restarting client port link

Shut down the client port then restart it.

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

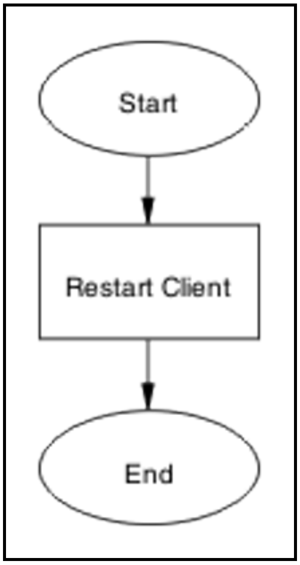
Client had green IP but was kicked to yellow or red

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 68
Client had green IP but was kicked to yellow or red



Navigation

- "Restart client" (page 162)

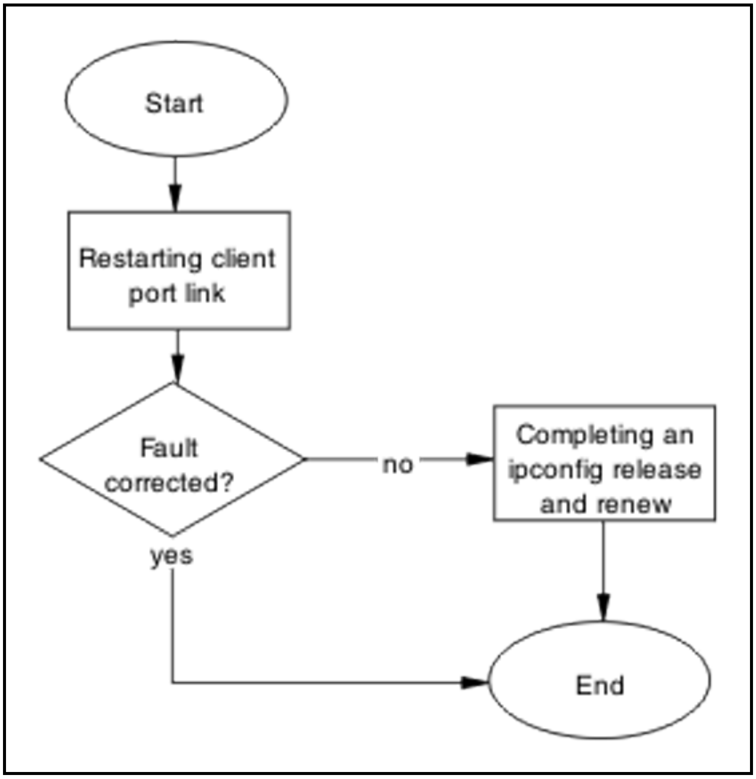
Restart client

Shut down the client then start to regain proper communication.

Task flow: Restart client

The following task flow assists you to restart the client.

Figure 69
Restart client


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

Navigation

- "Restarting client port link" (page 163)
- "Completing an ipconfig release and renew" (page 163)

Restarting client port link

Shut down the client port then restart it.

Procedure Steps

Action
Follow vendor procedures to shut don and restart the client port.

Completing an ipconfig release and renew

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

Procedure Steps

Step	Action
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.

--End--

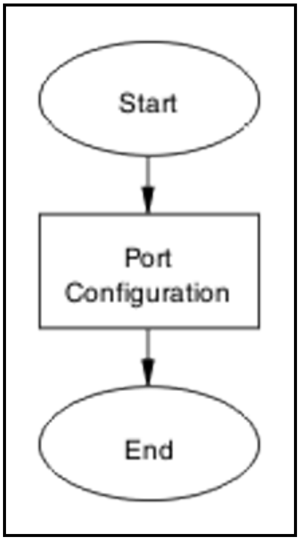
Client PC taking a long time to boot

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 70
Client PC taking a long time to boot



Navigation

- "Port configuration" (page 164)

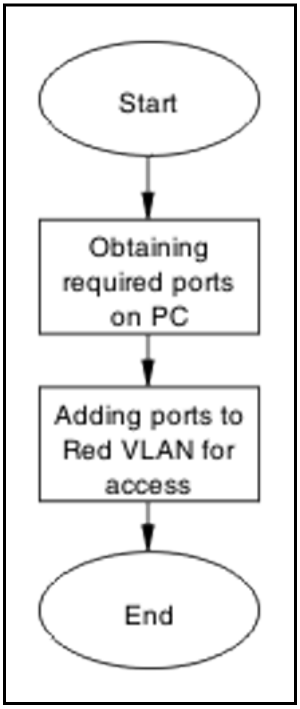
Port configuration

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.

Figure 71
Port configuration


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

Navigation

- "Obtaining required ports on PC" (page 165)
- "Adding ports to red VLAN for access" (page 165)

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.

Procedure Steps

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

--End--

Example of adding ports to a VLAN

Procedure Steps

Step	Action
1	Use the `qos Nortel 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 Nortel 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.

--End--

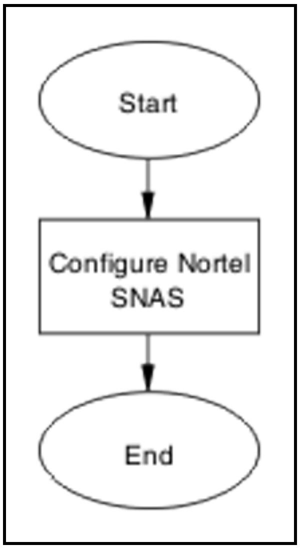
Mac-Auth client not authenticated or not assigned the correct filter

Correct the client that is not authenticating. When not assigned 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 72
Mac-Auth client not authenticated or not assigned the correct filter



Navigation

- "Configure Nortel SNAS" (page 167)

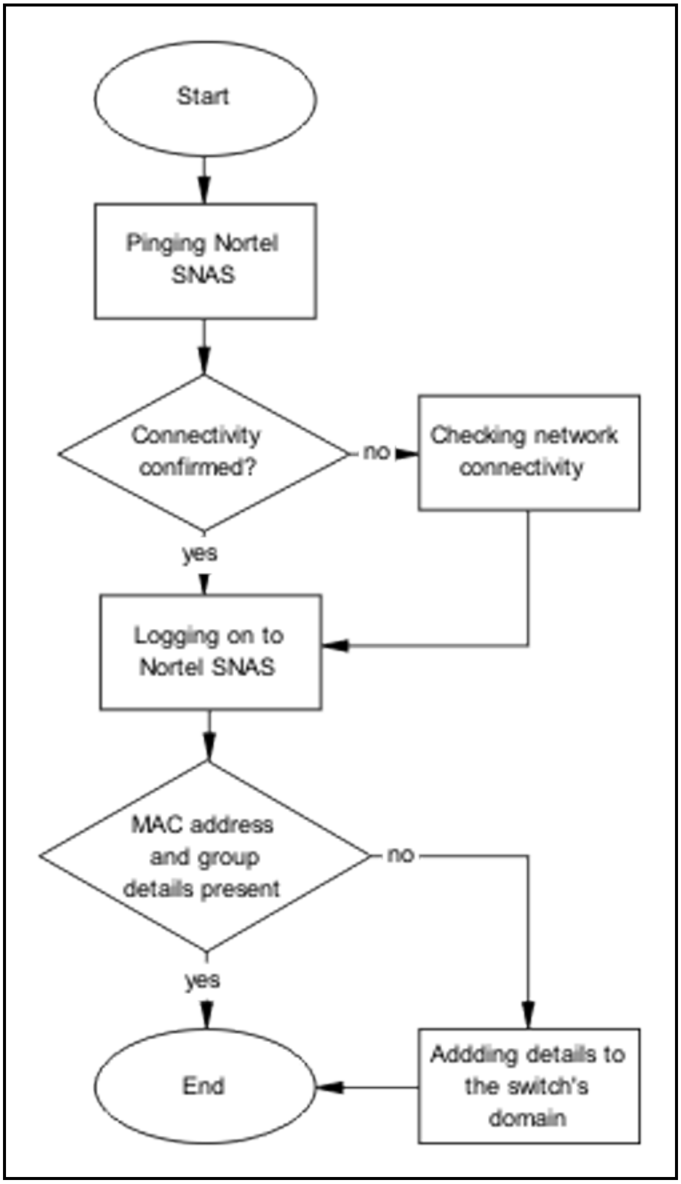
Configure Nortel SNAS

Change the Nortel SNAS settings to ensure authentication can occur.

Task flow: Configure Nortel SNAS

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

Figure 73
Configure Nortel SNAS


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

Navigation

- "Pinging Nortel SNAS" (page 168)
- "Checking network connectivity" (page 168)

- "Logging on to Nortel SNAS" (page 168)
- "Adding details to the switch domain" (page 168)

Pinging Nortel SNAS

Verify the network connectivity using ping.

Procedure Steps

Step	Action
1	Use the ping `<Nortel SNASIP>` command to ensure connectivity.
2	Observe the details delivered.

--End--

Checking network connectivity

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

Use local protocol and network information to correct any network issues.

Logging on to Nortel SNAS

Logon to Nortel SNAS to view more information.

Procedure Steps

Step	Action
1	Use vendor procedure to logon to Nortel SNAS.
2	Observe the following: • the macdb list for the switch's domain

--End--

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.

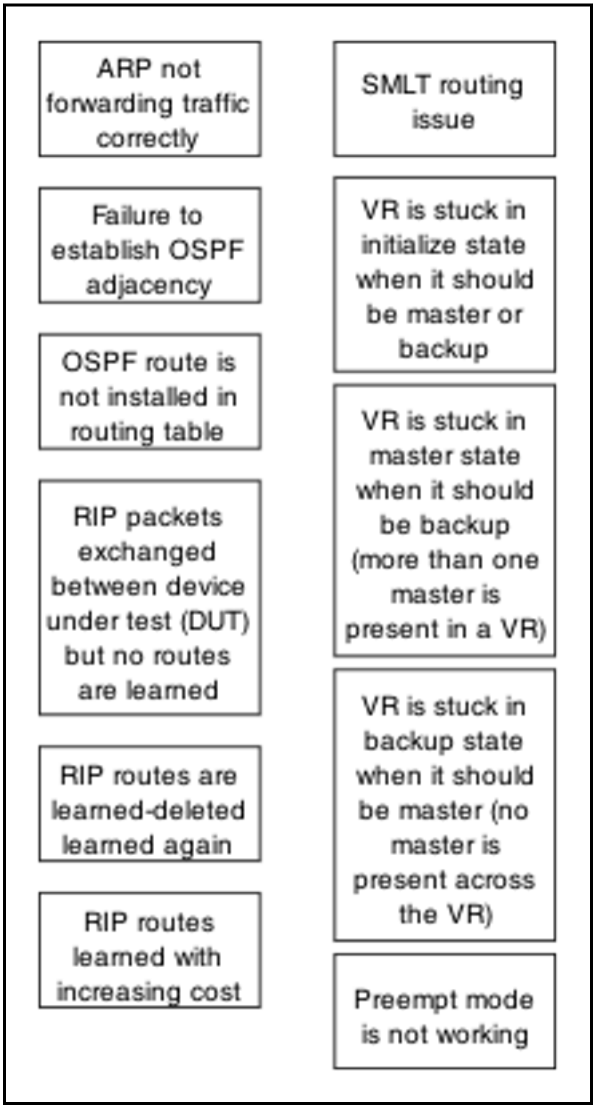
Troubleshooting Layer 2 and Layer 3

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.

Figure 74
Troubleshooting Layer 2 and Layer 3


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

Navigation

- "ARP not forwarding traffic correctly" (page 171)
- "Failure to establish OSPF adjacency" (page 186)
- "OSPF route is not installed in routing table" (page 211)
- "RIP packets exchanged between device under test (DUT) but no routes are learned" (page 216)
- "RIP routes are learned-deleted learned again" (page 223)
- "RIP routes learned with increasing cost" (page 226)
- "SMLT routing issue" (page 228)

- "VR is stuck in initialize state when it should be master or backup" (page 238)
- "VR is stuck in master state when it should be backup (more than one master is present in a VR)" (page 244)
- "VR is stuck in backup state when it should be master (no master is present across the VR)" (page 246)
- "Preempt mode is not working" (page 249)

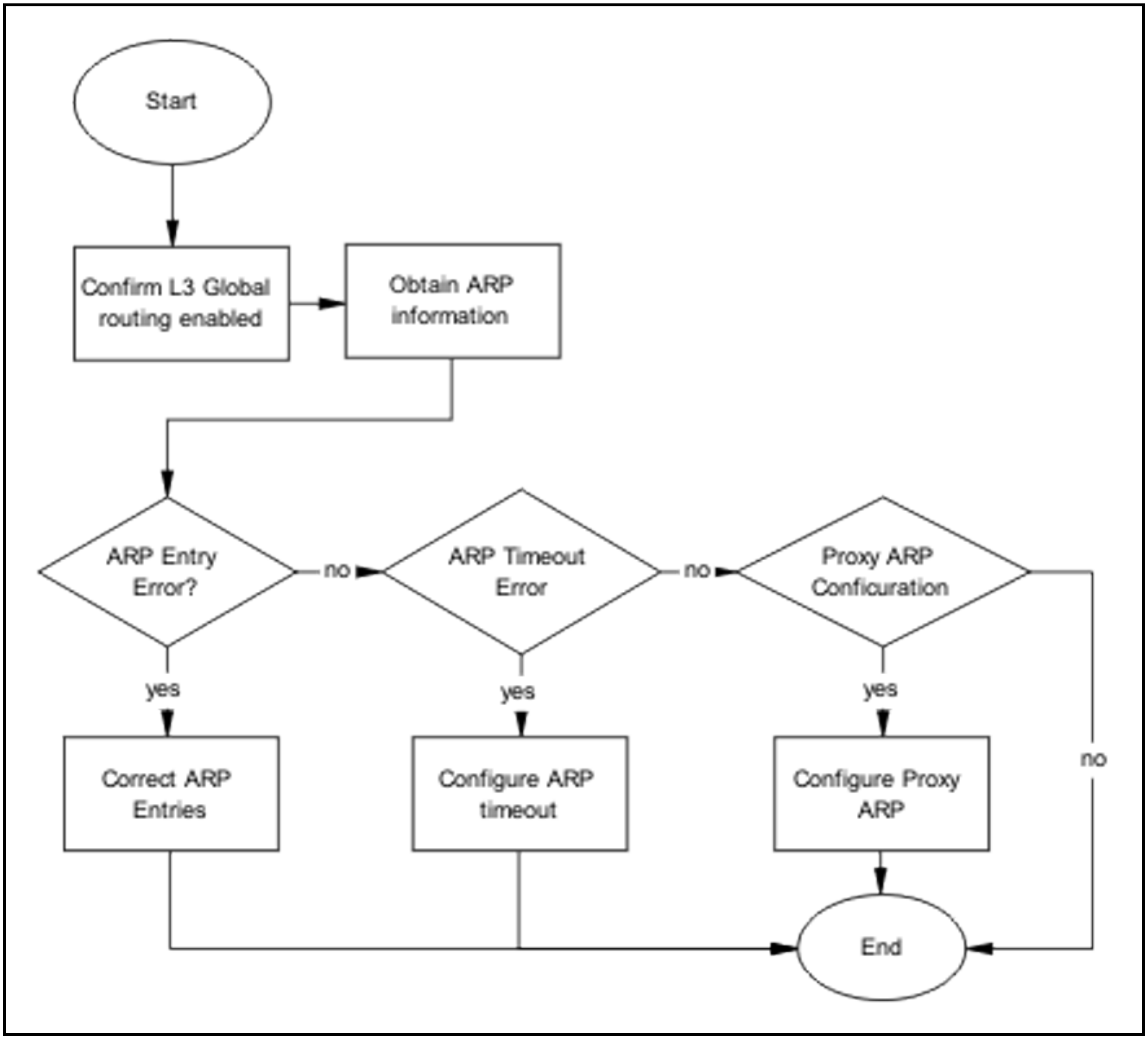
ARP not forwarding traffic correctly

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 75
Troubleshooting ARP



Navigation

- "Confirming global L3 routing enabled" (page 172)
- "Obtain ARP information" (page 174)
- "Correct ARP Entries" (page 176)
- "Configure ARP timeout" (page 181)
- "Configuring the proxy ARP" (page 183)

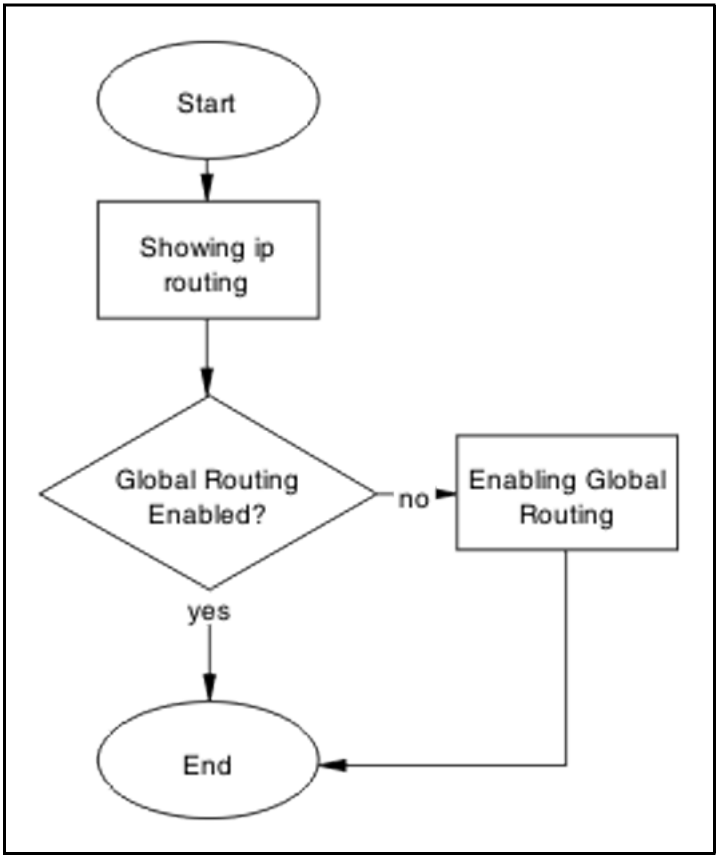
Confirming global L3 routing enabled

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 76
Confirming global L3 routing



Navigation

- "Showing IP Routing" (page 173)
- "Enabling global routing" (page 173)

Showing IP Routing

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

Procedure Steps

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

--End--

Enabling global routing

Enable the IP Routing on the switch.

