# Troubleshooting
# Avaya Ethernet Routing Switch 5000 Series

6.3
NN47200-700, 03.01
August 2012

**Notice**

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

**Documentation disclaimer**

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

**Link disclaimer**

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

**Warranty**

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

**Licenses**

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

**Copyright**

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

**Third-party components**

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

**Trademarks**

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

Avaya is a registered trademark of Avaya Inc.

All other trademarks are the property of their respective owners.

**Downloading documents**

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

**Contact Avaya Support**

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

## Contents

# Chapter 1: New in this release

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

# Chapter 2: Introduction

This document :

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

This documents assumes that you:

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

**Troubleshooting Tools:**

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

Certain protocols and tools are tailored for troubleshooting specific Ethernet Routing Switch 5000 Series network topologies. Other tools are more general in their application and can be used to diagnose and monitor ingress and egress traffic.

# Chapter 3: Troubleshooting planning

This chapter provides information to help you

- minimize the need for troubleshooting
- plan effective troubleshooting

**Become familiar with the technical documentation suite:**

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

**Ensure correct system installation and maintenance:**

Make sure your system is properly installed and maintained so that it operates as expected.

**Gather and maintain resources for effective troubleshooting:**

Gather, and keep up to date, the resources you require if you have to troubleshoot.

For example:

- the site network map
- logical connections
- device configuration information

A site network map identifies where each device is, physically, in your site. The site network map 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 the 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. Keep records of your previous passwords because, if you must restore a device to a previous software version, you must use the password that was valid for that version.

Maintain a device inventory that lists all devices and relevant information for your network so you can easily determine 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 where you can always retrieve them..

To save valuable time during an incident, make sure that you store the details of all key contacts where you can always retrieve them. Key contacts information can include support contacts, support numbers, engineer details, and telephone and fax numbers.

**Understand normal network behavior:**

You can do the following to help you understand the normal network behavior, so your troubleshooting is effective and efficient.

- Monitor your network to obtain statistics and data that help you observe traffic flow patterns; for example, which devices are typically accessed or when peak usage times occur.
- Use a baseline analysis as an important indicator of overall network health. You can expedite network problem isolation when you compare a baseline view of network traffic with network traffic data captured during troubleshooting.

# Chapter 4: Troubleshooting tools

These are the available troubleshooting tools and their applications.

## Port Mirroring

ERS 5000 Series switches have a port mirroring feature that helps you to monitor and analyze network traffic. The port mirroring feature supports both ingress (incoming traffic) and egress (outgoing traffic) port mirroring. After port mirroring is enabled, the ingress or egress packets of the mirrored (source) port are forwarded normally and a copy of the packets is sent from the mirrored port to the mirroring (destination) port. Although you can configure ERS 5000 Series to monitor both ingress and egress traffic, some restrictions apply:

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

You can also monitor traffic for specified MAC addresses.

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

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

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

# Port Mirroring commands

Please refer to the *Avaya Ethernet Routing Switch 5000 Series Configuration — System Monitoring* (NN47200-505) for port mirroring command information.

You can use the port mirroring commands to assist in diagnostics and information gathering.

# Port Statistics

Use port statistics commands to display information about received and transmitted packets at the ports. The ingress and egress counts occur at the MAC layer. Count updates occur once every second.

# Route Tracing

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

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

# Stack Loopback Testing

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

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

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

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

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

# Time Domain Reflectometer

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

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

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

# System Logs

You can use the syslog messaging feature of the ERS 5500 Series products to manage event messages. The ERS 5500 Series syslog software communicates with a server software component named syslogd that resides on your management workstation.

The daemon syslogd is a software component that receives and locally logs, displays, prints, or forwards messages that originate from sources that are internal and external to the workstation. For example, syslogd software concurrently handles messages received from applications running on the workstation, as well as messages received from an ERS 5500 Series device running in a network accessible to the workstation.

# Auto Unit Replacement (AUR)

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

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

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

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

For further detail regarding port statistics and commands, refer to *Avaya Ethernet Routing Switch 5000 Series Getting Started* (NN47200-303).

# Avaya Knowledge and Solution Engine

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

# Chapter 5: General diagnostic tools

The Ethernet Routing Switch 5000 Series device has diagnostic features available with EDM, and ACLI.

You can use these diagnostic tools to help you troubleshoot operational and configuration issues.

You can configure and display files, view and monitor port statistics, trace a route, run loopback and ping tests, test the switch fabric, and view the address resolution table.

This document focuses on using ACLI to perform the majority of troubleshooting.

You can access ACLI through either a direct console connection to the switch or by using the Telnet or SSH protocols to connect to the switch remotely.

## ACLI command modes

This section helps you to understand ACLI command modes and how they differ.

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

- User Executive mode

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

- Global configuration mode:

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

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

- Interface configuration mode:

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

- Router configuration mode:

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

Each mode provides a specific set of commands.

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

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

# Chapter 6: Initial troubleshooting

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

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

## Gather information

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

- Default and current configuration of the switch. To do this, you can use the **show running-config** command.
- System status. output from the **show tech** command. It displays technical information about system status and information about the hardware, software, and switch operation. This command displays more information than the similar **show sys-info** command.
- Information about past events. To do this, review the log files.
- The software version that is running on the device. To do this, use the **show sys-info** or **show system verbose** commands to display the software version that is running on all cards.
- A **network topology diagram**: Get an accurate and detailed topology diagram of your network that shows the nodes and connections. Your planning and engineering function should have this diagram.
- **Recent changes**: Find out about recent changes or upgrades to your system, your network, or custom applications (for example, has configuration or code been changed?). Get the date and time of the changes, and the names of the persons who made them. Get a list of events that occurred prior to the trouble, such as an upgrade, a LAN change, increased traffic, or installation of new hardware.
- **Connectivity information**: After connectivity problems occur, get information about at least five working source and destination IP pairs and five IP pairs with connectivity issues. To do this, use these commands:

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

- Use the MIB web page. See *Avaya Ethernet Routing Switch 5000 Series System - Monitoring* (NN47200-505) for detailed information.
- Use the trap Web page. See *Avaya Ethernet Routing Switch 5000 Series System - Monitoring* (NN47200-505) for detailed information.

# Chapter 7: Emergency recovery trees

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

## Emergency recovery trees

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

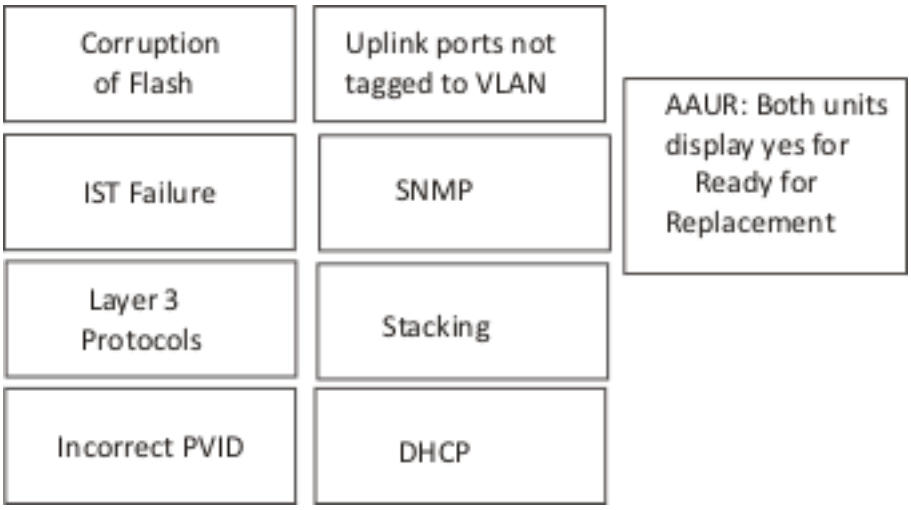



**Figure 1: Emergency recovery trees**

## 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

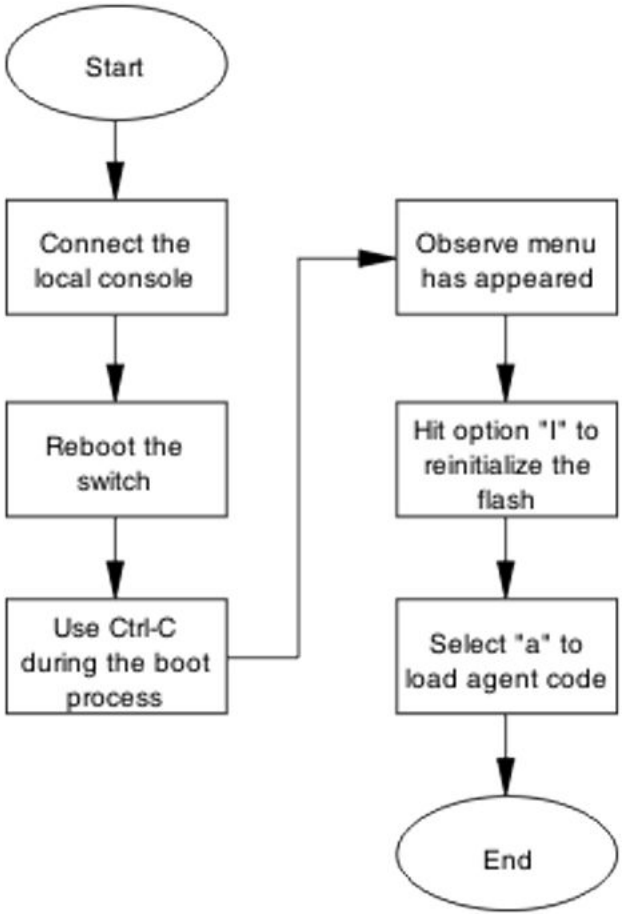



**Figure 2: Corruption of flash**

# IST failure

When two ERS 5500 Series switches run IST between them, if that IST link goes down they will experience a total loss of communication. Because all critical network traffic runs on the IST link, if an IST failure occurs then network protocols, for example RIP,VRRP,OSPF,VLACP, start flapping. This protocol flapping causes a network outage.

## IST failure recovery tree

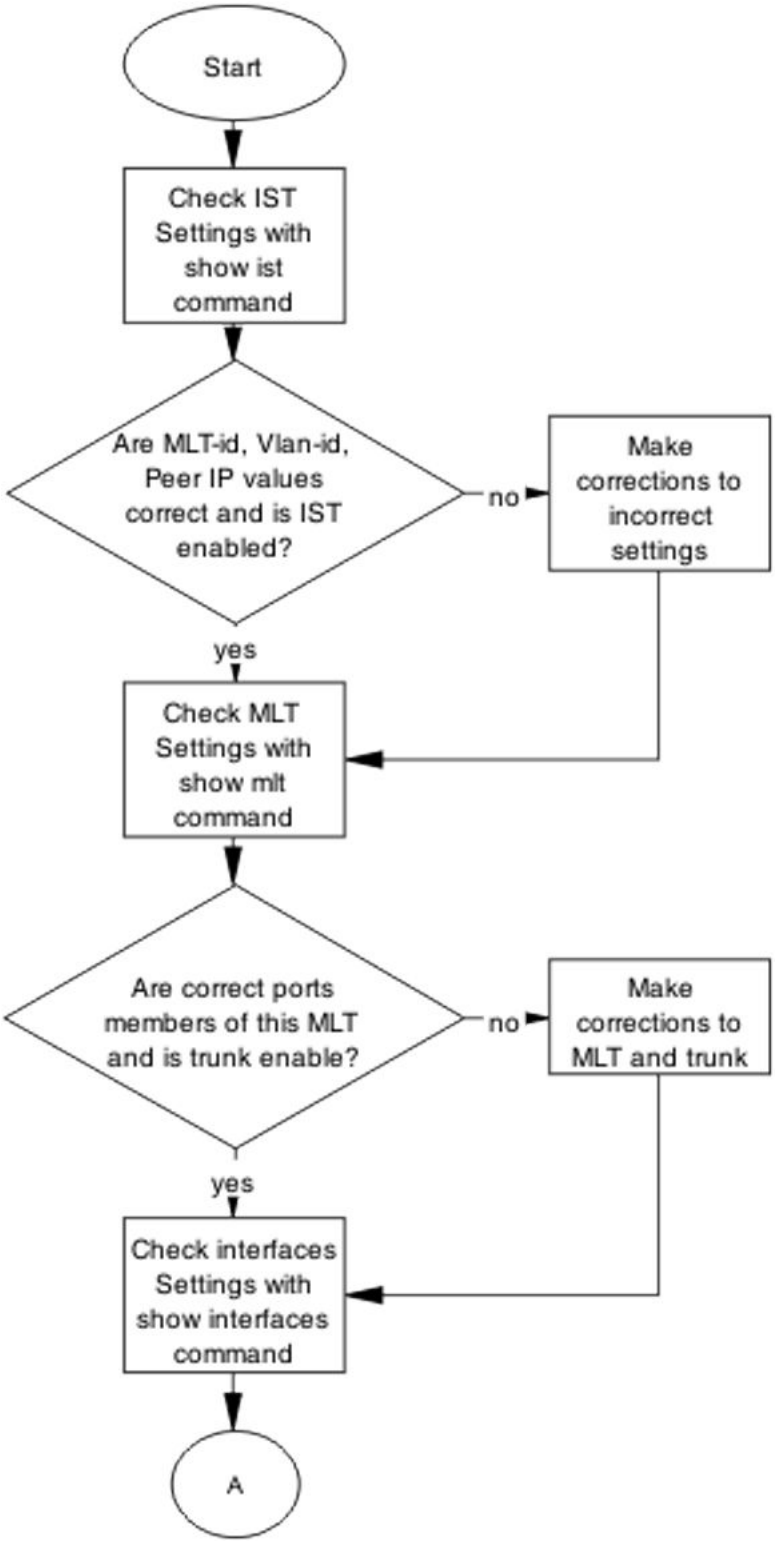



**Figure 3: IST failure part 1**

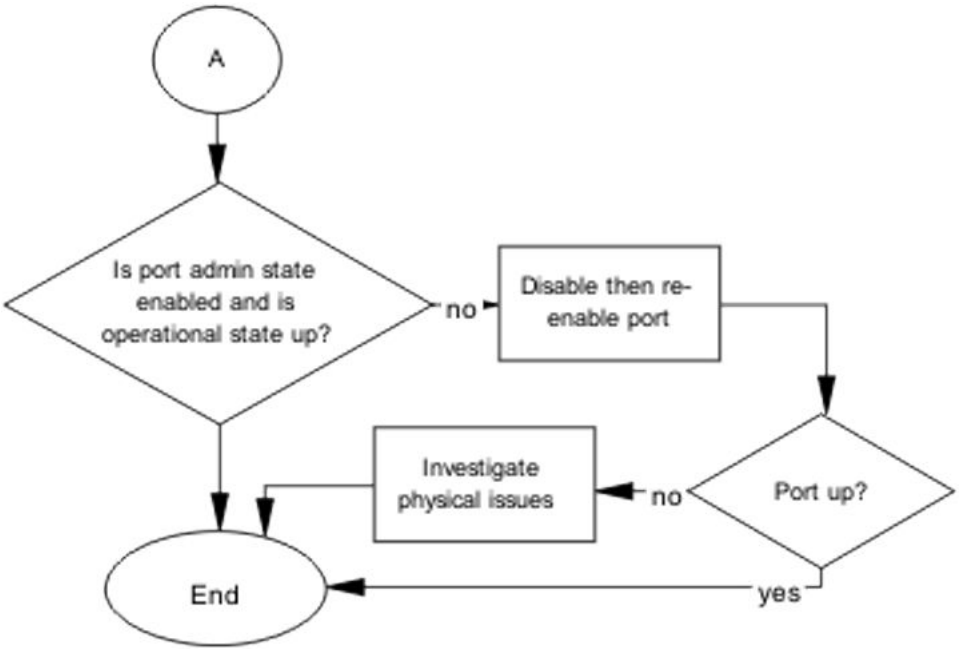



**Figure 4: IST failure part 2**

# Layer 3 protocols

To configure licensed Layer-3 protocols like OSPF, VRRP and IST/SMLT on ERS 5000 series devices, you must load a license file on the switch.

## Layer 3 protocols recovery tree

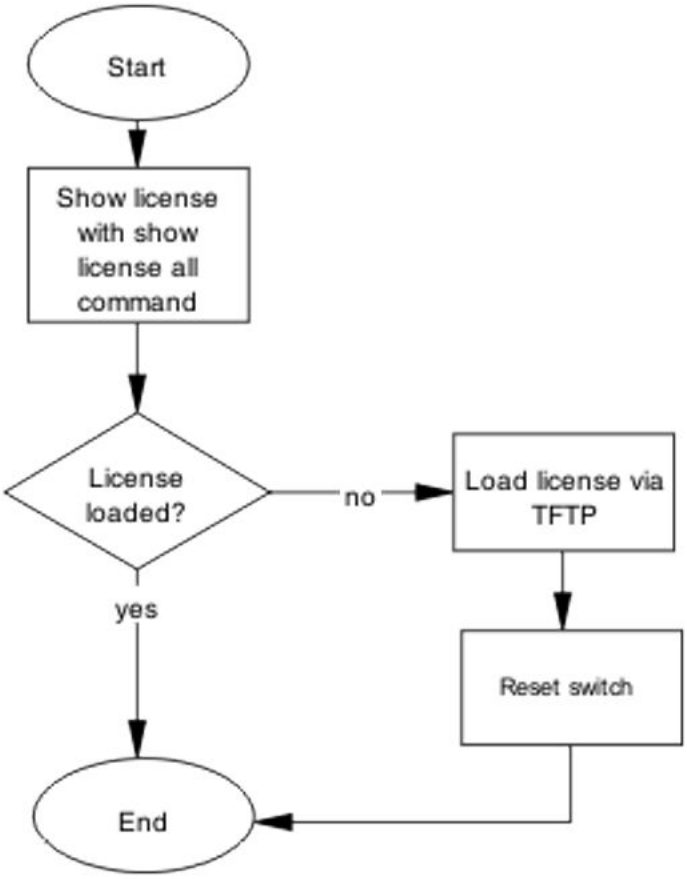



**Figure 5: Layer 3 protocols**

# Incorrect PVID

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

## Incorrect PVID recovery tree

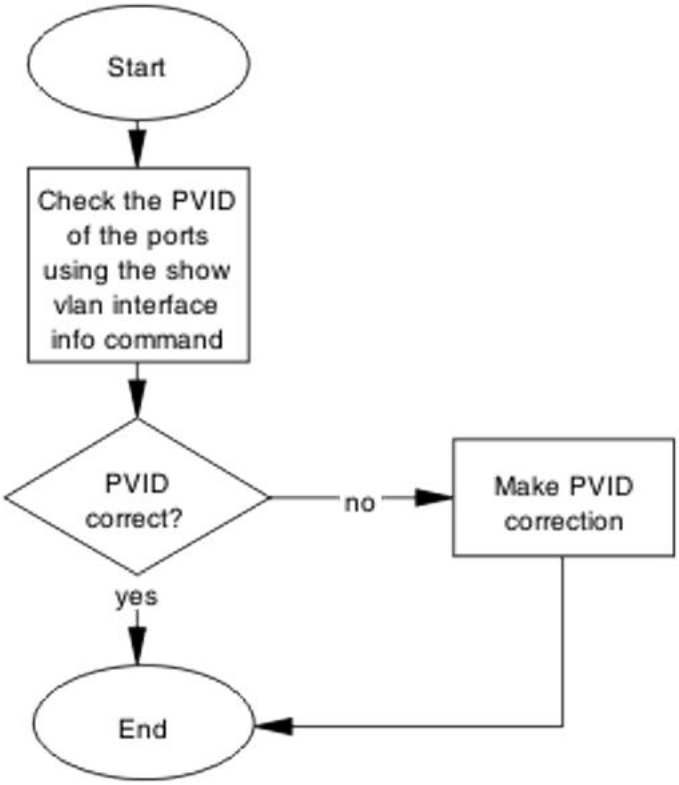



**Figure 6: Incorrect PVID**

# VLAN not tagged to uplink ports

After you connect an ERS 5500 Series switch to an ERS 8600 Series switch, if devices in a VLAN on the ERS 8600 Series switch cannot communicate with devices in the same VLAN on the ERS 5500 Series switch , then the uplink ports are not tagged to the VLAN on the ERS 5500 Series switch.