Procedure Steps

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

--End--

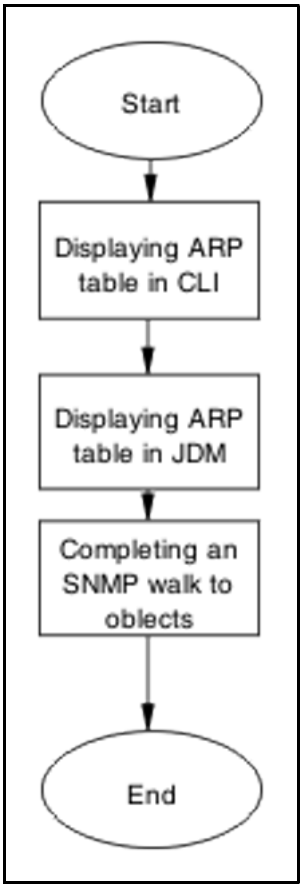
Obtain ARP information

View the ARP information in order 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, JDM, and SMTP.

Figure 77
Obtaining ARP information


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

Navigation

Displaying the ARP Table in the CLI

Use the CLI to obtain ARP table information.

- CLI Exec mode on base unit only

Procedure Steps

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

--End--

Displaying ARP table information in JDM

Use the JDM to obtain ARP table information.

Procedure Steps

Step	Action
1	Open the JDM for the ERS 5500 series device.
2	Connect to the ERS 5500 series device for which you wish to display the ARP information for.
3	Navigate to **`IP Routing->IP>ARP`** .
4	Observe ARP entries displayed.

--End--

Completing an SNMP walk to objects

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

Procedure Steps

Step	Action
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.

--End--

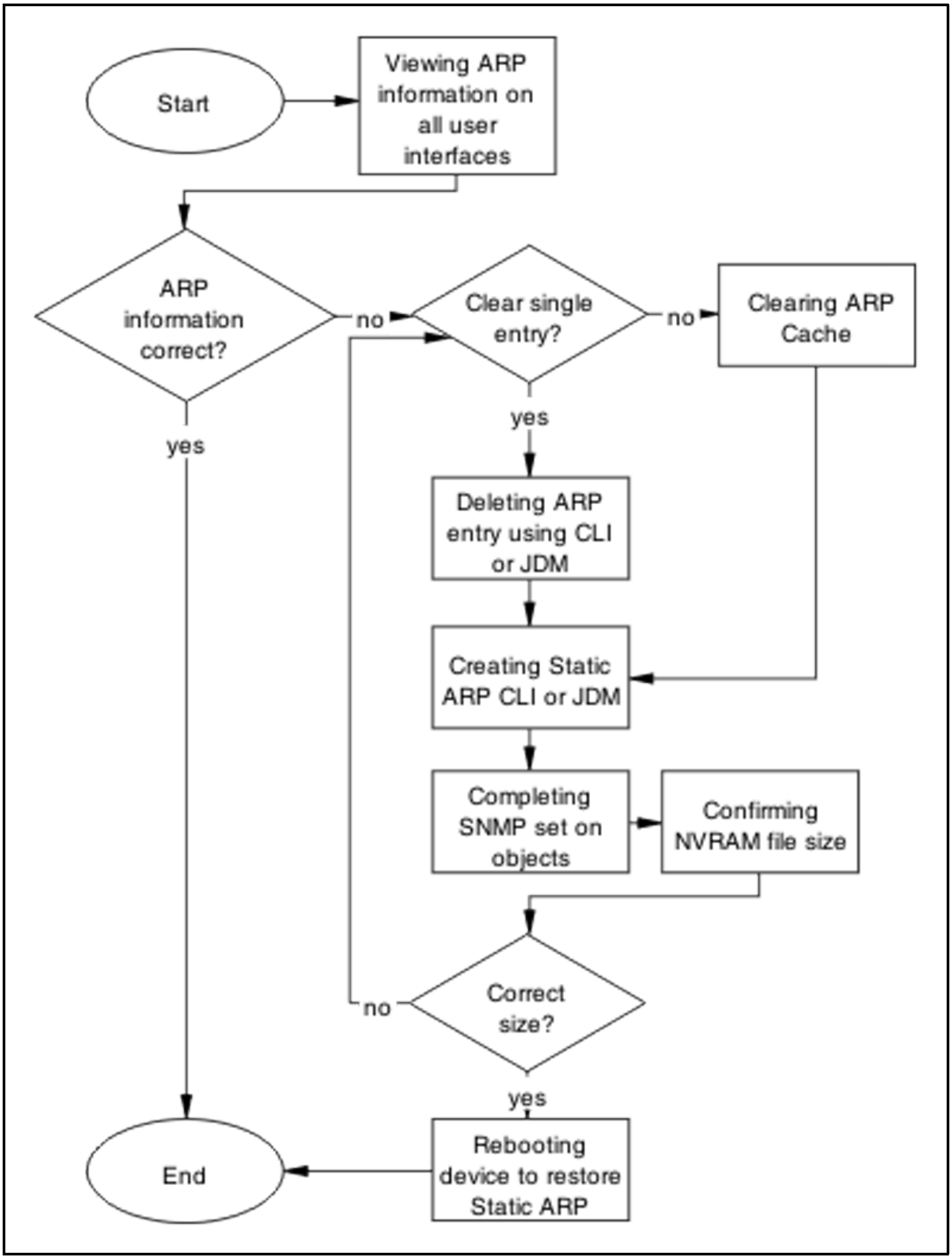
Correct ARP Entries

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

Task flow: Correct ARP entries

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

Figure 78
Correct ARP entries


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

Navigation

- "Confirming ARP entries are correct" (page 178)
- "Clearing ARP cache" (page 178)

Confirming ARP entries are correct

Comparing ARP entries to ensure they are correct.

Procedure Steps

Step	Action
1	Review the CLI, JDM, and SNMP data.
2	Compare entries to determine if any discrepancies exist.

--End--

Clearing ARP cache

The ARP cache can be completely cleared.

Procedure Steps

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

--End--

Deleting ARP entry in CLI or JDM

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

Procedure for CLI
Procedure Steps

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

--End--

Procedure for JDM
Procedure Steps

Step	Action
1	Navigate to JDM 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.

--End--

Creating Static ARP entries in CLI or JDM

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

Creating static ARP entries using the CLI

Procedure Steps

Step	Action
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.

--End--

Creating static ARP entries using the JDM

Procedure Steps

Step	Action
1	Select **IP Routing> IP>ARP** in the JDM.
2	Enter the values required and press the **Insert** button.

--End--

Deleting ARP entry using SNMP

Individual ARP entries removed using SNMP.

Procedure Steps

Step	Action
1	Set the corresponding ***ipNetToMediaType*** to value “2” . .

2	Observe the change.

--End--

Setting objects with SNMP

SNMP objects can be set.

Procedure Steps

Step	Action
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.

--End--

Confirming NVRAM file size

The NVRAM file size should conform to parameters.

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

Procedure Steps

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

--End--

Rebooting the device to restore static ARP

Restore static ARP entries on device after reboot.

Procedure Steps

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

--End--

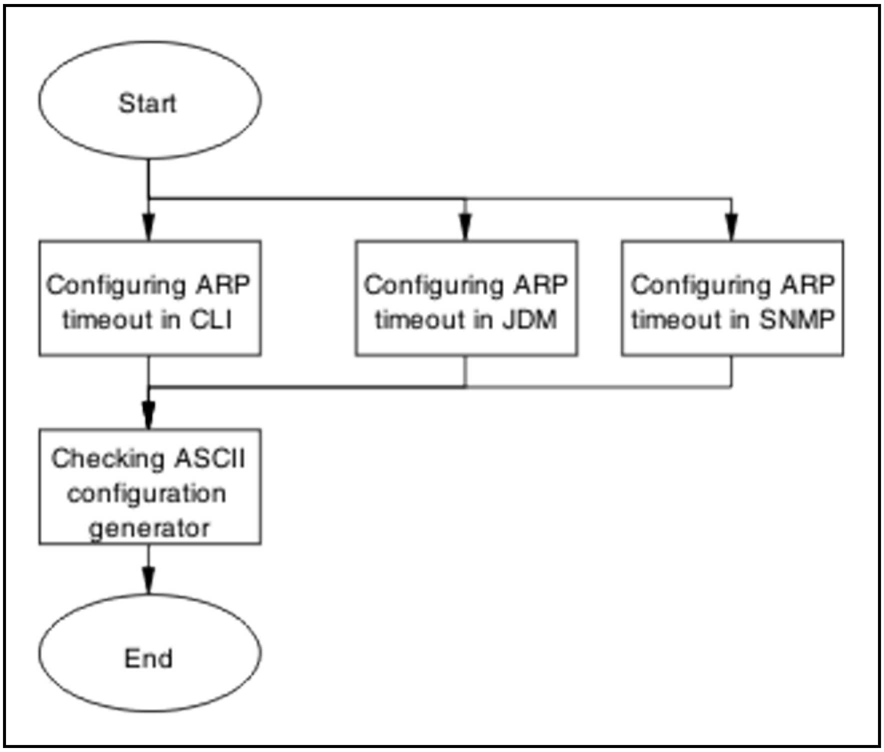
Configure ARP timeout

Change the ARP timeout value.

Task flow: Configure ARP timeout

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

Figure 79
Configure ARP timeout


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

Navigation

- "Configuring ARP timeout using CLI" (page 182)
- "Configuring ARP timeout using JDM" (page 182)
- "Configuring ARP timeout using SNMP" (page 182)
- "Checking ASCII configuration generator" (page 182)

Configuring ARP timeout using CLI

The CLI can be used to set the ARP timeout.

Procedure Steps

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

--End--

Configuring ARP timeout using JDM

The JDM can be used to set the ARP timeout.

Procedure Steps

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

--End--

Configuring ARP timeout using SNMP

The SNMP can be used to set the ARP timeout.

Procedure Steps

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

--End--

Checking ASCII configuration generator

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

Procedure Steps

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

--End--

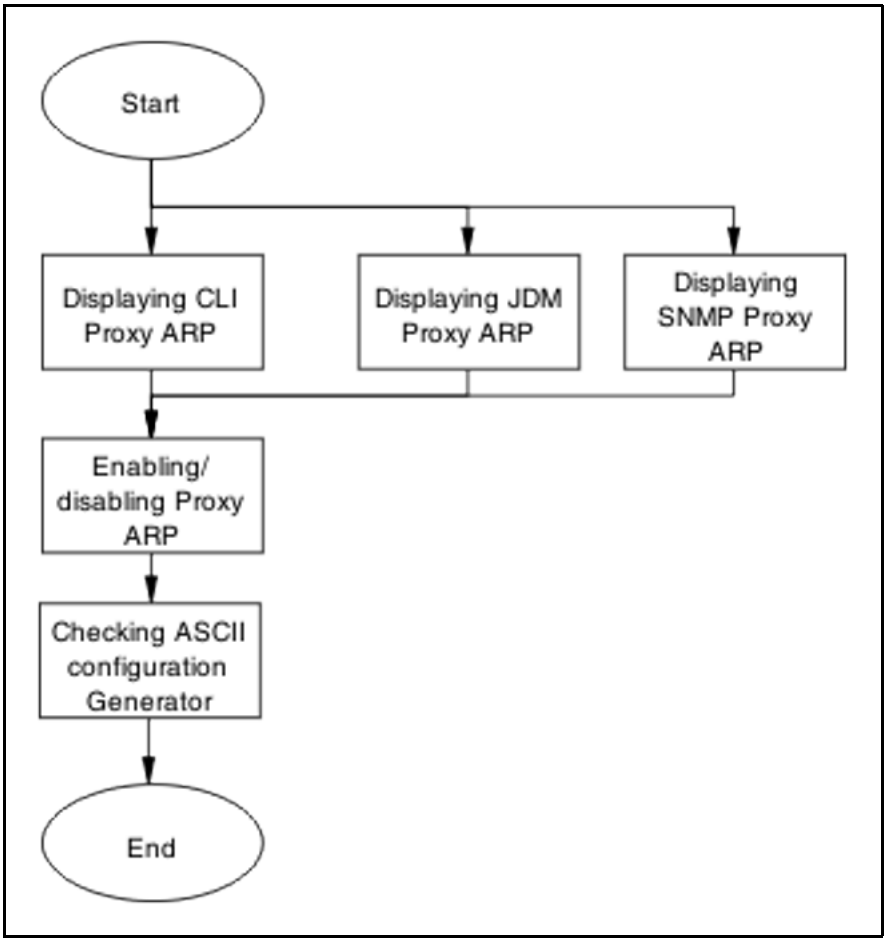
Configuring the proxy ARP

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.

Figure 80
Configuring 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

Navigation

Displaying CLI proxy ARP

The CLI can be used to set the Proxy ARP.

Procedure Steps

Step	Action
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.

--End--

Displaying JDM Proxy ARP

The JDM can be used to set the proxy ARP.

Procedure Steps

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

--End--

Displaying SNMP proxy ARP

The SNMP can be used to view the proxy ARP.

Procedure Steps

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

--End--

Enabling/disabling Proxy ARP

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

Enabling/disabling Proxy ARP using CLI
Procedure Steps

Step	Action
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.

--End--

Enabling/disabling Proxy ARP using JDM
Procedure Steps

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

--End--

Enabling/disabling Proxy ARP using SNMP
Procedure Steps

Step	Action
1	Do an SNMP set on the **rcArpExtEntDoProxy** object. .