# VLAN not tagged to uplink ports recovery tree

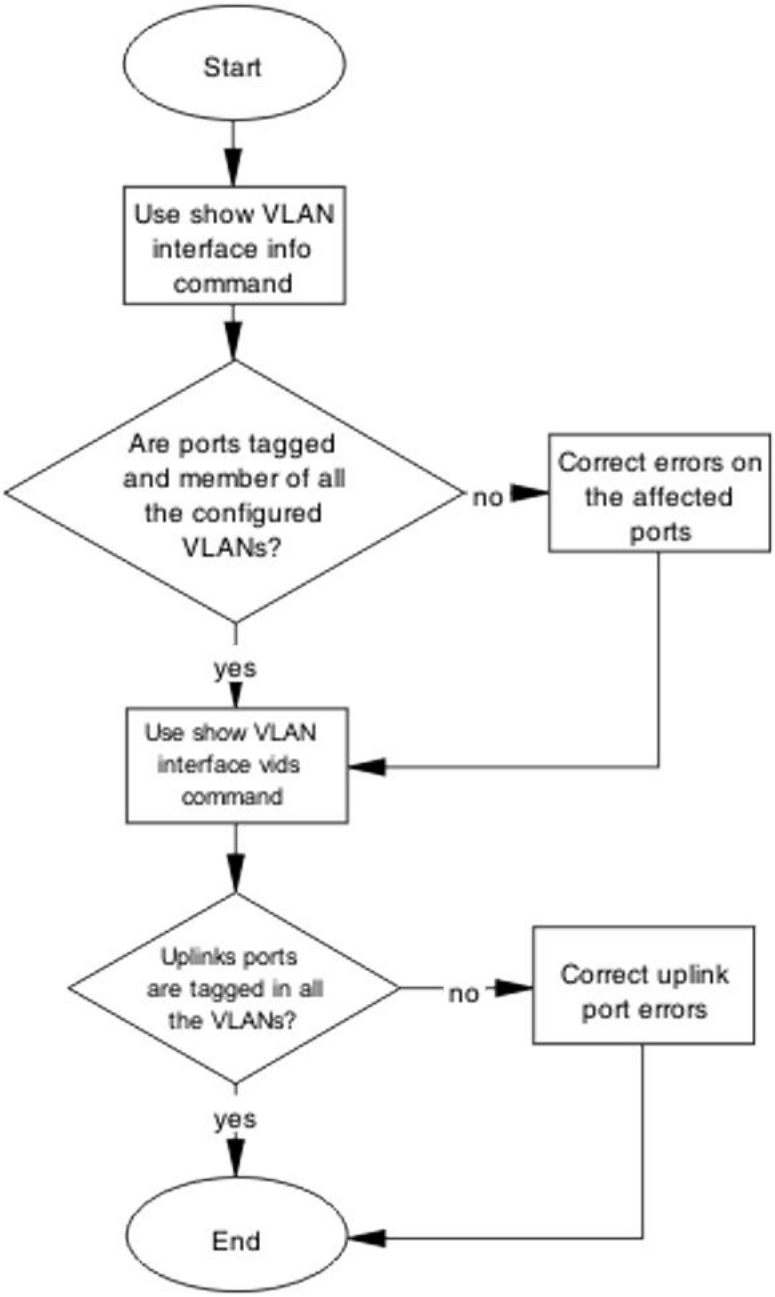



**Figure 7: VLAN not tagged to uplink ports**

# SNMP

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

## SNMP recovery tree

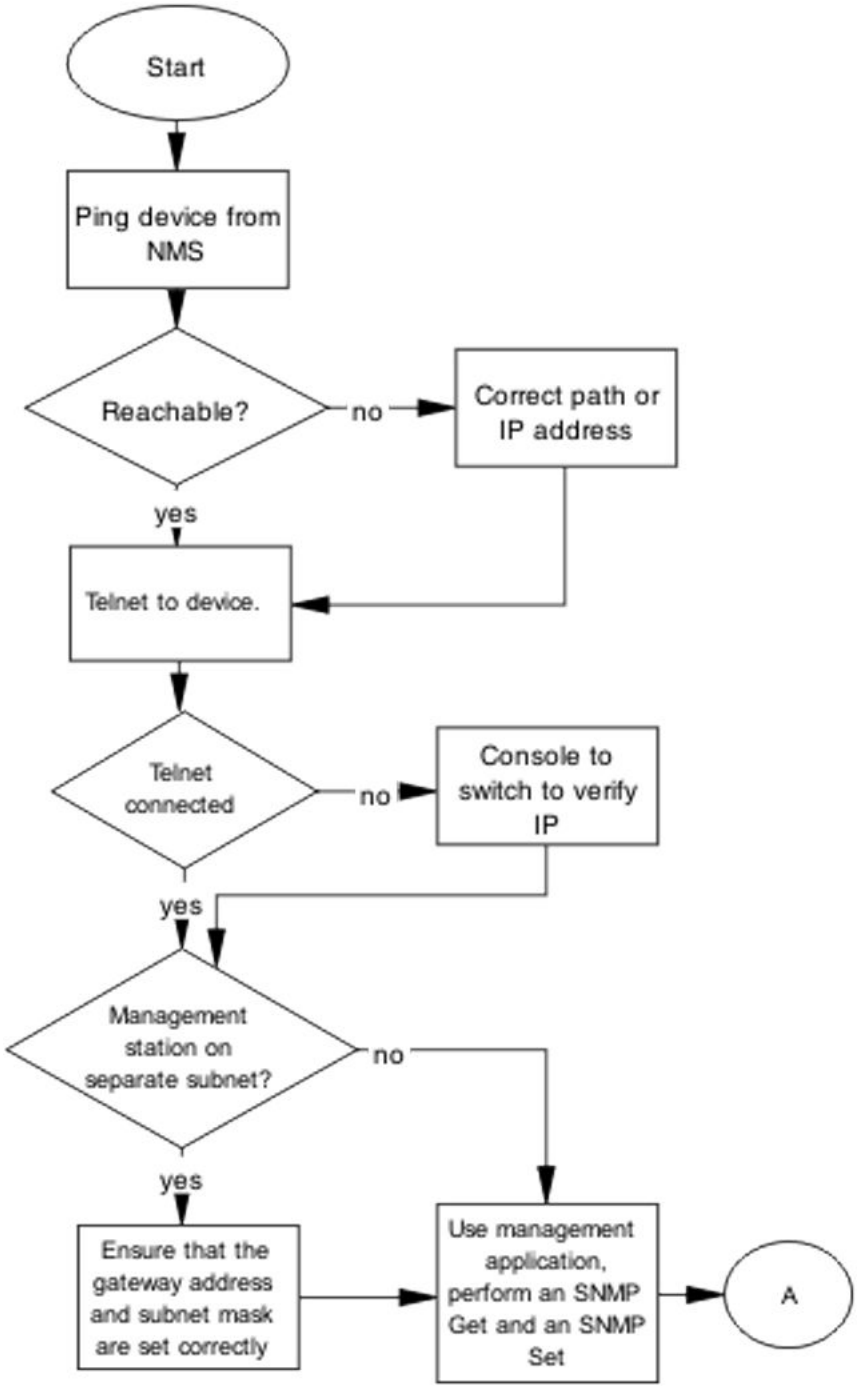



**Figure 8: SNMP part 1**

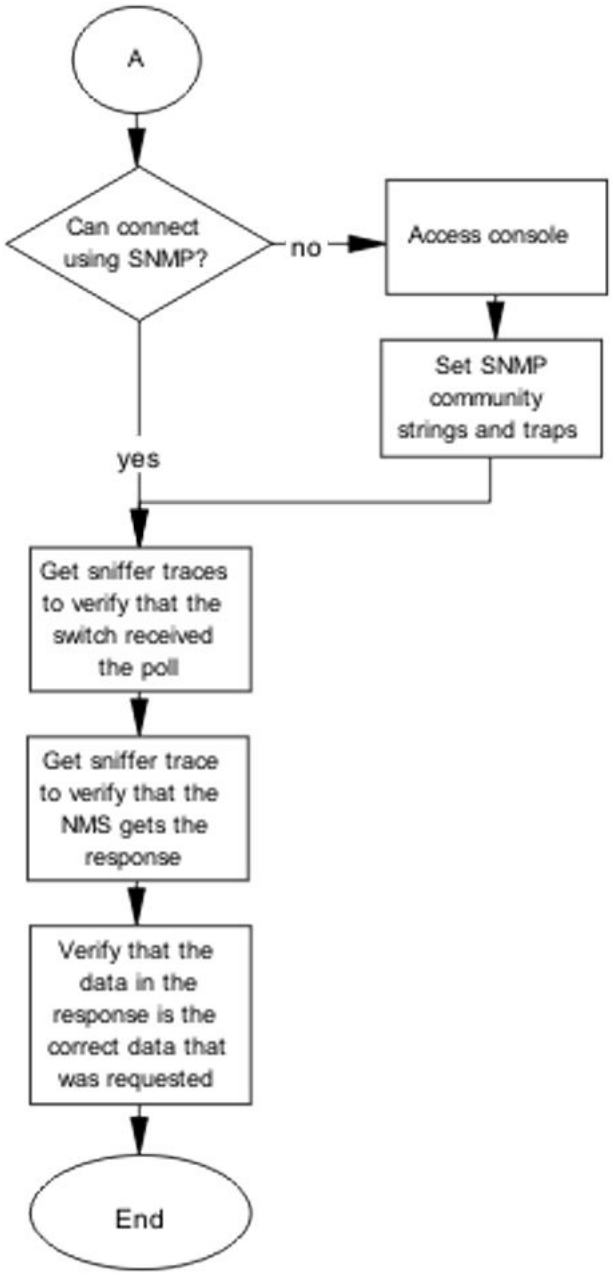



**Figure 9: SNMP part 2**

# Stack

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

## Stack recovery tree

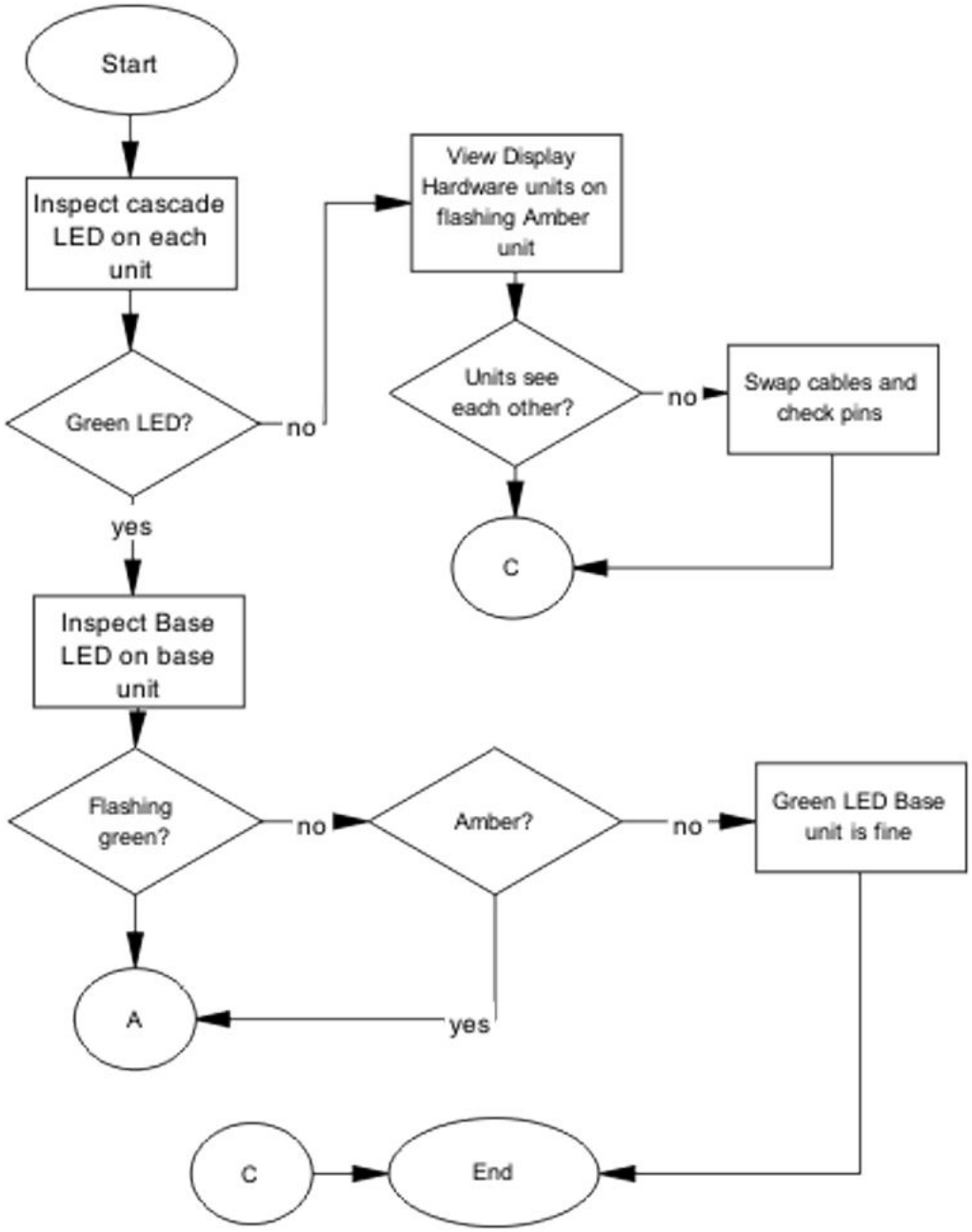



**Figure 10: Stack part 1**

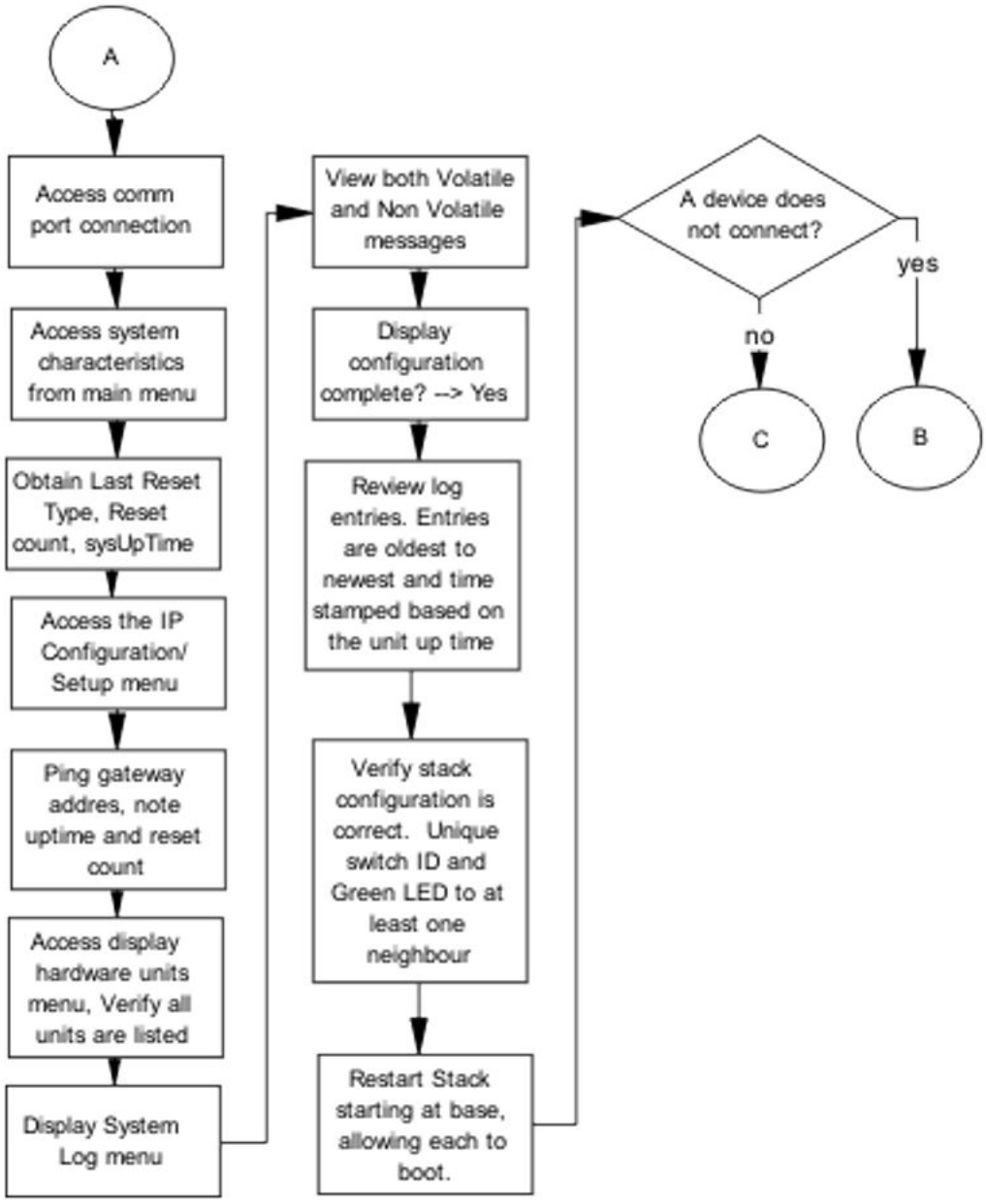



**Figure 11: Stack part 2**

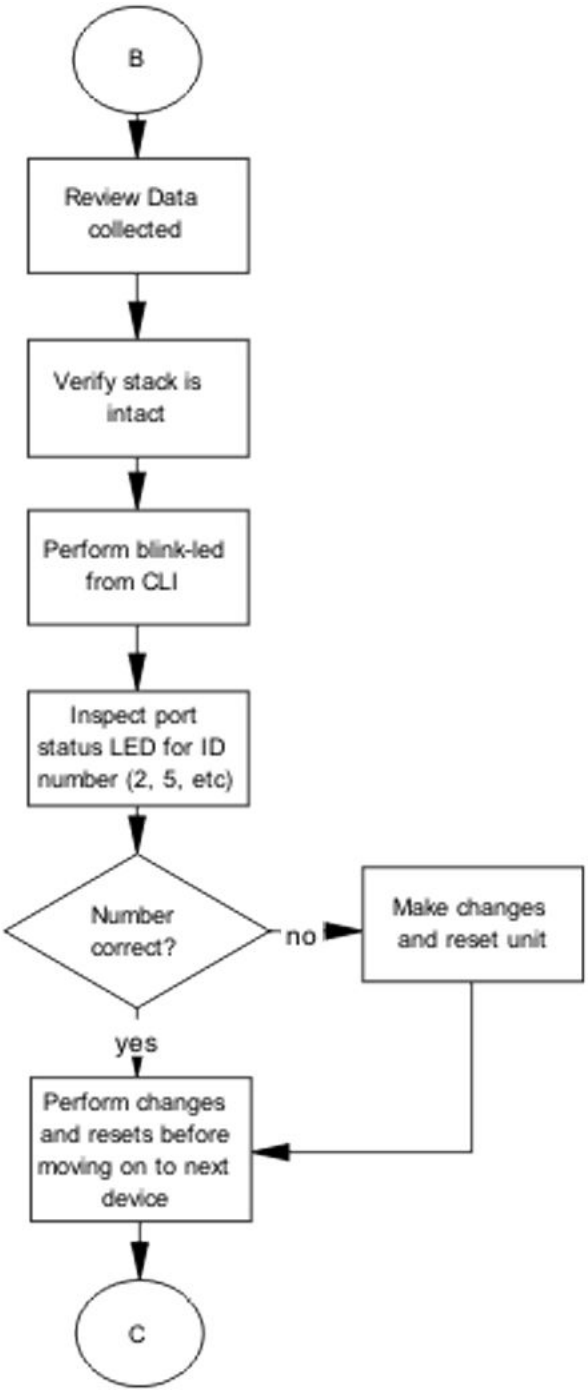



**Figure 12: Stack part 3**

# Dynamic Host Configuration Protocol (DHCP)

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

## DHCP recovery tree

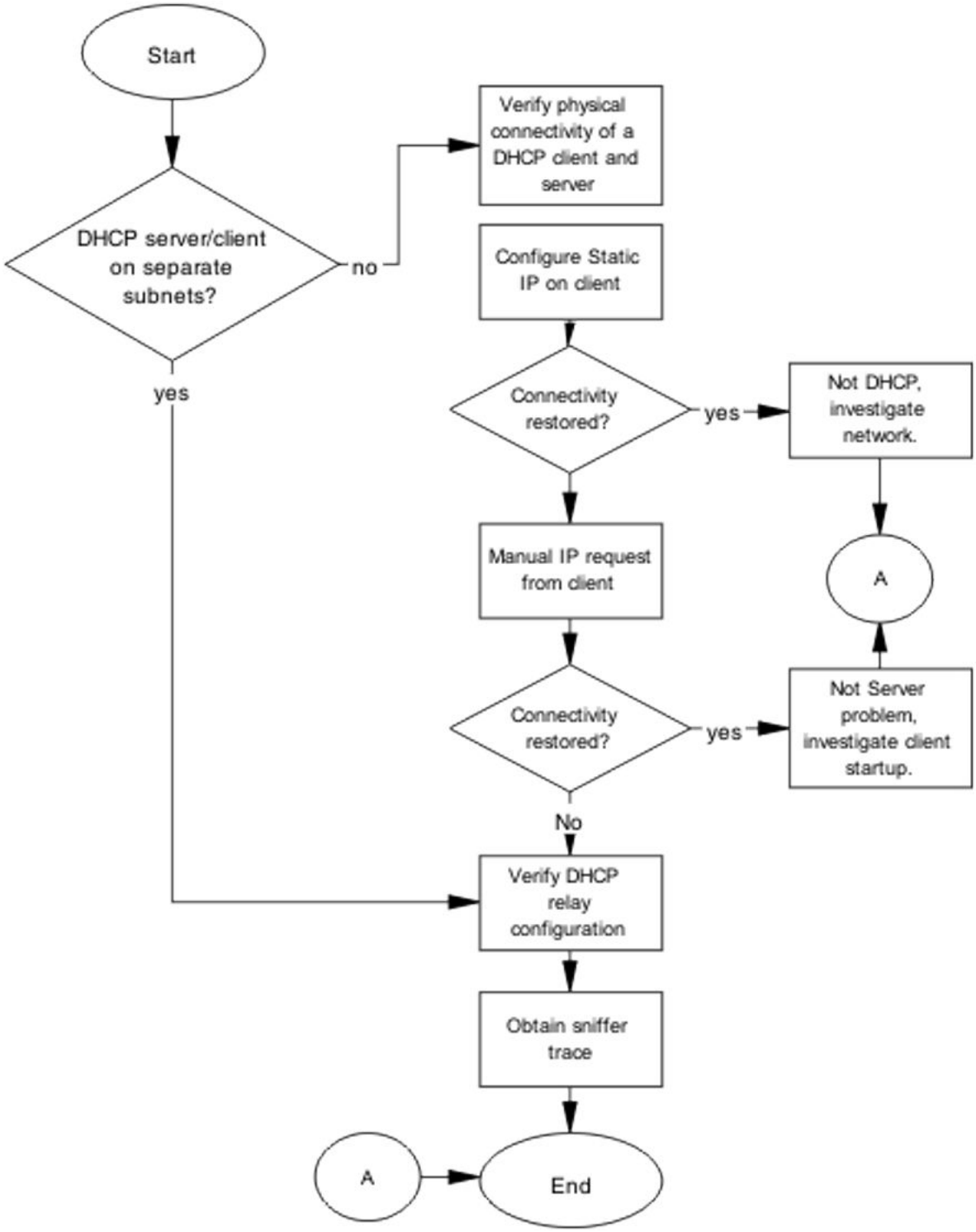



**Figure 13: DHCP**

# AAUR: Both units display yes for Ready for Replacement

In a stack of two units, when you enter the **show stack auto-unit-replacement** command and both units display as Ready for Replacement, only the non–base unit should be ready for replacement.

The following figure shows the recovery tree to correct the issue.

# Both units display yes for Ready for Replacement recovery tree

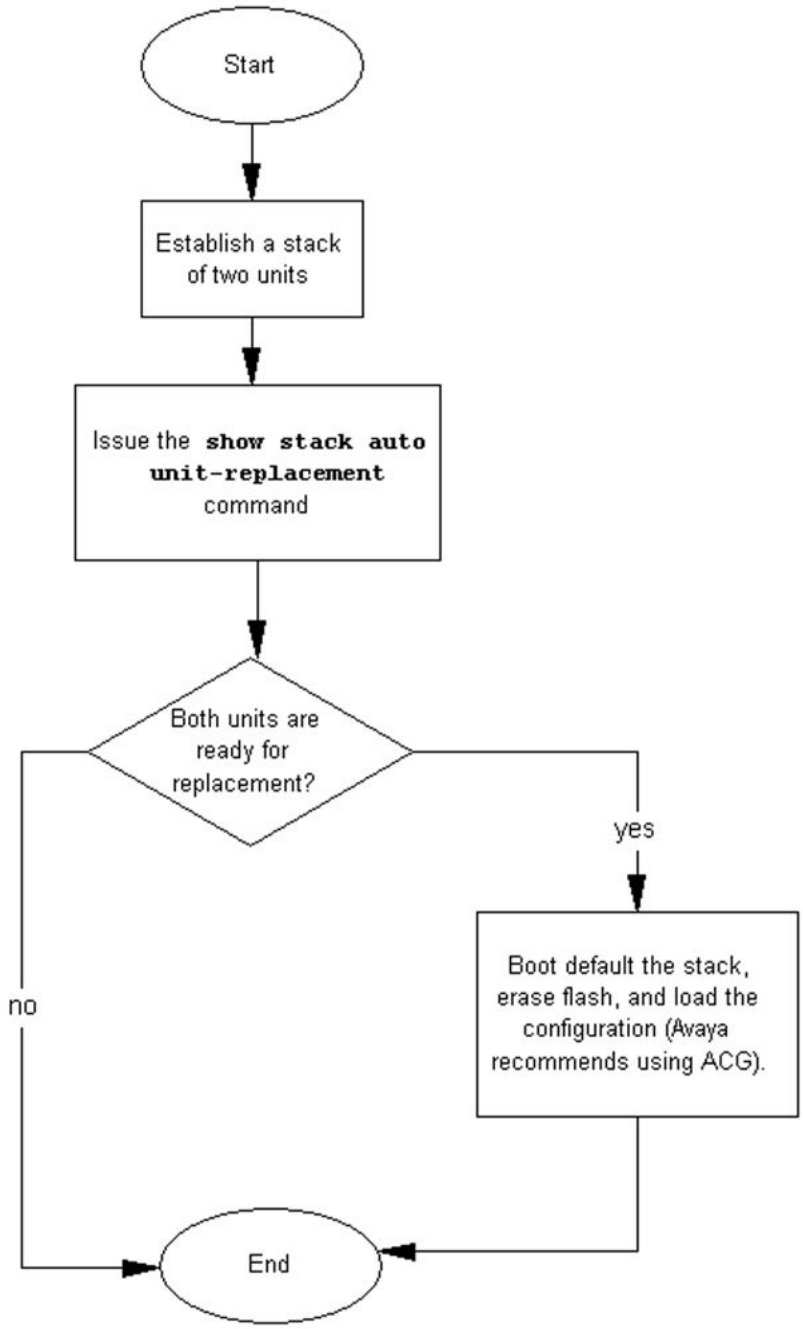



**Figure 14: Both units display yes for Ready for Replacement**

# Chapter 8: Troubleshooting hardware

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

## Work flow: Troubleshooting hardware

The following work flow can help you to determine solutions for some common hardware problems.

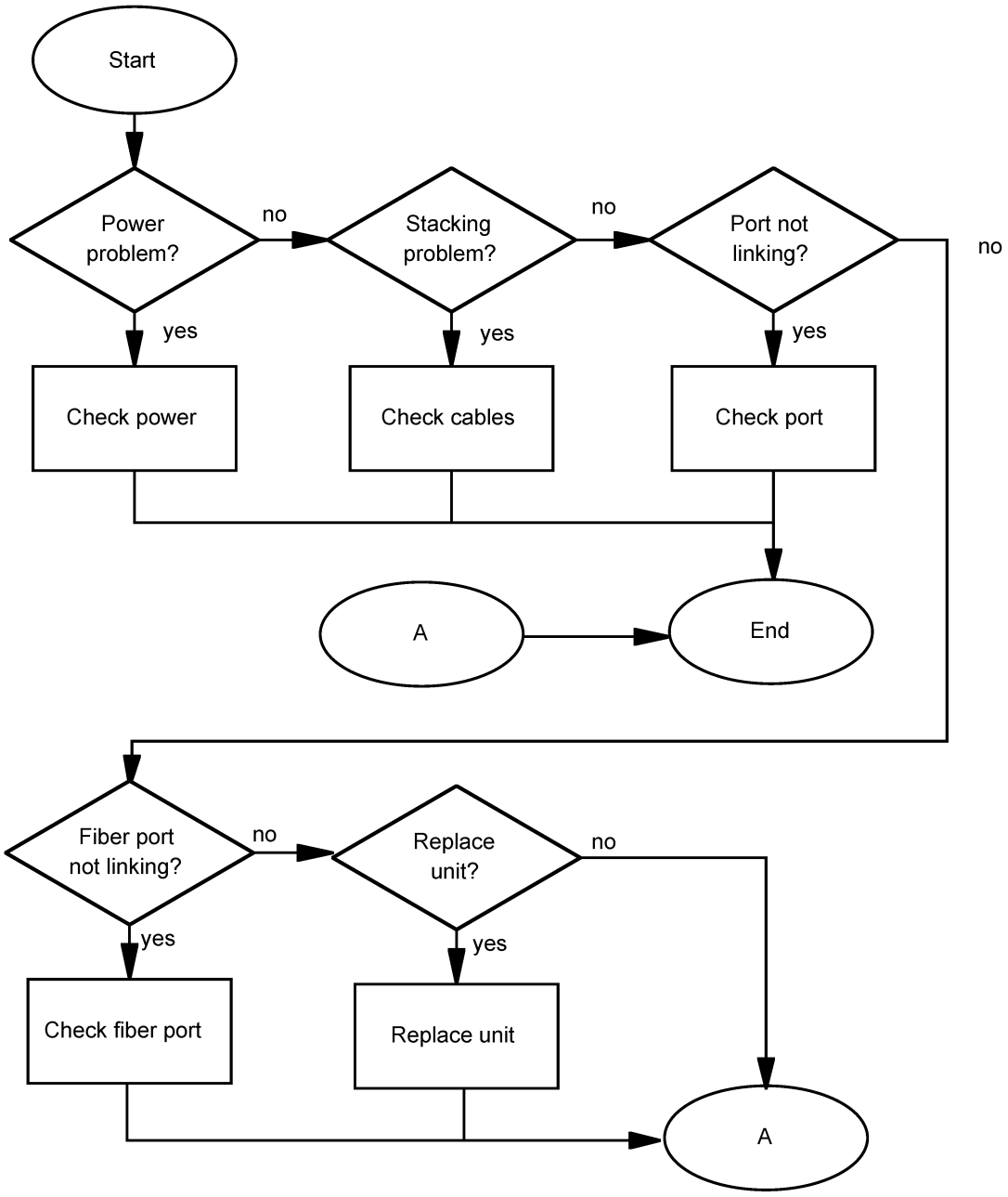



**Figure 15: Troubleshooting hardware**

# Check power

Confirm power is being delivered to the device.

# Task flow: Check power

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

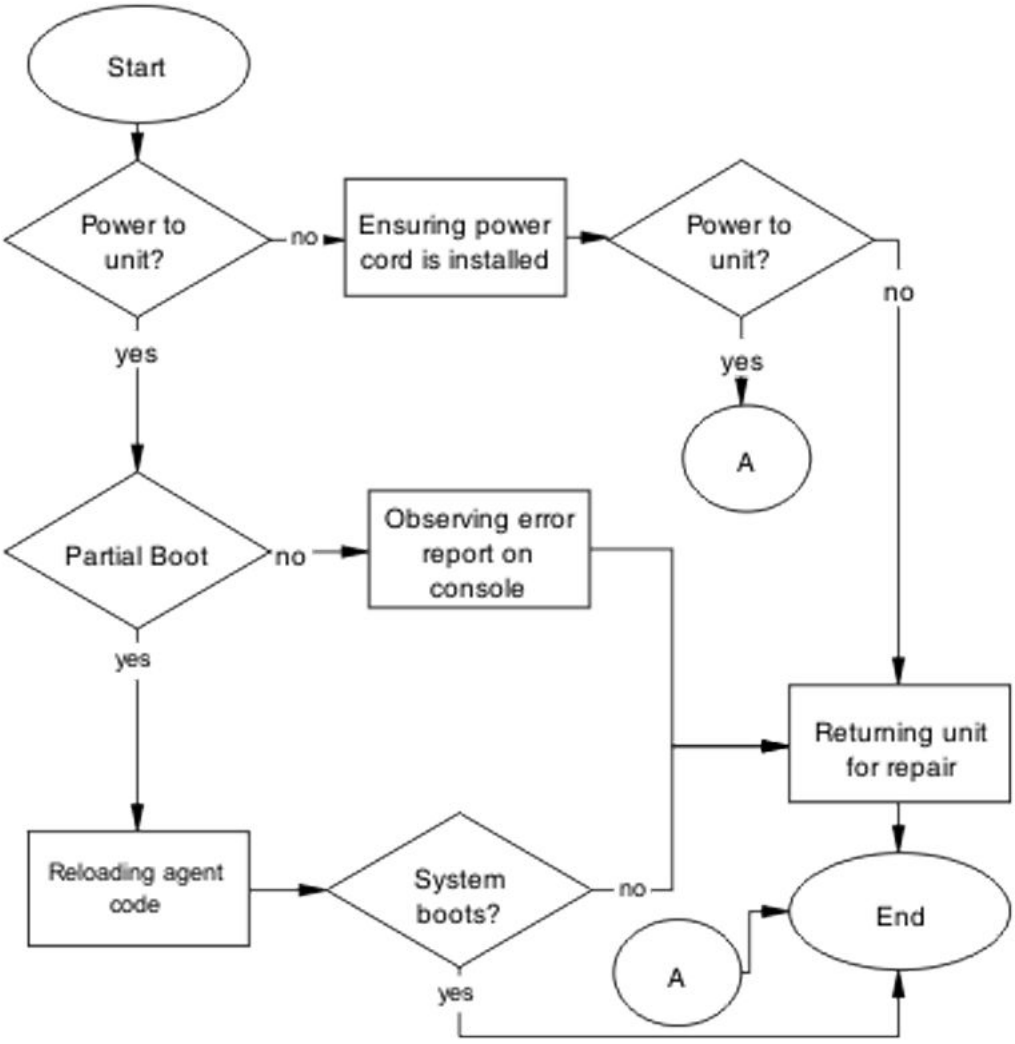



**Figure 16: Check power**

# Ensuring power cord is installed

## About this task

Confirm the power cord is properly installed for the device.

Refer to *Avaya Ethernet Routing Switch 5000 Series - Installation* (NN47200-300) for details regarding proper cord installation.

# Observing error report on console

### About this task

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

### Procedure

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

# Reloading agent code

### About this task

Reload the agent code on the ERS 5000 series device to eliminate corrupted or damaged code that causes a partial boot of the device.

**⚠ Caution:**

Ensure you adequately backup the switch configuration prior to reloading software.

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

### Procedure

1. Use the **`show sys-info command`** to view the software version.
2. Refer to the *Avaya Ethernet Routing Switch 5000 Series Getting Started* (NN47200-303) for software installation.

# Returning unit for repair

### About this task

Return unit to Avaya for repair

Contact Avaya for return instructions and RMA information.

# Check cables

Confirm the stacking cables are correctly connected.

## Task flow: Check cables

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

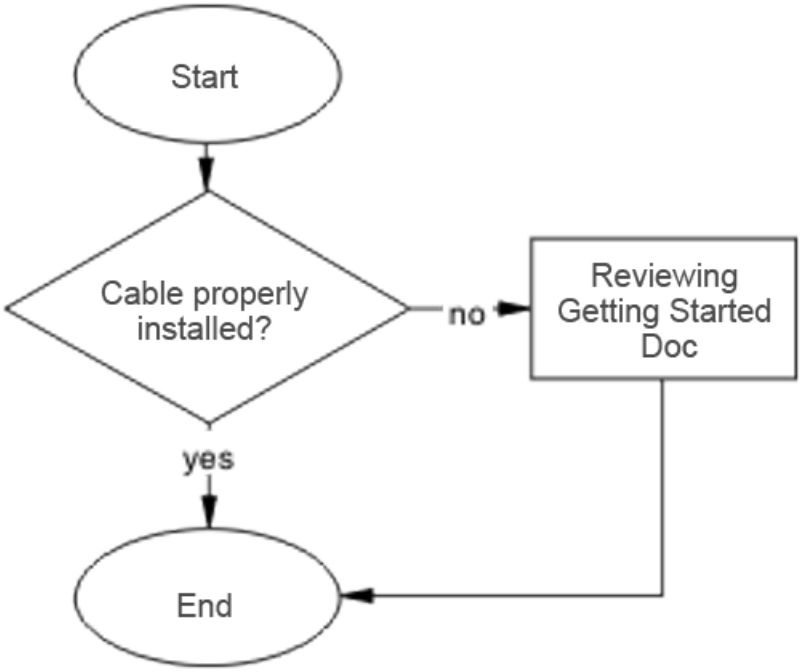



**Figure 17: Check cables**

## Reviewing the Getting Started document

### About this task

Review the Getting Started document to reapply the stacking cabling as required.

See the stacking procedures in *Avaya Ethernet Routing Switch 5000 Series Getting Started* (NN47200-303).

# Check fiber port

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

# Check port

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

## Task flow: Check port

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

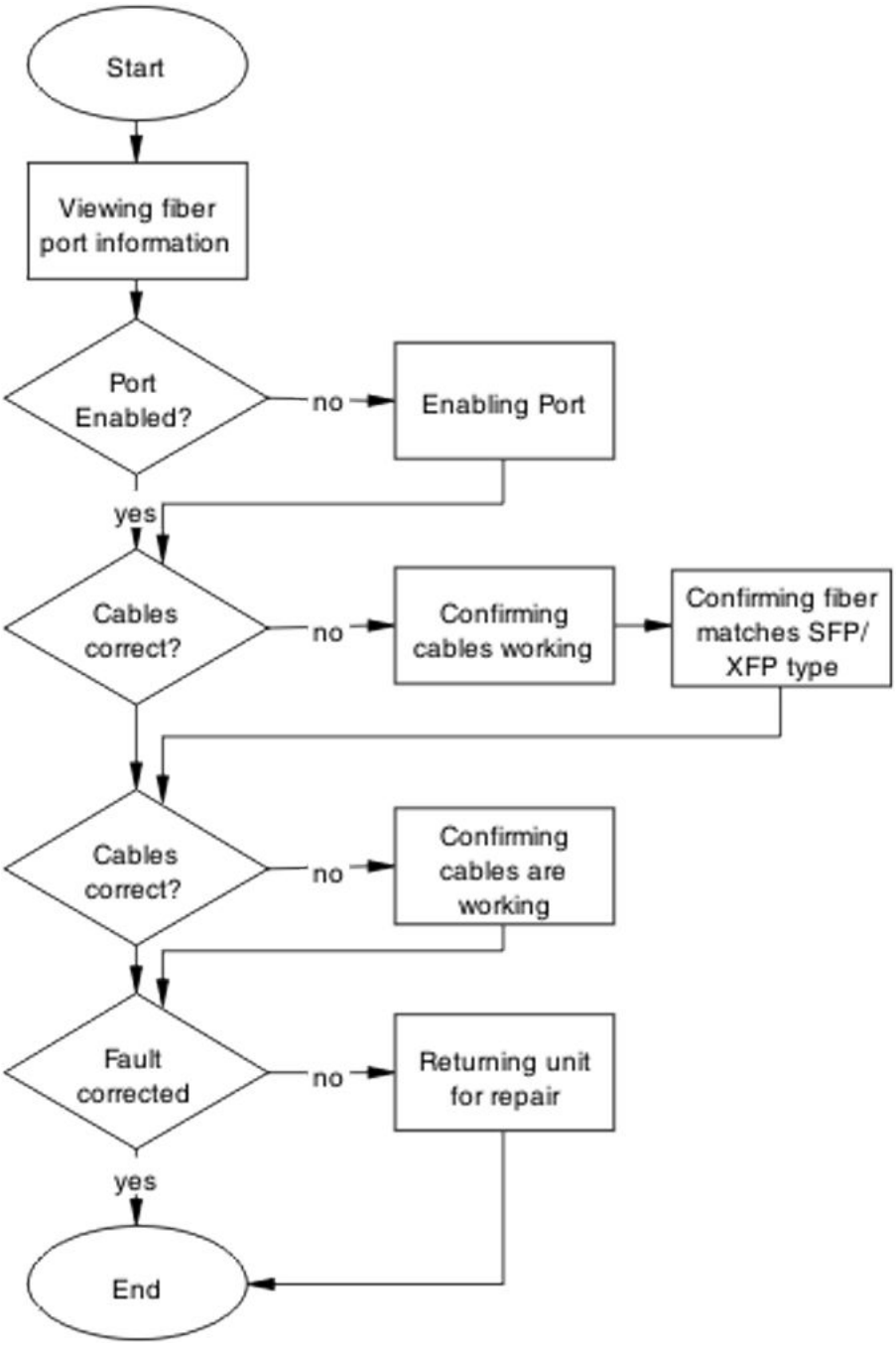



**Figure 18: Check port**

## Viewing port information

### About this task

Review the port information to ensure it is enabled.

### Procedure

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

## Enabling the port

### About this task

Enable the port.

### Procedure

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

## Confirming that the cables are working

### About this task

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

### Procedure

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

# Task flow: Check fiber port

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

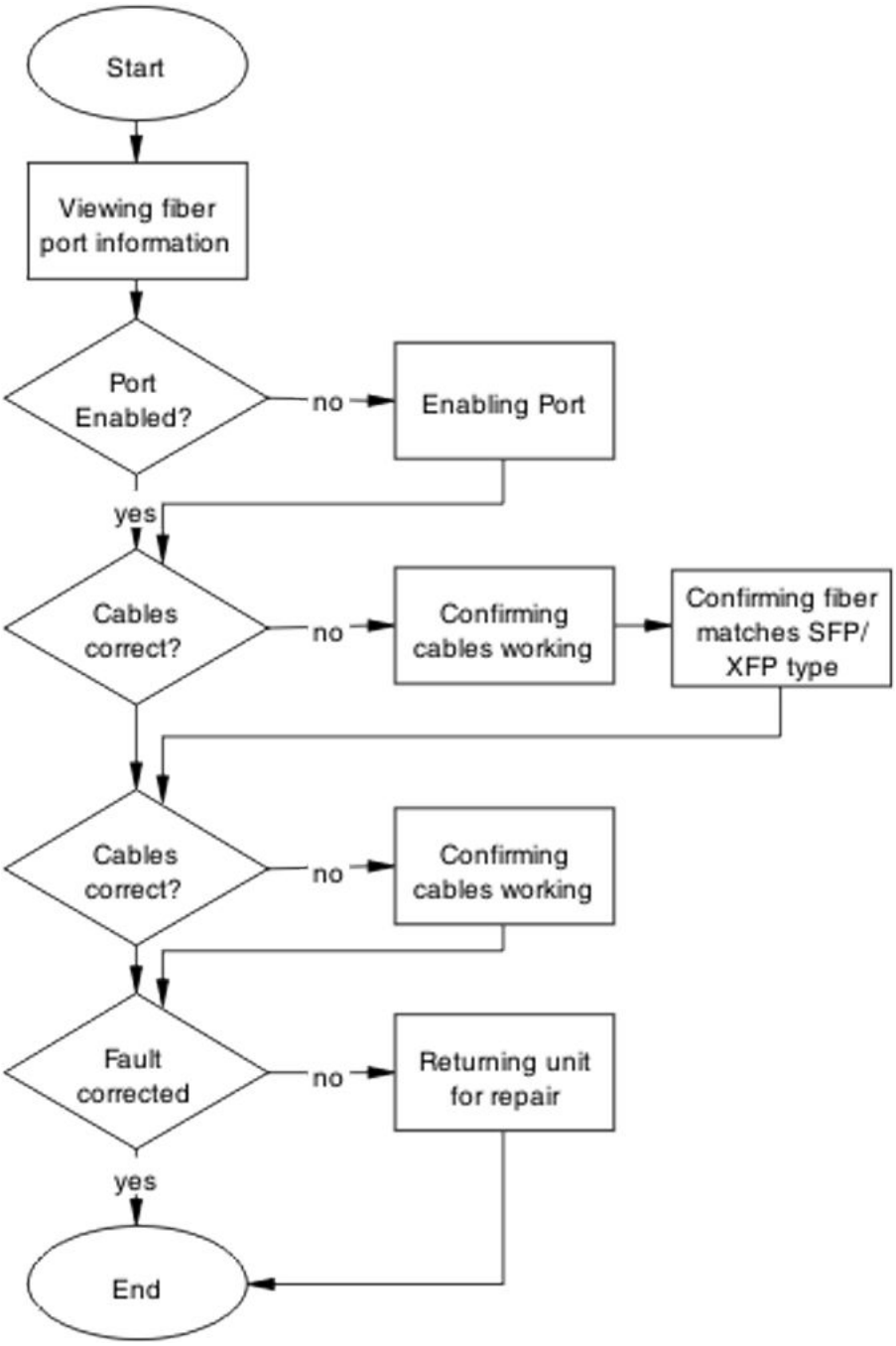



**Figure 19: Check fiber port**

## Viewing fiber port information

### About this task

Review the port information to ensure it is enabled.

### Procedure

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

## Enabling the port

### About this task

Ensure that the port on the ERS 5500 Series switch is enabled.

### Procedure

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

## Confirming that the cables are working on the port

### About this task

Confirm that the cables are working on the port.

### Procedure

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

## Confirming that the fiber matches the SFP/XFP type

### About this task

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

### Procedure

1. Inspect the fiber cables to ensure they are the correct type.
2. Review *Avaya Ethernet Routing Switch 5000 Series Installation — SFP* (NN47200-302) for details or RN's for list of approved SFP/XFP

3. Note the port status.

# Check fiber port

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

## Task flow: Check fiber port

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

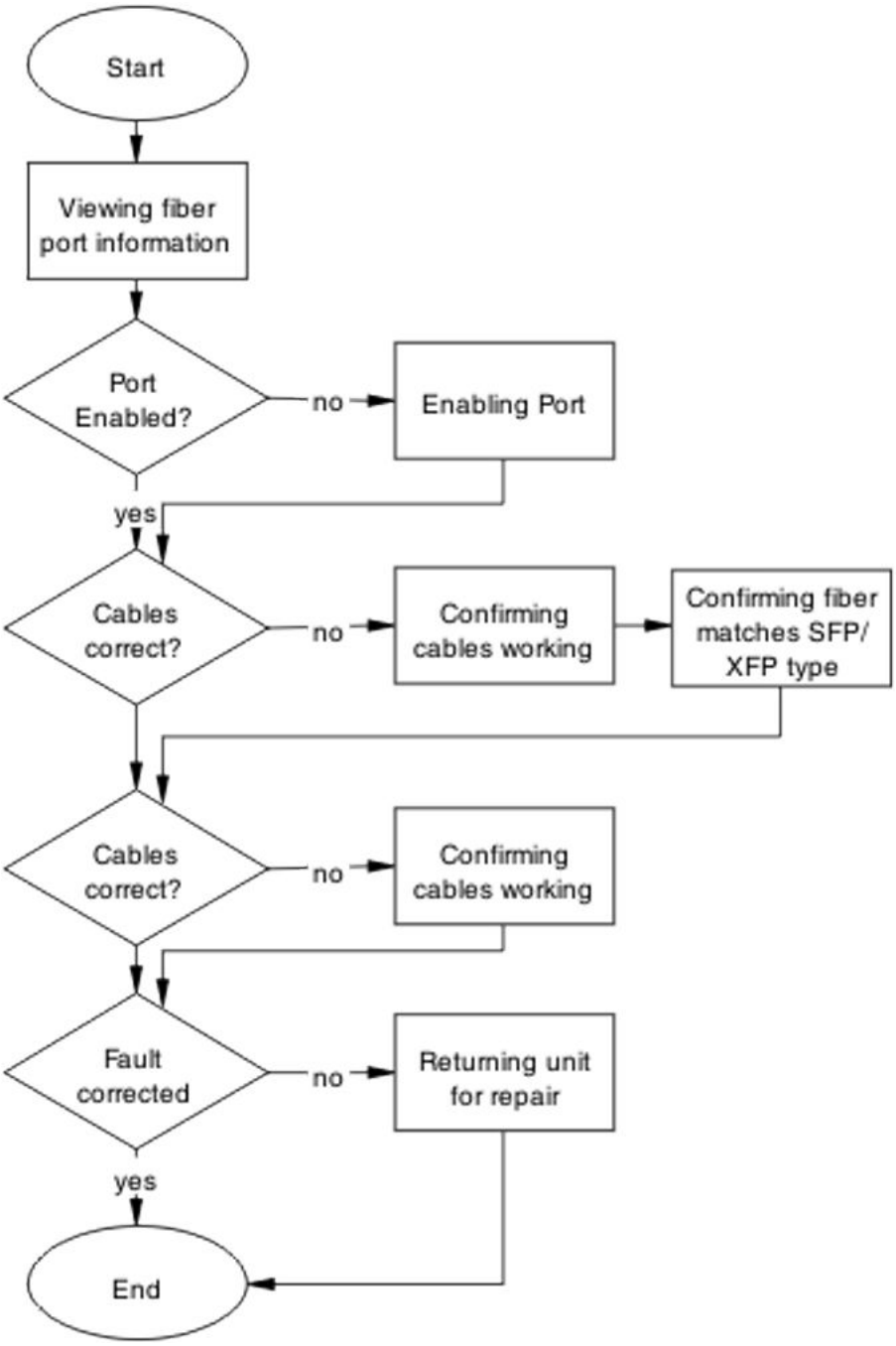



**Figure 20: Check fiber port**

# Viewing fiber port information

## About this task

Review the port information to ensure it is enabled.

### Procedure

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

## Enabling the port

### About this task

Ensure that the port on the ERS 5500 Series switch is enabled.

### Procedure

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

## Confirming that the cables are working on the port

### About this task

Confirm that the cables are working on the port.

### Procedure

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

## Confirming that the fiber matches the SFP/XFP type

### About this task

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

### Procedure

1. Inspect the fiber cables to ensure they are the correct type.

2. Review *Avaya Ethernet Routing Switch 5000 Series Installation — SFP* (NN47200-302) for details or RN's for list of approved SFP/XFP
3. Note the port status.

## Returning unit for repair

### About this task

Return unit to Avaya for repair

Contact Avaya for return instructions and RMA information.

# Replace unit

Remove defective unit and insert the replacement.

Prerequisites

**⚠ Caution:**

Due to physical handling of the device and your physical proximity to electrical equipment, review and adhere to all safety instructions and literature included with device and in *Avaya Ethernet Routing Switch 5000 Series Installation* (NN47200-300)

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

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

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

## Task flow: Replace unit

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

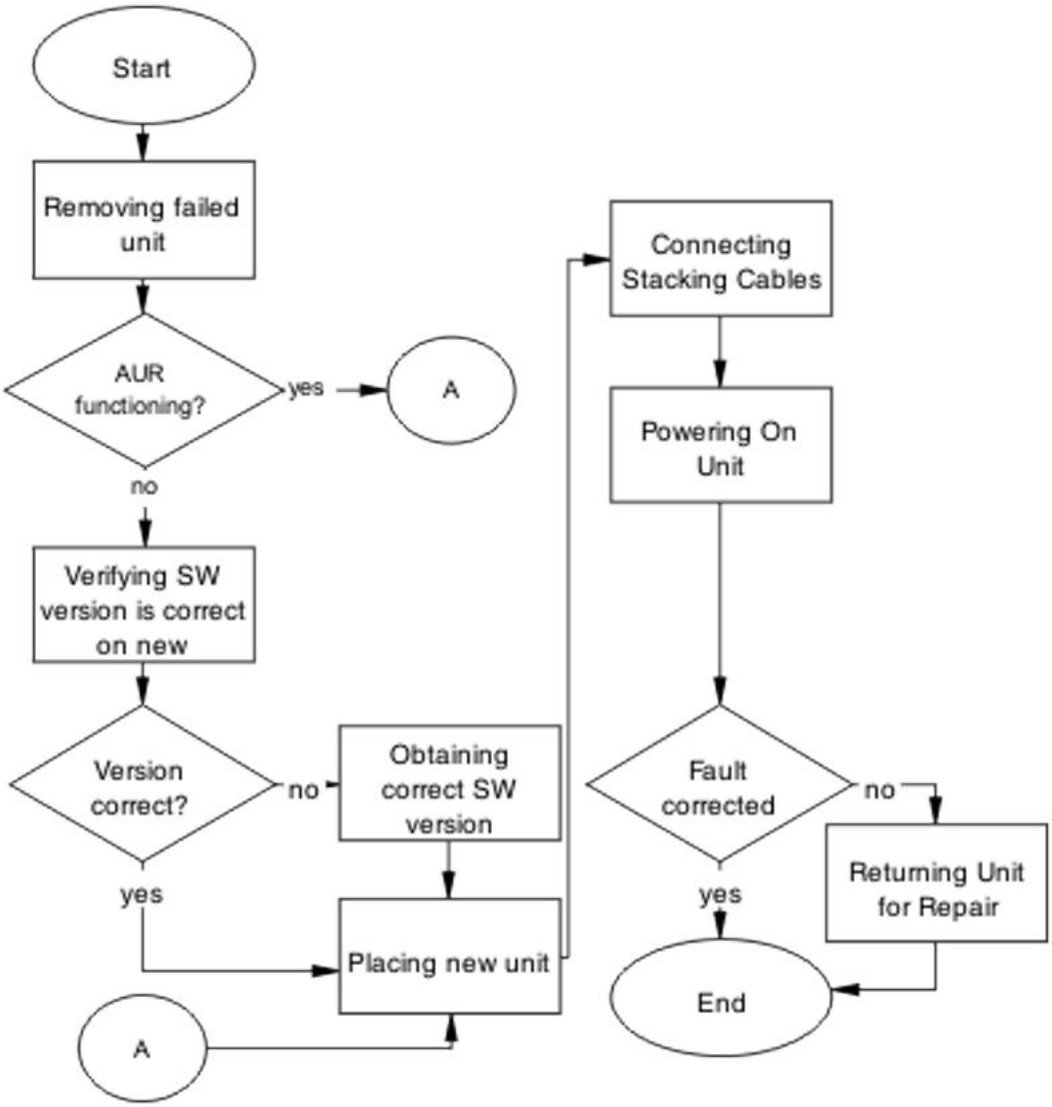



**Figure 21: Replace unit**

# Removing failed unit

## About this task

Remove the failed unit from the stack.

## Procedure

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

# Verifying software version is correct on new device

### About this task

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

### Procedure

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

# Obtaining correct software version

### About this task

Obtain and install correct software version

**⚠ Caution:**

Ensure you backup the switch configuration prior to reloading software.

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

### Procedure

Refer to the *Avaya Ethernet Routing Switch 5000 Series Getting Started* (NN47200-303) for software installation.

# Placing new unit

### About this task

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

Place the device in the stack in accordance with procedures outlined in *Avaya Ethernet Routing Switch 5000 Series Installation* (NN47200-300).

## Connecting stacking cables

### About this task

Reconnect the stacking cables to correctly stack the device.

### Procedure

1. Review the stacking section in *Avaya Ethernet Routing Switch 5000 Series Getting Started* (NN47200-303) for cabling details.
2. Connect the cables in accordance with physical stack requirements.

## Powering on unit

### About this task

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

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

### Procedure

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

# Returning unit for repair

### About this task

Return unit to Avaya for repair

Contact Avaya for return instructions and RMA information.

# Chapter 9: Troubleshooting authentication

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

## Work flow: Troubleshooting authentication

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

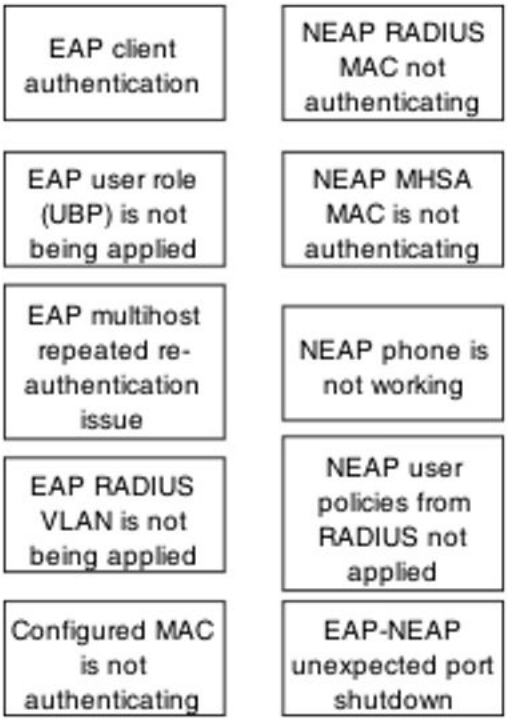



**Figure 22: Troubleshooting authentication**

## 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.

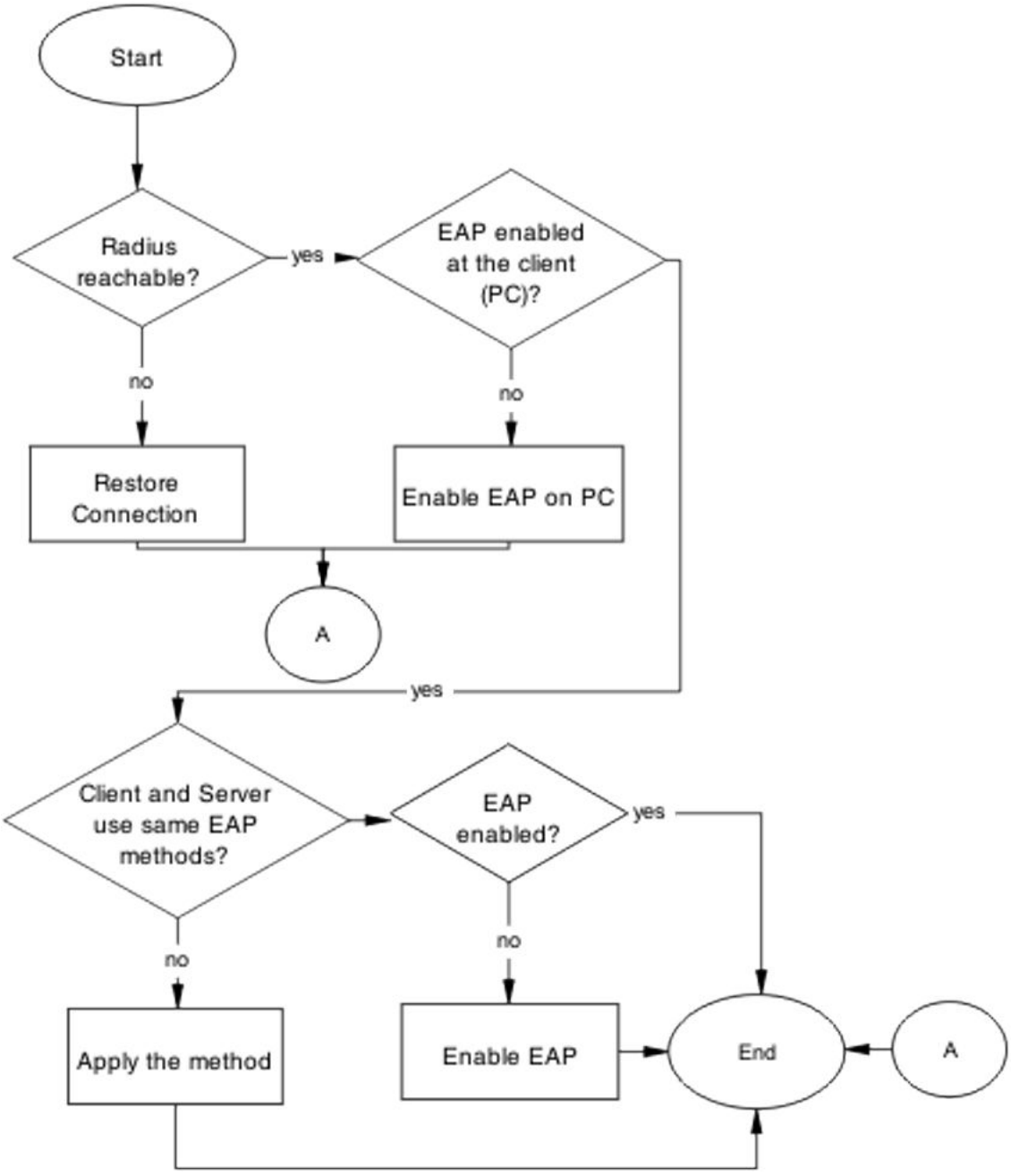



**Figure 23: EAP client is not authenticating**

# Restore RADIUS connection

Ensure that the RADIUS server has connectivity to the device

## Task flow: Restore RADIUS connection

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

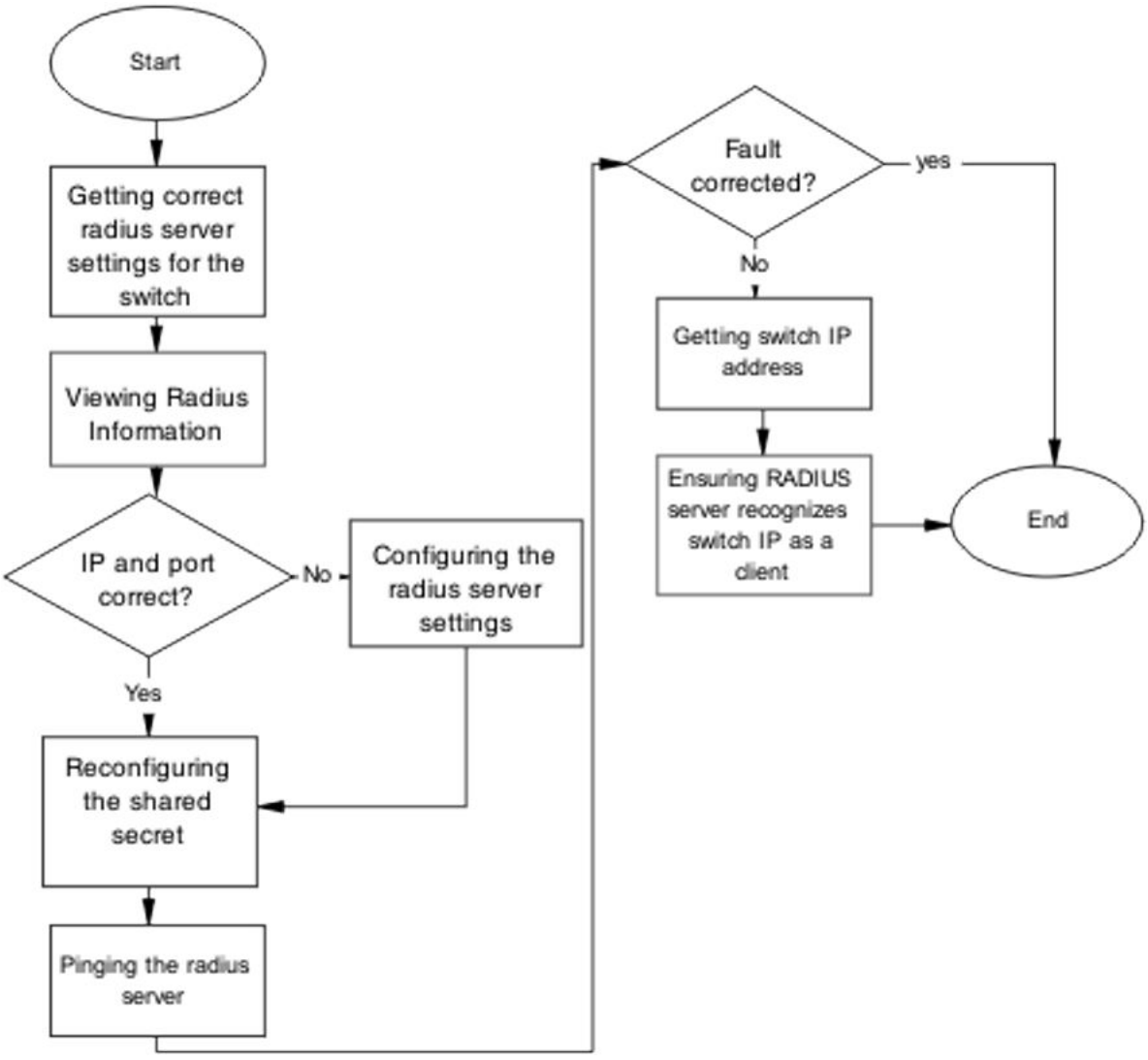



**Figure 24: Restore RADIUS connection**

## Getting correct RADIUS server settings for the switch

### About this task

This section provides troubleshooting guidelines for obtaining the RADIUS server settings

### Procedure

1. Obtain network information for the RADIUS server from the Planning and Engineering documentation.
2. Follow vendor documentation to set the RADIUS authentication method MD5.

## Viewing RADIUS information

### About this task

To review the RADIUS server settings in the device.

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

### Procedure

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

## Configuring the RADIUS server settings

### About this task

The RADIUS Server settings are to be correct for the network.

Follow vendor documentation to set the RADIUS server settings.

## Reconfiguring the shared secret

### About this task

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

### Procedure

1. Use the **`RADIUS-server key`** command.

2. Refer to the vendor documentation for server configuration.

## Pinging the RADIUS server

### About this task

Ping the RADIUS server to ensure connection exists.

### Procedure

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

# Enable EAP on the PC

The PC must have an EAP—enabled device that is correctly configured.

## Task flow: Enable EAP on the PC

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

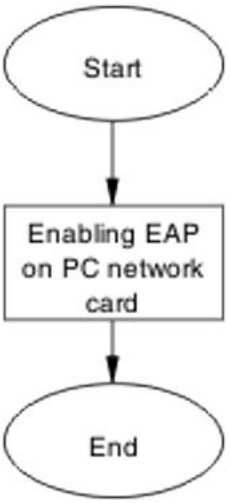



**Figure 25: Enable EAP on the PC**

## Enabling EAP on PC network card

### About this task

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

### Procedure

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

# Apply the method

The correct EAP method needs to be applied.

## Task flow: Apply the method

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

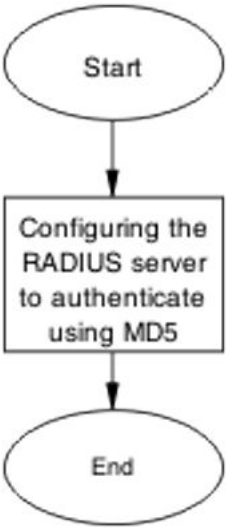



**Figure 26: Apply the method**

## Configuring the RADIUS server

### About this task

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

### Procedure

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

# Enable EAP globally

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

## Task flow: Enable EAP globally

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

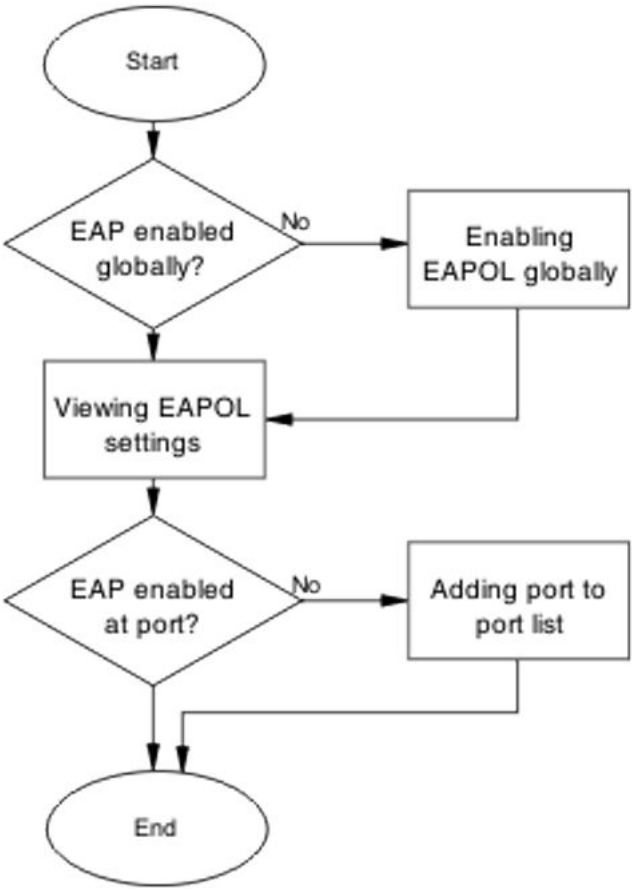



**Figure 27: Enable EAP globally**

## Enabling EAP globally

### About this task

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

### Procedure

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

## Viewing EAPOL settings

### About this task

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

### Procedure

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

## Setting EAPOL port administrative status to auto

### About this task

The port is to be included in the port list.

### Procedure

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

# EAP user role (UBP) is not being applied

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

## Work flow: EAP user role not being applied

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

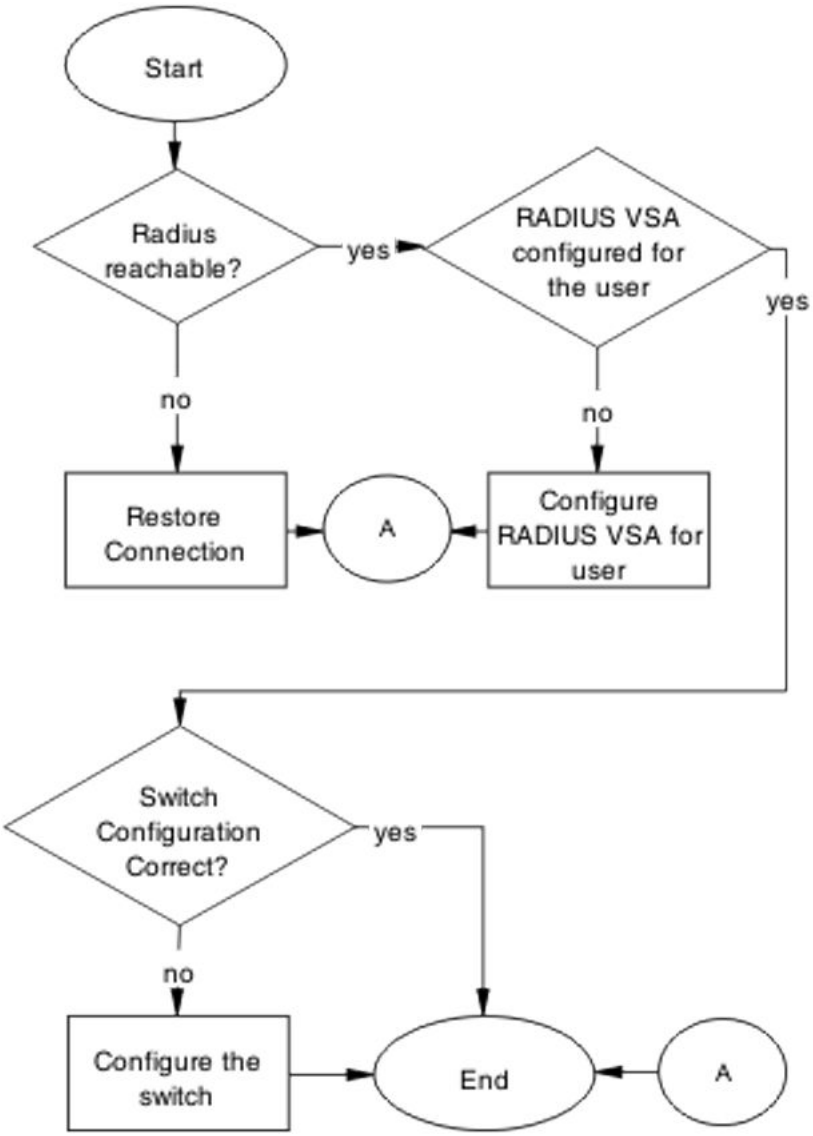



**Figure 28: EAP user role not being applied**

# 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.

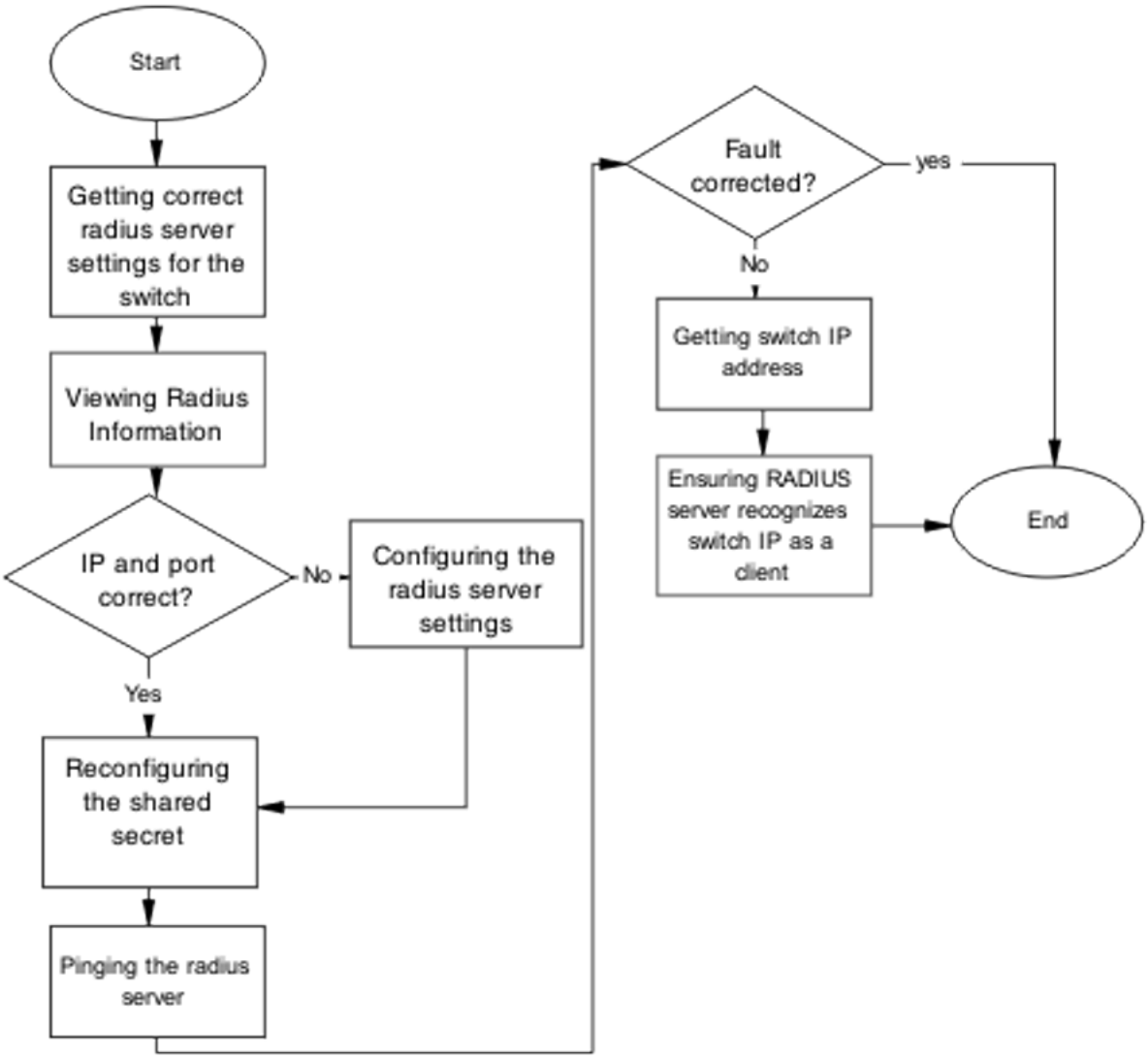



**Figure 29: Restore RADIUS connection**

## Getting correct RADIUS server settings for the switch

### About this task

Obtain the Radius server settings.

### Procedure

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

## Viewing Radius Information

### About this task

To review the Radius server settings in the device.

**Prerequisites:**

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

### Procedure

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

## Configuring the RADIUS server settings

### About this task

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

Follow vendor documentation to set the RADIUS server.

## Reconfiguring the shared secret

### About this task

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

### Procedure

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

## Pinging the RADIUS server

### About this task

Ping the Radius Server to ensure connection exists

### Procedure

1. Use the **`ping <server IP>`** command to ensure connection.

2. Observe no packet loss to confirm connection.

# Configure RADIUS VSA for the 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.

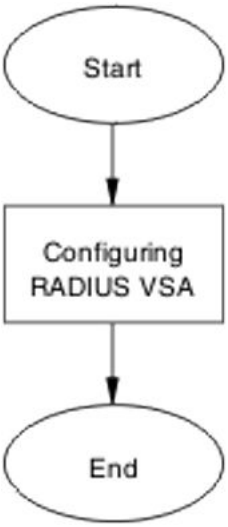



**Figure 30: Configure RADIUS VSA for user**

## Configuring RADIUS VSA for the user

### About this task

Configure the RADIUS VSA for the user.

### Procedure

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

# Configure the switch

Configure the switch for UBP globally.

## Task flow: Configure the switch

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

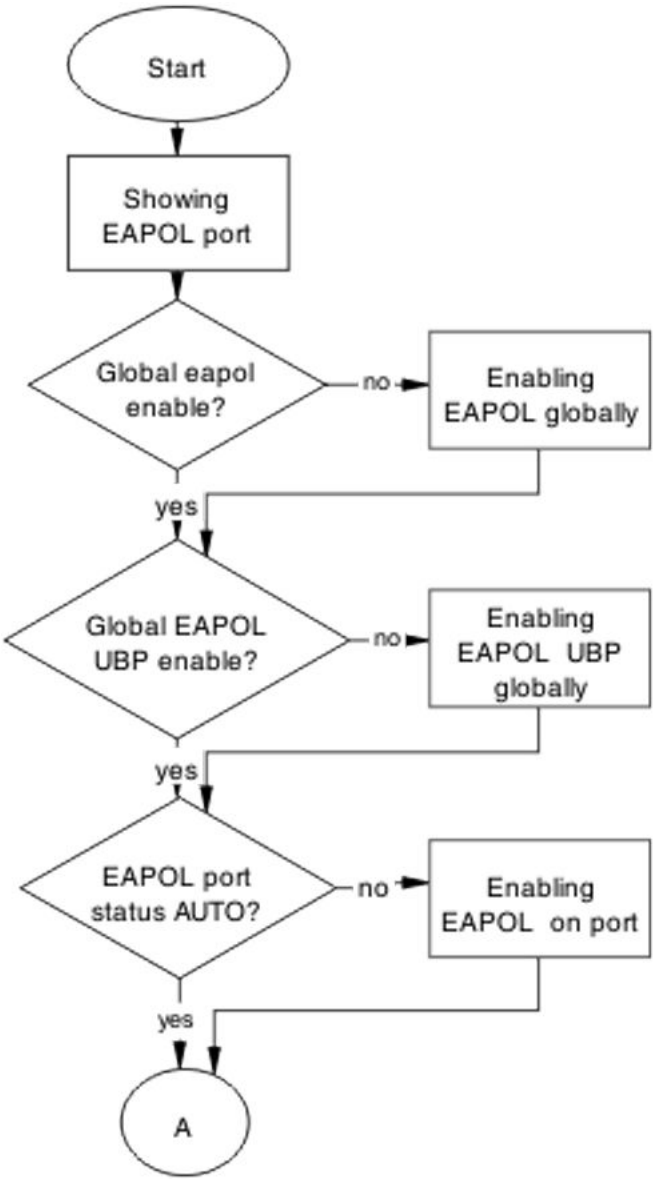



**Figure 31: Configure the switch part 1**

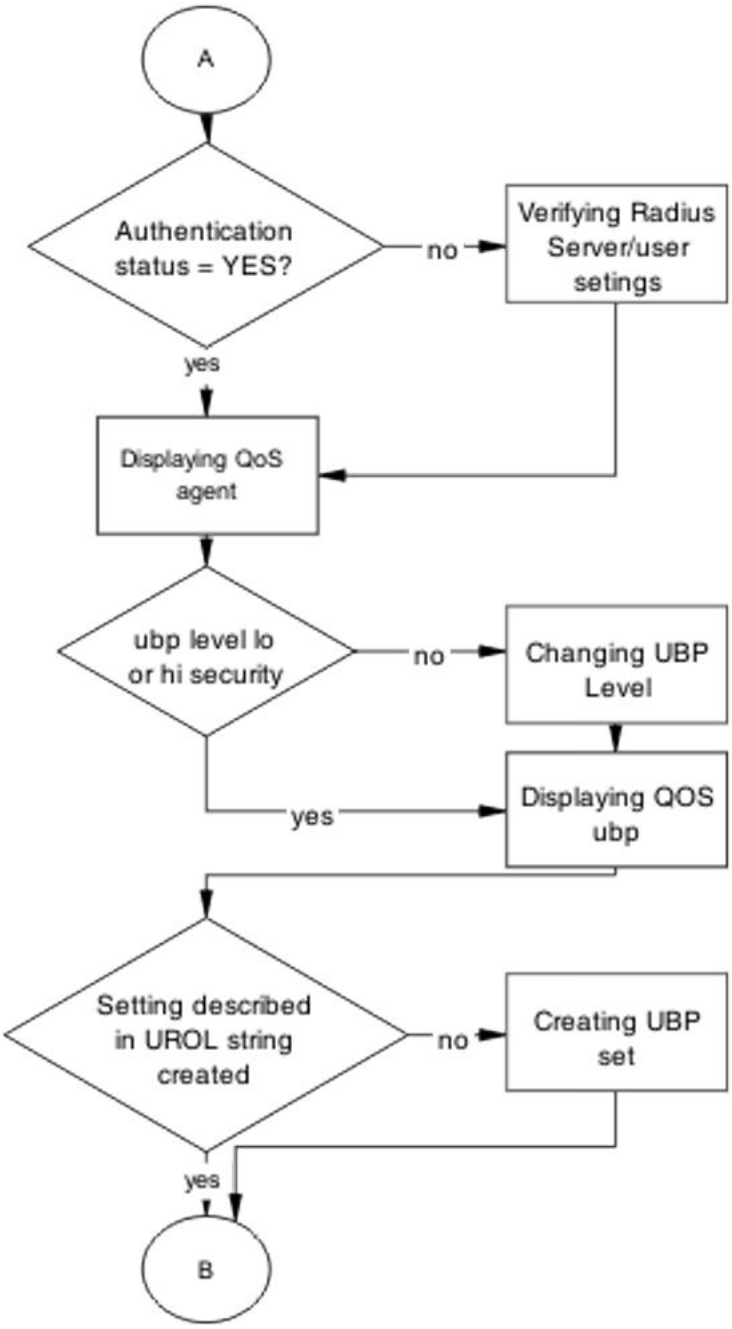



**Figure 32: Configure the switch part 2**

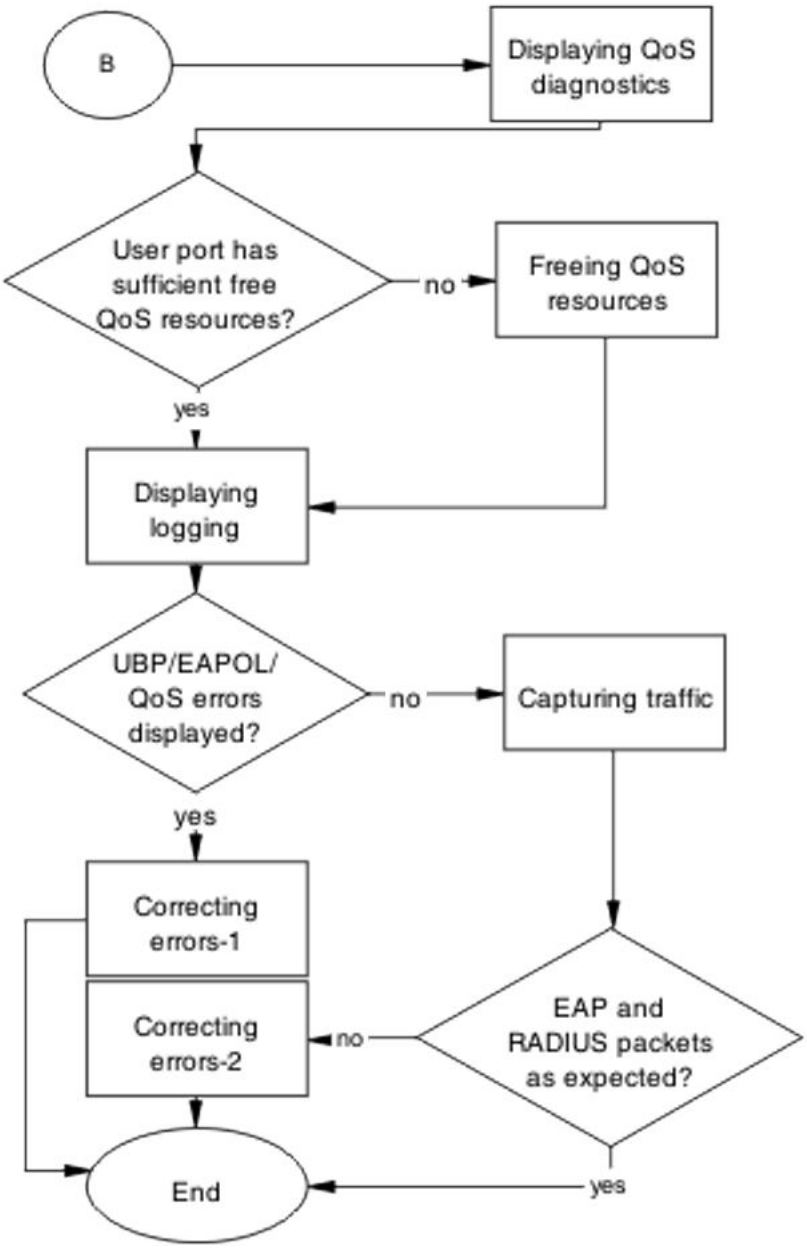



**Figure 33: Configure the switch part 3**

## Displaying EAPOL port configuration

### About this task

Obtain details of the EAPOL port configuration

### Procedure

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

2. Verify whether the EAPOL global setting is enabled.
3. Verify whether the EAPOL UBP global setting is enabled.
4. Verify whether the EAPOL port status is AUTO.

## Enabling EAPOL globally

### About this task

Enable EAPOL Globally for the switch.

### Procedure

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

## Enabling EAPOL UBP globally

### About this task

Enable EAPOL UBP globally for the switch.

### Procedure

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

## Enabling EAPOL on the user port

### About this task

Enable EAPOL on the user port.

### Procedure

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

## Verifying Radius Server and user settings

### About this task

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

Use vendor procedures to verify the information.

## Showing QoS Agent

### About this task

Obtain details of the QOS Agent.

### Procedure

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

## Changing UBP level

### About this task

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

### Procedure

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

## Displaying QoS UBP

### About this task

Obtain details of QoS agent settings.

### Procedure

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

## Creating UBP set

### About this task

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

### Procedure

1. Use the following commands to create the desired UBP set.
   a. qos ubp classifier
   b. qos ubp set
2. Verify whether errors are displayed.
   No error or warning messages should be displayed.

## Displaying QoS resource allocation

### About this task

Use this procedure to obtain details about QoS resources usage.

### Procedure

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

## Freeing QoS resources

### About this task

When you need to free resources you can

- delete some of the QoS policies configured on the user port
- disable some of the non-QoS applications configured on the port

### Procedure

1. Use the **`no qos policies`** command to delete unnecessary QoS policies.
2. Verify the following for the port designated for user authentication:
   if ((Non QoS masks + QoS mask < 16) and ( Non QoS Filters + QoS Filters < 128))

## Displaying logging

### About this task

Obtain log messages for the device.

### Procedure

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

## Correcting errors-1

### About this task

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

### Procedure

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

## Capturing traffic

### About this task

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

### Procedure

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

## Correcting errors-2

### About this task

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

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

# EAP multihost repeated re-authentication issue

Eliminate the multiple authentication of users.

## EAP Multihost repeated re-authentication issue

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

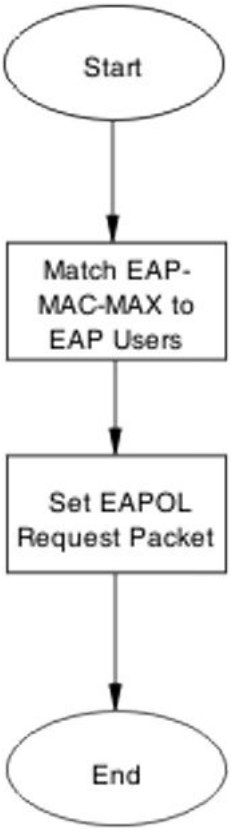



**Figure 34: EAP Multihost repeated re-authentication issue**

## Match EAP-MAC-MAX to EAP users

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

## Task flow: Match EAP-MAC-MAX to EAP users

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

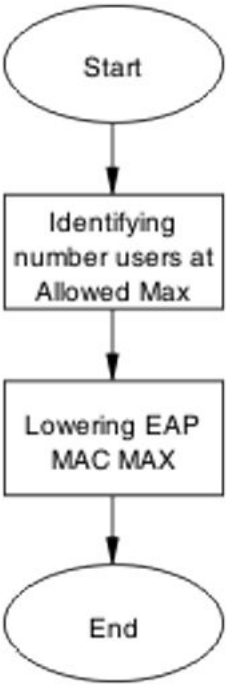



**Figure 35: Match EAP-MAC-MAX to EAP users**

## Identifying number users at allowed max

### About this task

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

### Procedure

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

## Lowering EAP max MAC

### About this task

Lower the mac-max value to match the users.

### Procedure

1. Use the **`eapol multihost eap-mac-max`** command to set the mac-max value.
2. Observe no errors after execution.

## Set EAPOL request packet

Change the request packet generation to unicast.

## Task flow: Set EAPOL request packet

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

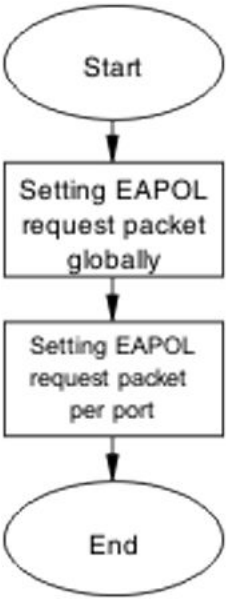



**Figure 36: Set EAPOL request packet**

## Setting EAPOL request packet globally

### About this task

Globally change the EAPOL request packet from multicast to unicast.

### Procedure

1. Use the **`eapol multihost eap-packet-mode unicast`** command to set the EAPOL request packet to unicast.
2. Observe no errors after execution.

## Setting EAPOL request packet per port

### About this task

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

### Procedure

1. Enter the interface configuration mode.
2. Use the **`eapol multihost eap-packet-mode unicast`** command to set the EAPOL request packet to unicast for the interface.

# EAP RADIUS VLAN is not being applied

Ensure that the RADIUS VLAN is applied correctly to support EAP.

## Work flow: EAP RADIUS VLAN is not being applied

The following work flow assists you to determine the cause and solution of the RADIUS VLAN is applied.

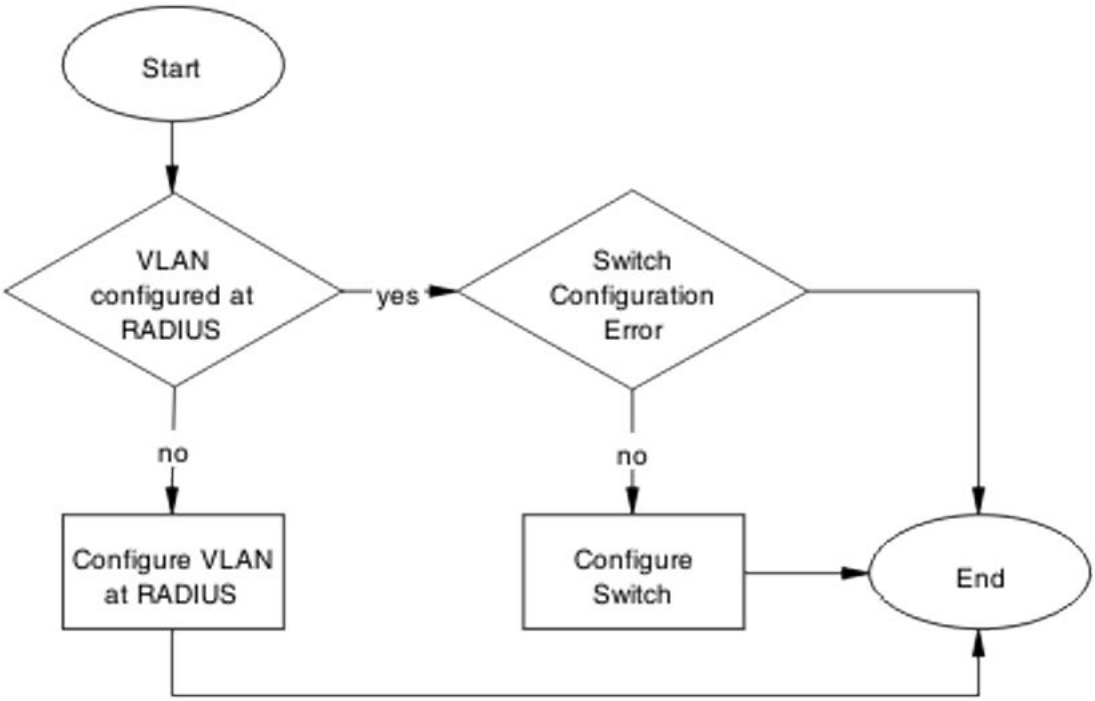



**Figure 37: EAP Radius VLAN is not being applied**

# Configure VLAN at RADIUS

Correct discrepancy at the RADIUS server for the VLAN information.