2 Observe no errors after execution.

--End--

Checking ASCII configuration Generator

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

Procedure Steps

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

--End--

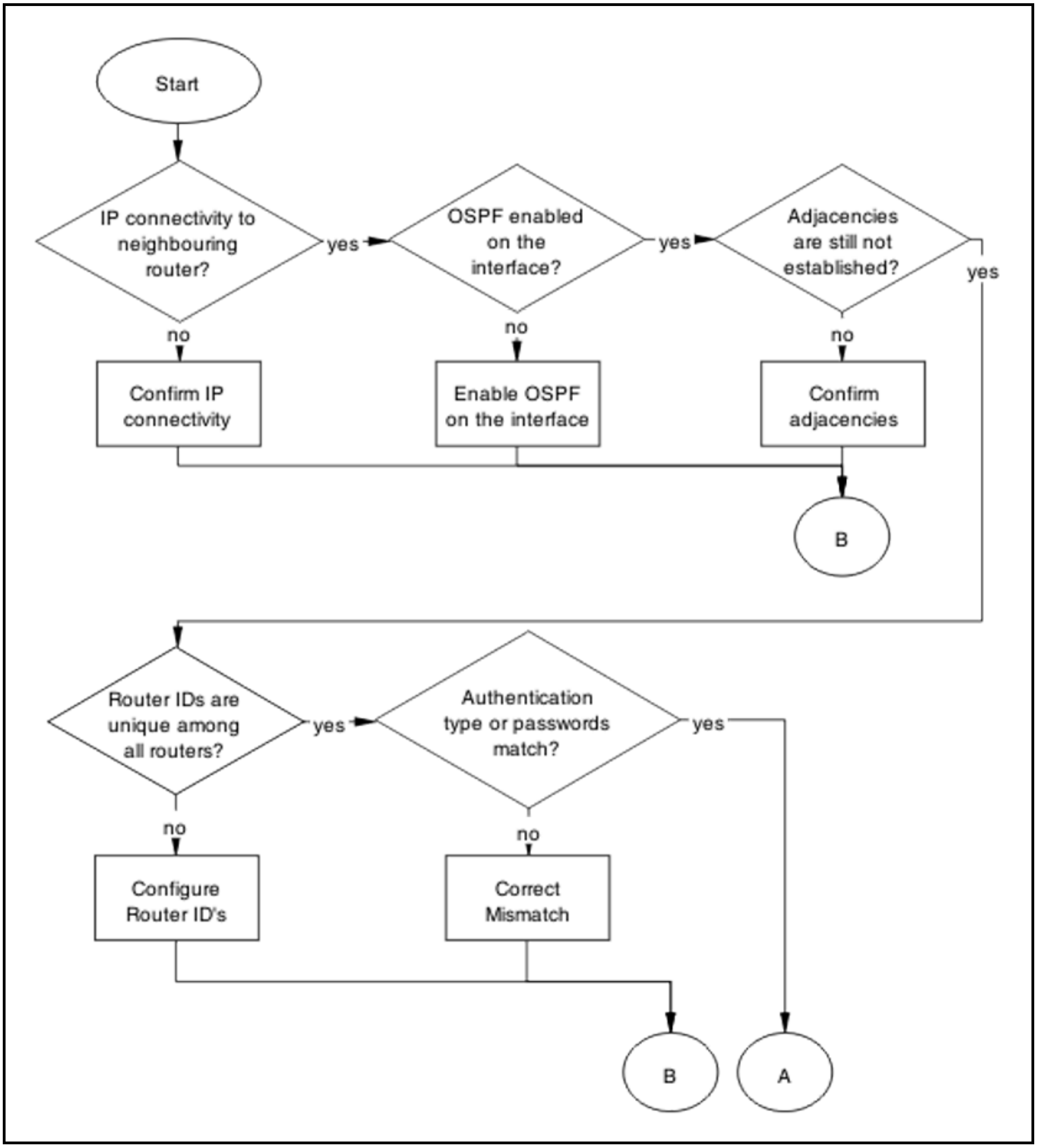
Failure to establish OSPF adjacency

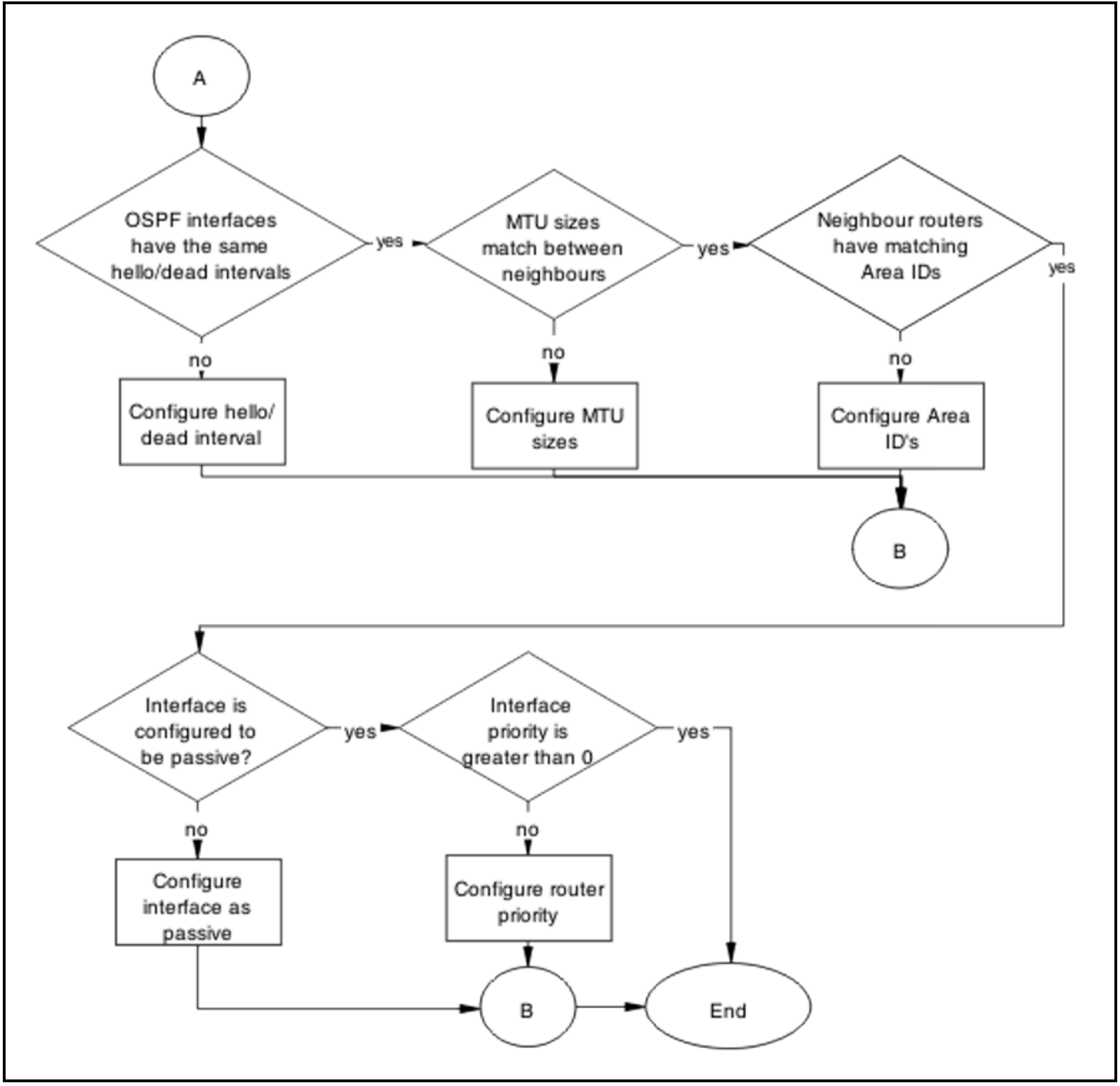
Correct the OSPF parameters to ensure that adjacencies are established.

Work flow: Failure to establish an OSPF adjacency

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

Figure 81
Failure to Establish an OSPF adjacency


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


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

Navigation

- "Confirm IP connectivity" (page 189)
- "Enable OSPF on interface" (page 190)
- "Confirm Adjacencies" (page 193)
- "Configure router IDs" (page 195)
- "Correct mismatch" (page 197)
- "Configure hello/dead interval" (page 201)
- "Configure MTU sizes" (page 203)
- "Configure area IDs" (page 205)

- "Configure an interface to not be passive" (page 207)
- "Configure router priority" (page 209)

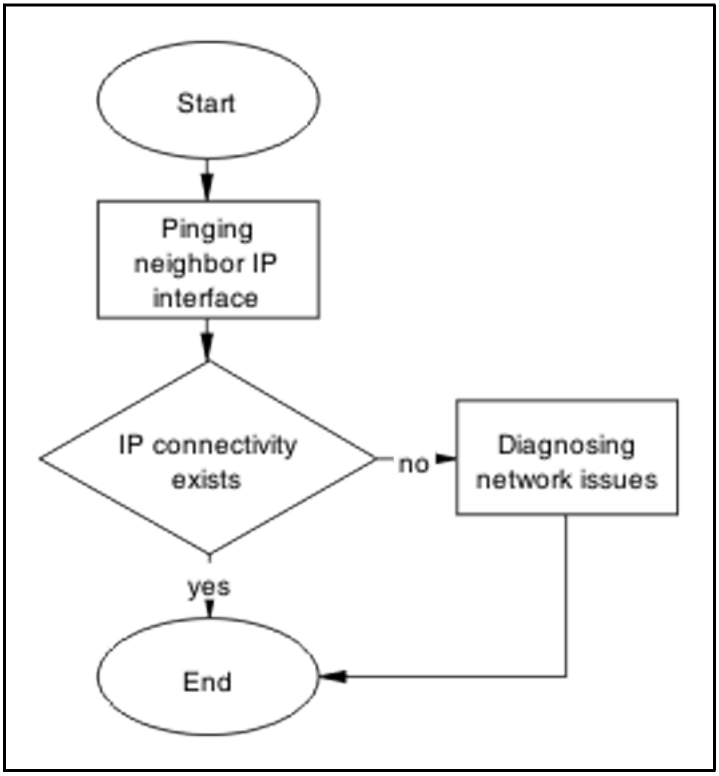
Confirm IP connectivity

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 82
Confirm IP connectivity



Navigation

- "Pinging IP Interface of neighbor" (page 189)
- "Diagnosing network issues" (page 190)

Pinging IP Interface of neighbor

Identify IP connectivity to neighbor.

Procedure Steps

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

--End--

Diagnosing network issues

Fundamental networking issues have to be resolved.

Follow local and vendor procedures to reestablish connectivity between devices.

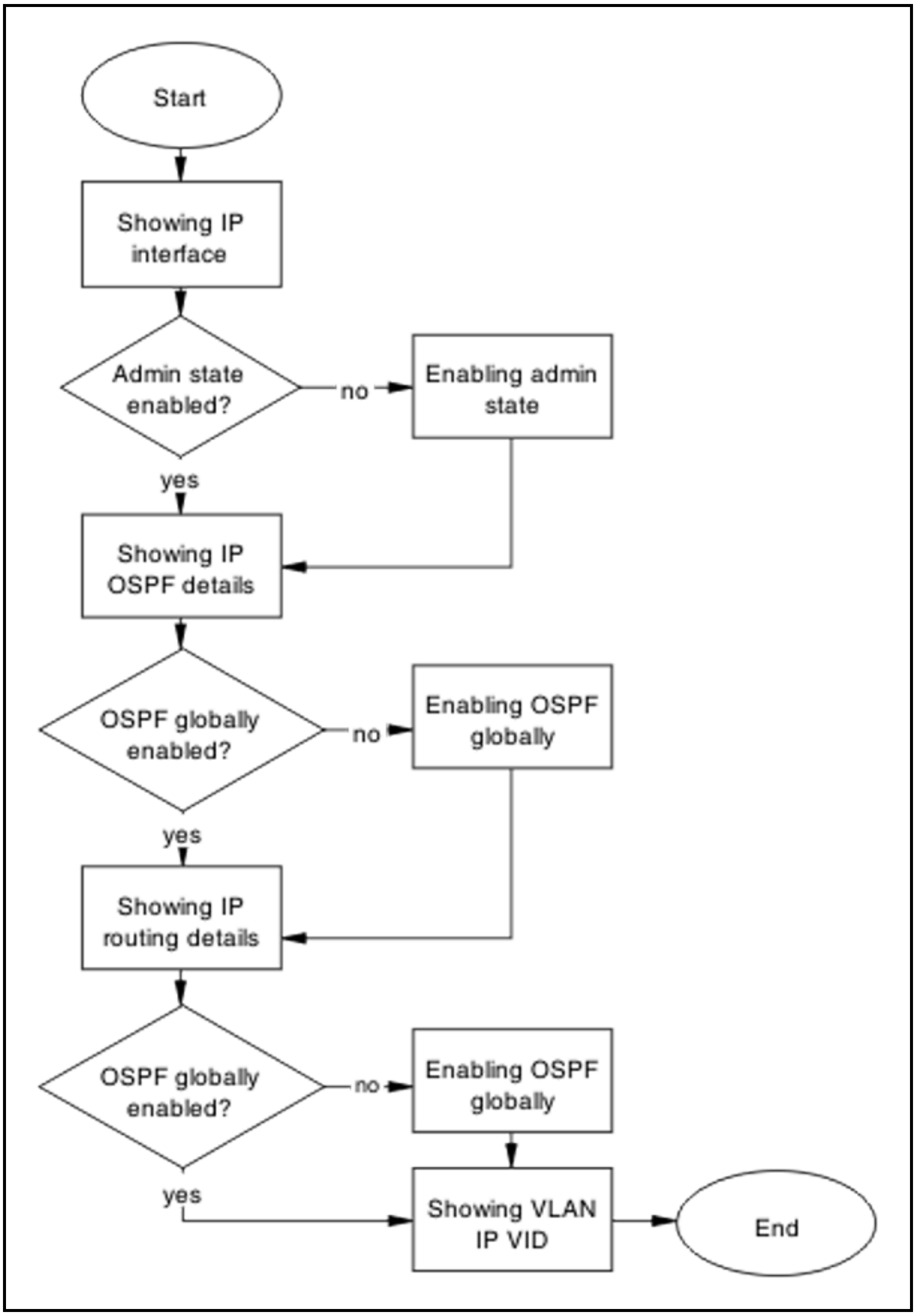
Enable OSPF on interface

Enable OSPF on interface level in order to establish an adjacency.

Task flow: Enable the OSPF on interface

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

Figure 83
Enable OSPF on interface



Navigation

- "Showing IP Interface" (page 192)
- "Enabling admin state" (page 192)
- "Showing IP OSPF" (page 192)
- "Enabling OSPF globally" (page 192)

- "Showing IP routing" (page 193)
- "Enabling OSPF globally" (page 192)
- "Showing VLAN IP VID" (page 193)

Showing IP Interface

Display the IP interface information.

Procedure Steps

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

--End--

Enabling admin state

Enable the admin state of the switch.

Procedure Steps

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

--End--

Showing IP OSPF

Identify if OSPF is globally enabled.

Procedure Steps

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

--End--

Enabling OSPF globally

Enable the OSPF globally for the device.

Procedure Steps

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

--End--

Showing IP routing

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

Procedure Steps

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

--End--

Showing VLAN IP VID

Verify that the IP routing is enabled on the interface.

Procedure Steps

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

--End--

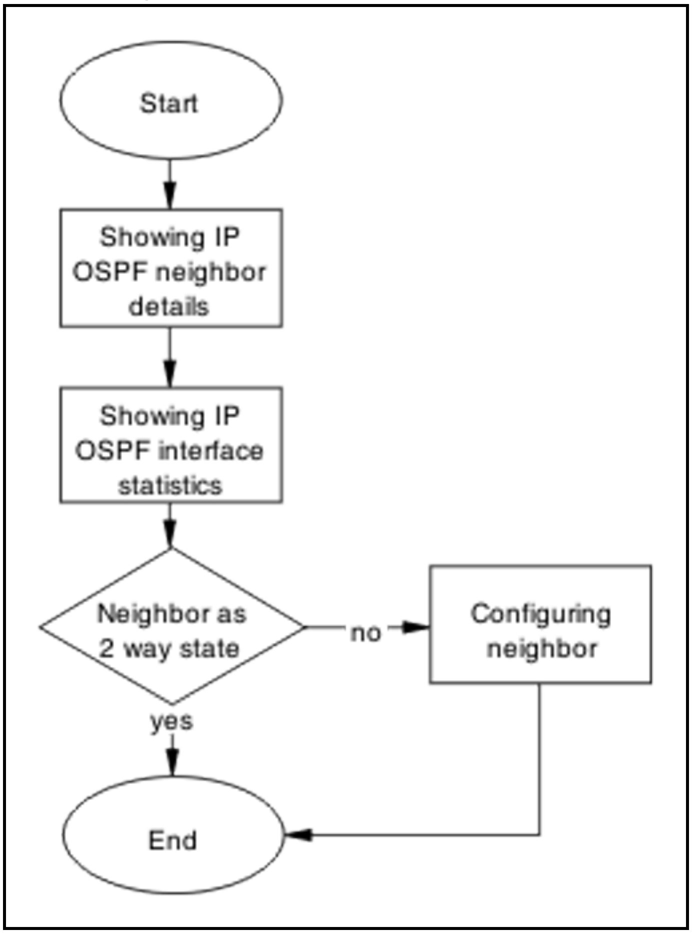
Confirm Adjacencies

Adjacencies between neighbor routers should 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.

Figure 84
Confirm adjacencies


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

Navigation

- "Showing IP OSPF neighbor" (page 194)
- "Showing IP OSPF IP stats" (page 195)
- "Configuring neighbor" (page 195)

Showing IP OSPF neighbor

Display the IP OSPF neighbor information.

Procedure Steps

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

--End--

Showing IP OSPF IP stats

Display the IP OSPF neighbor information.

Procedure Steps

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

--End--

Configuring neighbor

Configure the neighbor device properly.

Procedure Steps

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

--End--

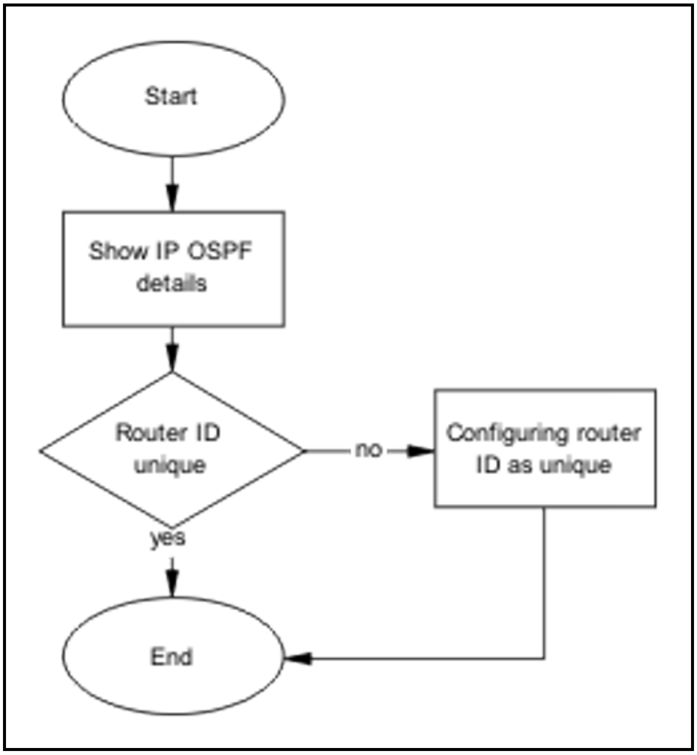
Configure router IDs

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 85
Configure router IDs



Navigation

- "Showing IP OSPF" (page 196)
- "Configuring router ID as unique" (page 196)

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 any time.

Procedure Steps

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

--End--

Configuring router ID as unique

Change the Router ID to ensure it is unique.

Procedure Steps

Step	Action
1	Use the `enable` command to enter userEXEC mode.
2	Use the `configure terminal` command to enter PrivExec mode.
3	Enter the configuration commands, one per line,`router ospf` command. 1. Use the `router ospf` command to enter the router OSPF configuration. 2. Use the `router-ID <A.B.C.D>` command to assign the router ID.
4	Enter **Control-Z** to exit the configuration.

--End--

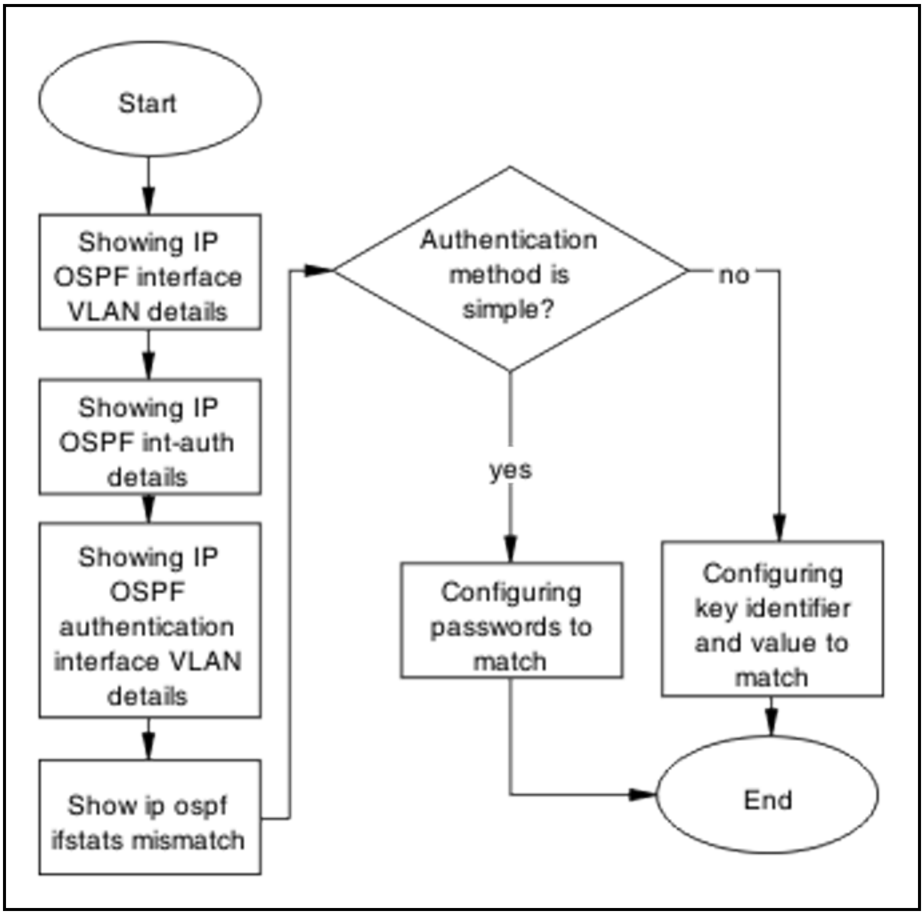
Correct mismatch

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.

Figure 86
Correct mismatch


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

Navigation

- "Showing IP OSPF interface VLAN" (page 198)
- "Showing IP ospf int-auth" (page 199)
- "Showing IP OSPF authentication interface VLAN" (page 199)
- "Showing IP OSPF IFSTATS mismatch" (page 199)
- "Configuring key identifier and value" (page 199)
- "Configuring passwords to match" (page 200)

Showing IP OSPF interface VLAN

Display OSPF information for each VLAN interface.

Procedure Steps

Step	Action
1	Use the **`show ip ospf interface vlan <vid>`** command to display the authentication type.

2	Verify the authentication type: `Authentication Type: None` ..

--End--

Showing IP ospf int-auth

Display the authentication methods for all interfaces.

Procedure Steps

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

--End--

Showing IP OSPF authentication interface VLAN

Displays the assigned MD5 IDs and keys.

Procedure Steps

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

--End--

Showing IP OSPF IFSTATS mismatch

Display statistics for mismatched OSPF parameters.

Procedure Steps

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

--End--

Configuring key identifier and value

When mismatched, both key identifier and key value must be matched.

Procedure Steps

Step	Action
1	Use the **`enable`** command to enter userEXEC mode.
2	Use the **`configure terminal`** command to enter PrivExec mode.
3	Enter the configuration commands: 1. Use the **`int vlan 2`** command to enter the interface configuration. 2. Use the **`ip ospf message-digest-key <MD5 Key ID> md5 <password>`** command to set the key. 3. 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.

--End--

Configuring passwords to match

Passwords must match on both endpoints.

Procedure Steps

Step	Action
1	Use the **`enable`** command to enter userEXEC mode.
2	Use the **`configure terminal`** command to enter PrivExec mode.
3	Enter the configuration commands: 1. Use the **`int vlan 2`** command to enter the interface configuration. 2. Use the **`ip ospf authentication-type simple`** command to set the authentication type to simple. 3. 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.

--End--

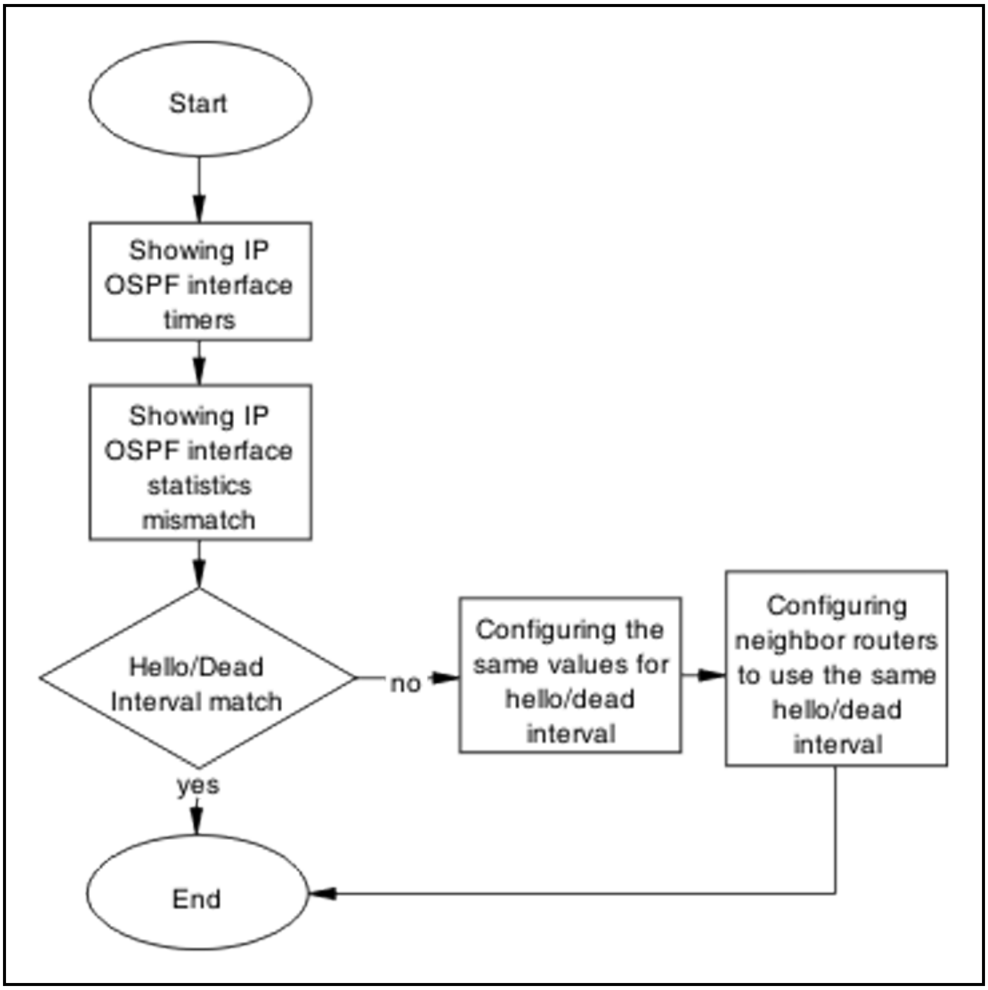
Configure hello/dead interval

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.

Figure 87
Configure hello/dead interval


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

Navigation

- "Showing IP OSPF interface timers" (page 202)
- "Showing IP OSPF ifstats mismatch" (page 202)
- "Configuring the same values for hello/dead interval" (page 202)
- "Configuring neighbor routers to use the same hello/dead interval " (page 203)

Showing IP OSPF interface timers

Display per interface OSPF timers.

Procedure Steps

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

--End--

Showing IP OSPF ifstats mismatch

Display statistics of each OSPF interface.

Procedure Steps

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

--End--

Configuring the same values for hello/dead interval

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

Procedure Steps

Step	Action
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.

--End--

Configuring neighbor routers to use the same hello/dead interval

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

Procedure Steps

Step	Action
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

--End--

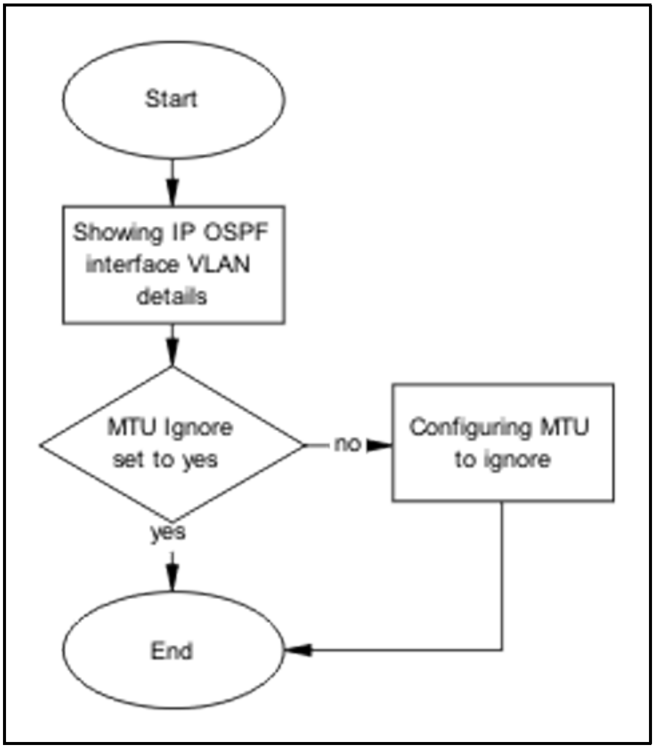
Configure MTU sizes

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.

Figure 88
Configure MTU sizes


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

Navigation

- "Showing IP OSPF interface VLAN" (page 204)
- "Configuring MTU To ignore" (page 204)

Showing IP OSPF interface VLAN

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

Procedure Steps

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

--End--

Configuring MTU To ignore

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

Procedure Steps

Step	Action
1	Use the **`enable`** command to enter userEXEC mode.
2	Use the **`configure terminal`** command to enter PrivExec 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.

--End--

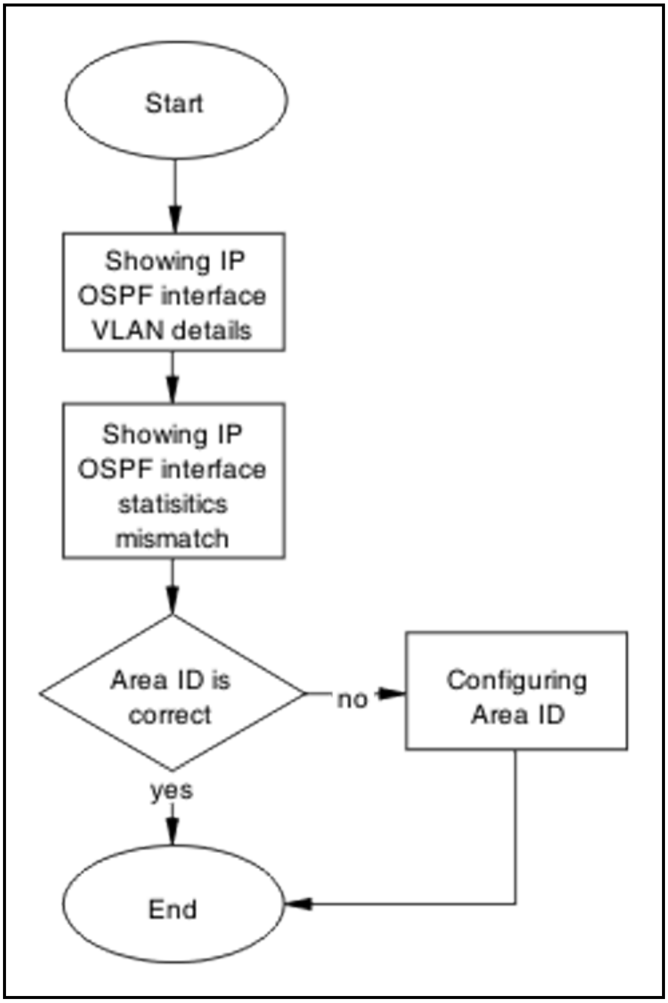
Configure area IDs

Configure neighboring routers to have matching area ID.

Task flow: Configure area ID

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

Figure 89
Configure area ID


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

Navigation

- "Showing IP OSPF interface VLAN" (page 206)
- "Showing IP OSPF IFSTATS mismatch" (page 207)
- "Configuring Area IDs" (page 207)

Showing IP OSPF interface VLAN

Display configuration of each interface OSPF.

Procedure Steps

Step	Action
1	Use the `show ip ospf interface vlan <vid>` command.

2	Verify the Area ID.

--End--

Showing IP OSPF IFSTATS mismatch

Display the statistics for mismatched OSPF parameters.

Procedure Steps

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

--End--

Configuring Area IDs

Configure the Area IDs to match.

Procedure Steps

Step	Action
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 PrivExec mode.
4	Enter the configuration commands: 1. Use the `router ospf` command to enter the OSPF configuration. 2. 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.

--End--

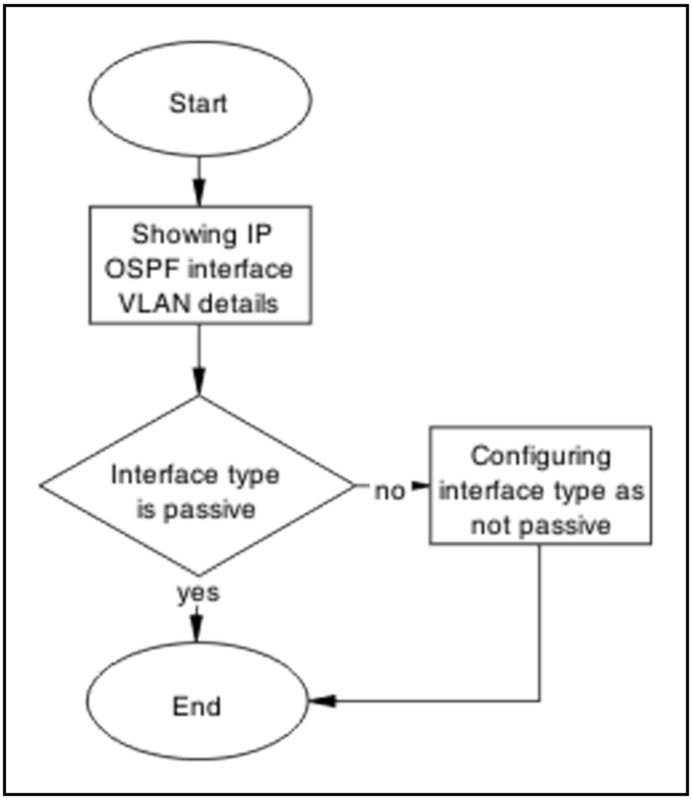
Configure an interface to not be passive

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.