## Task flow: Configure VLAN at RADIUS

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

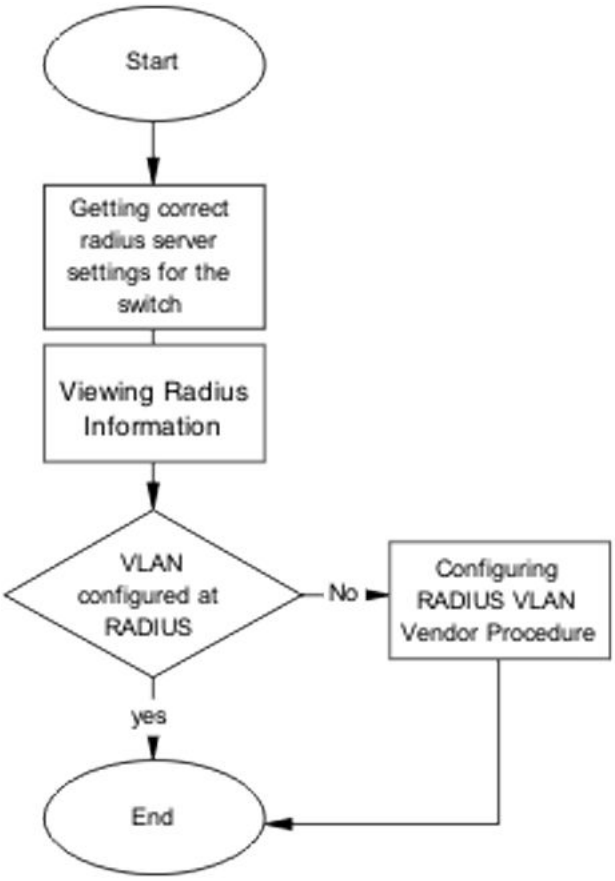



**Figure 38: Configure VLAN at RADIUS**

## Getting correct RADIUS server settings

### About this task

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

### Procedure

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

## Viewing RADIUS information

### About this task

Obtain the RADIUS information to identify its settings.

Use vendor documentation to obtain settings display.

## Configuring RADIUS

### About this task

Reconfigure the RADIUS server with the correct VLAN information.

Use vendor documentation to make the required changes.

Prerequisites

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

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

# Configure switch

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

## Task flow: Configure switch

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

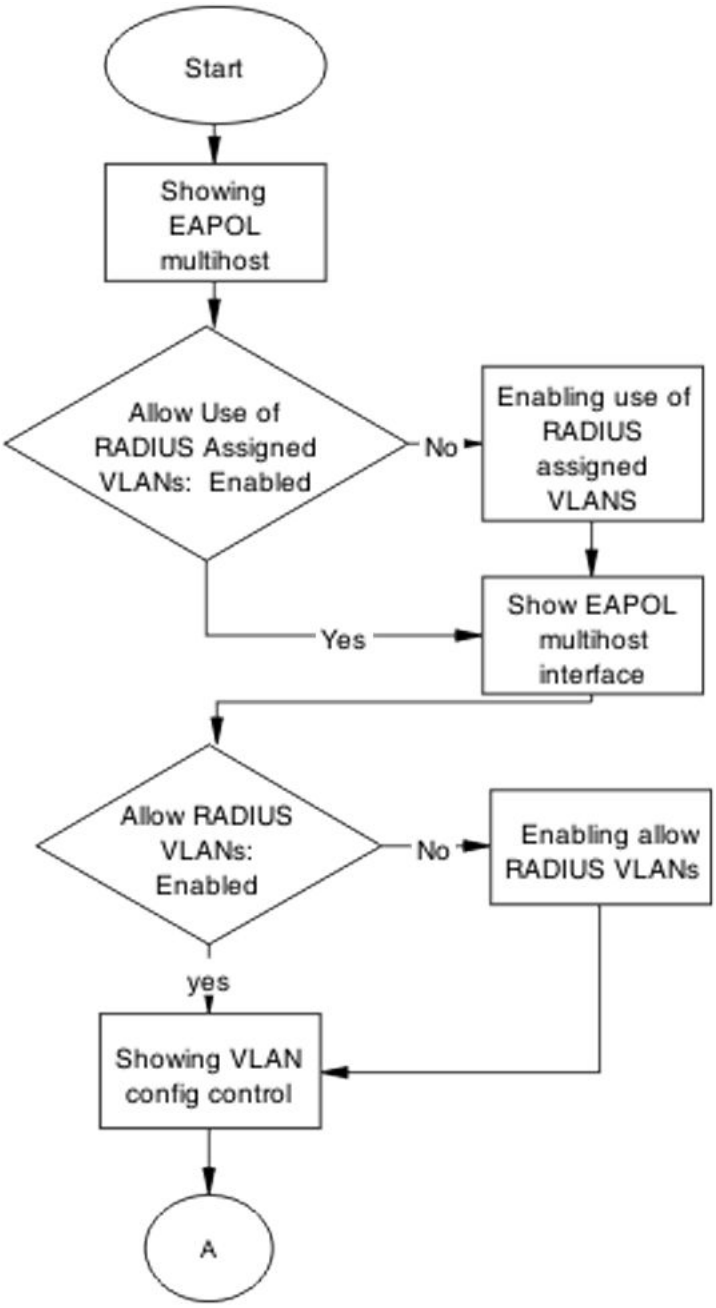



**Figure 39: Configure switch task part 1**

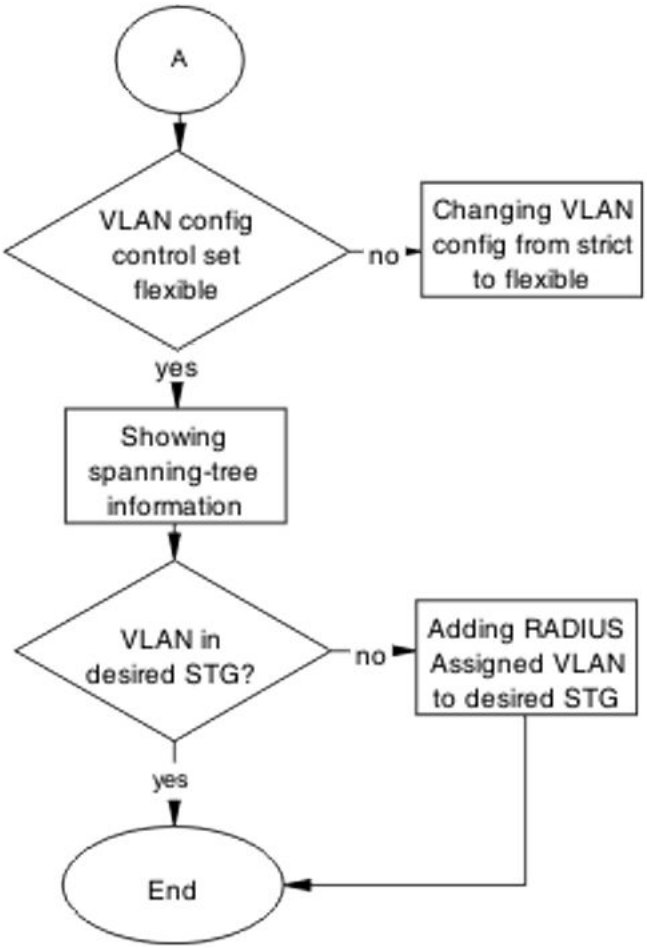



**Figure 40: Configure switch task part 2**

## Showing EAPOL Multihost

### About this task

Identify the EAPOL multihost information.

### Procedure

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

## Enabling allow RADIUS VLANs

### About this task

Change the allow RADIUS assigned VLAN to enable.

### Procedure

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

## Showing EAPOL multihost interface

### About this task

Display the EAPOL Interface.

### Procedure

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

## Showing VLAN config control

### About this task

Display the VLAN config control information.

### Procedure

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

## Changing VLAN config from strict to flexible

### About this task

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

### Procedure

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

## Showing Spanning Tree

### About this task

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

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

## Adding RADIUS assigned VLAN to desired STG

### About this task

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

### Procedure

1. Use the **spanning-tree stp <1-8> vlans**command to make the change.
2. Review output to identify that the change was made.

# Configured MAC is not authenticating

Correct a MAC to allow authentication.

# Work flow: Configured MAC is not authenticating

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

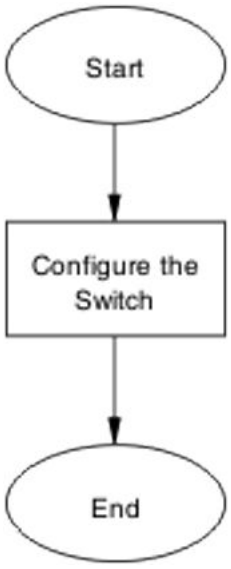



**Figure 41: Configured MAC is not authenticating**

# 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.

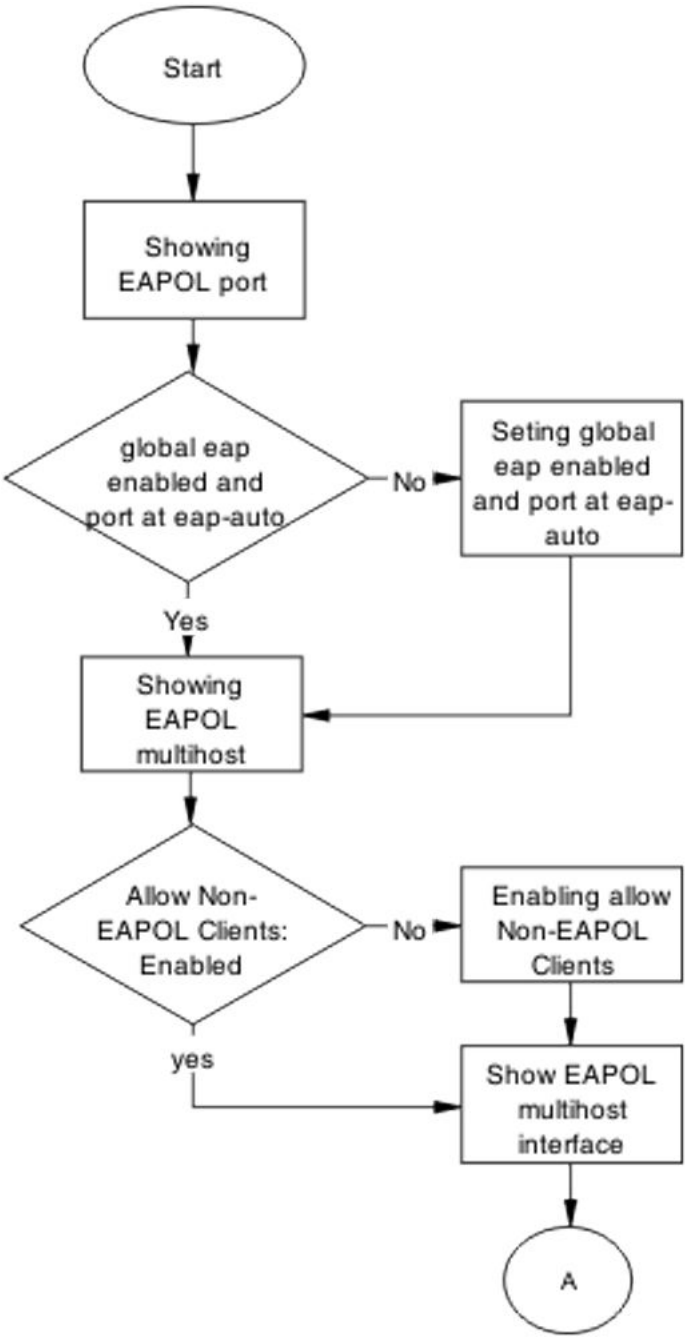



**Figure 42: Configure the switch part 1**

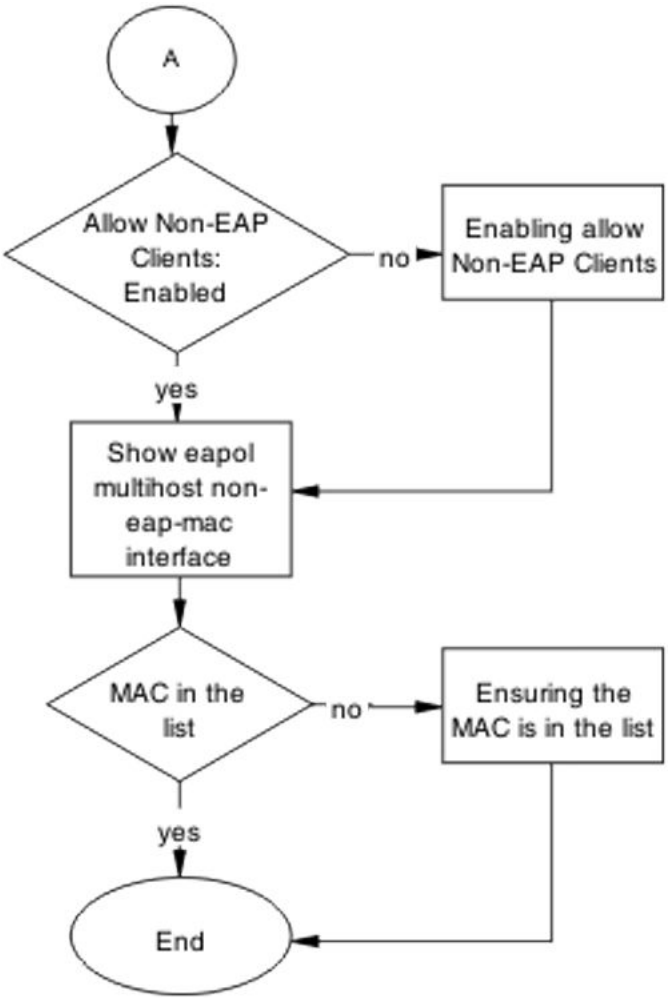



**Figure 43: Configure the switch part 2**

## Showing EAPOL port

### About this task

Display the EAPOL port information

### Procedure

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

## Setting global EAP enabled and port at eap-auto

### About this task

Make the corrections to ensure the settings as required.

### Procedure

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

## Showing EAPOL multihost

### About this task

Display the EAPOL multihost information.

### Procedure

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

## Allowing non-EAPOL clients

### About this task

Use the command in this procedure to enable Non-EAPOL clients.

### Procedure

1. Enter the **eapol multihost allow-non-eap-enable** command.
2. Verify that the command did not generate errors.

## Showing EAPOL multihost interface

### About this task

Display the EAPOL multihost interface information after you have executed the **eapol multihost allow-non-eap-enable** command.

### Procedure

Enter **show eapol multihost interface <port#>** to display the EAPOL multihost interface information.
Allow Non-EAPOL clients is enabled.

Multihost status is enabled.

## Enabling multihost and allowing non-EAPOL clients

### About this task

When you need to correct the Non-EAP client attribute, use this procedure.

### Procedure

1. Enter **eapol multihost allow-non-eap-enable** to allow non-EAPOL clients.
2. Enter **eapol multihost enable** to enable multihost .

## Showing EAPOL multihost non-eap-mac interface

### About this task

When you need to display EAPOL multihost interface information, use this procedure.

### Procedure

1. Enter the **show eapol multihost non-eap-mac interface <port>** command.
2. Verify that the MAC is in the list that the command displays.

## Ensuring the MAC is in the list

### About this task

If you need to add the MAC to the list, in case it was omitted, use the following procedure.

### Procedure

1. Use the **show eapol multihost non-eap-mac status <port>** command to view mac addresses.

2. Use the **`eapol multihost non-eap-mac <H.H.H> <port>`** command to add a mac address to the list.

# NEAP RADIUS MAC not authenticating

Correct a NEAP RADIUS MAC that is not authenticating.

## Work flow: NEAP RADIUS MAC not authenticating

The following work flow can assist you in determining the cause of, and solution for, a RADIUS MAC that does not authenticate.

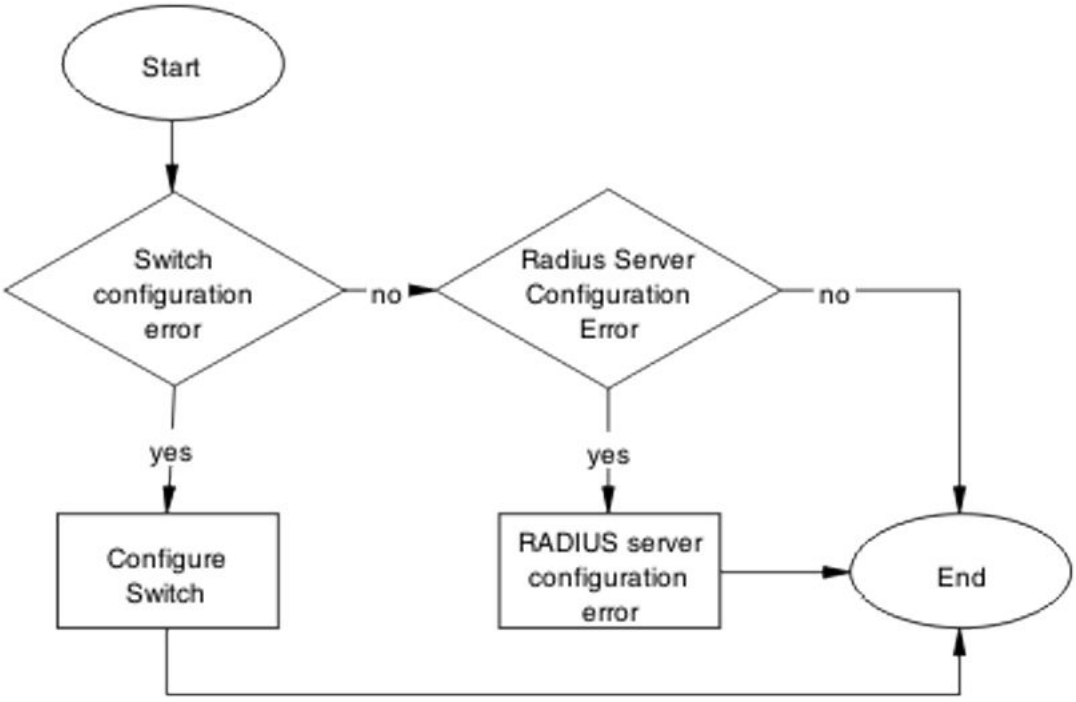



**Figure 44: NEAP RADIUS MAC not authenticating**

## Configure Switch

To correct the issue with RADIUS MAC, you may need to modify the switch configuration.

## Task flow: Configure switch

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

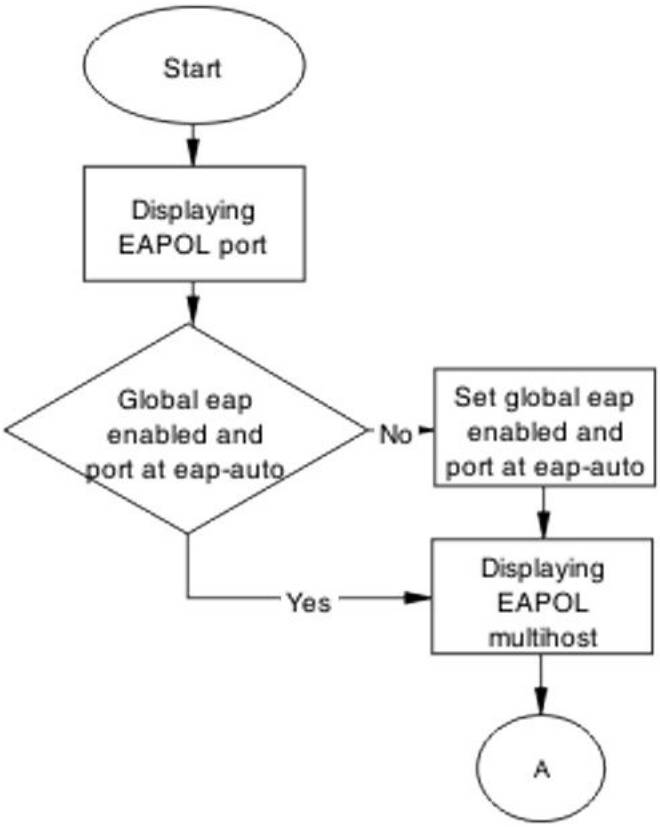



**Figure 45: Configure switch part 1**

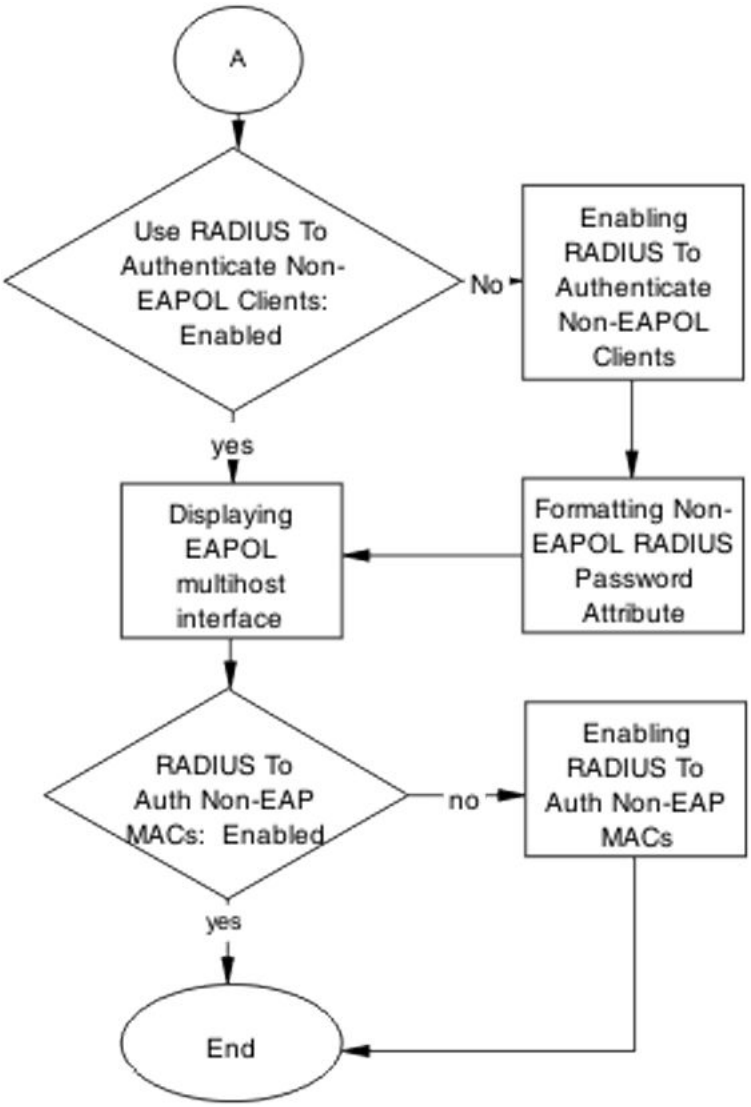



**Figure 46: Configure switch part 2**

## Displaying EAPOL port information

### About this task

To display the EAPOL port information for review, use this procedure.

### Procedure

1. Enter the show **`eapol port <port#>`** command to display the information.
2. Review the information to determine that:
   - Global EAP is enabled.

- The port is set to eap-auto.

## Enabling EAP globally and setting the port to EAP Automatic

### About this task

Make the required changes to ensure the settings are correct.

### Procedure

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

## Displaying EAPOL multihost

### About this task

Display the EAPOL multihost information for review.

### Procedure

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

## Enabling RADIUS to authenticate non-EAPOL clients

### About this task

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

### About this task

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

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

## Displaying the EAPOL multihost interface

### About this task

Display the EAPOL Multihost information for review.

### Procedure

1. Enter the **`show eapol multihost interface <port#>`** command to display the information
2. Review the information to verify that Use RADIUS To Authenticate Non EAP MAC is enabled

## Enabling RADIUS to authorize Non-EAP MACs

### About this task

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

Use the RADIUS server vendor documentation to help you apply changes to the RADIUS server.

# RADIUS server configuration error

The correct MAC address and password for the switch must be configured on the RADIUS server.

## Task flow: RADIUS server configuration error

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

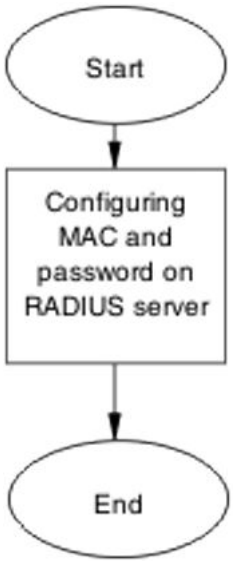



**Figure 47: RADIUS server configuration error**

### Configuring MAC and password on RADIUS server

#### About this task

The RADIUS server requires the correct MAC and password for the switch. If they are not correct, the switch cannot authenticate.

To configure the correct MAC and password for the switch on the RADIUS server, refer to 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

When an MHSA MAC is not authenticating you can use the following work flow to assist in determining the solution.

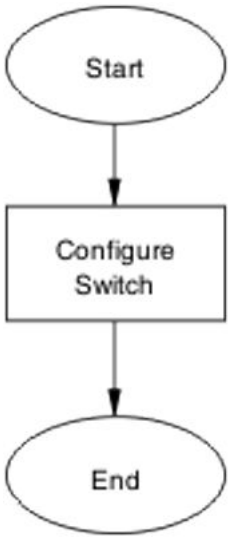



**Figure 48: NEAP MHSA MAC is not authenticating**

**NEAP MHSA MAC is not authenticating navigation:**

- Configure switch on page 104

# Configure switch

Configure the switch to enable MHSA.

## Task flow: Configure switch

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

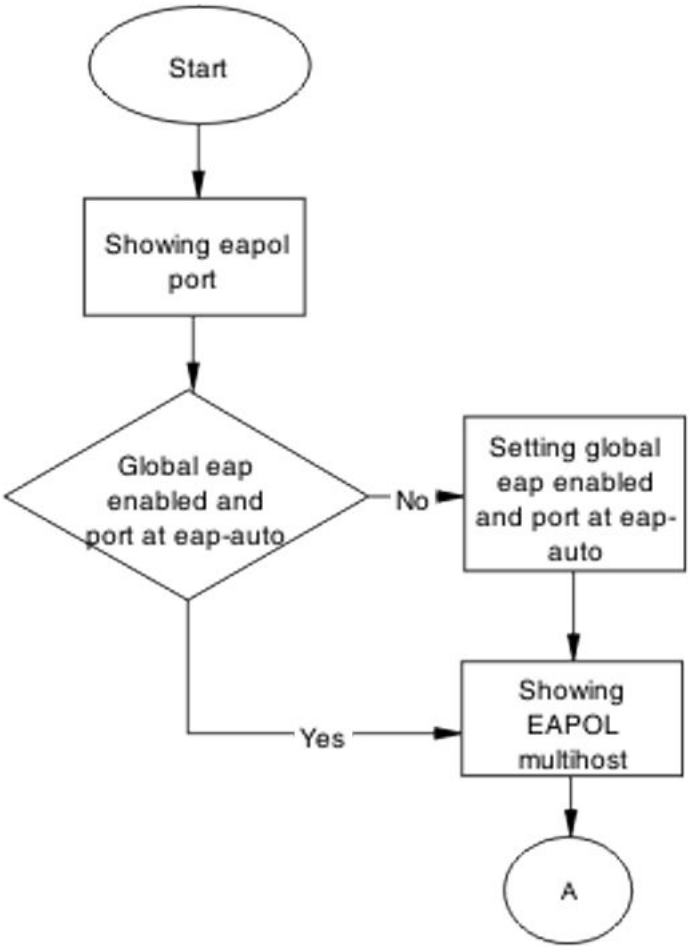



**Figure 49: Configure switch part 1**

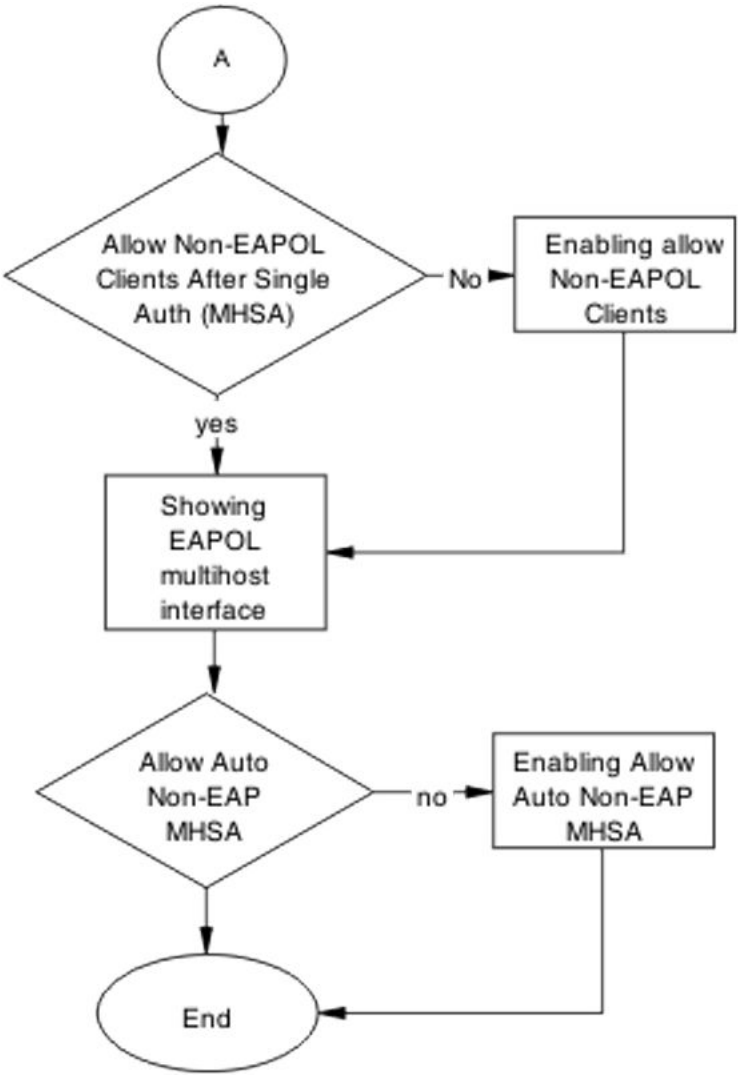



**Figure 50: Configure switch part 2**

## Displaying EAPOL port information

### About this task

Display the EAPOL port information for review.

### Procedure

1. Enter the show **`eapol port <port#>`** command to display the information.
2. Review the information to verify the following:
   - EAP is enabled globally.

- The port is set for EAP automatically (eap-auto).

## Enabling EAP globally and setting the port to automatic EAP

### About this task

Make the required changes to ensure the settings are correct.

### Procedure

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

## Showing EAPOL multihost

### About this task

Display the EAPOL Multihost information for review.

### Procedure

1. Enter the show **`eapol port multihost`** command to display the information.
2. Review the information to verify that Use RADIUS To Authenticate NonEAPOL Clients is enabled

## Formatting non-EAPOL RADIUS password attribute

### About this task

Use the RADIUS server vendor documentation to change the non-EAPOL RADIUS password attribute format to `IpAddr.MACAddr.PortNumber` on the RADIUS server.

## Enabling RADIUS to authenticate non-EAP clients

### About this task

Use the RADIUS server vendor documentation to make and apply the required changes to authenticate Non-EAP clients on the RADIUS server.

## Showing EAPOL multihost interface information

### About this task

Display the EAPOL multihost information for review.

### Procedure

1. Enter the **`show eapol multihost interface <port#>`** command to display the information.
2. Review the information to verity that `Allow Auto Non-EAP MHSA` is enabled.

## Enabling RADIUS to authorize non-EAP MACs

### About this task

Use the RADIUS server vendor documentation to make and apply the required changes to authenticate Non-EAP clients on the RADIUS server.

# 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.

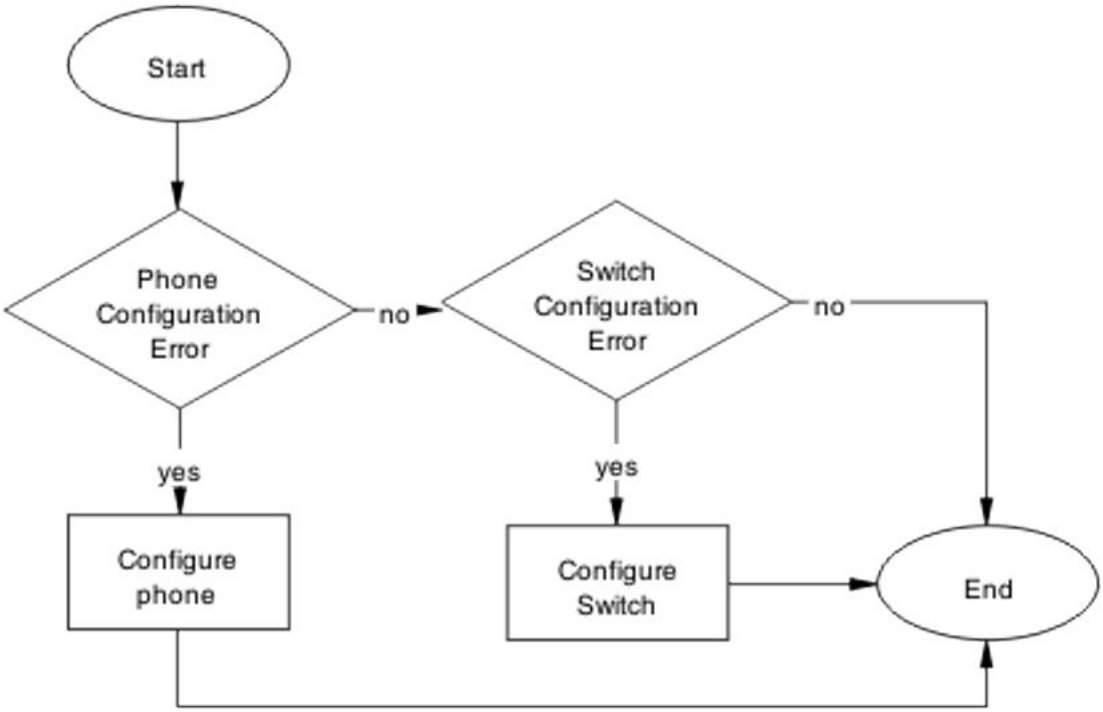



**Figure 51: NEAP phone is not working**

# 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 52: Configure phone**

## Setting the phone to full DHCP

### About this task

Configure the phone as full DHCP to obtain network information.

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

## Ensuring phone signatures are Avaya

### About this task

Configure the phone with Avaya signatures.

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

# Configure the switch

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

## Task flow: Configure the switch

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

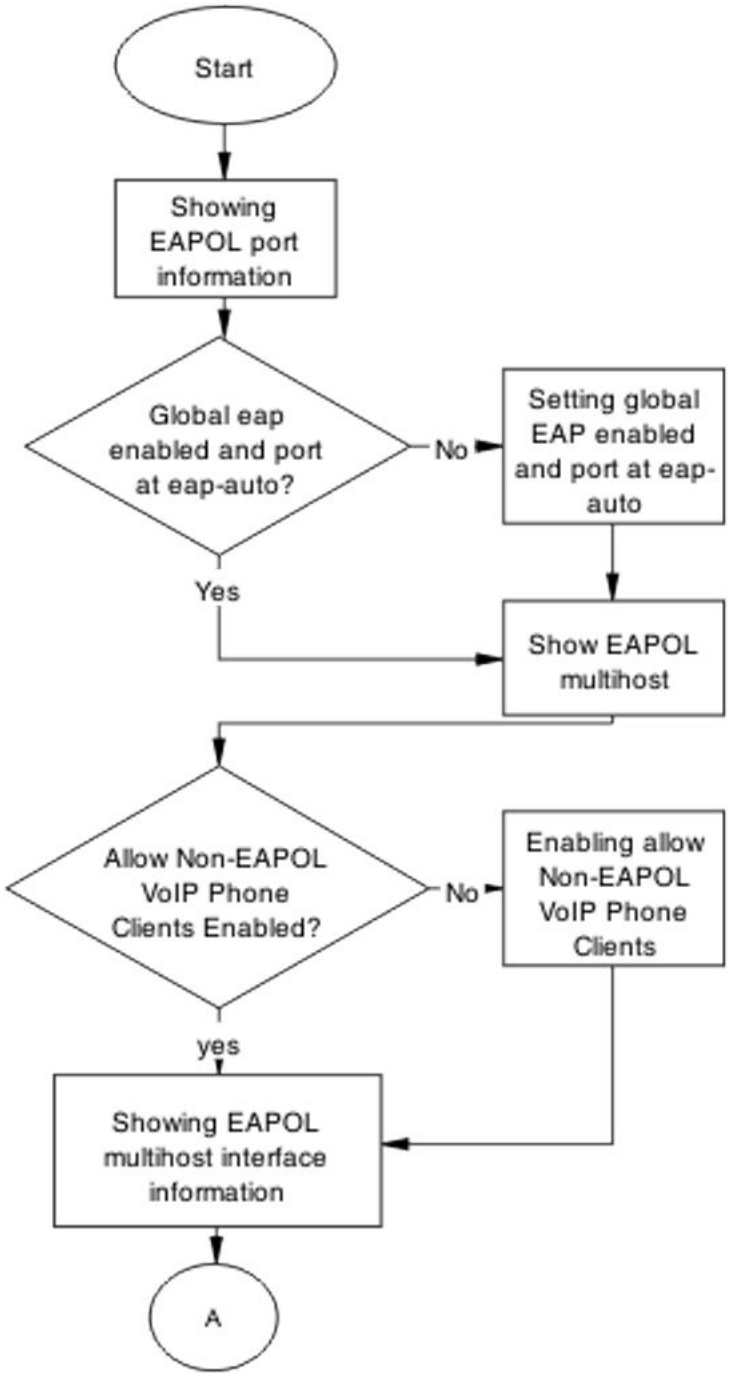



**Figure 53: Configure the switch part 1**

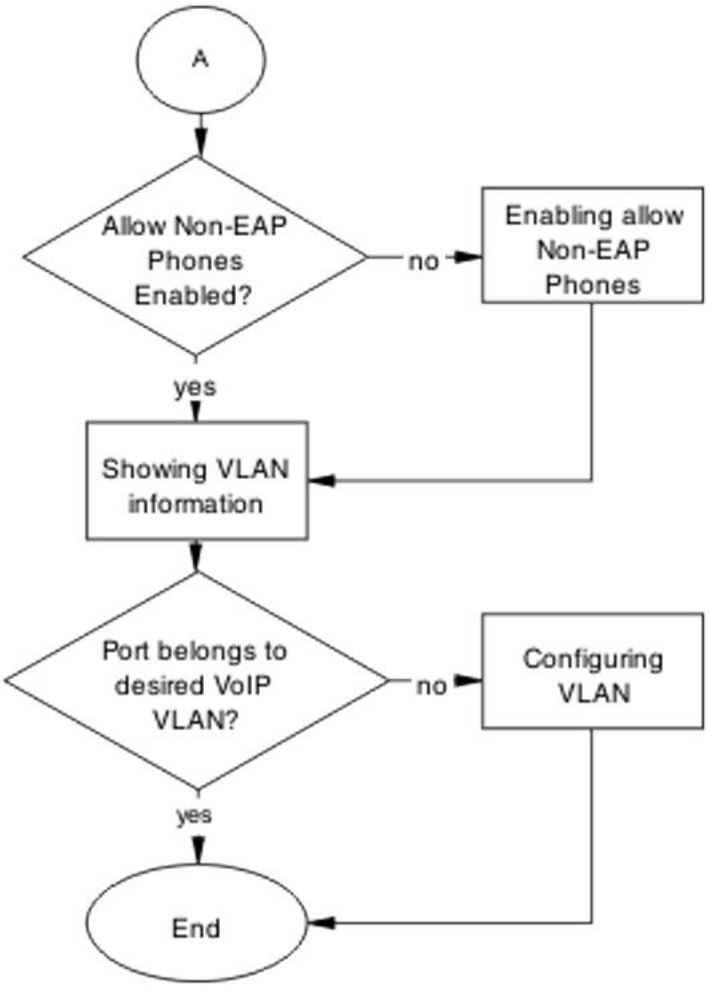



**Figure 54: Configure the switch part 2**

## Displaying EAPOL port information

### About this task

Display the EAPOL port information for review.

### Procedure

1. Enter the show **`eapol port <port#>`** command to display the information.
2. Review the information to verify that
   - the EAP is enabled globally
   - eap-auto is set on the port

## Enabling EAPOL globally and the port EAPOL automatic status

### About this task

Make the required changes to ensure the settings are correct.

### Procedure

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

## Displaying EAPOL multihost information

### About this task

Display the EAPOL Multihost information for review.

### Procedure

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

## Enabling non-EAPOL VoIP phone clients

### About this task

Verify that the multihost setting allows non-EAP VoIP phone clients..

### Procedure

1. Use the **`eapol multihost non-eap-phone-enable`** command to allow NEAP Phones.
2. Review the command output for errors.

## Displaying EAPOL multihost interface information

### About this task

Display the EAPOL multihost information for review.

### Procedure

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

## Enabling Non-EAP phones

### About this task

Change the multihost setting to allow non-EAP phones.

### Procedure

1. Use the **`eapol multihost non-eap-phone-enable`** command to allow NEAP Phones .
2. Review the command output for errors.

## Displaying VLAN information

### About this task

Display the VLAN information for review.

### Procedure

1. Enter the **`show vlan`** command to display the information.
2. Verify the following:
   - Ensure that the port belongs to the desired Voip VLAN.

### Adding a port to the VLAN

#### About this task

Change the VLAN setting to use the correct port.

#### Procedure

Use the **`vlan members add <1-4094> <port>`** command to move the port to desired VLAN.

# NEAP user policies from RADIUS not applied

If NEAP user policies from the RADIUS server are not applied, use the work flows and procedures in this section to help you correct the faults.

## Work flow: NEAP user policies from RADIUS not applied

When user policies from the RADIUS server are not applied, use the following work flow and associated procedures to assist you to develop a solution.

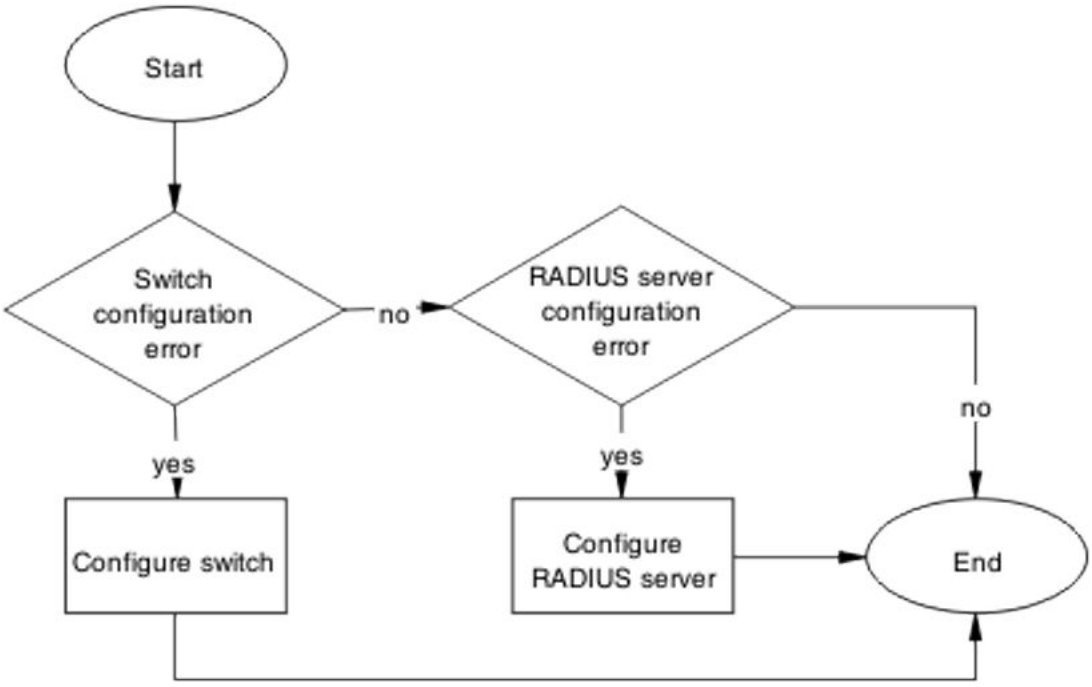



**Figure 55: NEAP user policies from RADIUS not applied**

# Configure the switch

Review switch configuration 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.

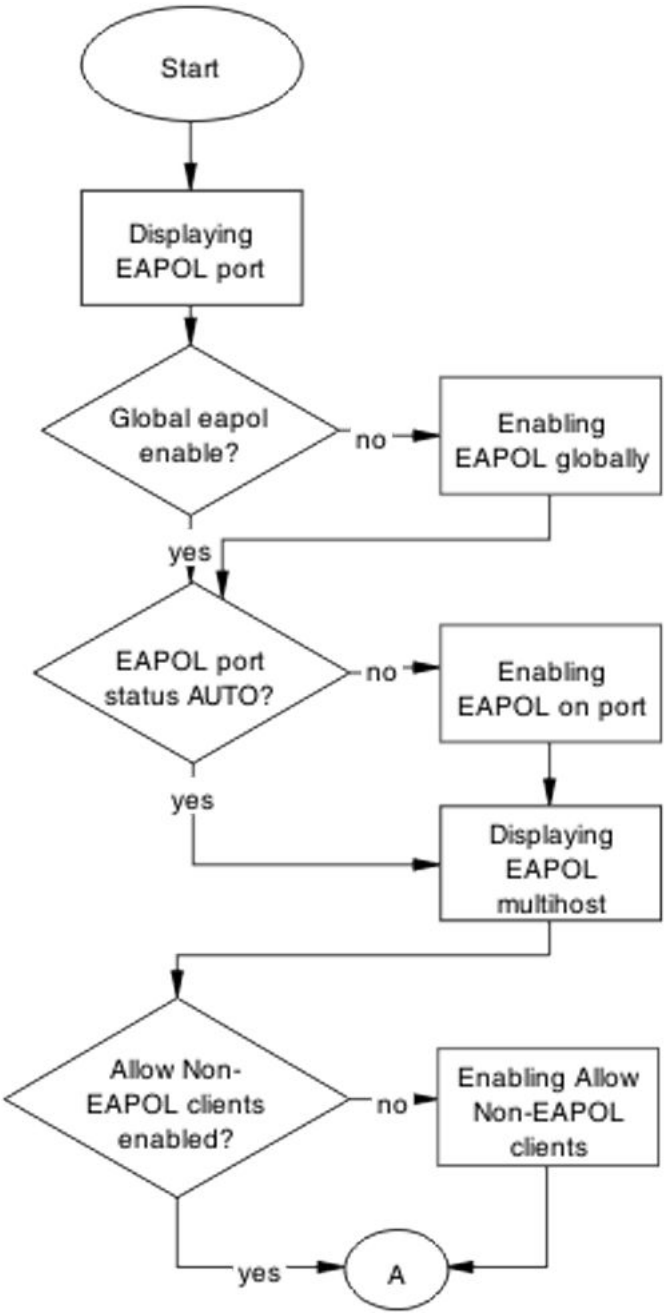



**Figure 56: Configure switch part 1**

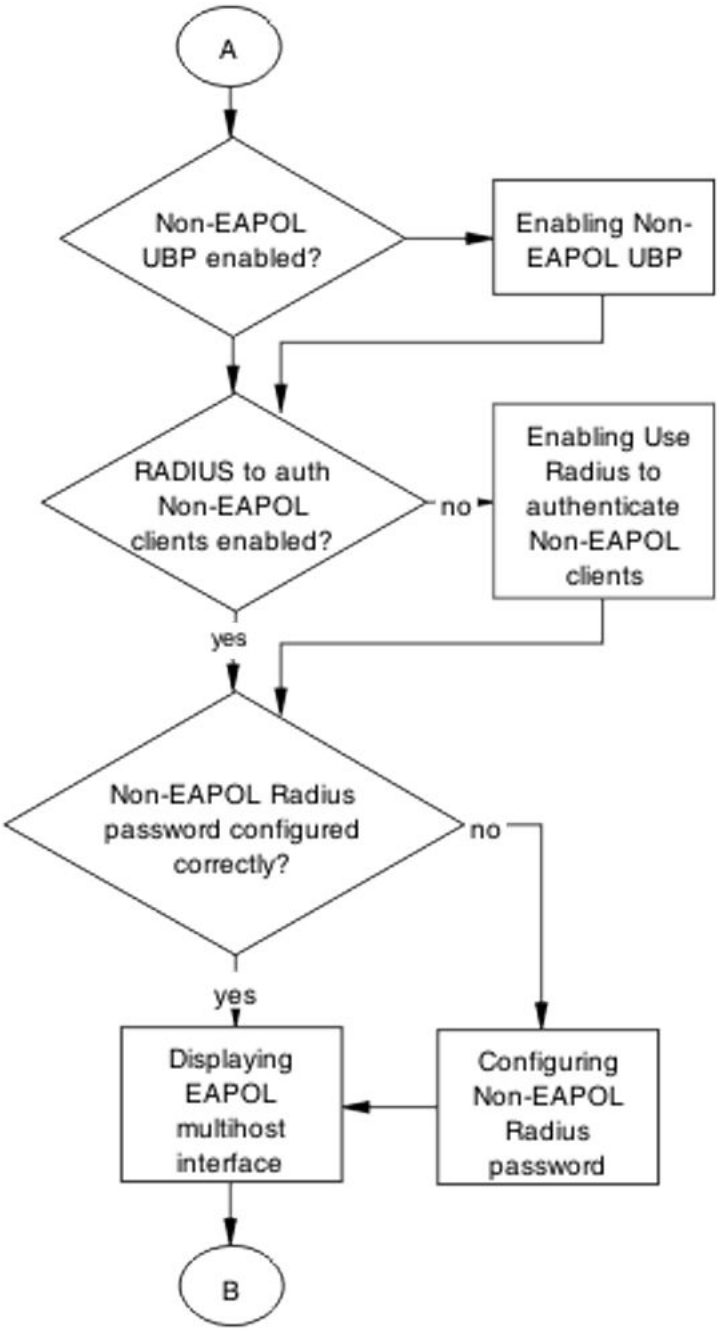



**Figure 57: Configure switch part 2**

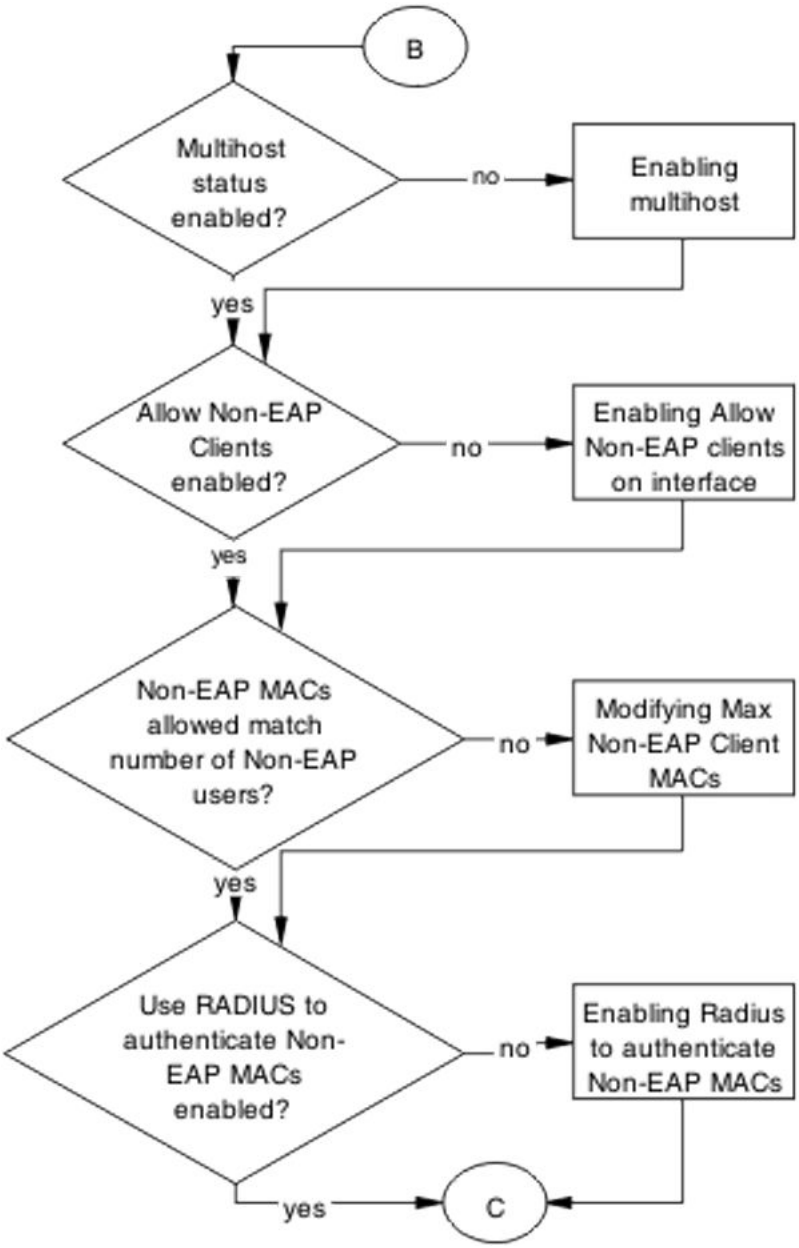



**Figure 58: Configure switch part 3**

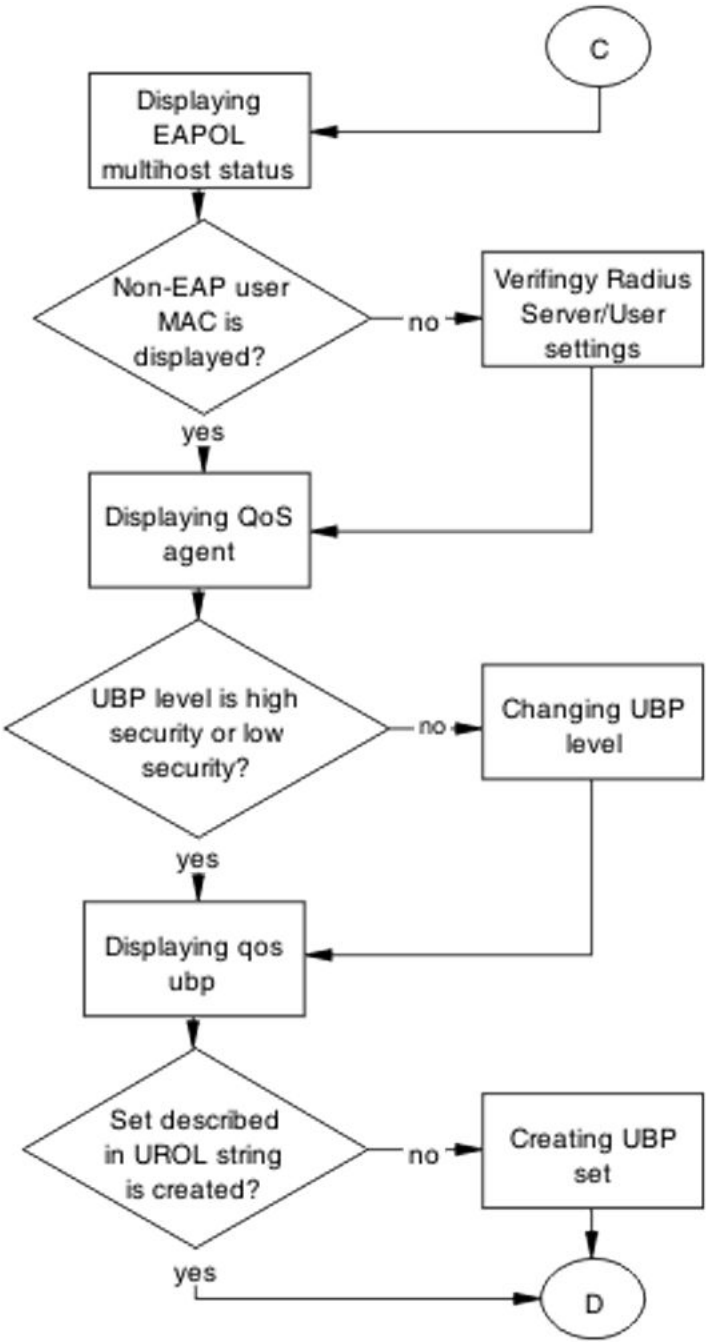



**Figure 59: Configure switch part 4**

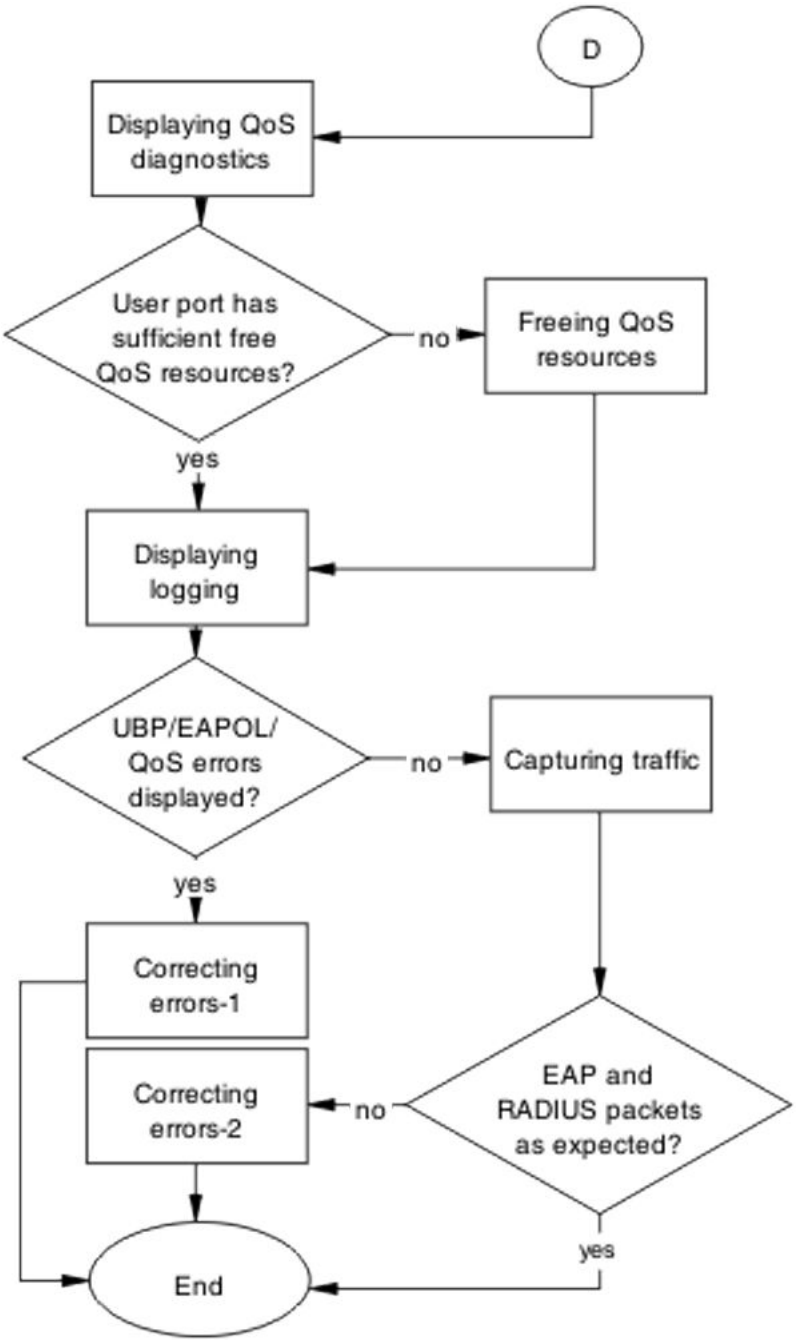



**Figure 60: Configure switch part 5**

## Displaying EAPOL port

### About this task

Obtain details of the EAPOL port configuration.

### Procedure

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

## Enabling EAPOL globally

### About this task

Enable EAPOL globally for the switch.

### Procedure

1. Use the **eapol enable** command to enable EAPOL globally.
2. Ensure that no error or warning messages display.

## Enabling EAPOL UBP globally

### About this task

Enable EAPOL UBP globally for the switch.

### Procedure

1. Use the **eapol user-based-policies enable** command to enable EAPOL globally.
2. Verify that no error or warning messages display.

## Enabling EAPOL on a port

### About this task

Enable EAPOL on a user port.

### Procedure

1. Use the **eapol port <port>** command to enable EAPOL on a port.

2. Verify that no error or warning messages display.

## Displaying EAPOL multihost information

### About this task

Obtain the details for EAPOL multihost global settings.

### Procedure

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 if Radius Non-EAP password is configured correctly.

## Allowing non-EAPOL clients

### About this task

Enable processing for non-EAPOL clients.

### Procedure

1. Use the **`eapol multihost allow-non-eap-enabled`** command to enable Allow Non-EAPOL on the switch.
2. Ensure that no error or warning messages display.

## Enabling Non-EAP user based policies

### About this task

Enable Non-EAP UBP.

### Procedure

1. Use the **`eapol multihost non-eap-user-based-policies enable`** command to enable Non-EAPOL UBP on the switch.

2. Verify that no error or warning messages display.

## Enabling use RADIUS to authenticate Non-EAPOL clients

### About this task

Enable authentication using Radius Server for Non-EAP clients.

### Procedure

1. Use the **`eapol multihost RADIUS-non-eap-enabled`** command to enable authentication using a Radius Server for Non-EAPOL clients.
2. Verify that no error or warning messages display.

## Configuring a Non-EAPOL RADIUS password

### About this task

Configure a password for use with Radius authentication for Non-EAPOL clients.

### Procedure

1. Use the **`eapol multihost non-eap-pwd-fmt [ip-aadr|mac-addr| port-number]`** command to configure the password used in Radius authentication.
2. Verify that no error or warning messages display.

## Displaying EAPOL multihost interface

### About this task

Obtain the details for EAPOL multihost interface settings.

### Procedure

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.

- The maximum number of Non-EAP MAC addresses is configured correctly.

## Enabling multihost on an interface

### About this task

Enable multihost processing on a specific interface.

### Procedure

1. Use the **`eapol multihost port <port> enable`** command to enable multihost processing on a specific interface.
2. Verify that no error or warning messages display.

## Allowing non-EAP clients on a specific interface

### About this task

Enable processing for Non-EAPOL clients on a specific interface.

### Procedure

1. Use the **`eapol multihost port <port> allow-non-eap-enabled`** command to enable Allow Non-EAPOL on a specific interface.
2. Verify that no error or warning messages display.

## Modifying the maximum number of non-EAP client MAC addresses

### About this task

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

### Procedure

1. Use the **`eapol multihost port <port> non-eap-mac-max`**command to modify the number of allowed Non-EAPOL clients on an interface.
2. Verify that no error or warning message display.

## Displaying EAPOL multihost status

### About this task

Obtain the status for an EAPOL multihost interface.

### Procedure

1. Use the **`show eapol multihost status <port>`** command to display authenticated MAC addresses on a port.
2. Verify whether the user MAC displays.

## Verifying RADIUS server and user settings

### About this task

Verify that the user and password configured on the Radius Server match the Non-EAPOL user MAC and password (created by the switch).

Refer to vendor documentation for the RADIUS server configuration.

## Displaying QoS agent

### About this task

Obtain details of QoS agent settings.

### Procedure

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

## Changing the QoS agent user based policy security level

### About this task

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

### Procedure

1. Use one of the following commands to enable a QoS UBP security level on the device:
   - **`qos agent ubp high-security-local`**

- **qos agent ubp low-security-local**

2. Verify that no error or warning messages display.

## Displaying QoS user based policy information

### About this task

Obtain details of QoS agent UBP settings.

### Procedure

1. Use the **show qos ubp** command to display QoS UBP settings.
2. Verify whether the UBP set name matches the UROL string configured on the RADIUS server. For example, if the UBP Set is named student then the UROL string sent by the RADIUS server must be UROLstudent.

## Creating a user based policy set to apply to an authenticated user port

### About this task

Create a user based policy (UBP) set to configure the template policy to apply to the authenticated user port.

### Procedure

1. Use the following commands to create the UBP set:
   a. At the ACLI command prompt, enter **qos ubp classifier**.
   b. At the ACLI command prompt, **qos ubp set**.
2. Verify that no error or warning messages display.

## Displaying QoS resource use

### About this task

Obtain details of QoS resource use.

### Procedure

1. Use the **show qos diag** command to display QoS resource use.
2. Verify the following for the port that will be used for user authentication:

- Non QoS masks + QoS mask < 16
- Non QoS Filters + QoS Filters < 128

## Freeing QoS resources

### About this task

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

### Procedure

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

## Displaying log messages for the switch

### About this task

Obtain log messages for the device.

### Procedure

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

## Correcting errors-1

### About this task

If errors display in log messages, verify the EAPOL and/or QoS configuration.

### Procedure

1. If EAPOL error 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, review UBP sets for conflicts inside the set or conflicts with the QoS policies already installed on the port.

## Capturing traffic

### About this task

Capture traffic between a user PC and a switch, and between a user PC and a RADIUS server.

### Procedure

1. User another PC and a hub or port mirroring feature to capture traffic between the user PC and the switch.
2. Save the captured data.
3. Use another PC and a hub or port mirroring feature to capture traffic between the user PC and the Radius Server.
4. Save the captured data.

## Correcting errors -2

### About this task

Using captured traffic data, verify whether all of the expected packets are exchanged between the user PC and the switch and/or between the switch and the RADIUS Server.

### Procedure

1. Search the data captured between the User PC and the switch for correct EAP packets.

   Verify the following:

   - The correct MAC is sent by the user PC in the EAP packet.
   - The switch sends an EAP success packet at the end of the EAP exchange.
2. If authentication fails, recheck user and password on the Radius Server and MAC address and created password.
3. Search the data captured between the switch and the 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 switch in the request.

4. If the VSA is incorrect, check the RADIUS server configuration.

# RADIUS Server Configuration

Correct the RADIUS server configuration.

## Task flow: RADIUS server configuration

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

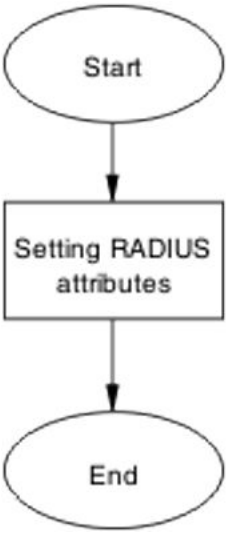



**Figure 61: RADIUS server configuration**

## Setting RADIUS attributes

### About this task

Ensure that the RADIUS attributes match the EAP user based policies.

### Procedure

Refer to the RADIUS server 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.

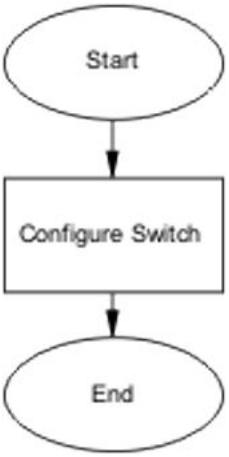



**Figure 62: EAP-NEAP unexpected port shutdown**

## Configure the switch ports

Configure ports to allow more unauthorized clients.

### Task flow: Configure the switch

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

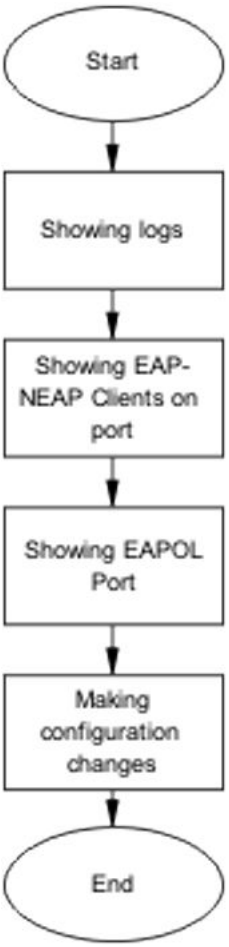



**Figure 63: Configure switch**

## Displaying logs

### About this task

If you need more detailed information to help you identify the reason for an unexpected EAP-NEAP port shutdown, you can display the log messages.

### Procedure

1. Use the **show logging** command to display the log messages.
2. Review the command output for errors and take appropriate action.

**Note:**

You can consult *Logs Reference — Avaya Ethernet Routing Switch 2000, 3000, 4000, and 5000 Series and Virtual Services Platform 7000 Series*, NN47216–600.

This is a consolidated log message reference document and it may provide additional information about log messages for your product.

## Displaying EAP-NEAP clients on a port

### About this task

Display EAP-NEAP clients on the port.

### Procedure

1. Use the **`show mac-address-table`** command to display the clients on the port.
2. Review the command output for anomalies.

## Displaying EAPOL port information

### About this task

Display EAPOL port information.

### Procedure

1. Use the **`show eapol port`** command to display EAPOL information for a port or ports.
2. Observe the command output for discrepancies or errors.

## Making changes

### About this task

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

### Procedure

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 mode.

# Chapter 10: Troubleshooting Secure Network Access Solution

Secure Network Access Solution (SNAS) issues can interfere with device operation and function.

The following work flow contains some common authentication problems.

## Troubleshooting Secure Network Access Solution work flow

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

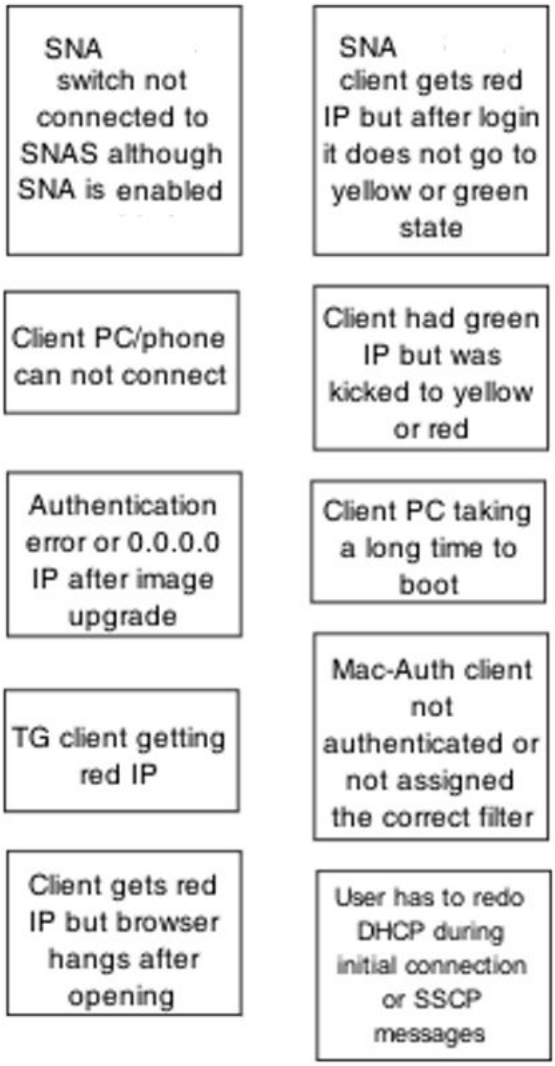



**Figure 64: Troubleshooting Secure Network Access Solution**

# SNA switch not connected to Secure Network Access Solution although SNA is enabled

Ensure the Secure Network Access Solution is displayed as connected to the ERS 5000 series switch.

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

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

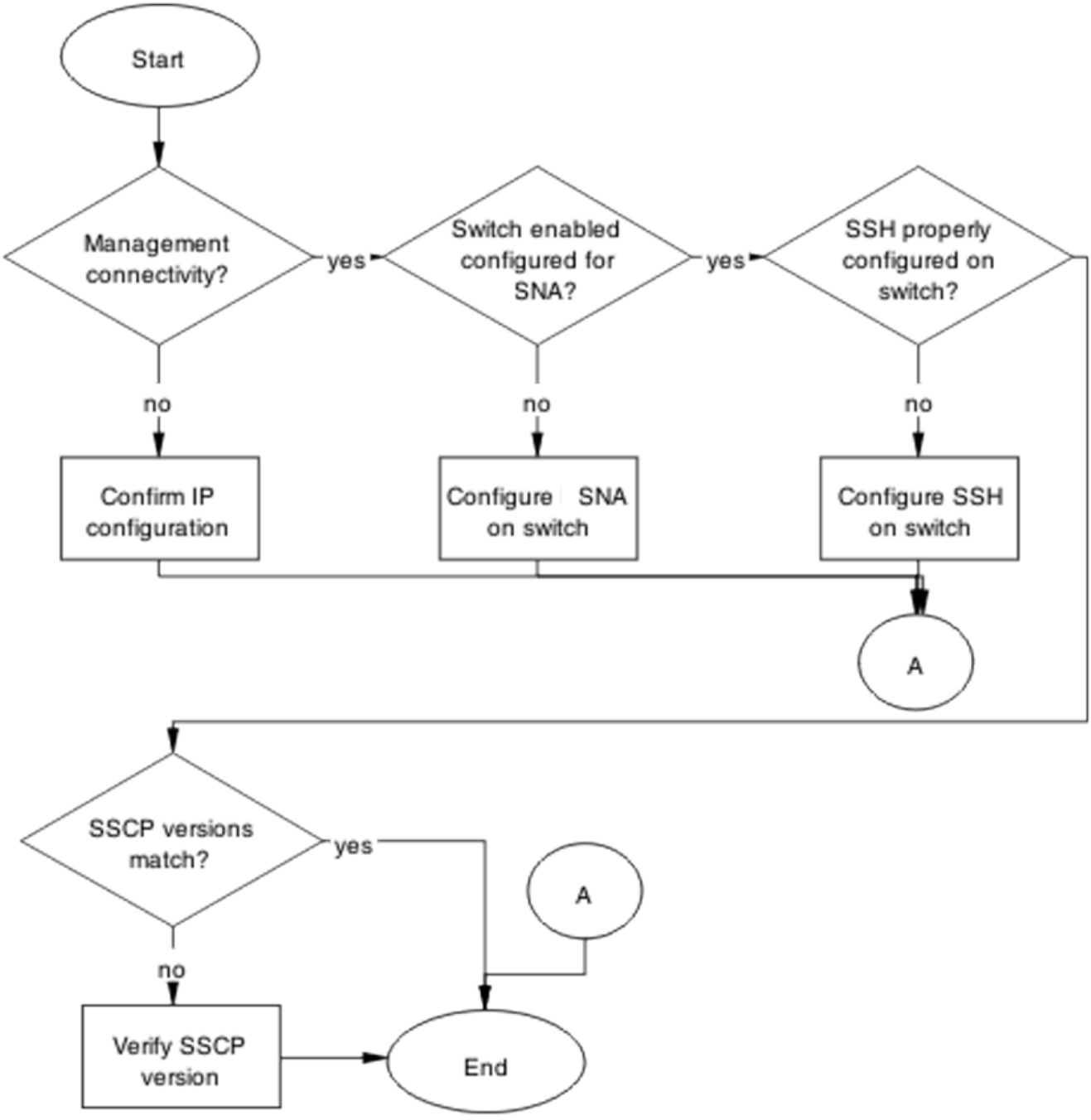



**Figure 65: Secure Network Access switch not connected to Secure Network Access Solution although Secure Network Access is enabled**

## Confirm IP Configuration

Correct IP connectivity to restore management connectivity.

## Task flow: Confirm IP configuration

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

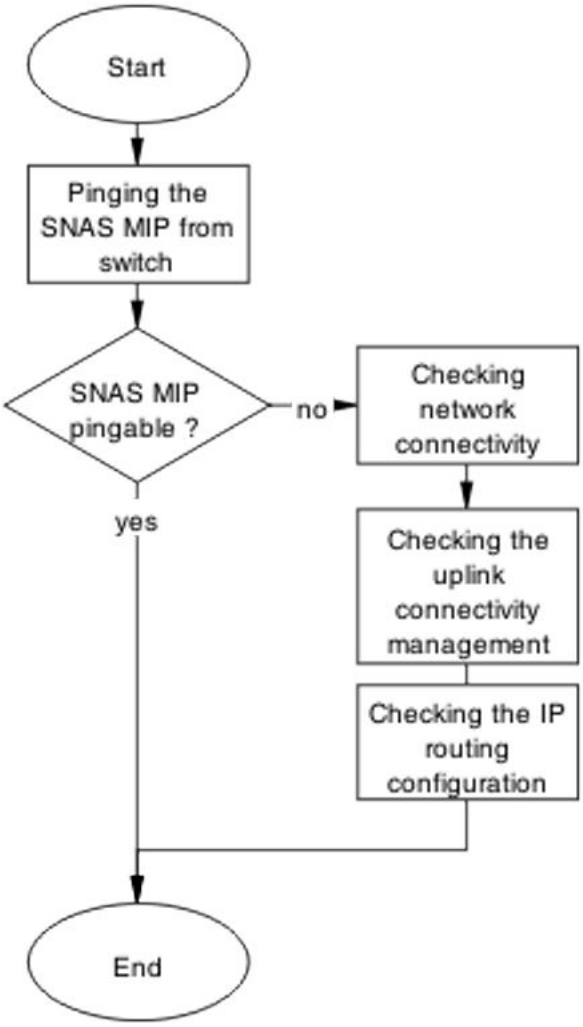



**Figure 66: Confirm IP configuration**

## Pinging the Secure Network Access Solution MIP from the switch

### About this task

Confirm IP connectivity from the switch.