Figure 90
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

Navigation

- "Showing IP OSPF interface VLAN" (page 208)
- "Configuring interface type as not passive" (page 209)

Showing IP OSPF interface VLAN

Display the OSPF interface VLAN information.

Procedure Steps

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

--End--

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).

Procedure Steps

Step	Action
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.

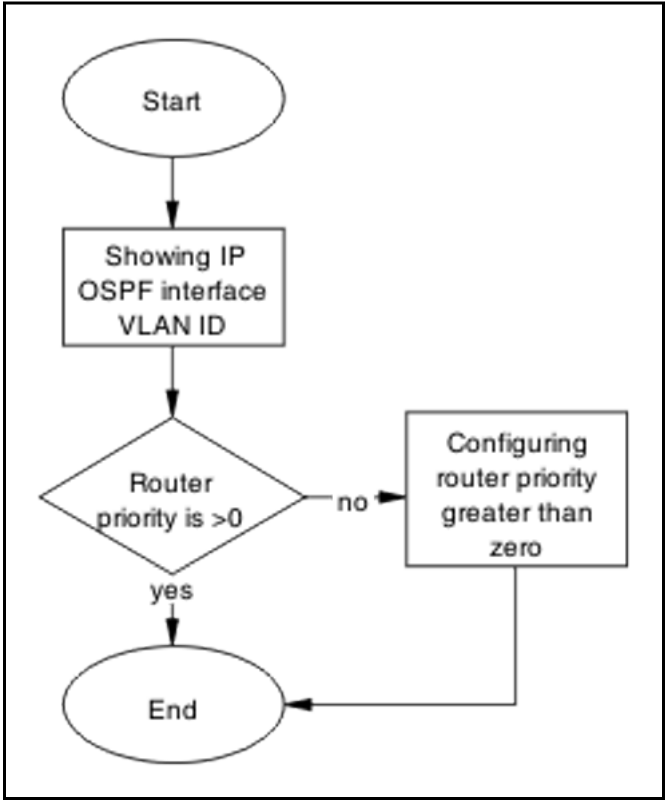
--End--

Configure router priority

Verify that the interfaces of all routers do not have a router priority of 0. At least one router must have 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

Navigation

- "Showing IP OSPF interface VLAN" (page 210)
- "Configuring router priority greater than zero" (page 210)

Showing IP OSPF interface VLAN

Display the OSPF interface VLAN information

Procedure Steps

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

--End--

Configuring router priority greater than zero

Configure the router so the priority is greater than zero.

Procedure Steps

Step	Action
1	Use the **`configure terminal`** command to enter PrivExec mode.
2	Enter the configuration commands: 1. Use the **`int vlan 2`** command to enter the interface configuration. 2. Use the **`ip ospf priority 1`** command to change the priority.
3	Enter **Control-Z** on the keyboard to exit the configuration.

--End--

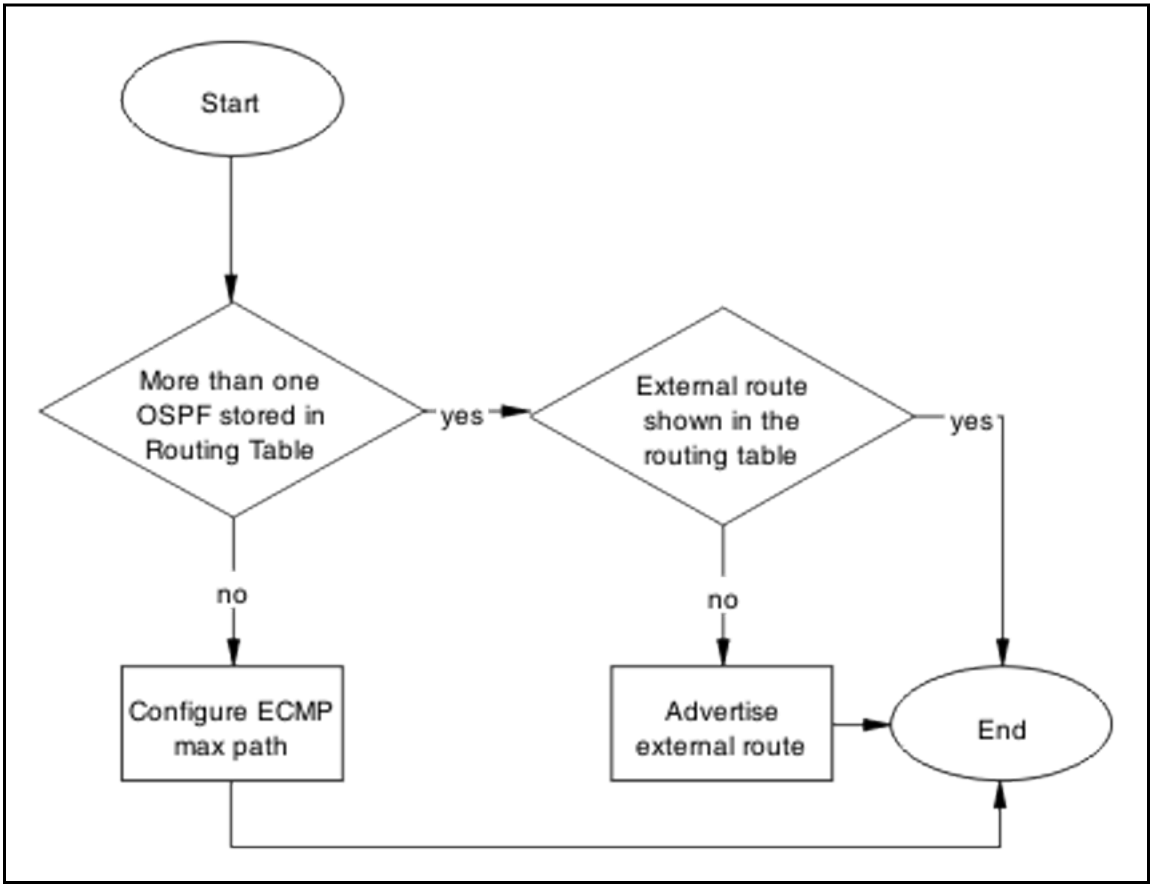
OSPF route is not installed in routing table

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.

Figure 91
OSPF route is not installed in routing table


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

Navigation

- "Confirm ECMP max path" (page 212)
- "Advertise external route" (page 214)

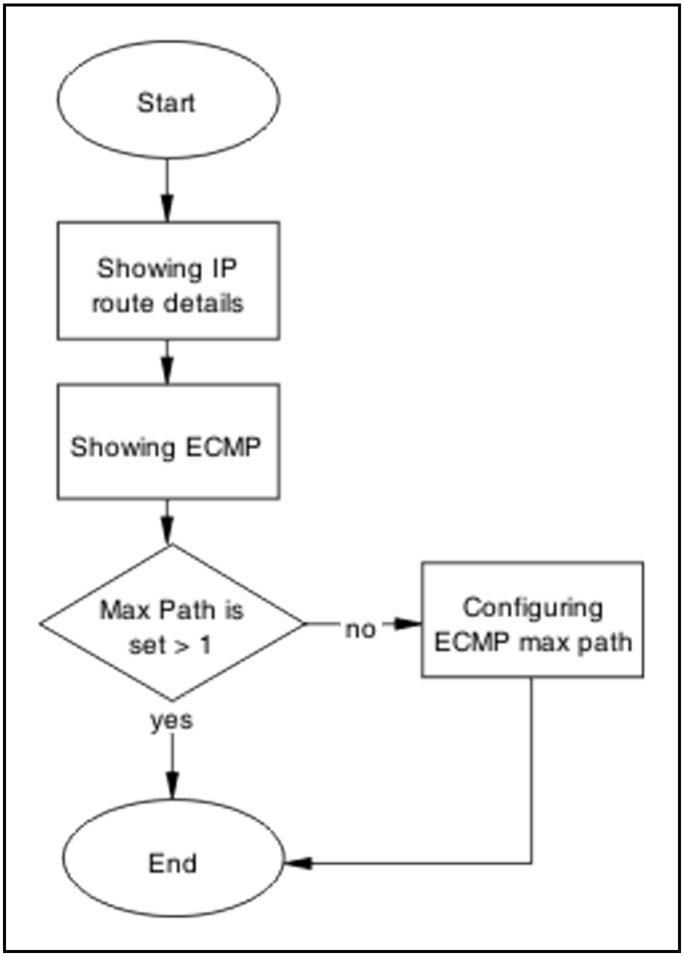
Confirm ECMP max path

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 92
Confirm ECMP max path



Navigation

- "Showing IP Route" (page 213)
- "Showing ECMP" (page 214)
- "Configuring ECMP" (page 214)

Showing IP Route

Display the routing table information.

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

Procedure Steps

Step	Action
1	Enter the `show ip route` to display the routing information.

2	Use the `show ip ospf redistribute` command to view the redistribution policy.

--End--

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.

Procedure Steps

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

--End--

Configuring ECMP

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

An ECMP license is required to enable this feature.

Procedure Steps

Step	Action
1	Use the `enable` command to enter UserEXEC mode.
2	Use the `configure terminal` command to enter PrivEXEC 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.

--End--

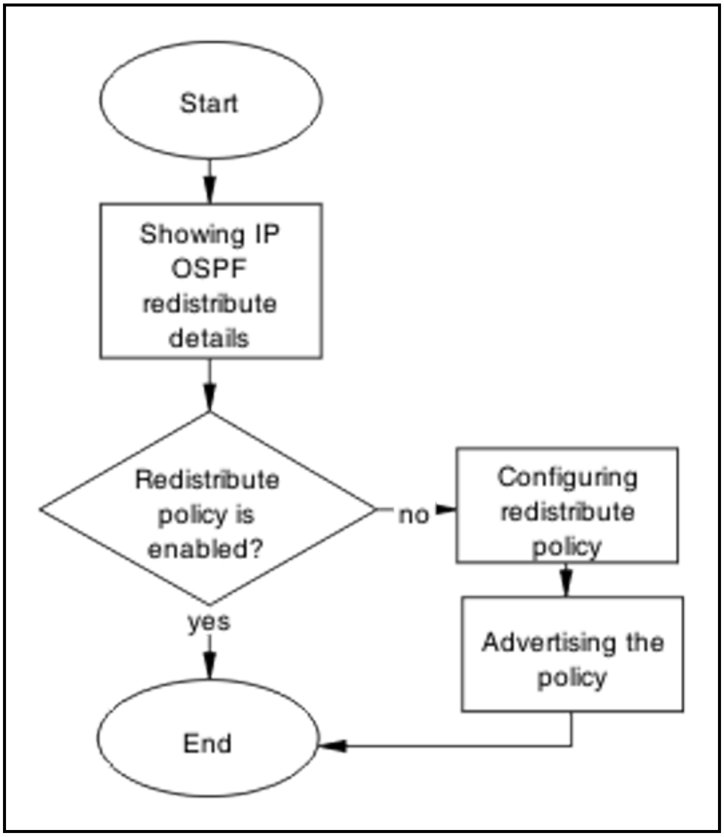
Advertise external route

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.

Figure 93
Advertise external route


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

Navigation

- "Showing IP OSPF redistribute" (page 215)
- "Configuring Redistribute Policy" (page 215)

Showing IP OSPF redistribute

Display the routing table information.

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

Procedure Steps

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

--End--

Configuring Redistribute Policy

Redistribute external routes into OSPF network.

Procedure Steps

Step	Action
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.

--End--

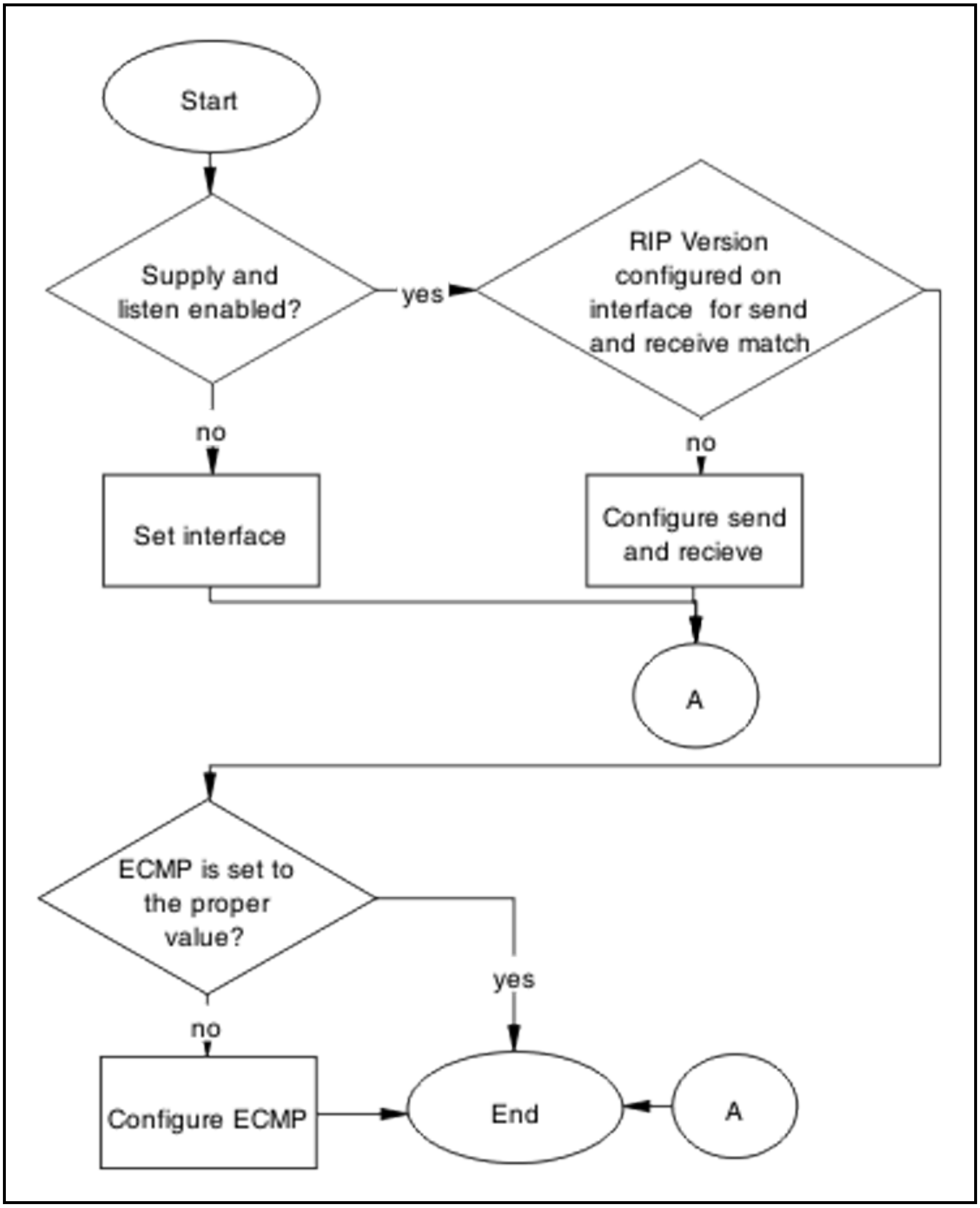
RIP packets exchanged between device under test (DUT) but no routes are learned

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.

Figure 94
RIP Packets exchanged between device under test (DUT) but no routes are learned


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

Navigation

- "Set interface" (page 217)
- "Configure send and receive" (page 219)
- "Configure ECMP" (page 221)

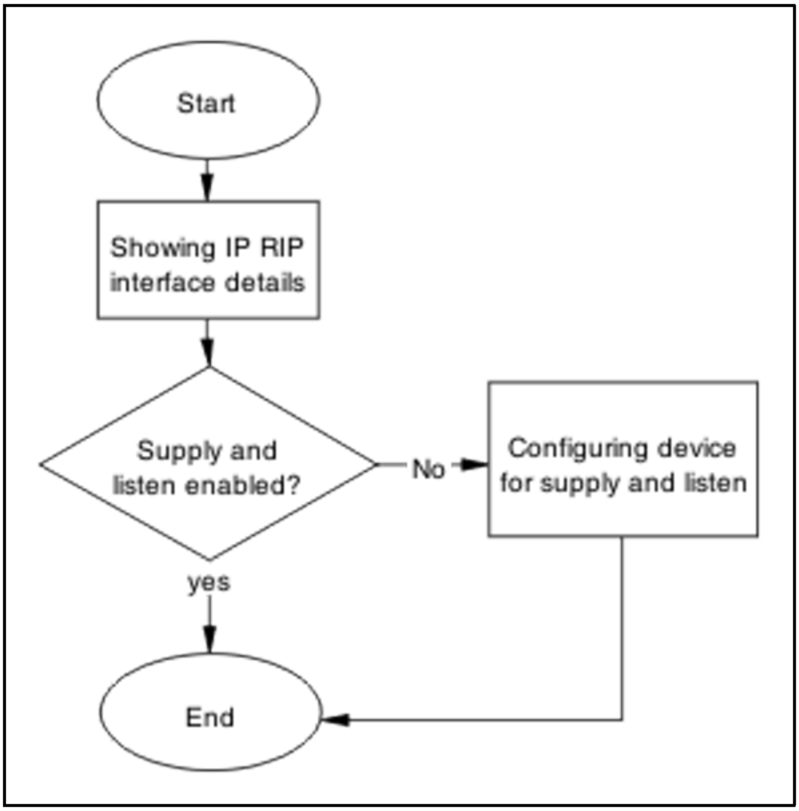
Set interface

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.