### Procedure

1. Use the **`ping <IP>`** command from the switch.

2. Note the ping response displayed.

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

### About this task

Confirm that a valid network connection from the switch to Secure Network Access Solution exists.

### Procedure

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

## Checking the uplink connectivity management

Confirm that uplink connectivity exists.

### Procedure

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

## Checking IP routing configuration

### About this task

Confirm that the IP routing configuration is correct in Layer 3 mode

### Procedure

1. Use the **`show ip routing`** command to display IP routing information.
2. Confirm that Layer 3 mode is enabled.

# Configure Secure Network Access Solution on switch

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

## Task flow: Configure Secure Network Access Solution on switch

The following task flow assists you to ensure the ERS 5000 series device has Secure Network Access (SNA) enabled.

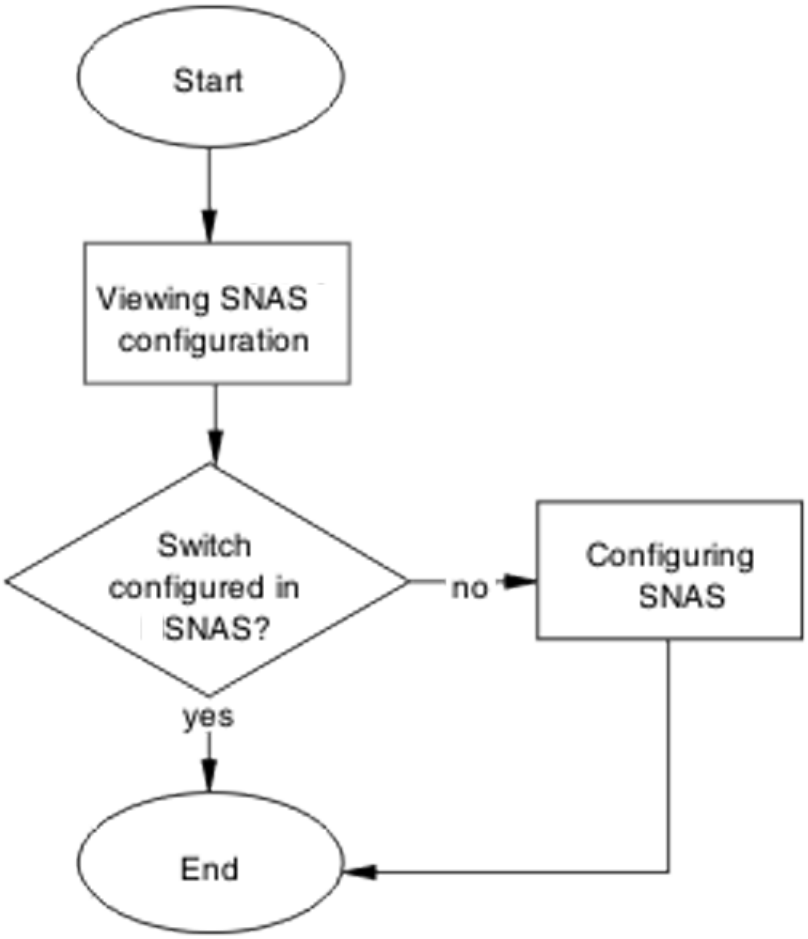



**Figure 67: Configure Troubleshooting Secure Network Access on switch**

## Checking Secure Network Access Solution configuration

### About this task

Verify the current configuration

### Procedure

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

2. Determine whether the switch is configured in the Secure Network Access Solution.

## Configuring Secure Network Access

### About this task

Configure Secure Network Access (SNA) for the switch

### Procedure

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

# Configure SSH on switch

Ensure that the SSH configuration on the switch is correct.

## Task flow: Configure SSH on switch

The following task flow assists you to ensure SSH is configured on the ERS 5o00 series device.

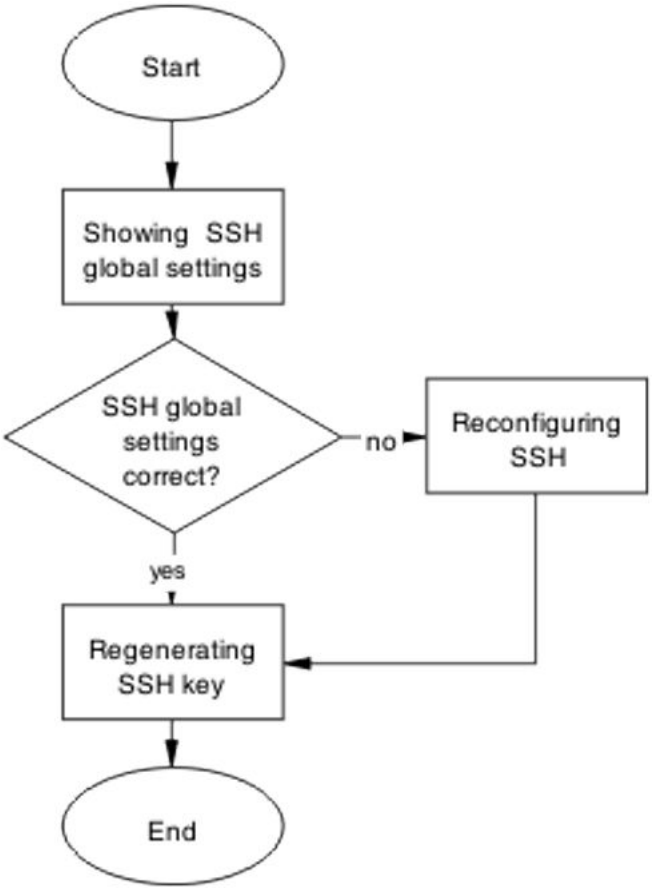



**Figure 68: Configure SSH on switch**

## Showing SSH globally

### About this task

Display the SSH configuration for the switch.

### Procedure

1. Use the **`show ssh global`** command to display the current configuration.
2. Review the command output to determine whether the SSH settings are correct.

## Reconfiguring SSH

### About this task

If the SSH settings are incorrect, use this procedure to change the SSH settings.

### Procedure

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

## Regenerating the SSH key

### About this task

If you determine that all SSH settings are correct but the problem persists, regenerate the SSH Key.

### Procedure

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

# 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 that the SSCP version on the ERS 5000 series switch is correct.

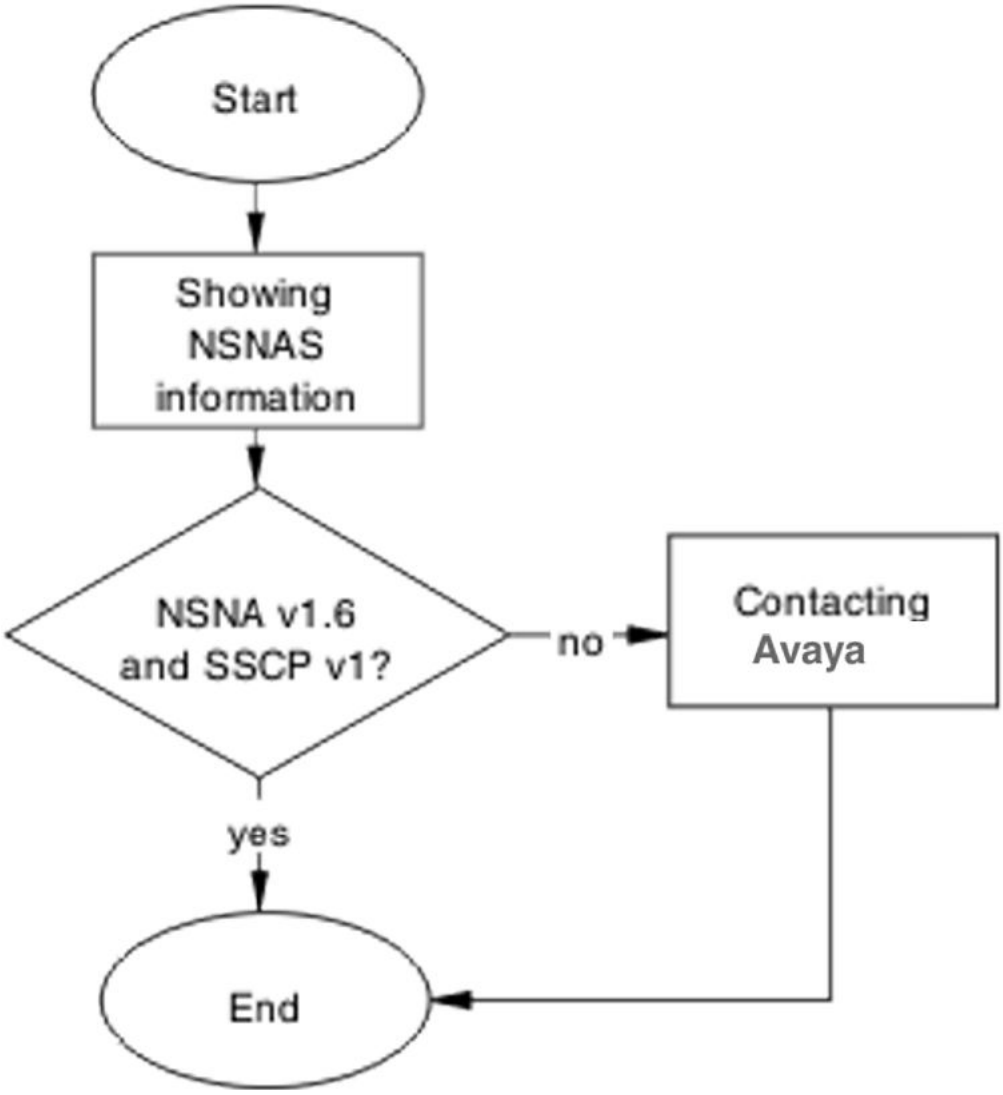



**Figure 69: Verify SSCP version**

## Show Secure Network Access

### About this task

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

### Procedure

1. Enter the **show SNA** command to display the configuration.
2. In SNAS, enter the **/info/local** command to display the software version for Secure Network Access Solution (SNAS).
3. Verify that the following appears on the switch configuration:
   • Secure Network Access Solution Connection Version: SSCPv1

   Higher versions are backward compatible.
4. Verify that the following appears on the Secure Network Access Solution:
   • Software version: 1.6.1.2

   Higher versions are be backward compatible.

## Contacting Avaya

### About this task

If you determine that there is a software discrepancy, follow the Avaya customer service contact procedures for your product.

# Client PC or phone cannot connect

You can use the information in this section to help you correct connection issues between the PC or phone and the switch.

## Work flow: Client PC or phone cannot connect

Use the following work flow to help you reconnect a client PC or phone that cannot connect to the switch.

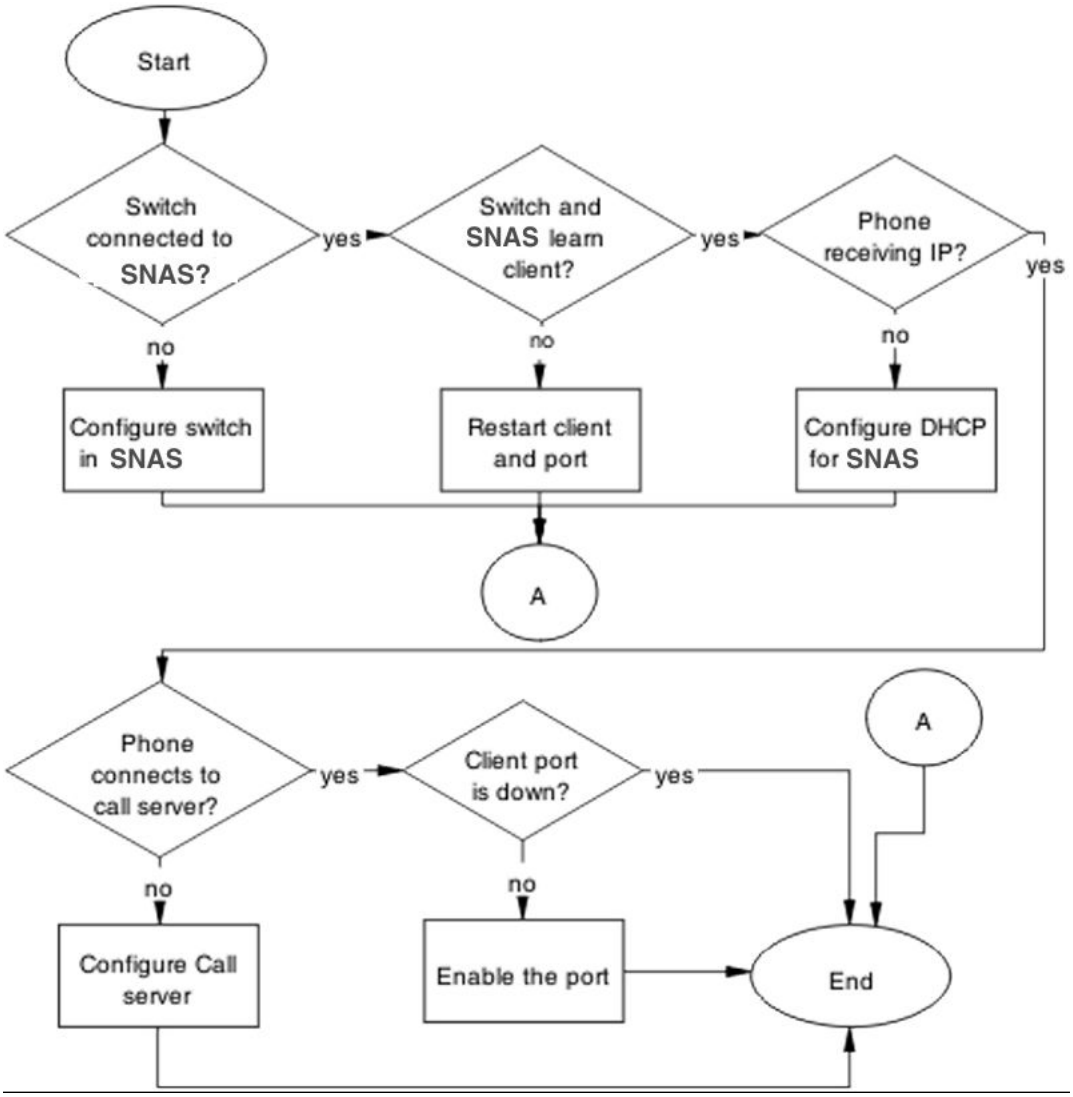



**Figure 70: Client PC or phone cannot connect**

# Configure the switch on Secure Network Access Solution

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

## Task flow: Configure the switch on Secure Network Access Solution

The following task flow assists you to enable the ERS 5000 Series switch on Secure Network Access Solution (SNAS).

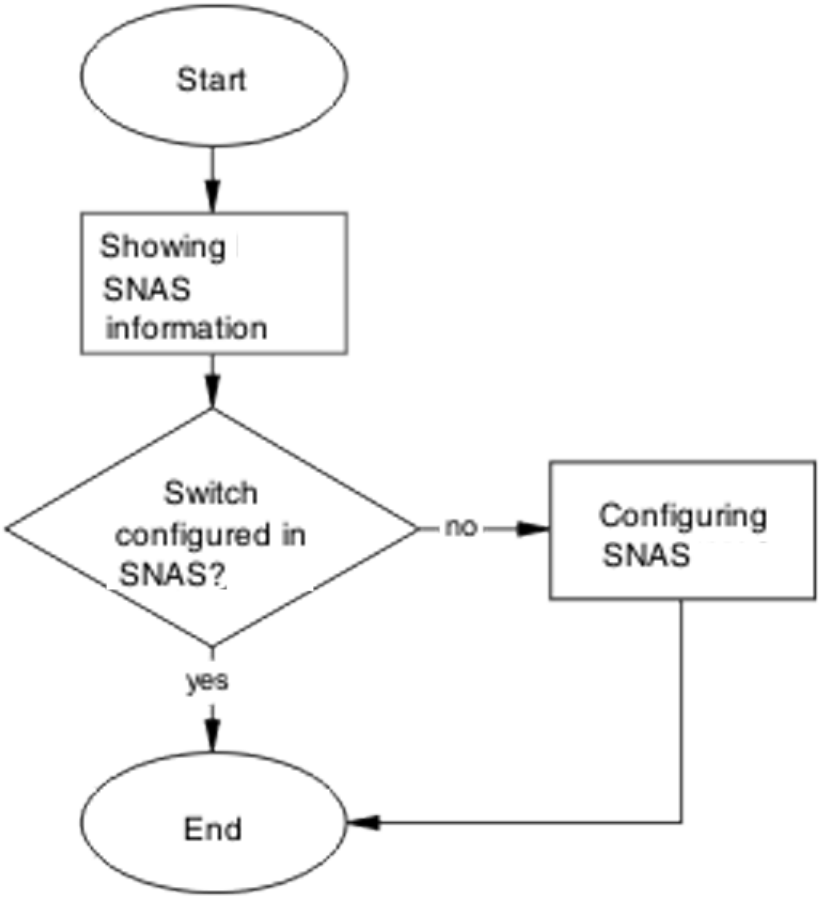



**Figure 71: Configure the switch on Secure Network Access Solution**

## Displaying Secure Network Access information

### About this task

Display SNA information to Verify the current configuration

### Procedure

1. In the SNA application, enter the **`cfg/domain 1/switch Y`** command followed by `cur`.
2. Review the command output to determine whether the switch is configured in the Secure Network Access Solution.

## Configuring Secure Network Access Solution for a switch

### About this task

Configure the Secure Network Access Solution (SNAS) with the settings for the ERS 5000 Series switch.

### Procedure

For information about configuring the switch on the application, refer to the Secure Network Access Solution Technical Configuration document.

# Restart client and port

Ensure that the client and port restart.

## Task flow: Restart client and port

Use the following task flow to help you restart both the client and port.

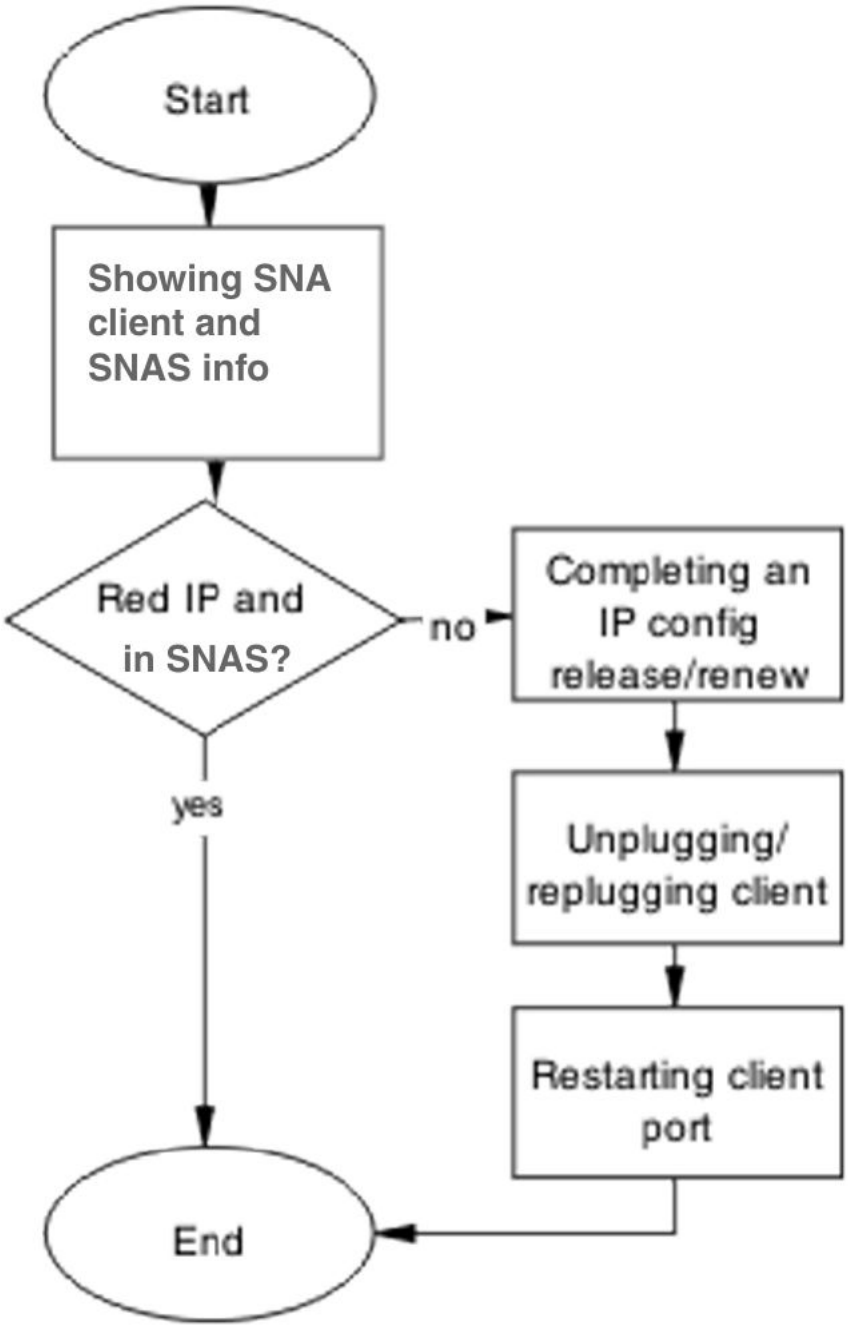



**Figure 72: Restart client and port**

## Displaying Secure Network Access client and Secure Network Access Solution information

### About this task

Use this procedure to display the Secure Network Access client and solution information.

### Procedure

1. In the switch ACLI, enter the **`show SNA client`** command.
2. Review the command output for errors or anomalies.
3. In Secure Network Access Solution, enter the **`info/switch 1 n`** command.
4. Compare the ACLI and SNAS command output for consistency.

## Completing an IP config release and renew

### About this task

When you need to force a full IP config release and renew of IP information:

### Procedure

1. Refer to the vendor documentation to perform an ipconfig release on the client PC.
2. Refer to the vendor documentation to perform an ipconfig renew on the client PC.

## Cycling the client connection to the network

### About this task

Physically disconnect client from the network, then reconnect the client to the network.

### Procedure

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

## Restarting the client port

### About this task

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

# Configure DHCP for Secure Network Access Solution

If the phone is still not getting an IP address you need to eliminate DHCP configuration issues.

## Task flow: Configure DHCP for Secure Network Access

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

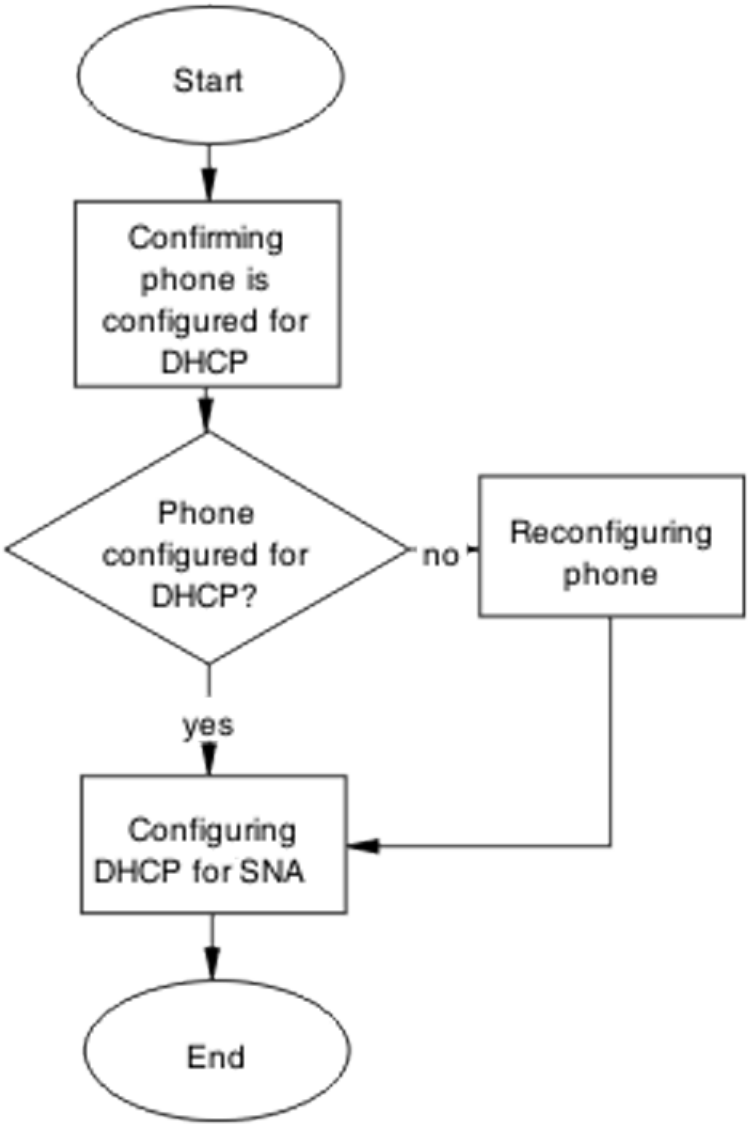



**Figure 73: Configure DHCP for Secure Network Access**

## Confirming phone is configured for DHCP

### About this task

Review phone vendor documentation to ensure that the phone is properly configured as a DHCP client.

## Reconfiguring phone

### About this task

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

## Configuring DHCP for Secure Network Access

### About this task

Review vendor documentation to help you change the settings of the DHCP server to work with Secure Network Access.

# Configure call server

Ensure that the call server is properly configured.

## Task flow: Configure call server

Use the following task flow to help you configure the call server.

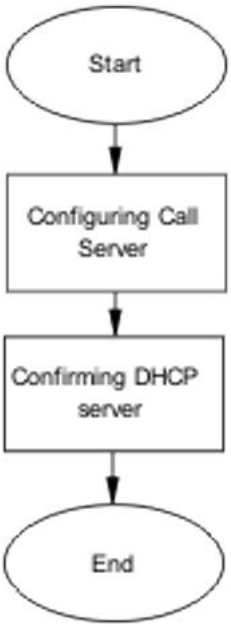



**Figure 74: Configure call server**

## Configuring call server

### About this task

Review the call server vendor documentation to ensure that the call server is properly configured.

## Configuring DHCP server

### About this task

Review the DHCP Server vendor documentation to ensure that the DHCP Server is properly configured.

# Enable the port

Enable the port when

- a new client PC or Phone (behind a hub) is not able to get an IP address or connect
- OR when the ERS 5000 series client port is down

## Task flow: Enable the port

Use the following task flow to help you enable the port.

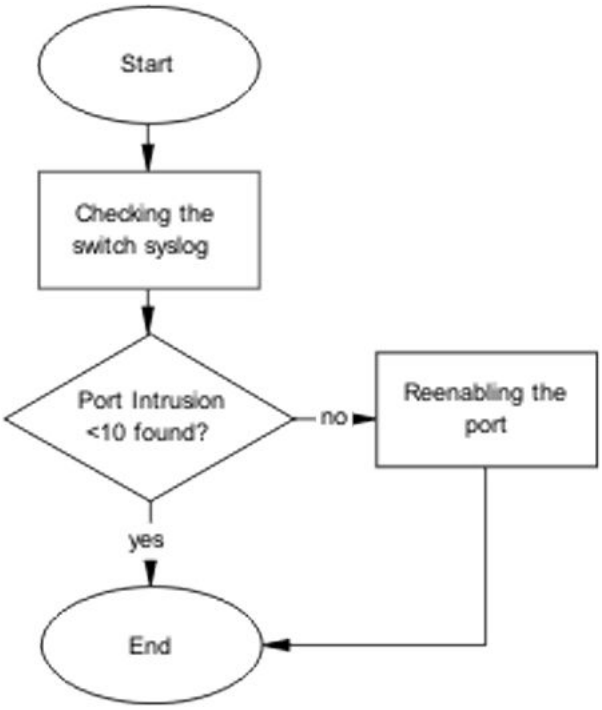



**Figure 75: Enable the port**

## Checking the switch log

### About this task

Review the switch log messages to determine if more than 10 intruders were detected.

### Procedure

1. Use the ACLI command **`show logging`** to display the log messages.
2. Review the command output and look for messages about intruders.

## Reenabling the port

### About this task

Re-enable the port after it was shut down due to a detected intrusion.

### Procedure

1. Use the ACLI command **`no shutdown <port>`** to re-enable a port that was disabled due to detection of an intrusion.
2. Observe switch behavior to ensure that there are no errors after you execute the command.

# Authentication error or 0.0.0.0 IP after image upgrade

After an image upgrade, some common problems that lead to errors can occur. This work flow and the accompanying procedures can help you eliminate these common problems.

## Work flow: Authentication error or 0.0.0.0 IP after image upgrade

You can use the following work to flow to help you find the solution to authentication errors or an IP address of 0.0.0.0 that can occur immediately following an upgrade of the image.

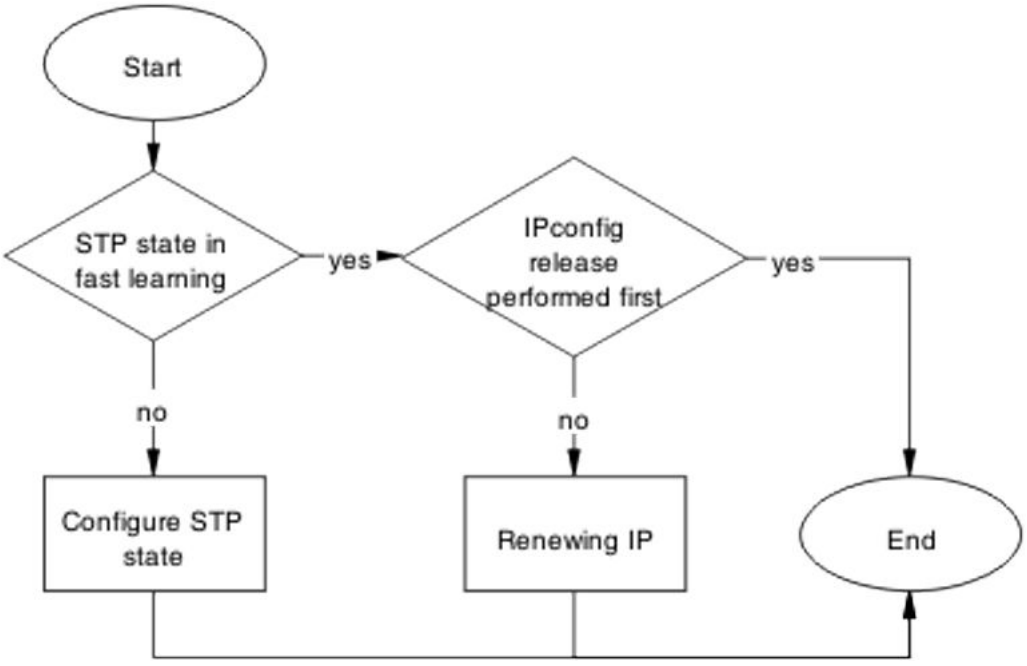



**Figure 76: Authentication error or 0.0.0.0 IP after image upgrade**

# Configure STP state

If ports come up too fast you can place the STP state in fast learning mode.

**Important:**

To prevent loops, ensure that your clearly understand the consequences of performing this action on an uplink.

## Task flow: Configure STP state task flow

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

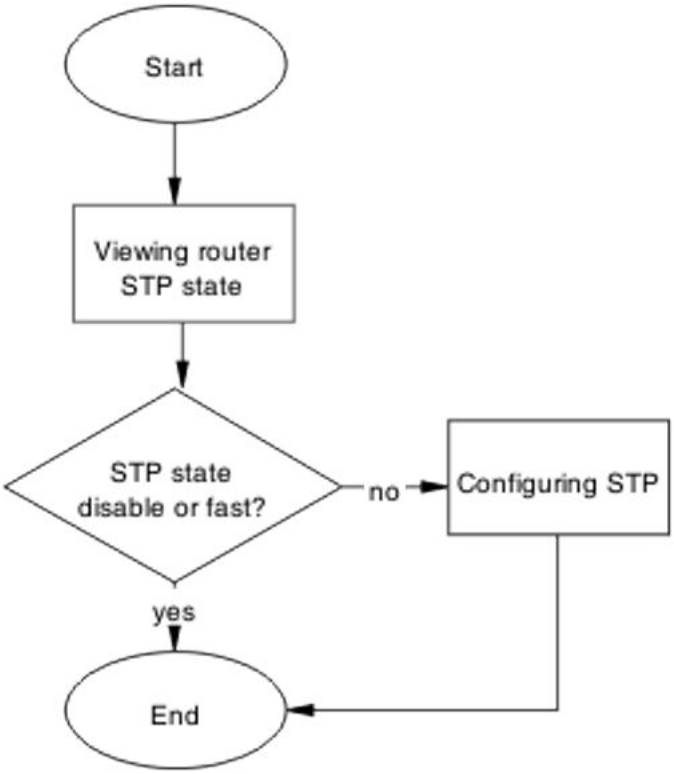



**Figure 77: Configure STP state**

## Viewing the router STP state

### About this task

Use the show command to determine the STP state on the router.

### Procedure

Use the **show spanning-tree port** command to display the router STP state.

STP states are:

- disable
- fast

## Configuring the STP state

### About this task

Use this procedure to configure the STP state as fast learning and to verify the STP state change.

### Procedure

1. Use the **spanning-tree port 1 learning fast** command to set the STP state to fast learning.
2. Use the **show spanning-tree port 1** command to verify the STP state.

# Renewing the IP address

To restore the connection, renew the IP address.

## Task flow: Renewing the IP address

You can use the following task flow to help you release and renew an IP address correctly.

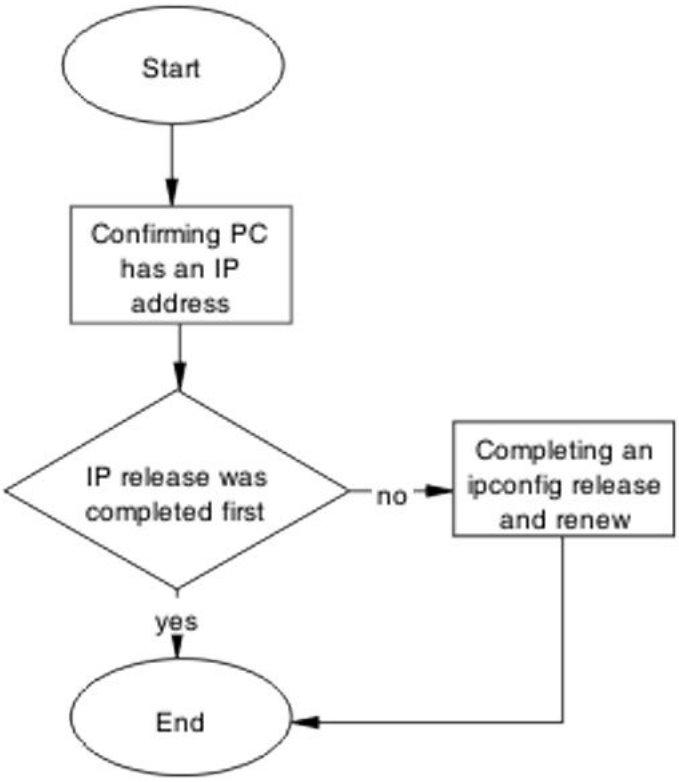



**Figure 78: Renewing IP**

## Confirming that the PC has an IP address

### Before you begin

- Refer to the PC vendor documentation to ensure that you follow recommendations for the specific PC

### About this task

Use the following procedure to confirm that the PC has a valid IP address.

### Procedure

1. Use the **`ipconfg /all`** command to view the IP information for the PC.
2. Record the IP address and additional IP information.

## Completing an ipconfig release and renew

### Before you begin

- Refer to the PC vendor documentation to ensure that you adhere to PC-specific recommendations

### About this task

Use this procedure to help you perform an ipconfig /release operation prior to an ipconfig / renew operation.

### Procedure

1. Use the **`ipconfg /release`** command to release the IP information for the PC.
2. Use the **`ipconfg /renew`** command to renew the IP information for the PC.

# TG client getting red IP

This section can help you eliminate the switch blocking traffic to NSAS.

## Work flow: TG client receives a red IP

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

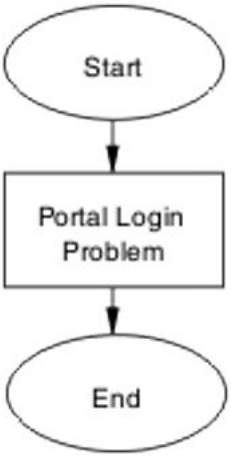



**Figure 79: TG Client getting red IP**

# Portal Login Problem

If required, eliminate the location of the interruption so you can properly configure the NSAS port IP

## Task flow: Portal login problem

The following task flow can assist you to eliminate the interruption so you can configure the NSAS port IP.