Figure 95
Set interface


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

Navigation

- "Showing RIP IP interface" (page 218)
- "Configuring device for supply and listen" (page 219)

Showing RIP IP interface

Display the RIP interface information.

Procedure Steps

Step	Action
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.

--End--

Configuring device for supply and listen

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

Procedure Steps

Step	Action
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: 1. The **`enable`** command to enter userEXEC mode. 2. The **`configure terminal`** command to enter PrivExec mode. 3. The **`interface vlan <1-4094>`** command to enter the interface VLAN. 4. The **`ip rip supply/listen enable`** command to enable the supply/listen. 5. The **`exit`** command to exit the configuration.

--End--

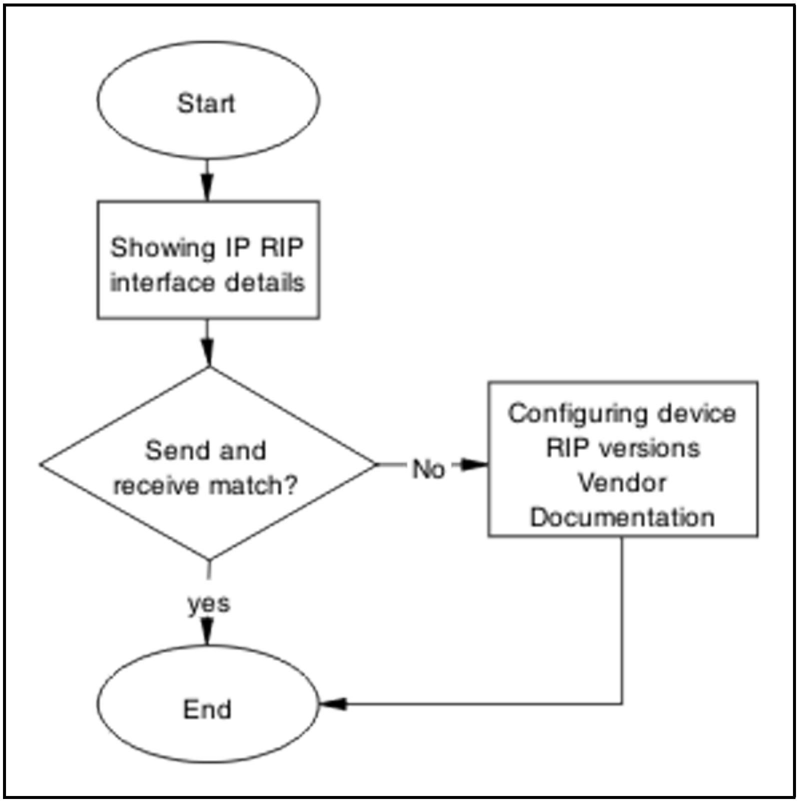
Configure send and receive

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.

Figure 96
Configure send and receive


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

Navigation

- "Showing RIP IP interface" (page 220)
- "Configuring device RIP versions" (page 220)

Showing RIP IP interface

Display the RIP interface information

Procedure Steps

Step	Action
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.

--End--

Configuring device RIP versions

Configure the device to send and receive RIP packets.

Procedure Steps

Step	Action
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: 1. The **`enable`** command to enter userEXEC mode. 2. The **`configure terminal`** command to enter PrivExec mode. 3. The **`interface vlan <1-4096>`** command to enter the interface. 4. **`ip rip send version notsend/rip1/rip1comp/rip2`**. 5. **`ip rip receive version rip1/rip1orrip2/rip2`**.

--End--

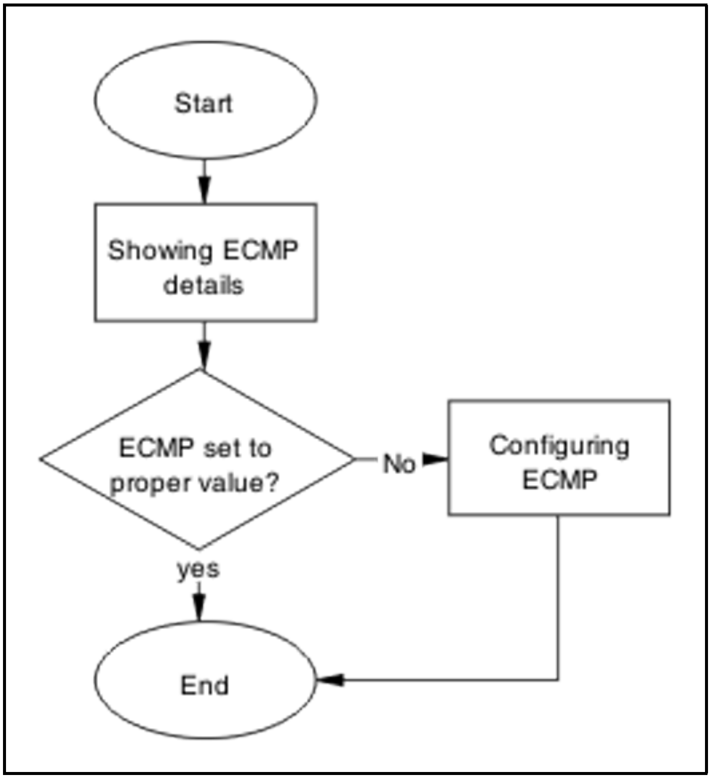
Configure ECMP

Set ECMP to proper value.

Task flow: Configure ECMP

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

Figure 97
Configure ECMP



Navigation

- "Showing ECMP details" (page 222)
- "Configuring ECMP" (page 222)

Showing ECMP details

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

Procedure Steps

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

--End--

Configuring ECMP

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

Prerequisites An ECMP license is required to enable this feature.

Procedure Steps

Step	Action
1	Use the **enable** command to enter UserEXEC mode.
2	Use the **configure terminal** command to enter PrivEXEC 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.

--End--

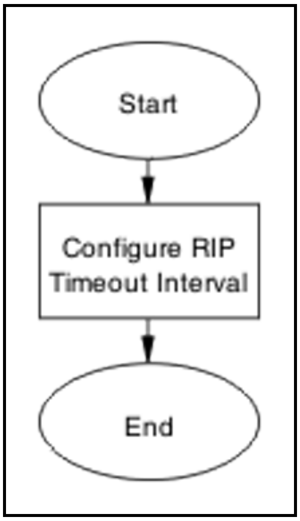
RIP routes are learned-deleted learned again

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 in order to stop the RIP routed from being deleted after being learned.

Figure 98
RIP routes are learned-deleted learned again



Navigation

- "Configuring RIP timeout interval" (page 223)

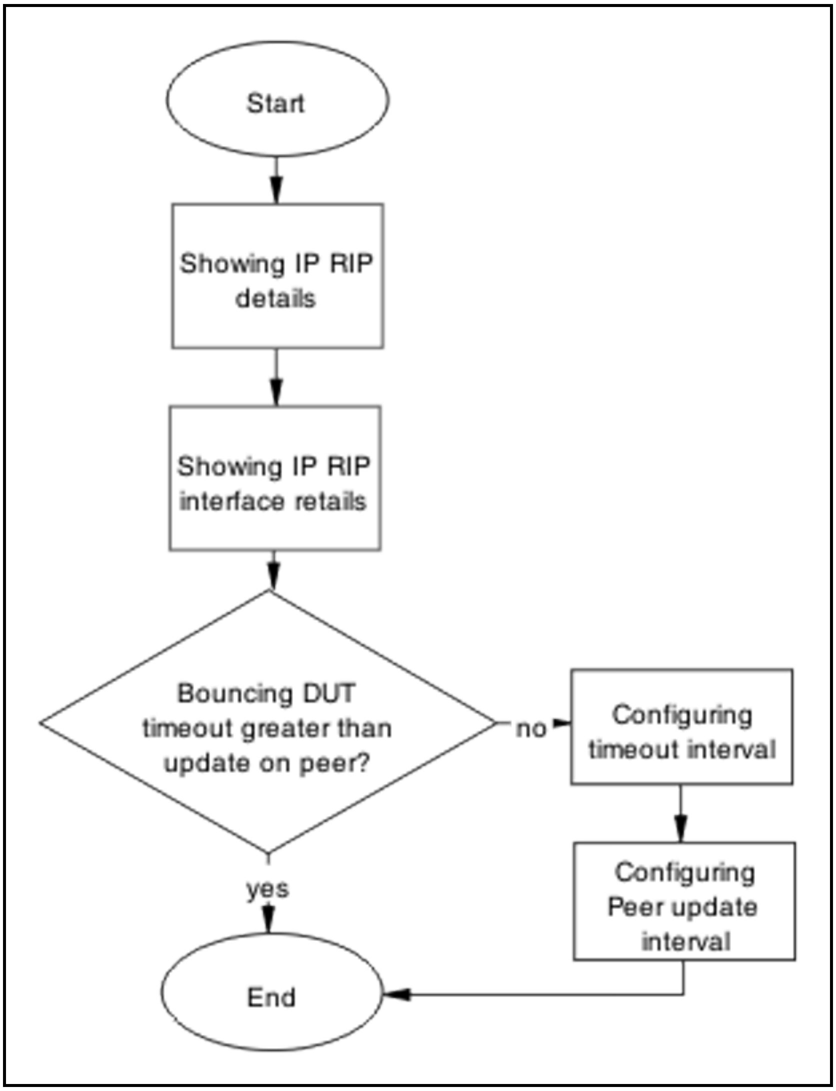
Configuring RIP timeout interval

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.

Figure 99
Configure RIP timeout interval


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

Navigation

- "Showing IP RIP" (page 224)
- "Showing RIP IP interface" (page 225)
- "Configuring timeout Interval" (page 225)
- "Configuring peer update interval" (page 225)

Showing IP RIP

Display the IP RIP information to observe the timeout intervals.

Procedure Steps

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

--End--

Showing RIP IP interface

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

Procedure Steps

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

--End--

Configuring timeout Interval

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

Procedure Steps

Step	Action
1	Use the `enable` command to enter user EXEC mode.
2	Use the `configure terminal` command to PrivEXEC 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.

--End--

Configuring peer update interval

Configure the peer update timeout interval.

Procedure Steps

Step	Action
1	Use the **`enable`** command to enter user EXEC mode.
2	Use the **`configure terminal`** command to PrivEXEC 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.

--End--

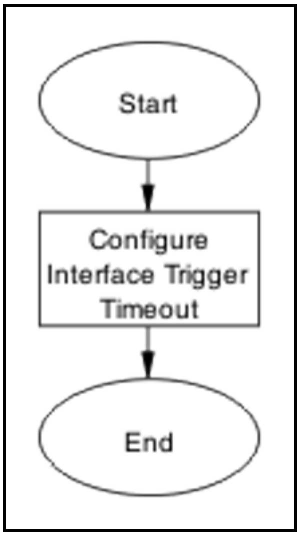
RIP routes learned with increasing cost

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 100
RIP routes learned with increasing cost



Navigation

- "Configure interface trigger timeout " (page 227)

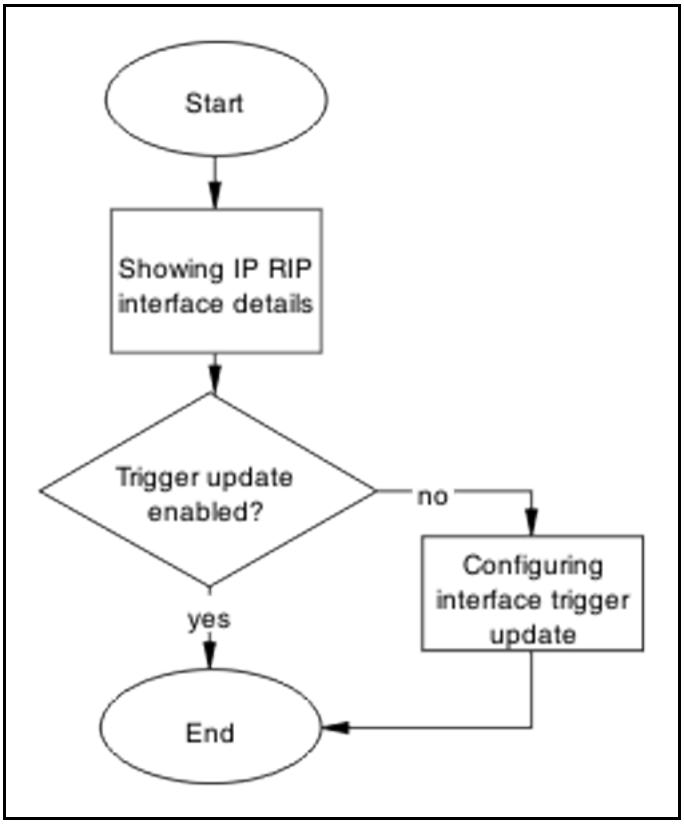
Configure interface trigger timeout

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 in order to send RIP updates after a device goes down.

Figure 101
Configure interface trigger timeout


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

Navigation

- "Showing IP RIP interface" (page 227)
- "Configuring interface trigger update" (page 228)

Showing IP RIP interface

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

Procedure Steps

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

--End--

Configuring interface trigger update

Change the trigger update to enabled.

Procedure Steps

Step	Action
1	Use the **`enable`** command to enter user EXEC mode.
2	Use the **`configure terminal`** command to PrivEXEC 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.

--End--

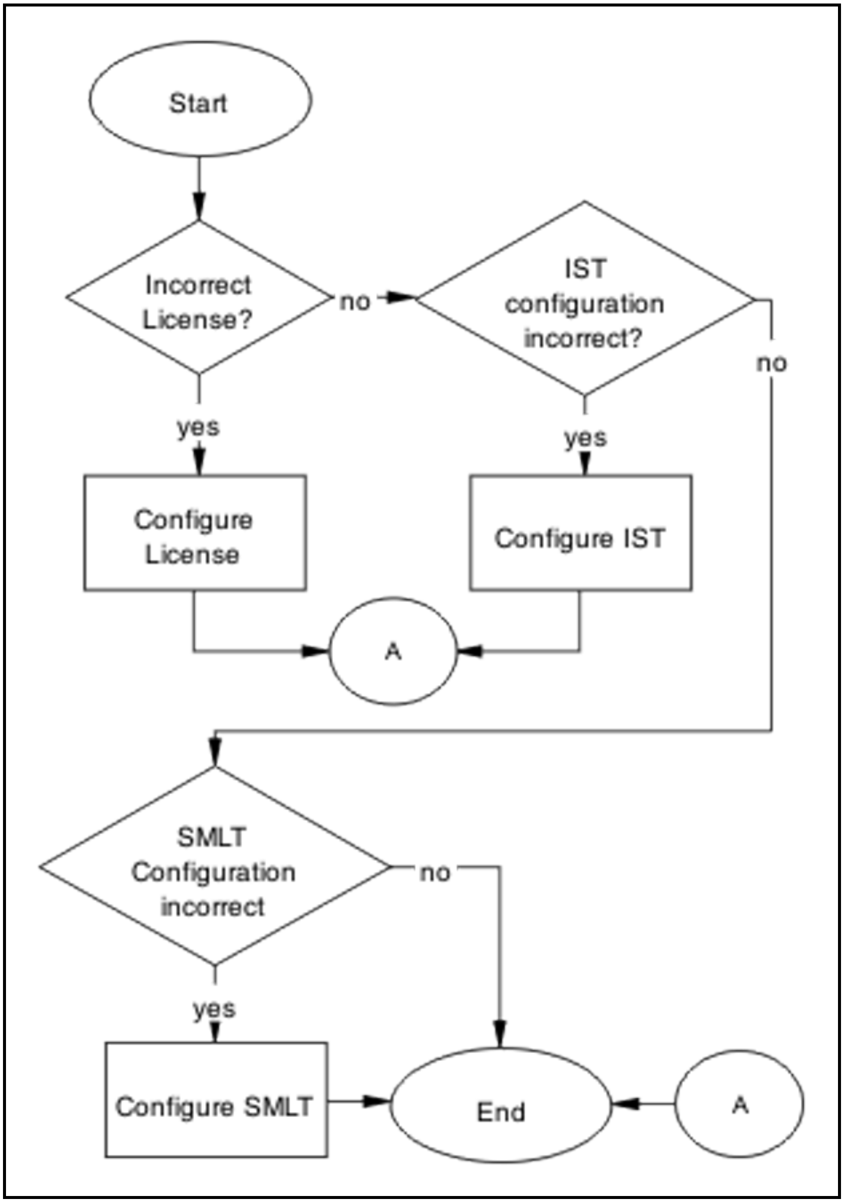
SMLT routing issue

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 102
SMLT routing issue



Navigation

- "Configure License" (page 229)
- "Configure IST" (page 231)
- "Configure SMLT" (page 236)

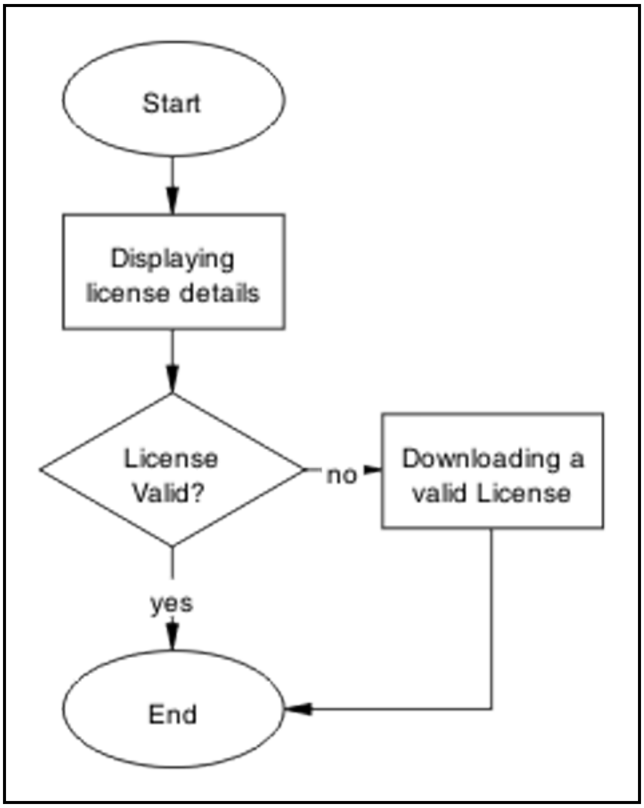
Configure License

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 103
Configure license



Navigation

- "Displaying license details" (page 230)
- "Downloading a valid license" (page 231)

Displaying license details

View license information on the edge and aggregation devices.

Procedure Steps

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

--End--

Downloading a valid license

Download the valid license to the switch.

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

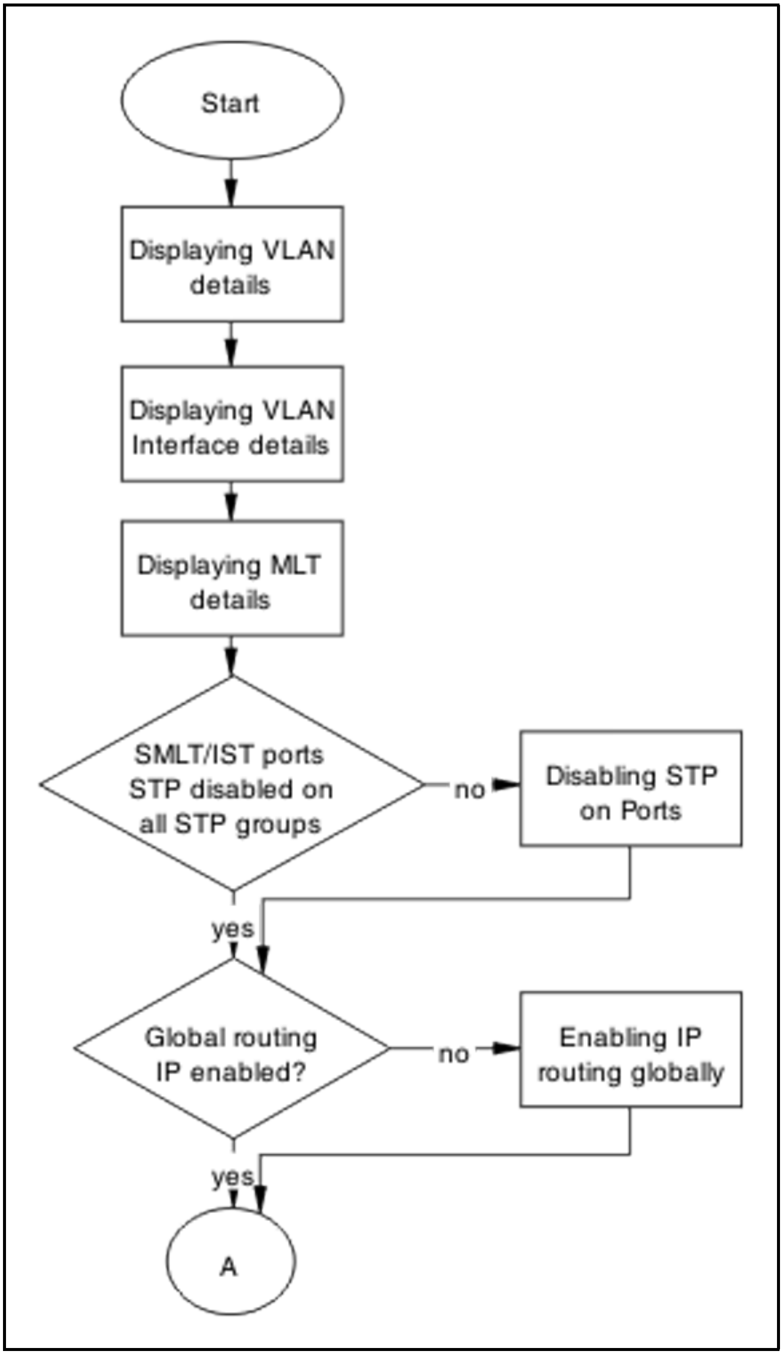
Configure IST

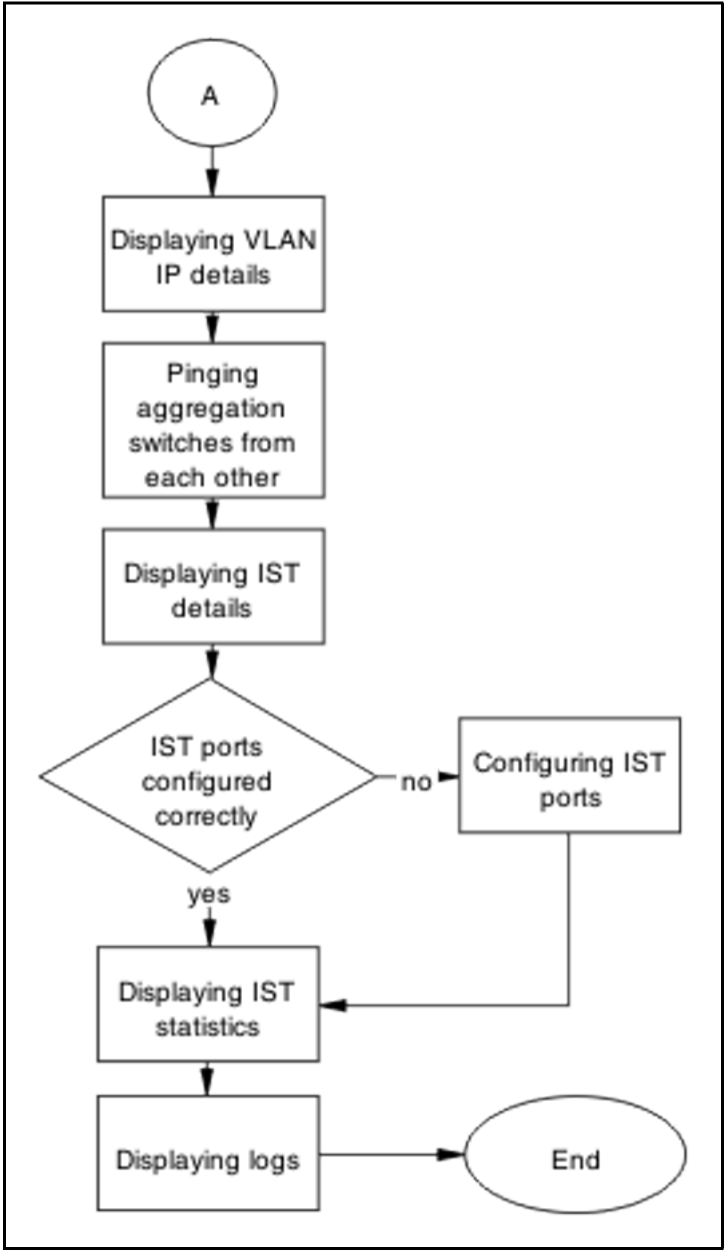
Set IST to ensure routing is correctly configured.

Task flow: Configure IST

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

Figure 104
Configure IST


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


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

Navigation

- "Displaying VLAN details" (page 234)
- "Displaying VLAN interface details" (page 234)
- "Displaying MLT details" (page 234)
- "Disabling STP on ports" (page 234)
- "Enabling IP routing globally" (page 235)
- "Displaying VLAN IP details" (page 235)
- "Pinging aggregation switches from each other" (page 235)
- "Configuring IST ports" (page 236)

- "Displaying IST statistics" (page 236)
- "Displaying logs" (page 236)

Displaying VLAN details

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

Procedure Steps

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

--End--

Displaying VLAN interface details

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

Procedure Steps

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

--End--

Displaying MLT details

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

Procedure Steps

Step	Action
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.

--End--

Disabling STP on ports

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

Procedure Steps

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

--End--

Enabling IP routing globally

View the IP routing information

Procedure Steps

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

--End--

Displaying VLAN IP details

Display the VLAN IP information.

Procedure Steps

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

--End--

Pinging aggregation switches from each other

Test the IP connection between two switches.

Procedure Steps

Step	Action
1	Use the **`ping <switch2>`** from the first switch.

Step	Action
2	Use the **`ping <switch1>`** from the second switch.

--End--

Configuring IST ports

View the IST configuration and operational mode.

Procedure Steps

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

--End--

Displaying IST statistics

Check the counters between two aggregate switches for messages.

Procedure Steps

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

--End--

Displaying logs

Check the logging to see possible messages related to IST.

Procedure Steps

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

--End--

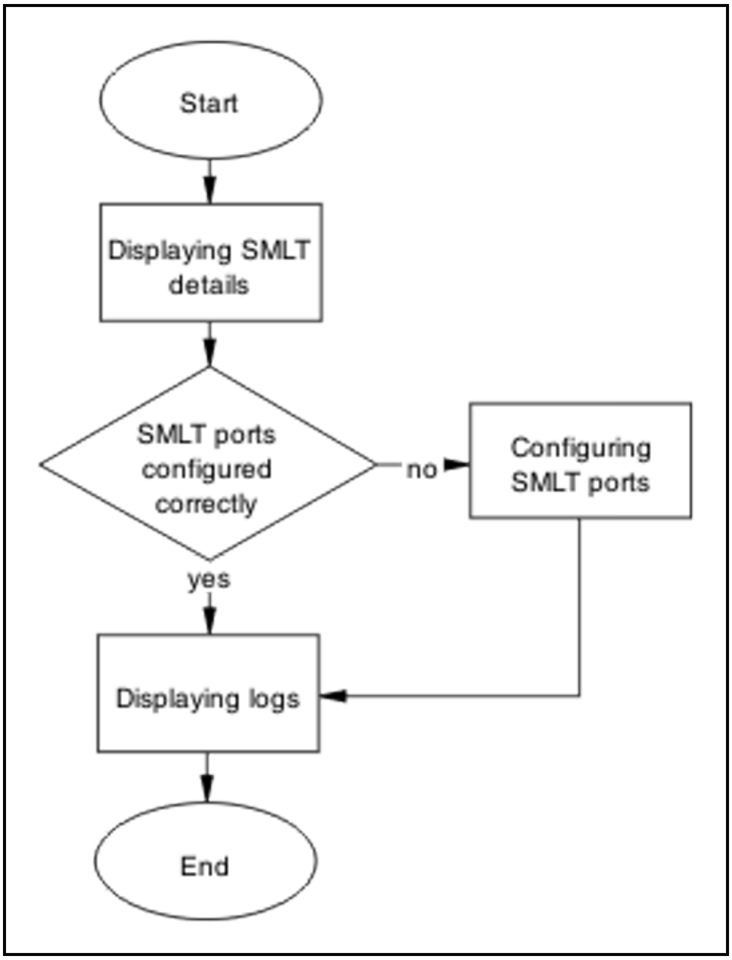
Configure SMLT

Configure SMLT to ensure it is functioning correctly.

Task flow: Configure SMLT

The following task flow assists you to properly configure SMLT.

Figure 105
Configure SMLT



Navigation

- "Displaying SMLT details" (page 237)
- "Configuring SMLT ports" (page 238)
- "Displaying logs" (page 238)

Displaying SMLT details

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

Procedure Steps

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

--End--

Configuring SMLT ports

Configure the SMLT on the ports.

Procedure Steps

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

--End--

Displaying logs

Check the logging to see possible messages related to SMLT.

Procedure Steps

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

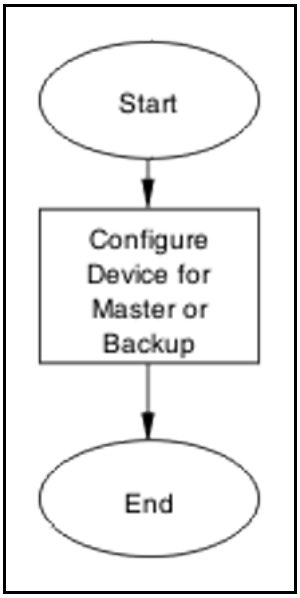
--End--

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 backupwork flow

Figure 106
VR is stuck in initialize state when it should be master or backup



Navigation

- "Configure device for master or backup" (page 239)