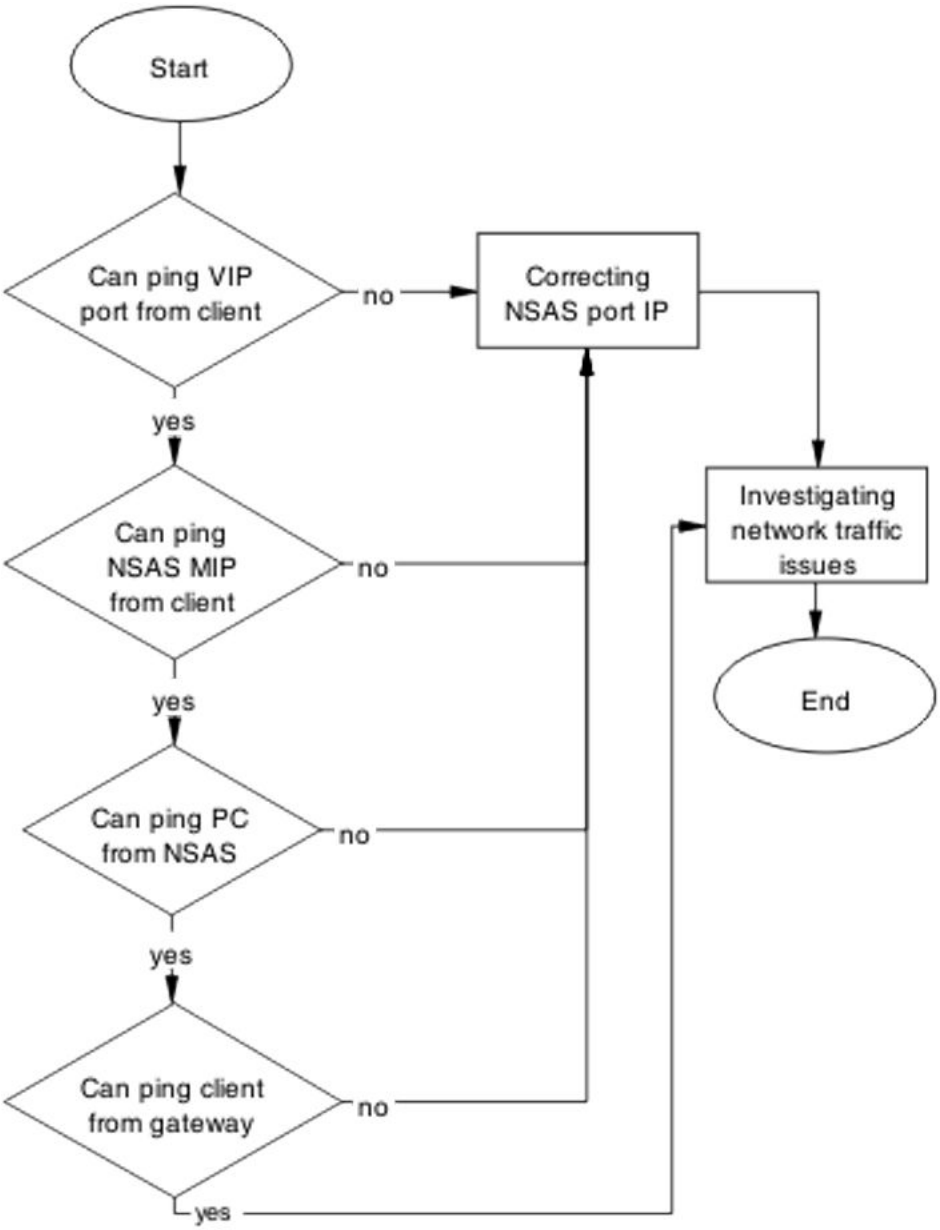



**Figure 80: Portal login problem**

## Correcting SNAS port IP

### About this task

Use this procedure to help you make changes to Secure Network Access Solution (SNAS) port IP.

### Procedure

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

## Investigating network traffic issues

### About this task

Eliminate network traffic issues that impede the browser.

Use local documentation and protocols to investigate network traffic issues. You can also refer to Planning and Engineering documentation.

# Client gets red IP but browser hangs after opening

Terminate the browser session and restart the browser.

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

You can use the following work flow to assist you to correct the situation when a client obtains a red IP but the browser hangs after it appears.

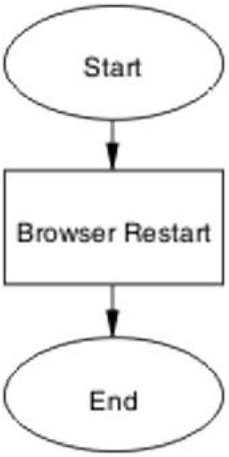



**Figure 81: Client gets red IP but browser hangs after opening**

# Browser restart

To regain connectivity, restart the browser.

## Task flow: Browser restart

The following task flow lists tasks to assist you to restart the browser.

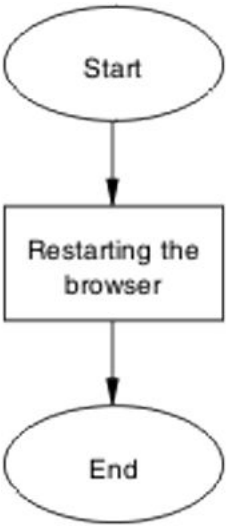



**Figure 82: Browser restart**

## Restarting the browser

### About this task

Use this procedure to fully close the browser and restart it.

### Procedure

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

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

Secure Network Access Solution communication failed; you must correct the failure that allows the client to maintain the red state for too long.

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

The following work flow can help you find the way to fix a Secure Network Access client that obtains a red IP but fails to move to yellow or green state after login.

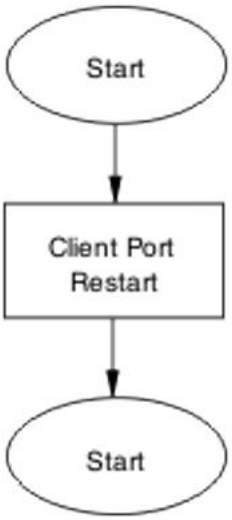



**Figure 83: Secure Network Access client gets red IP but after login it does not go to yellow or green state**

## Client port restart

Shut the client link down and restart it.

### Task flow: Client port restart

The following task flow can help you to restart the client port.


**Figure 84: Client port restart**

### Restarting the client port link

#### About this task

Use the procedures in the vendor documentation to help you shut down the client port and restart it.

## Client had green IP but status was changed to yellow or red

Correct the communication issue causing the IP status to change.

## Work flow: Client had green IP but status was changed to yellow or red

The following work flow can help you determine the solution for a client that had a green IP that changed to yellow or red.

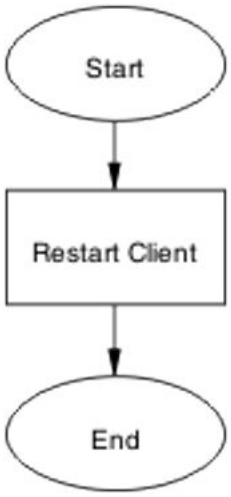



**Figure 85: Client had green IP but was kicked to yellow or red**

# Restart client

Shut down then restart the client to regain communication.

## Task flow: Restart client

The following task flow can help you restart the client.

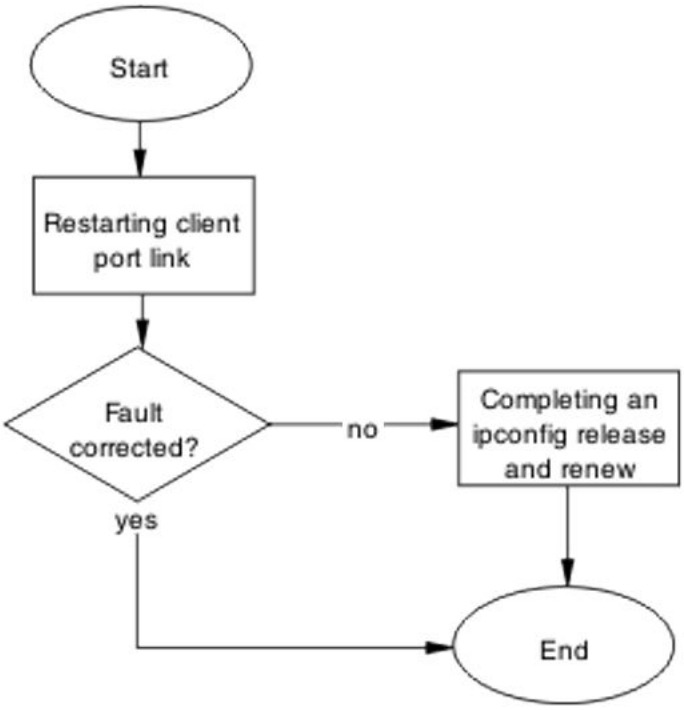



**Figure 86: Restart client**

## Restarting client port link

### About this task

Shut down the client port and then restart it.

### Procedure

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

## Completing an ipconfig release and renew

### Before you begin

- Refer to the vendor documentation for the correct procedures to perform ipconfig release and renew operations

### About this task

Perform an ipconfig release prior to an ipconfig renew.

### Procedure

1. Use the vendor procedure to enter the **`ipconfg /release`** command to release the IP information of the PC.
2. Use the vendor procedure to enter the **`ipconfg /renew`** command to renew the IP information of the PC.

# Client PC slow to start

Correct a port configuration issue that is causing the PC to experience a long startup time.

## Work flow: Client PC is slow to start up

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

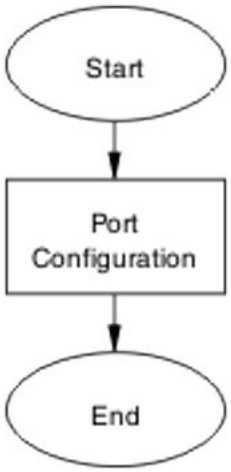



**Figure 87: Client PC taking a long time to boot**

## Port configuration

Identify and open the ports needed by the client PC to log into the red VLAN.

## Task flow: Port configuration

The following task flow can help you to correct the port configuration.

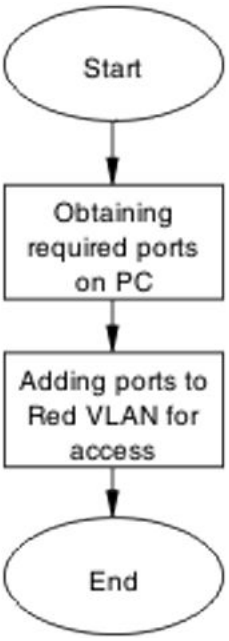



**Figure 88: Port configuration**

## Obtaining ports on the PC

### About this task

Identify the ports that are required for the VLAN.

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

## Adding ports to red VLAN for access

### About this task

Ensure the ports you identified in the previous task are added to the red VLAN so that all traffic has access.

### Procedure

Refer to the document *Avaya Ethernet Routing Switch 5500 Series Configuration — Quality of Service* to obtain the procedures and commands required to add the ports to the red VLAN.

### Example

Adding ports to a VLAN:

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

:

## Mac-Auth client is not authenticated or was not assigned the correct filter

Take corrective action so that the client can authenticate.

**Note:**

If the correct filter was not assigned to the client, authentication can fail.

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

The following work flow can help you determine the solution for a MAC authentication client that does not authenticate or that was not assigned the correct filter.

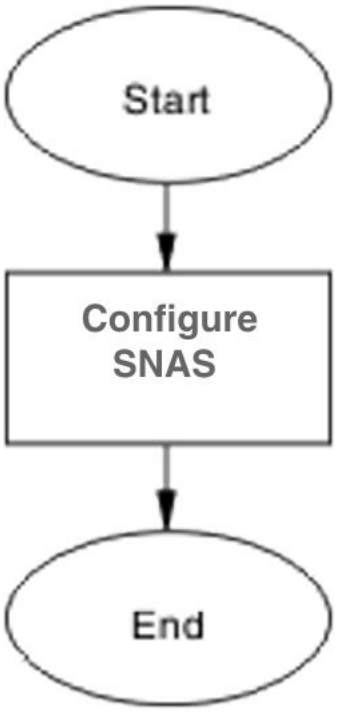



**Figure 89: Mac-Auth client not authenticated or not assigned the correct filter**

# Configure Secure Network Access Solution

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

## Task flow: Configure Secure Network Access Solution

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

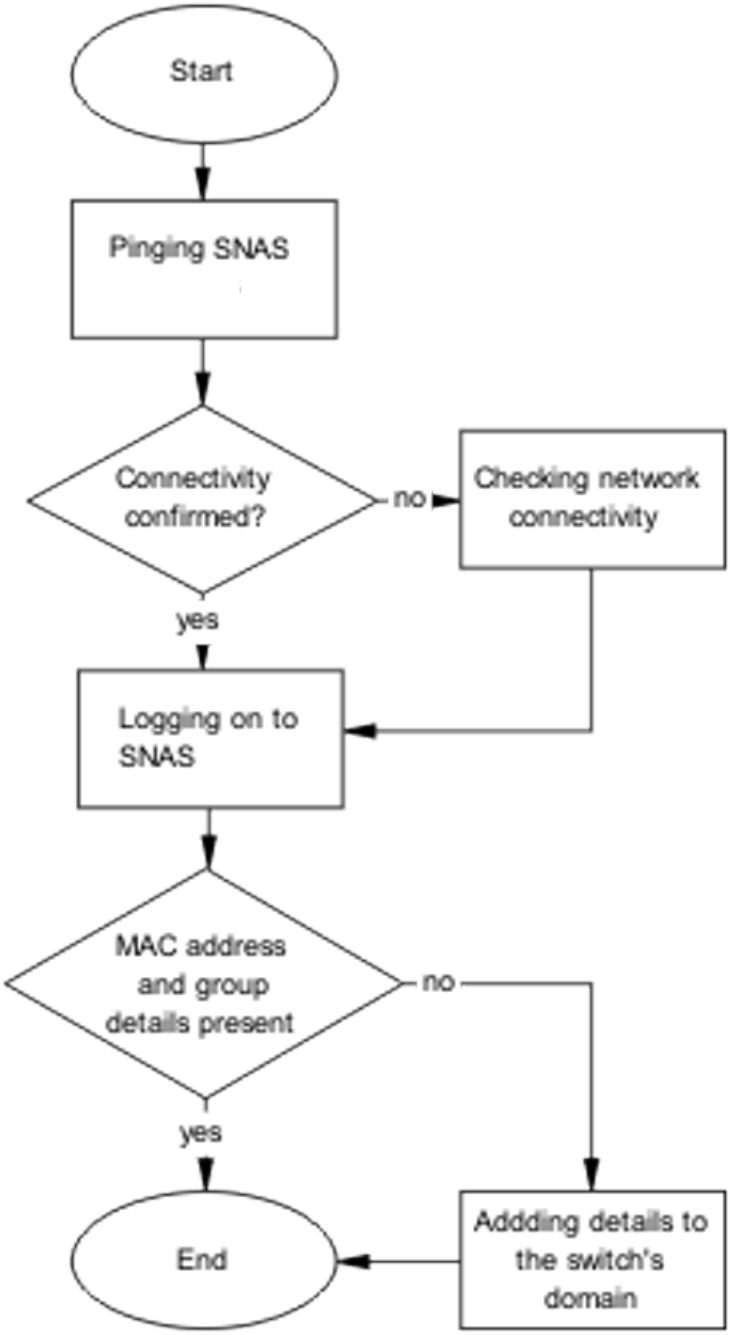



**Figure 90: Configure Secure Network Access Solution**

## Pinging Secure Network Access Solution

### About this task

Verify network connectivity.

### Procedure

1. Use the ping **<SNASIP>** command to ensure connectivity.
2. Review the command output to determine network connectivity status.

## Checking network connectivity

### About this task

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

### Procedure

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

## Logging on to Secure Network Access Solution

### About this task

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

### Procedure

1. Use vendor procedures to log onto the Secure Network Access Solution.
2. Review the *macdb* list for the switch domain.

## Adding details to the switch domain

### About this task

Add MAC address and group details to the switch domain.

### Procedure

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

# Chapter 11: Troubleshooting layer 2 and layer 3

Layer 2 and layer 3 issues can interfere with device operation and function. This chapter includes some possible ARP, OSPF, RIP, and VRRP problems.

## 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 dependant upon each other normally.

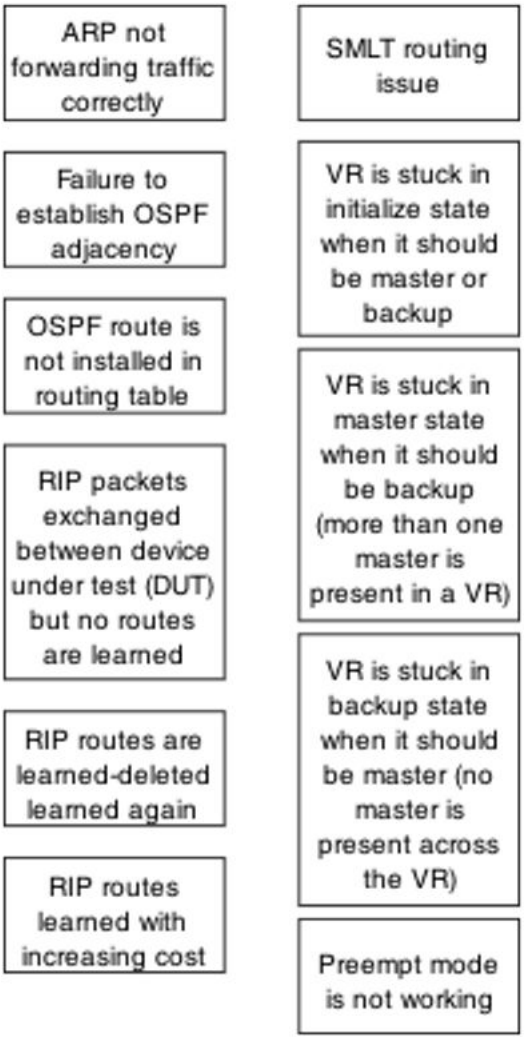



**Figure 91: Troubleshooting Layer 2 and Layer 3**

# ARP not forwarding traffic correctly

Address Resolution Protocol (ARP) table and routing table information can help you determine whether Layer 3 traffic is forwarding correctly or not.

## Work flow: Troubleshooting ARP

The following work flow can help you to determine why ARP is not forwarding traffic as expected and the procedures in this section provide some suggested solutions.

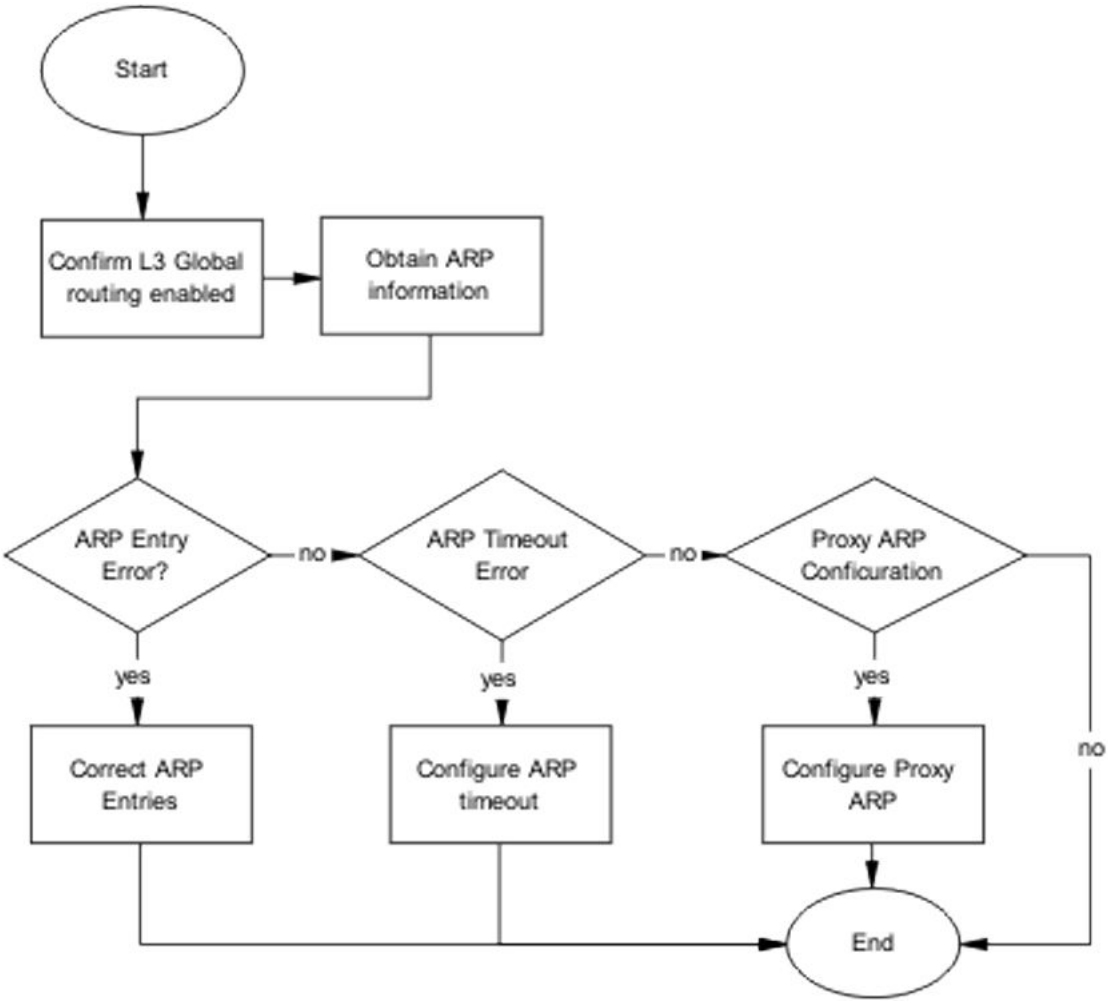



**Figure 92: Troubleshooting ARP**

# Confirming that global L3 routing is enabled

This section helps you confirm that L3 global routing is enabled.

## Task flow: Confirming global L3 routing

### About this task

The following task flow and the procedures in this section can help you to determine the status of Layer 3 routing and enable L3 routing globally.

### Procedure

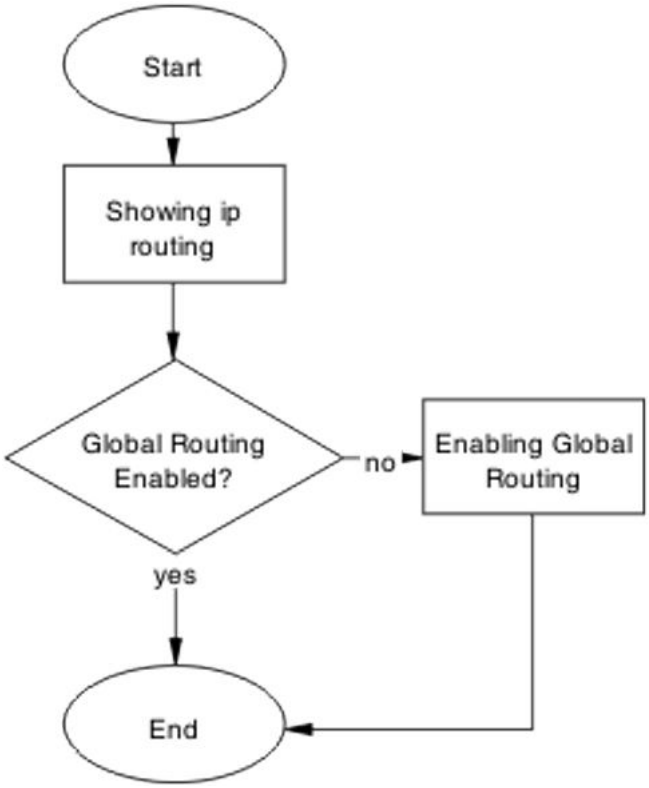



**Figure 93: Confirming global L3 routing**

## Displaying IP Routing information

### About this task

Display IP Routing Information for the switch to determine whether it is enabled.

### Procedure

1. Enter the ACLI Privileged EXEC command mode.
2. At the prompt, type the **`show ip routing`** command.
3. Review the command output to determine whether or not IP Routing is enabled.

### Enabling IP Routing globally

#### About this task

If you determine that IP Routing is disabled, use this procedure to enable IP Routing globally on the switch.

#### Procedure

1. Enter the ACLI Global Configuration mode.
2. At the command prompt, type the **`ip routing enable`** command to enable IP Routing.

## Obtain ARP information

Display and compare ARP information using the methods described in this section.

### Task flow: Obtaining ARP information

The following task flow and the procedures in this section can help you to obtain ARP information from ACLI, EDM, and SNMP.

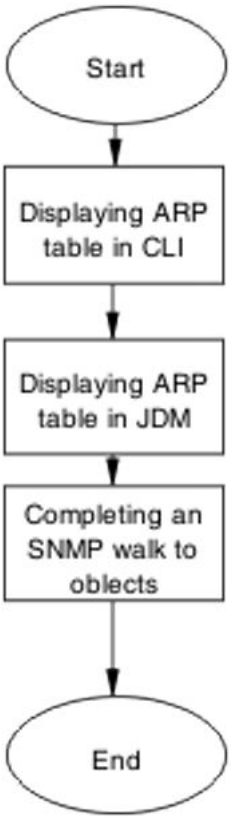



**Figure 94: Obtaining ARP information**

## Displaying the ARP Table in ACLI

### About this task

Use the following procedure to display ARP table information in ACLI.

### Procedure

1. Enter the ACLI Privileged EXEC mode.
2. At the prompt, type the **`show ip arp`** command.
3. Review the command output.
   From software Release 5.1 onward, the number of ARP entries is also displayed.

## Displaying ARP table information in EDM

### About this task

Use the following procedure to obtain ARP table information in EDM.

### Procedure

1. In EDM, navigate to **IP Routing** > **IP** > **ARP**.
2. Review the information on the ARP page.

## Completing an SNMP walk to objects

### About this task

Use the SNMP walk to assist in the diagnosis of the ARP situation.

### Procedure

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. Enter the **SNMP walk** command on the **ipNetToMediaType** object.

# Correct ARP entries

You can use ACLI, EDM, or SNMP to correct ARP entries.

## Task flow: Correct ARP entries

The following task flow can help you to correct ARP entries using ACLI, EDM, or SNMP.

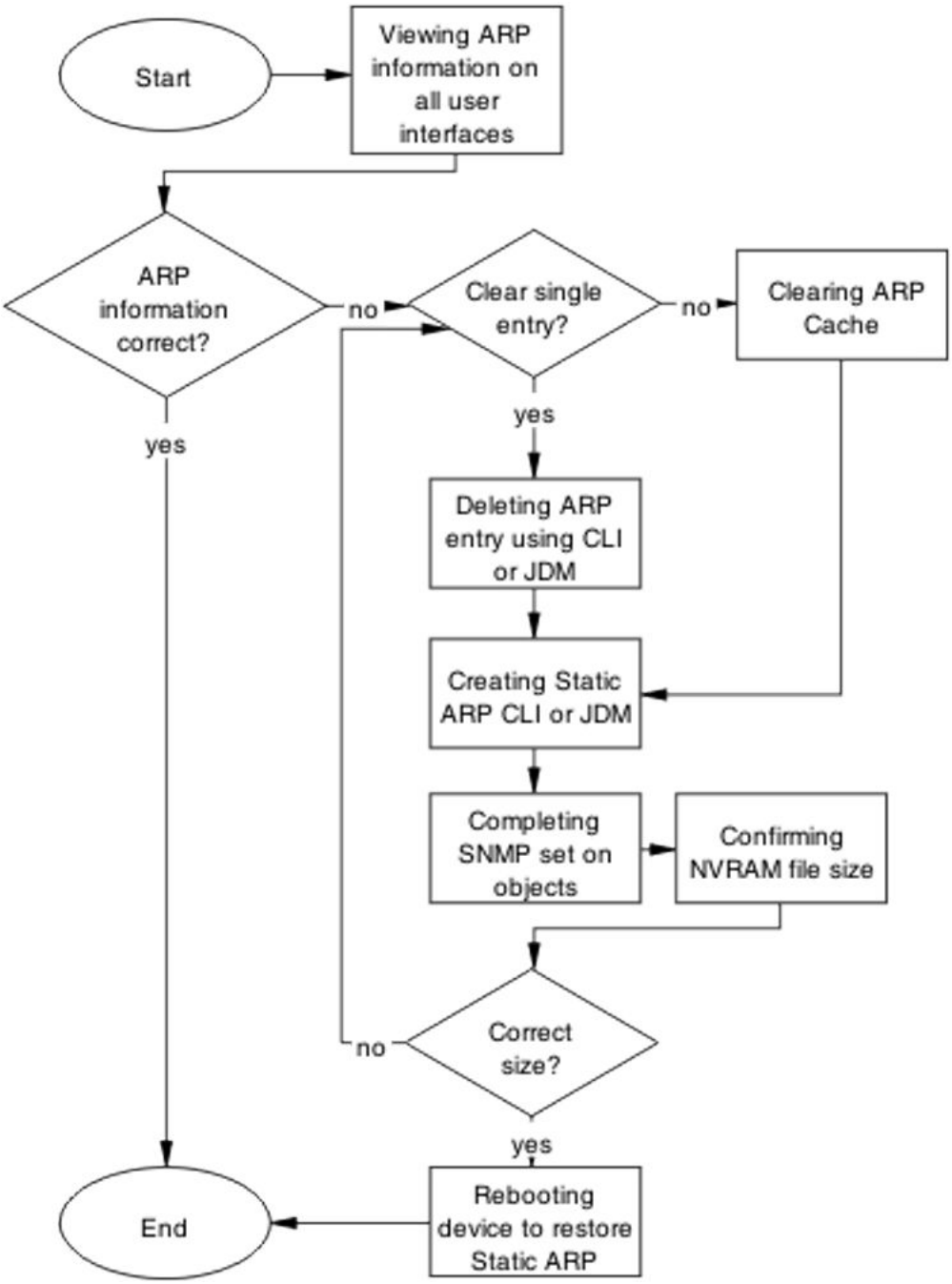



**Figure 95: Correct ARP entries**

## Confirming that ARP entries are correct

### About this task

Use this procedure to compare ARP entries to ensure they are correct.

### Procedure

1. Review the ACLI, EDM, and SNMP ARP information.
2. Compare ARP table entries for discrepancies.

## Clearing the ARP cache

### About this task

Use the following procedure to completely clear the ARP cache of both static and dynamic entries.

### Procedure

1. Enter the Privileged EXEC mode in ACLI.
2. At the prompt, type the **`clear arp-cache`** command.

## Deleting an ARP entry in ACLI or EDM

### About this task

You can use ACLI or EDM to remove individual ARP entries.

#### Procedure for ACLI

### Procedure

1. Enter the ACLI Privileged Exec mode.
2. At the prompe, type the **`no ip arp <a.b.c.d>`** command to delete the entry.

#### Procedure for EDM

### Procedure

1. In EDM, select **IP Routing** > **IP** > **ARP**
2. In the ARP table, select the entry to delete.
3. Click **delete**.

## Creating Static ARP entries in ACLI or EDM

### About this task

Use the following procedures to create static ARP entries in ACLI and EDM.

#### Creating static ARP entries using ACLI

### Procedure

1. Enter the Global Configuration mode in ACLI.
2. At the prompt, type the **`ip arp <a.b.c.d> <h.h.h> <unit/port> <vid>`** command to create the static ARP entry.

#### Creating static ARP entries using EDM

### Procedure

1. In EDM, select **IP Routing** > **IP** > **ARP**.
2. Enter the values required and press the **Insert** button.

## Deleting an ARP entry using SNMP

### About this task

You can use SNMP to remove individual ARP entries.

### Procedure

1. Set the corresponding **ipNetToMediaType** to value “2” .
2. Review the display to ensure that the entry was removed.

## Setting objects with SNMP

### About this task

SNMP objects for IP Net to Media can be set if required.

### Procedure

1. Use the **`SNMP set`** command on the **ipNetToMediaIfIndex** object.
2. Use the **`SNMP set`** command on the **ipNetToMediaPhysAddress** object.

3. Use the **SNMP set** command on the **ipNetToMediaNetAddress** object.
4. Use the **SNMP set** command on the **ipNetToMediaType** object.

## Confirming NVRAM file size

### About this task

Use the information and procedure in this task to ensure that the NVRAM file size conforms to the correct parameters.

**Prerequisites:**

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

### Procedure

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

## Rebooting the device to restore static ARP

### About this task

You can reboot the device to restore the static ARP entries.

### Procedure

1. Reboot the device.
2. Ensure that the device has rebooted correctly.

# Configure ARP timeout

This section provides tasks and procedures that you can use to change the ARP timeout value.

## Task flow: Configure ARP timeout

Use the following task flow to help you change the ARP timeout value.

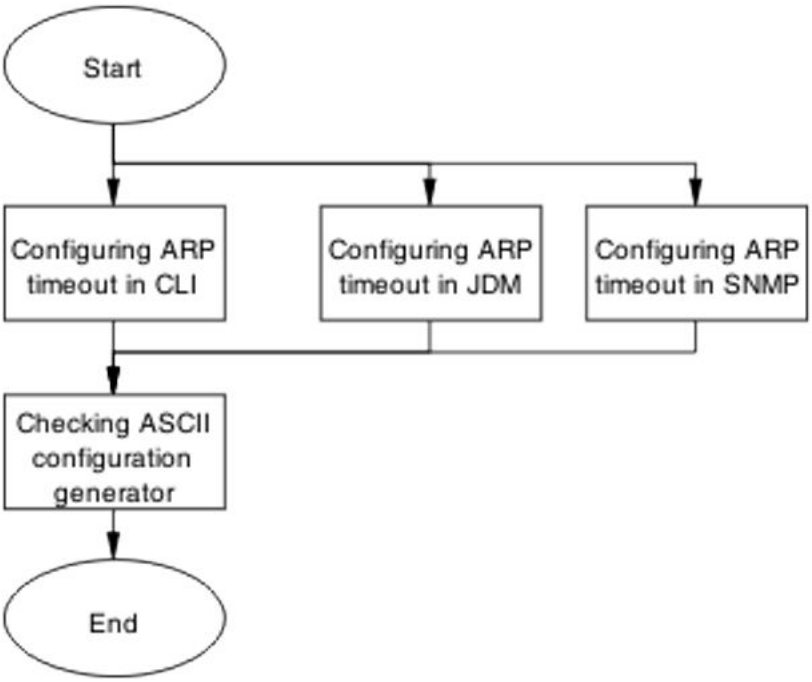



**Figure 96: Configure ARP timeout**

## Configuring ARP timeout using ACLI

### About this task

You can use ACLI toset the ARP timeout.

### Procedure

1. Open ACLI in the Global Configuration mode.
2. At the prompt, enter the **`ip arp timeout <value>`** command.

## Configuring ARP timeout using EDM

### About this task

You can use EDM to set the ARP timeout.

### Procedure

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

## Configuring ARP timeout using SNMP

### About this task

You can use Simple Network Management Protocol (SNMP) to set the ARP timeout.

### Procedure

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

## Checking ASCII configuration generator

### About this task

You can use the ASCII Configuration Generator to display the static ARP entries and for the ARP timeout.

### Procedure

1. Use the **`show running-config`** command .
2. Review the output in the L3 section.

# Configuring the proxy ARP

### About this task

You can enable or disable the Proxy ARP.

## Task flow: Configuring the proxy ARP

You can use the following task flow to help you enable or disable Proxy ARP.

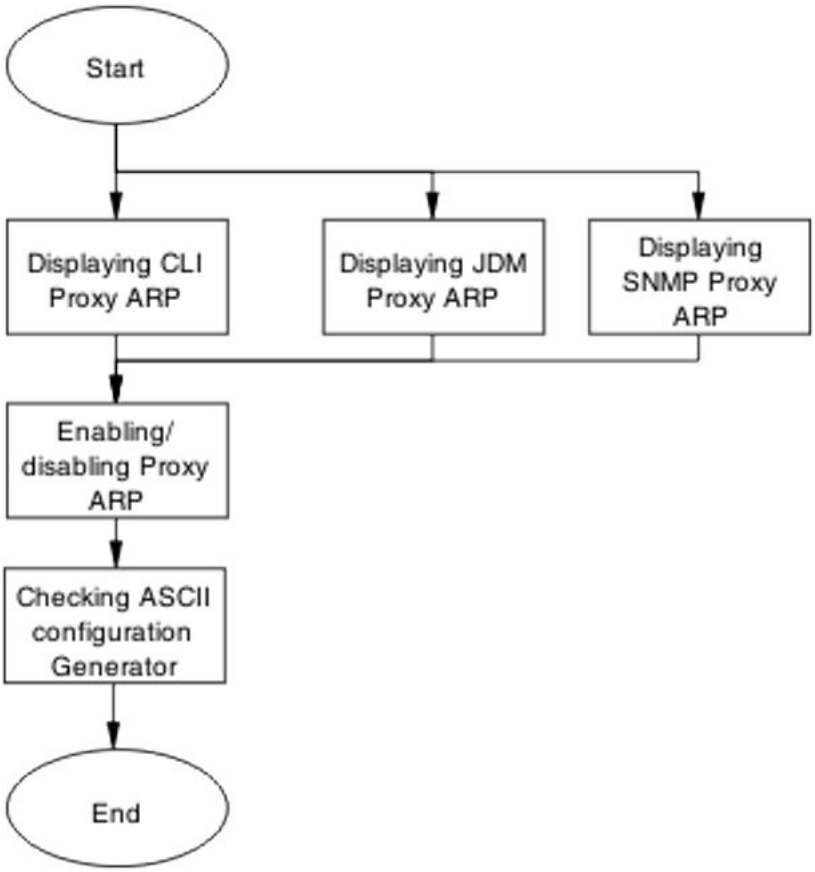



**Figure 97: Configuring the proxy ARP**

## Displaying and enabling proxy ARP using ACLI

### About this task

You can use ACLI to set the Proxy ARP.

### Procedure

1. Open ACLI Privileged Exec mode.
2. At the prompt, enter the **`show ip arp-proxy interface`** command.
3. At the prompt, enter the **`show ip arp-proxy interface [vlan <vid>]`**command.
4. Open ACLI IP VLAN configuration mode.
5. To enable proxy ARP, at the prompt enter the **`ip arp proxy [enable]`** command.

   To disable proxy ARP, at the prompt enter the **`no ip arp proxy [enable]`** command.

To return proxy ARP to the default state, at the prompt enter the **default ip arp proxy [enable]** command.

## Displaying Proxy ARP using EDM

### About this task

You can use EDM to set proxy ARP.

### Procedure

1. Navigate to **IP Routing** > **IP** > **ARP Interfaces**.
2. Select an interface.
3. Set desired value in the **DoProxyfield**.