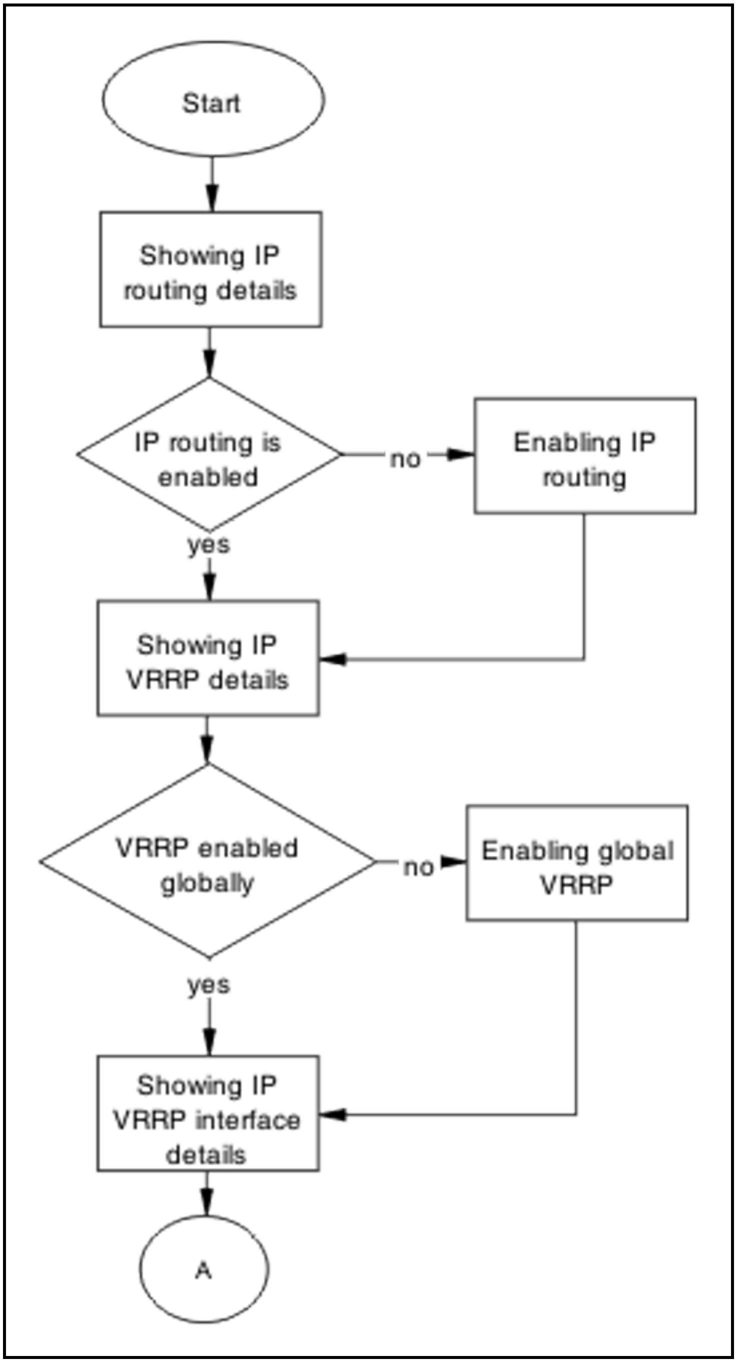
Configure device for master or backup

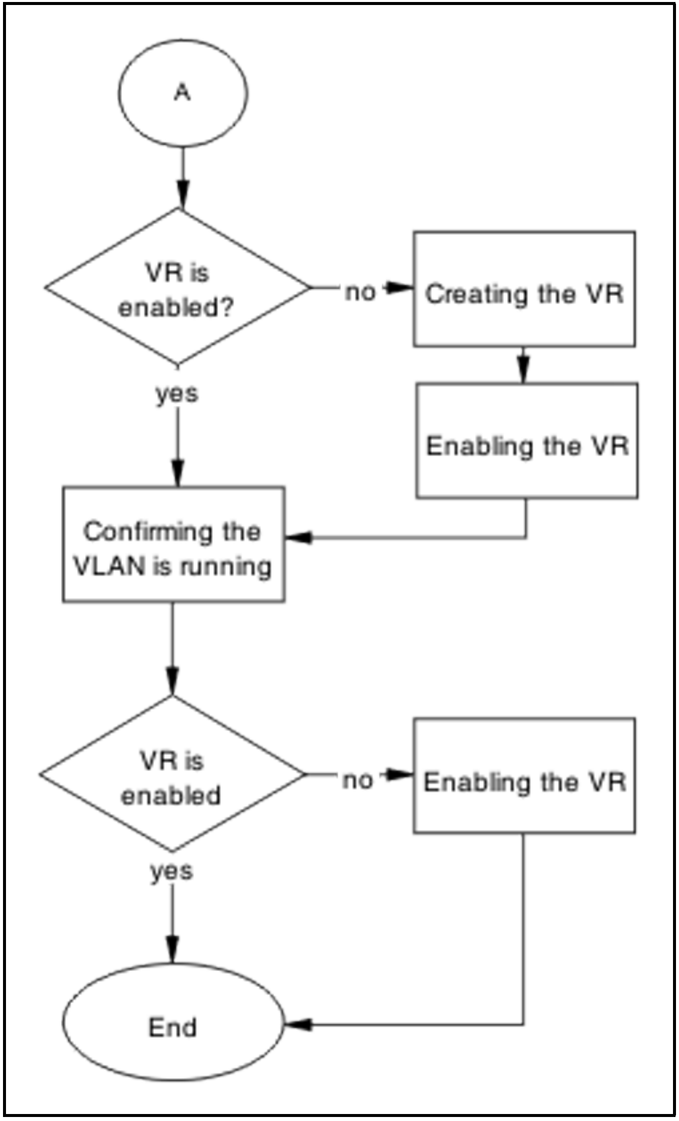
Set the device for master or backup under VRRP.

Task flow: Configure device for master or backup

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

Figure 107
Configure device for master or backup





Navigation

- "Showing IP routing details" (page 241)
- "Enabling IP routing" (page 242)
- "Showing IP VRRP details" (page 242)
- "Enabling global VRRP" (page 242)
- "Showing IP VRRP interface details" (page 243)
- "Creating the VR" (page 243)
- "Enabling the VR" (page 243)
- "Confirming VLAN is running" (page 243)

Showing IP routing details

Verify that IP routing is enabled.

Procedure Steps

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

--End--

Enabling IP routing

IP routing should be globally enabled on the switch.

Procedure Steps

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

--End--

Showing IP VRRP details

Verify that VRRP is enabled globally.

Procedure Steps

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

--End--

Enabling global VRRP

This procedure assists you to enable VRRP globally.

Procedure Steps

Step	Action
1	Use **`router vrrp enable`** global configuration mode command to enable VRRP globally on the ERS 5500 Series device.

Step	Action
2	Observe no errors after execution.

--End--

Showing IP VRRP interface details

Verify that the VR itself is enabled.

Procedure Steps

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

--End--

Creating the VR

The following procedure assists you to create a VR.

Procedure Steps

Step	Action
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.

--End--

Enabling the VR

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

Procedure Steps

Step	Action
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.

--End--

Confirming VLAN is running

Verify that the VR itself is enabled.

Procedure Steps

Step	Action
1	Use the command `ip vrrp`.
2	Confirm there is at least one active link.

--End--

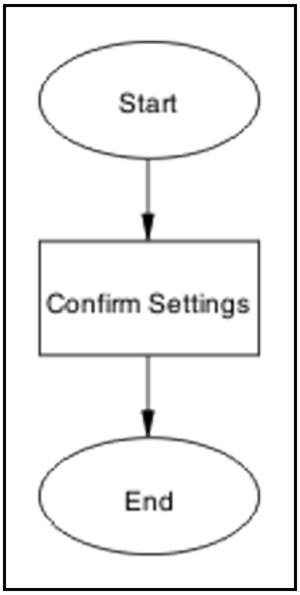
VR is stuck in master state when it should be backup (more than one master is present in a VR)

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 108
VR stuck in master state when it should be backup (more than one master is present in a VR)



Navigation

- "Confirm settings" (page 244)

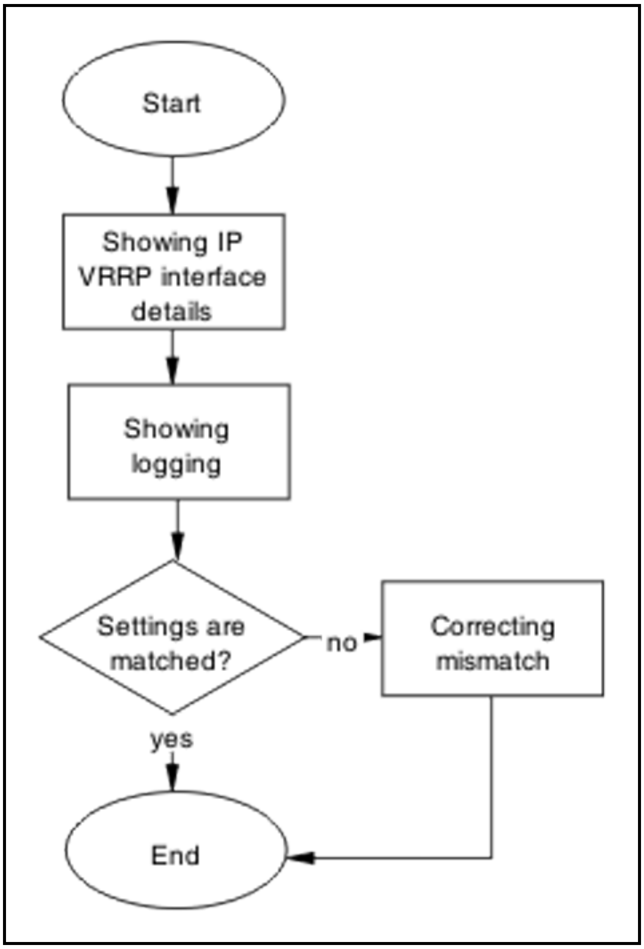
Confirm settings

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 109
Confirm settings



Navigation

- "Showing IP VRRP interface details" (page 245)
- "Showing logging" (page 246)
- "Correcting mismatch" (page 246)

Showing IP VRRP interface details

Verify critical information for the VRRP interface.

Procedure Steps

Step	Action
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.

--End--

Showing logging

Obtain log messages for the device.

Procedure Steps

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

--End--

Correcting mismatch

Configure the VRRP interface eliminate the mismatch.

Procedure Steps

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

--End--

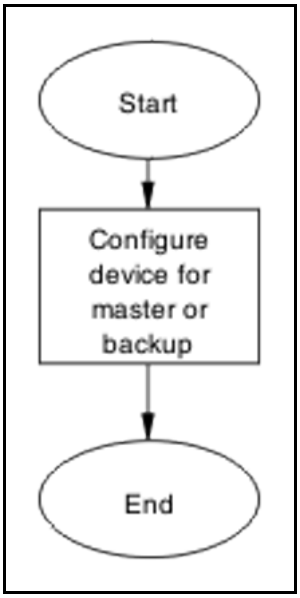
VR is stuck in backup state when it should be master (no master is present across the VR)

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. There is no master present in the VR

Figure 110
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" (page 247)

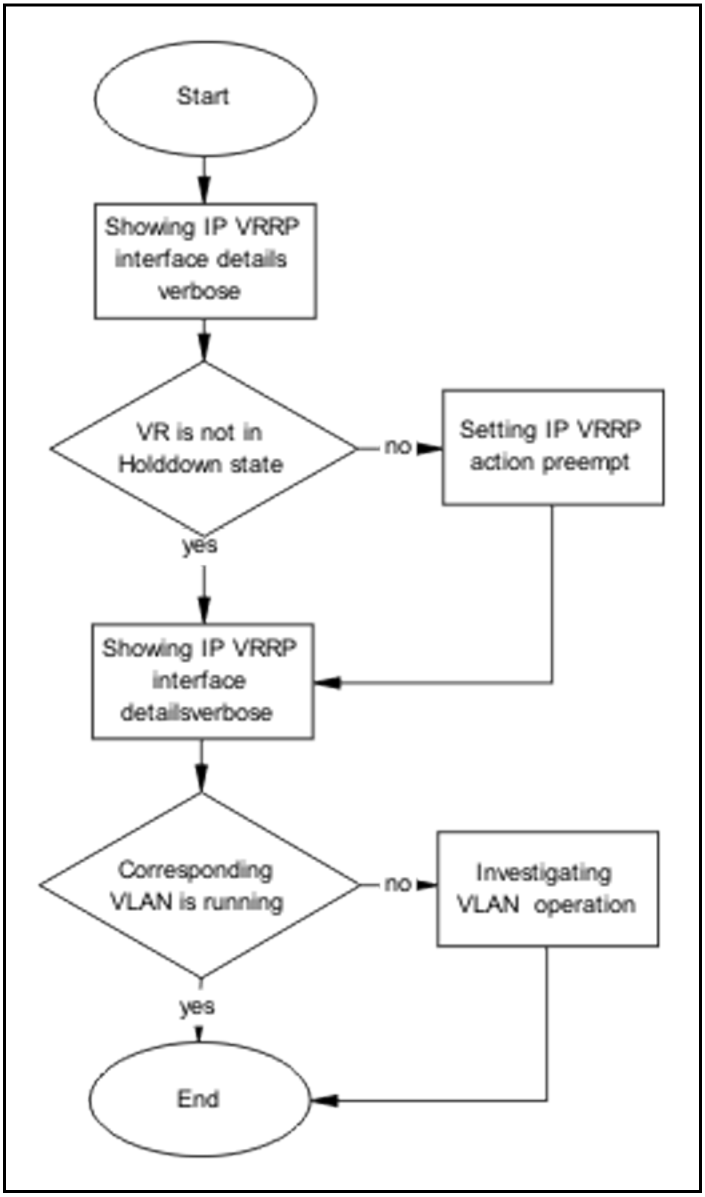
Configure device for master or backup

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.

Figure 111
Configure device for 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

Navigation

- "Showing IP VRRP interface details verbose" (page 248)
- "Setting IP VRRP action preempt " (page 249)
- "Investigating VLAN operation" (page 249)

Showing IP VRRP interface details verbose

Verify critical information for the VRRP interface.

Procedure Steps

Step	Action
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.

--End--

Setting IP VRRP action preempt

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

Procedure Steps

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

--End--

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.

Procedure Steps

Step	Action
1	Enter the command `show vlan` to view VLAN information.
2	Note that the VLAN in question is up.

--End--

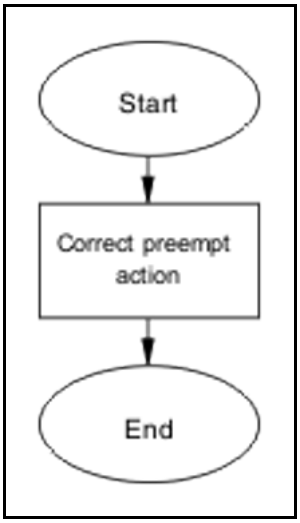
Preempt mode is not working

The ‘preempt mode’ setting as per 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 112
Preempt mode is not working



Navigation

- "Preempt mode is not working" (page 249)

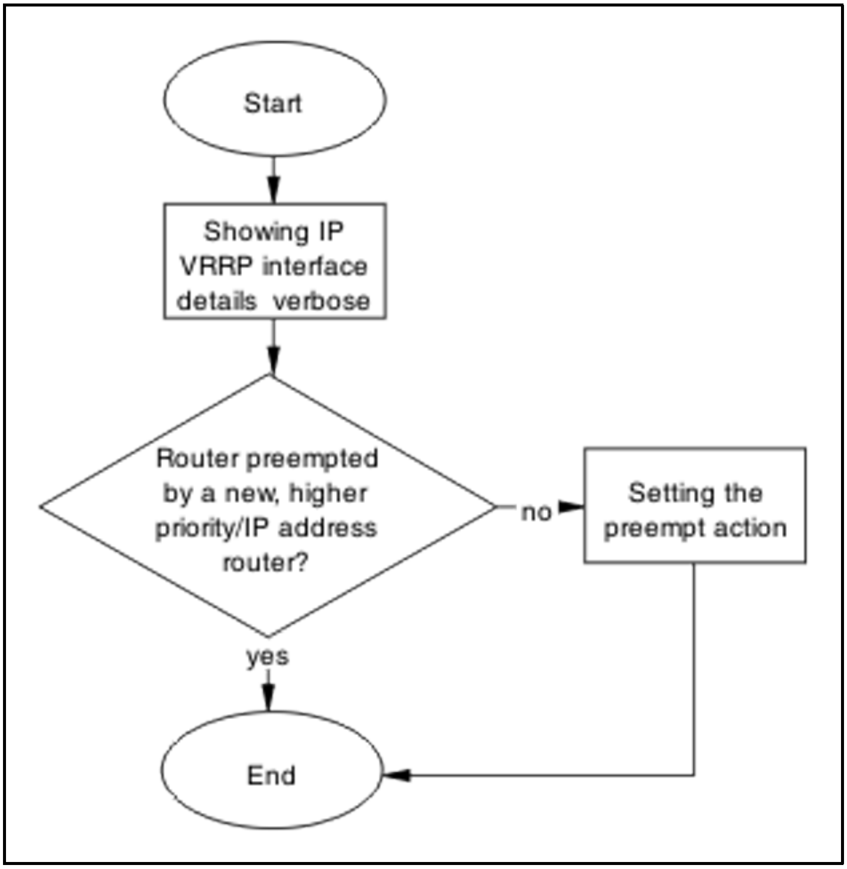
Configure preempt action

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.

Figure 113
Configure 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

Navigation

- "Showing IP VRRP interface verbose" (page 251)
- "Setting the preempt action" (page 252)

Showing IP VRRP interface verbose

Verify critical information for the VRRP interface.

Procedure Steps

Step	Action
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.

--End--

Setting the preempt action

Configure the preempt for manual operation.

Procedure Steps

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

--End--

Common Procedures

Prerequisites

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

It is possible to move from User EXEC 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 Exec Mode

User Exec mode is the default command mode for the CLI. The command prompt will look similar to: `5530-24TFD>`.

Procedure Steps

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

--End--

Privileged Exec Mode

Privileged Exec mode prompt will look similar to: `5530-24TFD#`.

Procedure Steps

Step	Action
1	To enter the this command mode from User EXEC mode, type the **`enable`** command.
2	To exit the CLI, type the exit or **`logout`** command.

--End--

Global Configuration Mode

Global configuration mode will look similar to: `5530-24TFD(config)#`.

Procedure Steps

Step	Action
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.

--End--

Interface Configuration Mode

Interface configuration mode prompt will look similar to: `5530-24TFD(config-if)#`.

Procedure Steps

Step	Action
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.

--End--

Ethernet Routing Switch 5500 Series

Troubleshooting

Printed in Canada
Release: 5.1
Publication: NN47200-700
Document status: Standard
Document revision: 01.01
Document release date: 1 April 2008

To provide feedback or to report a problem in this document, go to www.nortel.com/documentfeedback.

www.nortel.com

This document contains Nortel confidential and proprietary information. It is not to be copied, disclosed or distributed in any manner, in whole or in part, without Nortel's express written authorization. While the information in this document is believed to be accurate and reliable, except as otherwise expressly agreed to in writing NORTEL PROVIDES THIS DOCUMENT "AS IS" WITHOUT WARRANTY OR CONDITION OF ANY KIND, EITHER EXPRESS OR IMPLIED. The information and/or products described in this document are subject to change without notice.