## Displaying proxy ARP using SNMP

### About this task

You can use SNMP display proxy ARP.

### Procedure

1. Use the **snmp walk** command on the **rcArpExtEntDoProxy** object.
2. Review the output for errors.

## Enabling or disabling proxy ARP

### About this task

You can use the procedures in this section to enable or disable proxy ARP.

By default, ARP is disabled.

#### Enabling or disabling proxy ARP using ACLI

### Procedure

1. Go to the ACLI Global Configuration mode.
2. At the prompt, enter one of the following commands.
   - **ip arp proxy enable** command to enable proxy ARP

- **`no ip arp proxy [enable]`** command to disable proxy ARP
- **`default ip arp proxy [enable]`** command to set proxy ARP to the default value

3. Review the command output details under the L3 section.

### Enabling or disabling Proxy ARP using EDM

#### Procedure

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

### Enabling or disabling proxy ARP using SNMP

You can use SNMP to enable or disable proxy ARP.

#### Procedure

1. Enter the **`SNMP set`** command on the **rcArpExtEntDoProxy** object.
2. Review the command output for errors.

## Using ASCII Configuration Generator to check proxy ARP configuration

#### About this task

You can use the ASCII Configuration Generator (ACG) to check proxy ARP configuration.

#### Procedure

1. Enter the command **`show running-config`**.
2. Review the command output under the following subsections:
   - L3 Protocols
   - Proxy ARP

# Failure to establish OSPF adjacency

You may need to correct the OSPF parameters to ensure that adjacencies are established.

# Work flow: Failure to establish an OSPF adjacency

You can use the following work flow to help you determine the solution for adjacencies that do not form.

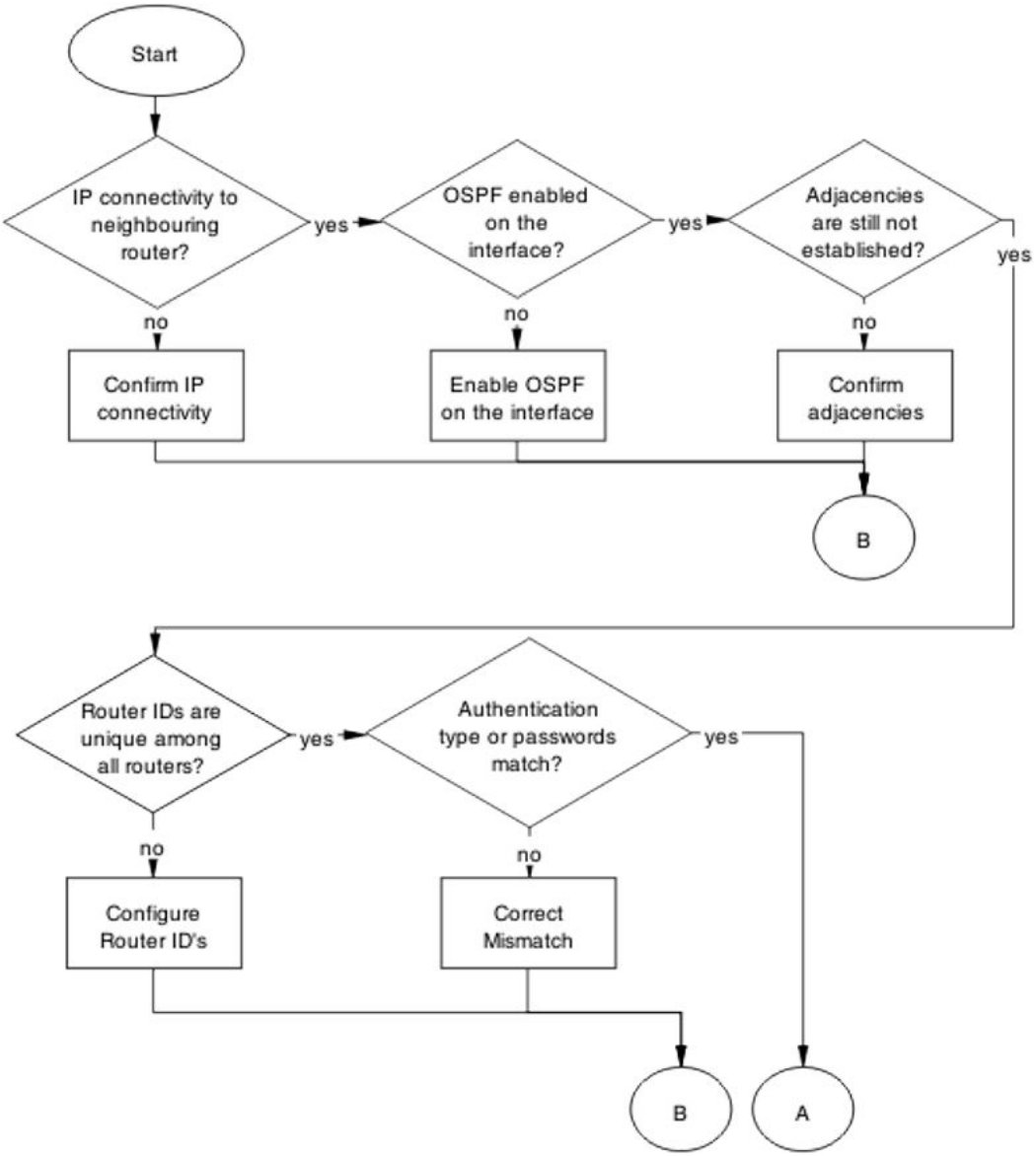



**Figure 98: Failure to Establish an OSPF adjacency part 1**

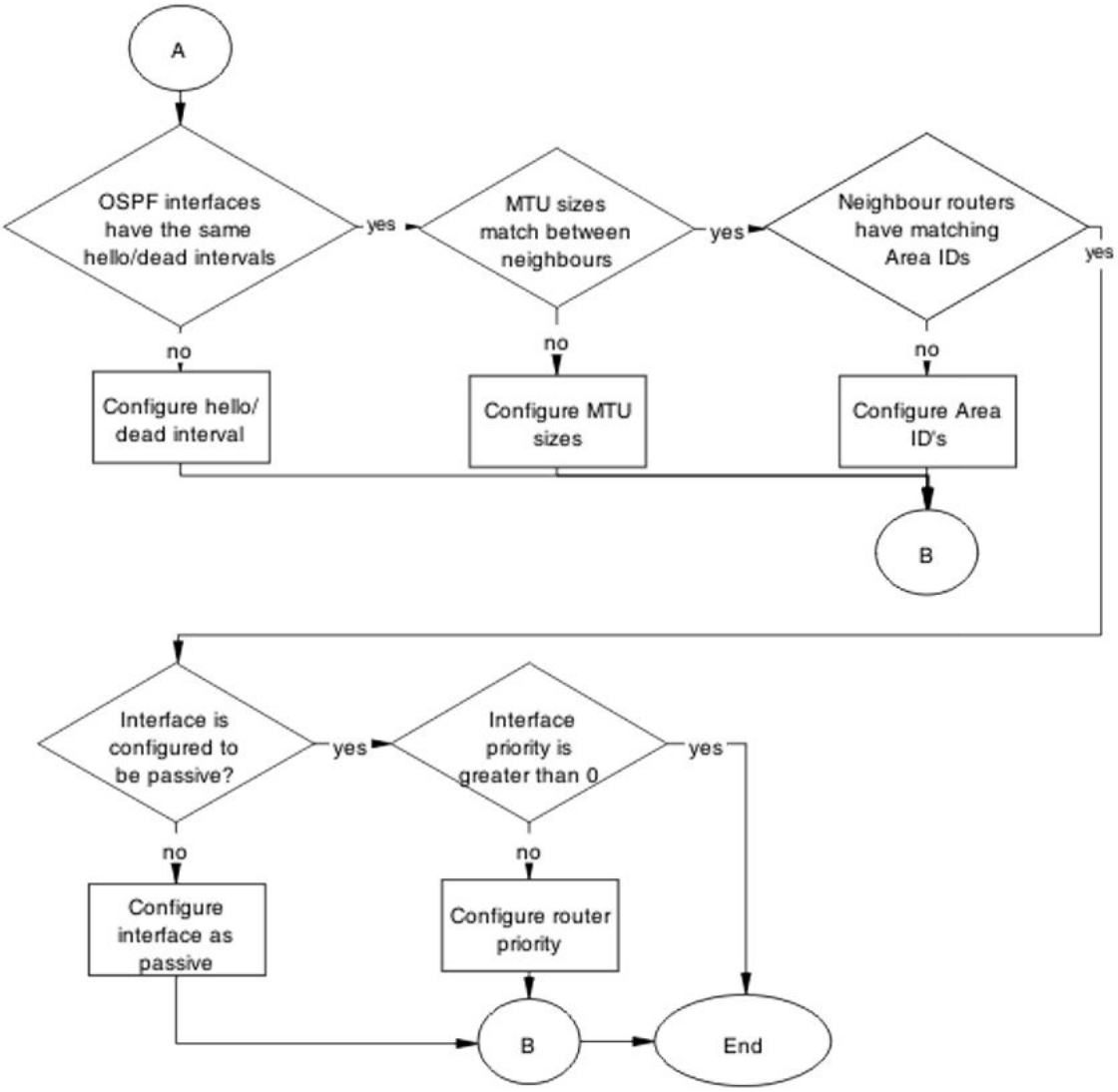



**Figure 99: Failure to Establish an OSPF adjacency part 2**

# 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.

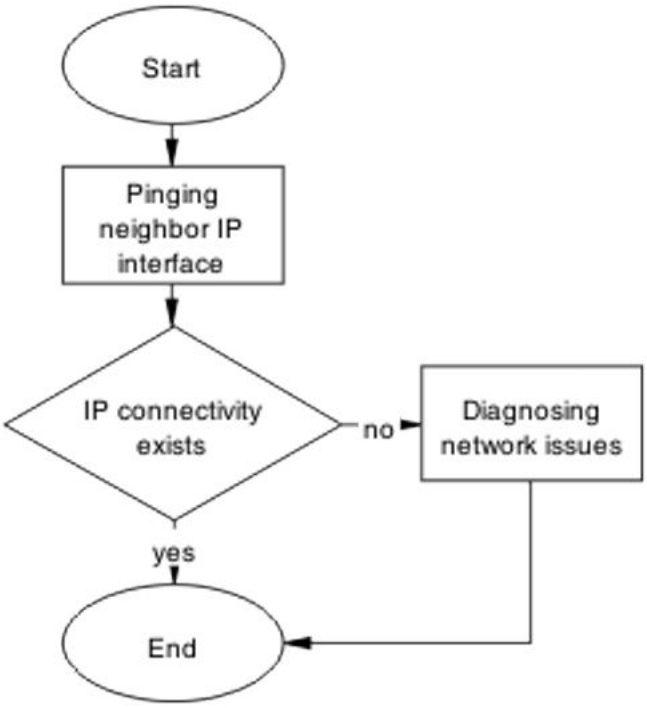



**Figure 100: Confirm IP connectivity**

## Pinging IP Interface of neighbor

### About this task

Identify IP connectivity to neighbor.

### Procedure

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

## Diagnosing network issues

### About this task

Fundamental networking issues are to be resolved.

Follow local and vendor procedures to reestablish connectivity between devices.

# Enable OSPF on interface

Enable OSPF on interface level to establish an adjacency.

## Task flow: Enable the OSPF on interface

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

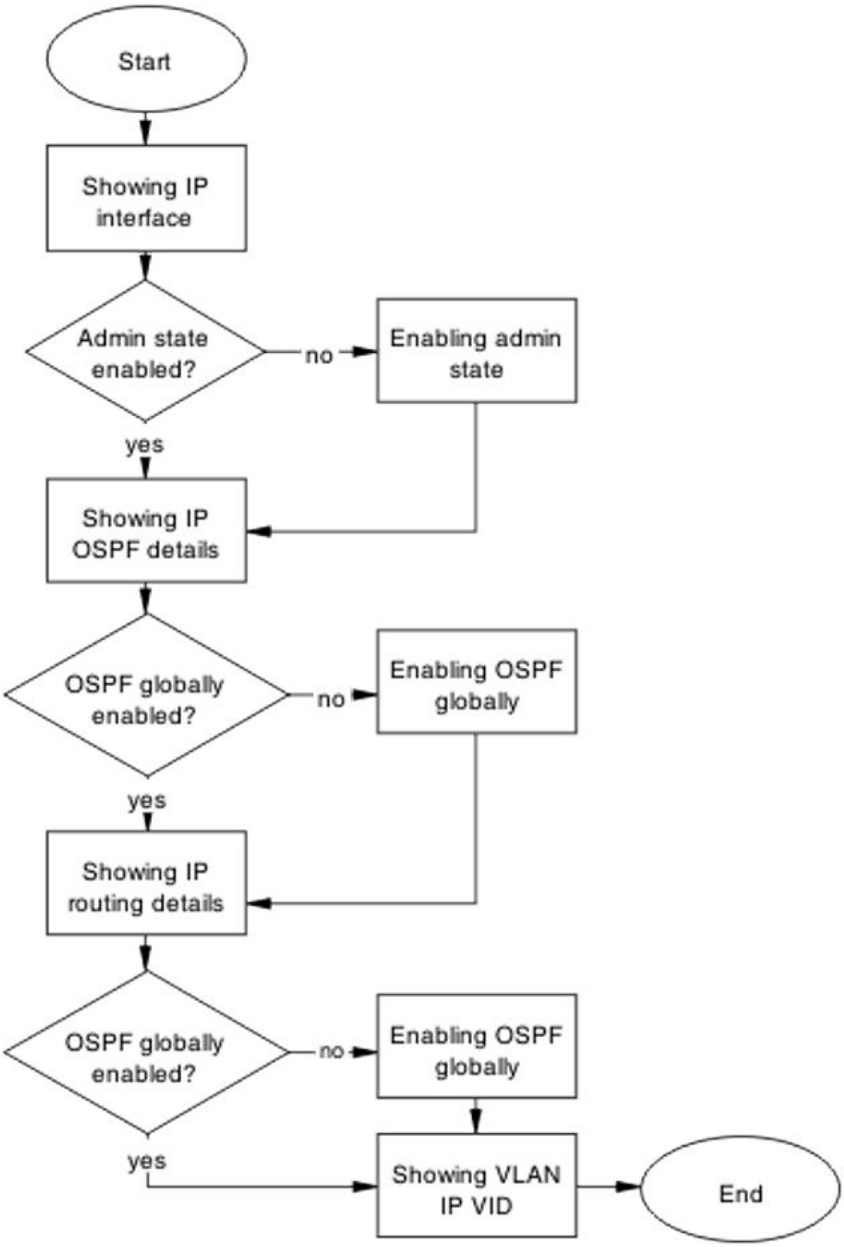



**Figure 101: Enable OSPF on interface**

## Showing IP Interface

### About this task

Display the IP interface information.

### Procedure

1. Use the **`show ip ospf interface vlan`** command.

2. Verify the admin state.

## Enabling admin state

### About this task

Enable the admin state of the switch.

### Procedure

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

## Showing IP OSPF

### About this task

Identify if OSPF is globally enabled.

### Procedure

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

## Enabling OSPF globally

### About this task

Enable the OSPF globally for the device.

### Procedure

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

## Showing IP routing

### About this task

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

### Procedure

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

## Showing VLAN IP VID

### About this task

Verify that the IP routing is enabled on the interface.

### Procedure

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

# Confirm Adjacencies

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

## Task flow: Confirm adjacencies

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

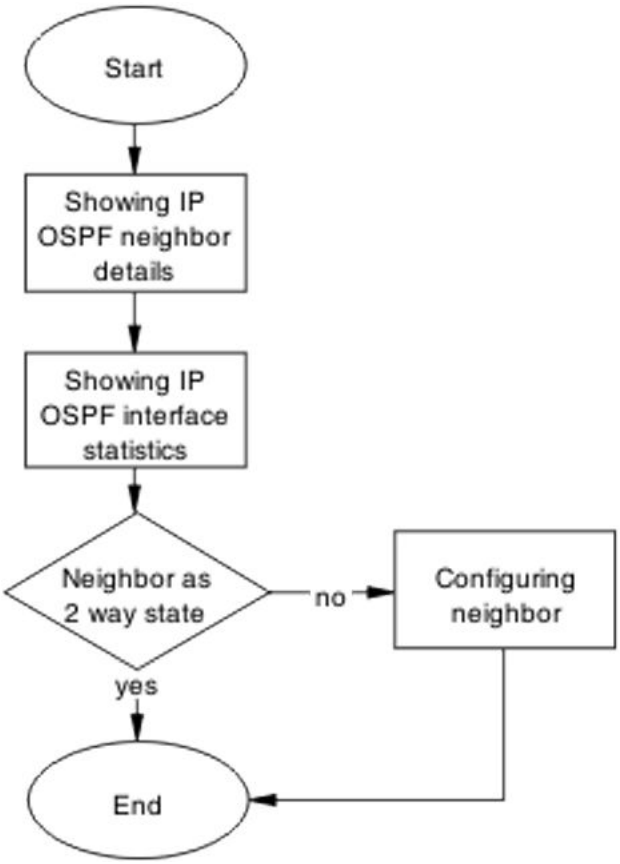



**Figure 102: Confirm adjacencies**

## Showing IP OSPF neighbor

### About this task

Display the IP OSPF neighbor information.

### Procedure

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

## Showing IP OSPF IP stats

### About this task

Display the IP OSPF neighbor information.

### Procedure

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

## Configuring neighbor

### About this task

Configure the neighbor device properly.

### Procedure

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

# Configure router IDs

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

## Task flow: Configure router IDs

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

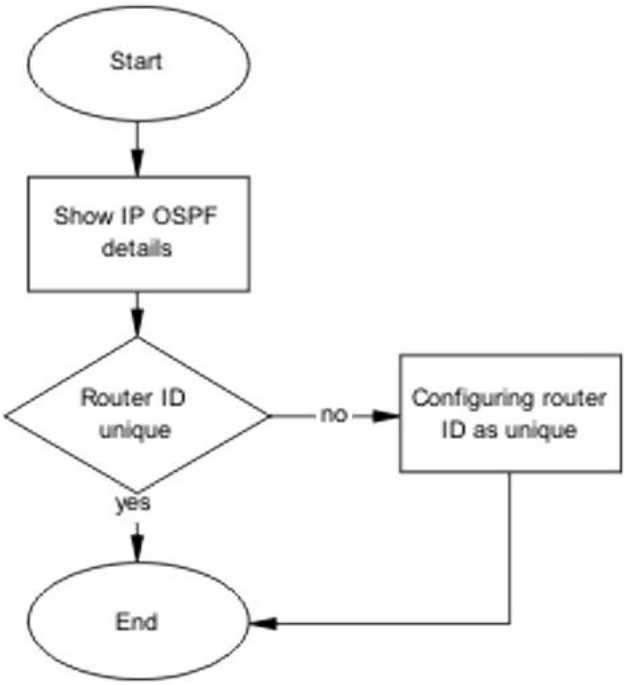



**Figure 103: Configure router IDs**

## Showing IP OSPF

### About this task

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

### Procedure

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

## Configuring router ID as unique

### About this task

Change the Router ID to ensure it is unique.

### Procedure

1. Use the **`enable`** command to enter userEXEC mode.

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

# Correct mismatch

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

## Task flow: Correct mismatch

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

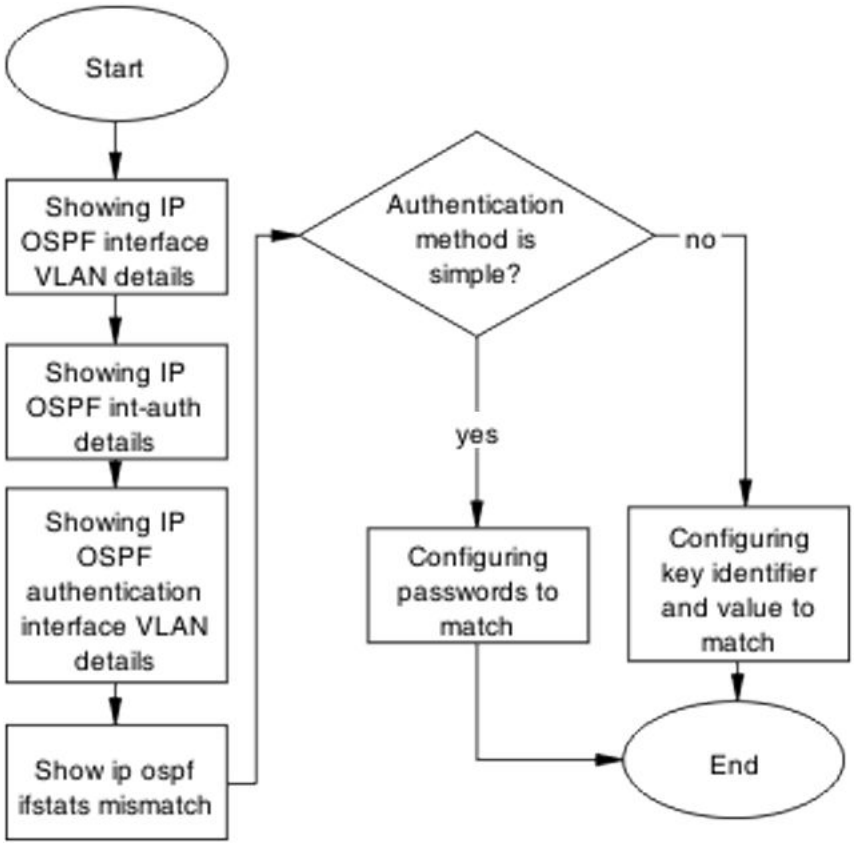



**Figure 104: Correct mismatch**

## Showing IP OSPF interface VLAN

### About this task

Display OSPF information for each VLAN interface.

### Procedure

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

## Showing IP ospf int-auth

### About this task

Display the authentication methods for all interfaces.

### Procedure

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

## Showing IP OSPF authentication interface VLAN

### About this task

Displays the assigned MD5 IDs and keys.

### Procedure

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

## Showing IP OSPF IFSTATS mismatch

### About this task

Display statistics for mismatched OSPF parameters.

### Procedure

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

## Configuring key identifier and value

### About this task

Both the key identifier and value must be matched.

### Procedure

1. Use the **enable** command to enter userEXEC mode.
2. Use the **configure terminal** command to enter Privileged Executive mode.

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

### Configuring passwords to match

#### About this task

Passwords must match on both endpoints.

#### Procedure

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

## Configure hello/dead interval

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

### Task flow: Configure hello/dead interval

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

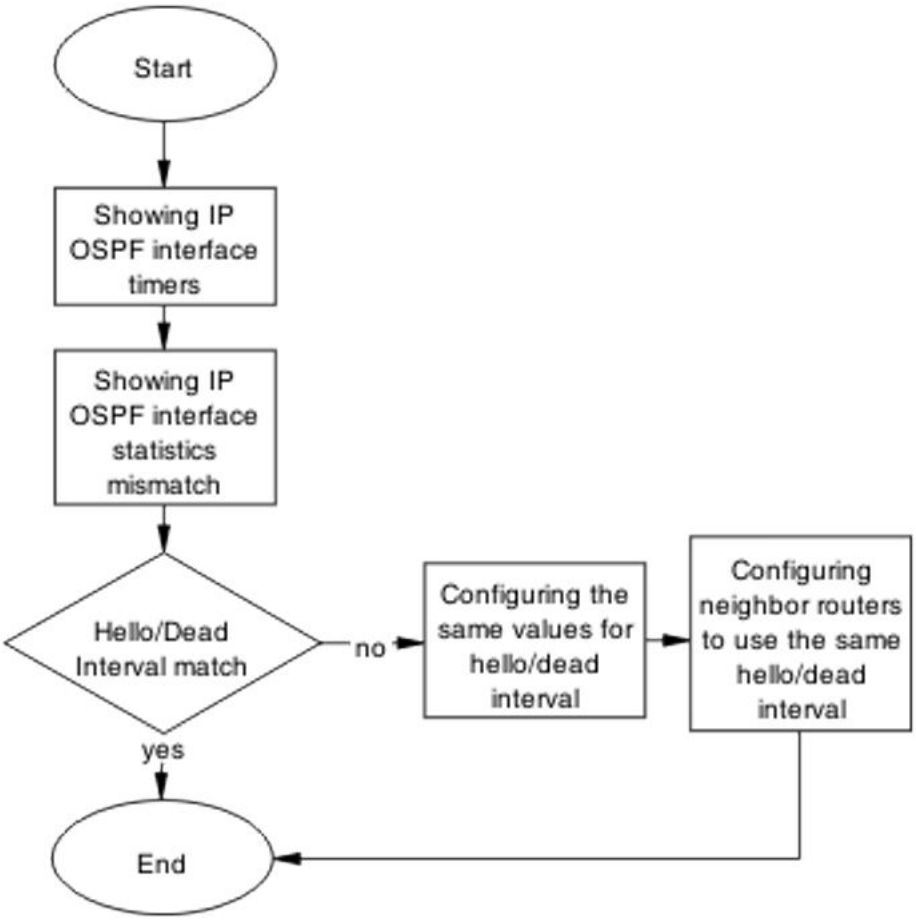



**Figure 105: Configure hello/dead interval**

## Showing IP OSPF interface timers

### About this task

Display OSPF timers for each interface.

### Procedure

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

## Showing IP OSPF ifstats mismatch

### About this task

Display statistics of each OSPF interface.

### Procedure

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

## Configuring the same values for hello/dead interval

### About this task

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

### Procedure

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

## Configuring neighbor routers to use the same hello/dead interval

### About this task

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

### Procedure

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

- Dead interval is 40

# Configure MTU sizes

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

## Task flow: Configure MTU sizes

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

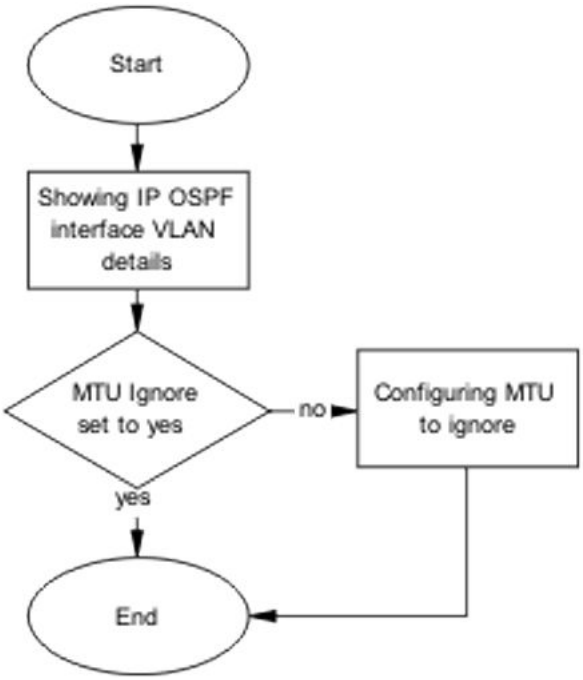



**Figure 106: Configure MTU sizes**

## Showing IP OSPF interface VLAN

### About this task

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

### Procedure

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

## Configuring MTU To ignore

### About this task

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

### Procedure

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

# Configure area IDs

Configure neighboring routers to use matching area ID.

## Task flow: Configure area ID

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

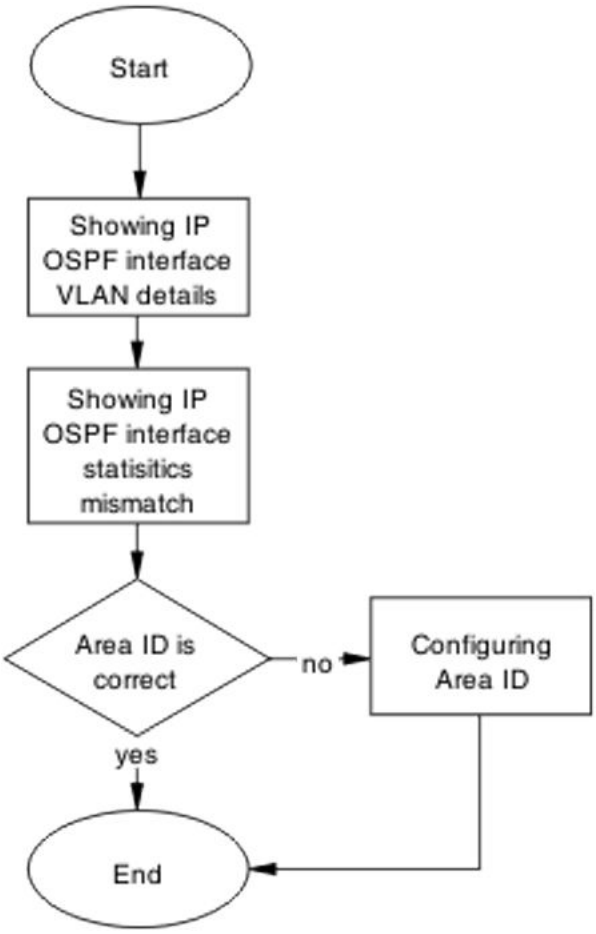



**Figure 107: Configure area ID**

## Showing IP OSPF interface VLAN

### About this task

Display configuration of each interface OSPF.

### Procedure

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

## Showing IP OSPF IFSTATS mismatch

### About this task

Display the statistics for mismatched OSPF parameters.

### Procedure

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

## Configuring Area IDs

### About this task

Configure the Area IDs to match.

### Procedure

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

# Configure an interface to not be passive

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

## Task flow: Configure an interface to not be passive

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

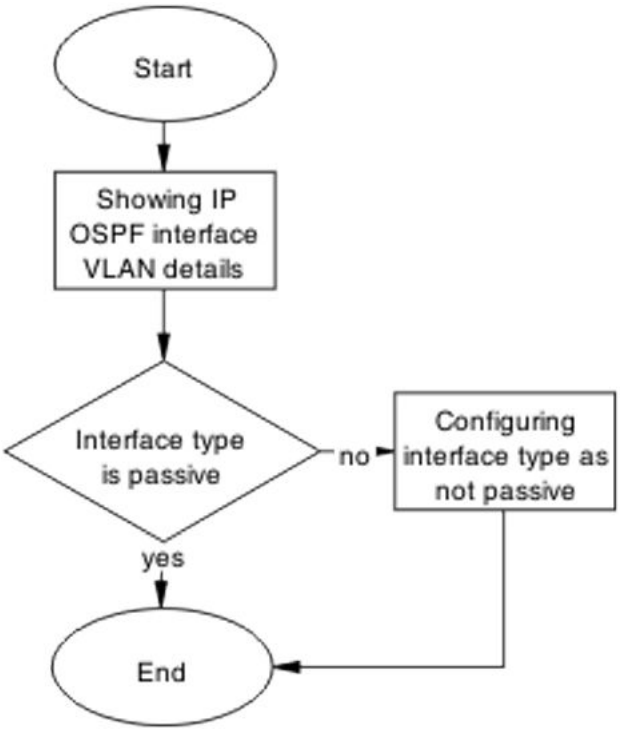



**Figure 108: Configure an interface to not be passive**

## Showing IP OSPF interface VLAN

### About this task

Display the OSPF interface VLAN information.

### Procedure

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

## Configuring interface type as not passive

### About this task

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

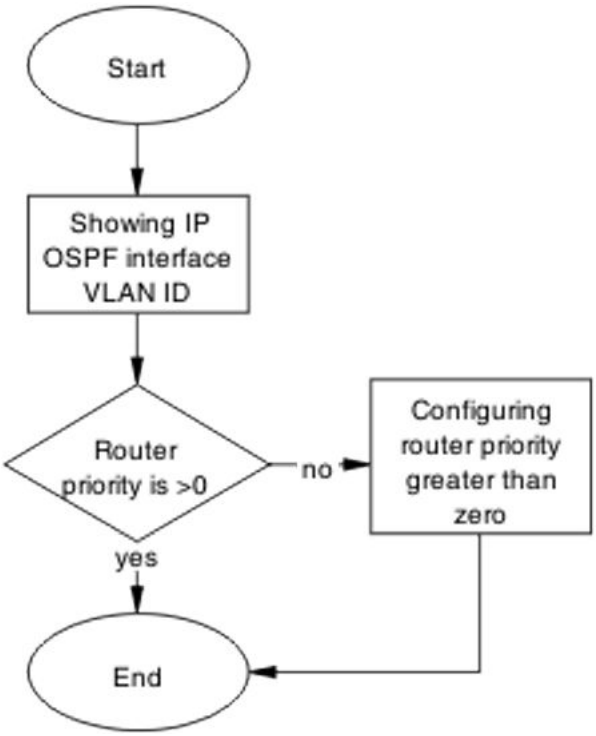
1. Use the **`show ip ospf interface vlan 2`** command to verify OSPF is not enabled on the interface on which you are planning to modify.
2. Use the **`int vlan 2`** command to enter the VLAN interface configuration.
3. Use the **`ip ospf network broadcast`** command to change the type to broadcast.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

## Configure router priority

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

### Task flow: Configure router priority

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



### Showing IP OSPF interface VLAN

#### About this task

Display the OSPF interface VLAN information

#### Procedure

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

### Configuring router priority greater than zero

#### About this task

Configure the router so the priority is greater than zero.

#### Procedure

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

## OSPF route is not installed in routing table

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

## Work flow: OSPF route is not installed in routing table

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

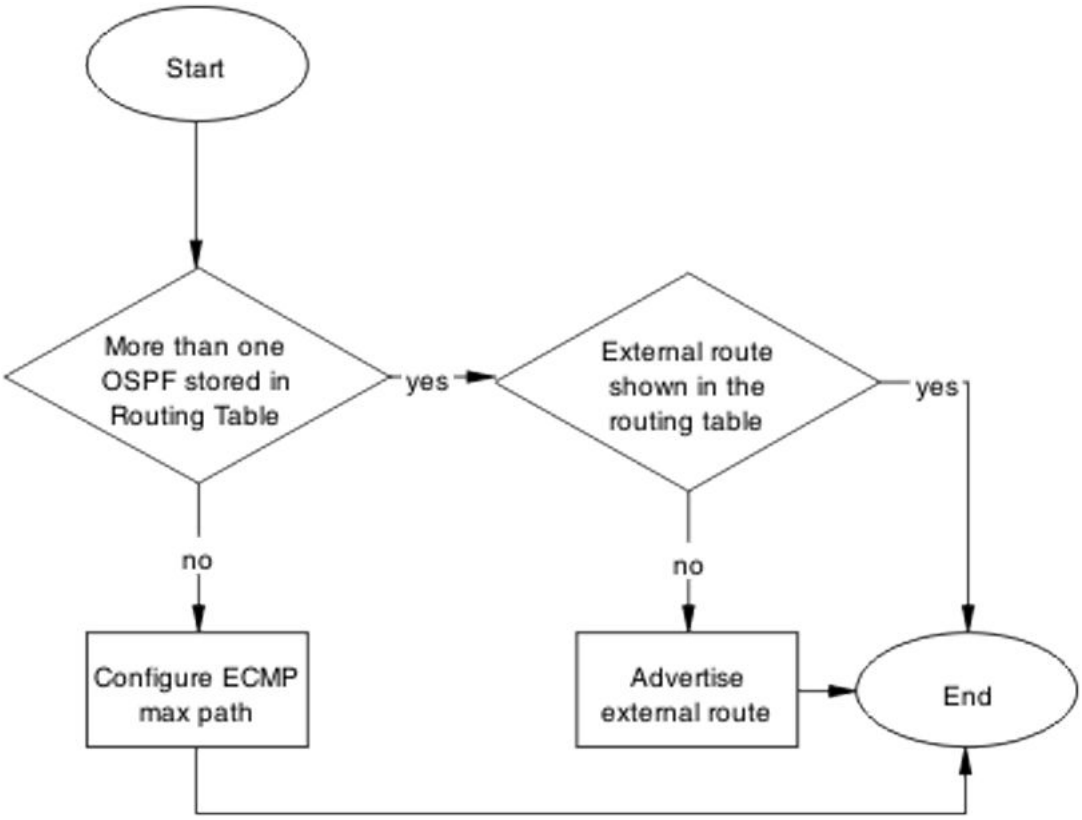



**Figure 109: OSPF route is not installed in routing table**

# 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.

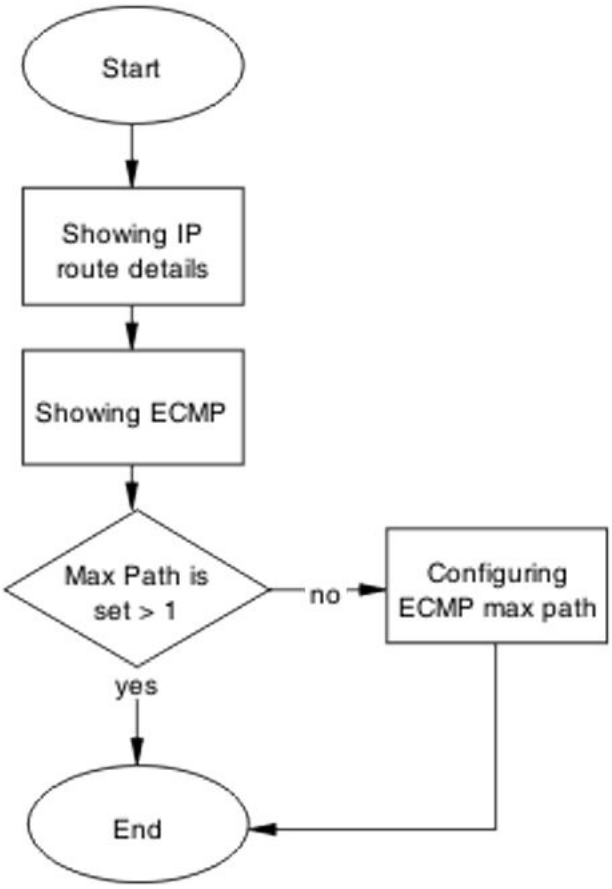



**Figure 110: Confirm ECMP max path**

## Showing IP Route

### About this task

Display the routing table information.

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

### Procedure

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

## Showing ECMP

### About this task

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

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

## Configuring ECMP

### About this task

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

An ECMP license is required to enable this feature.

### Procedure

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

# Advertise external route

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

## Task flow: Advertise external route

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

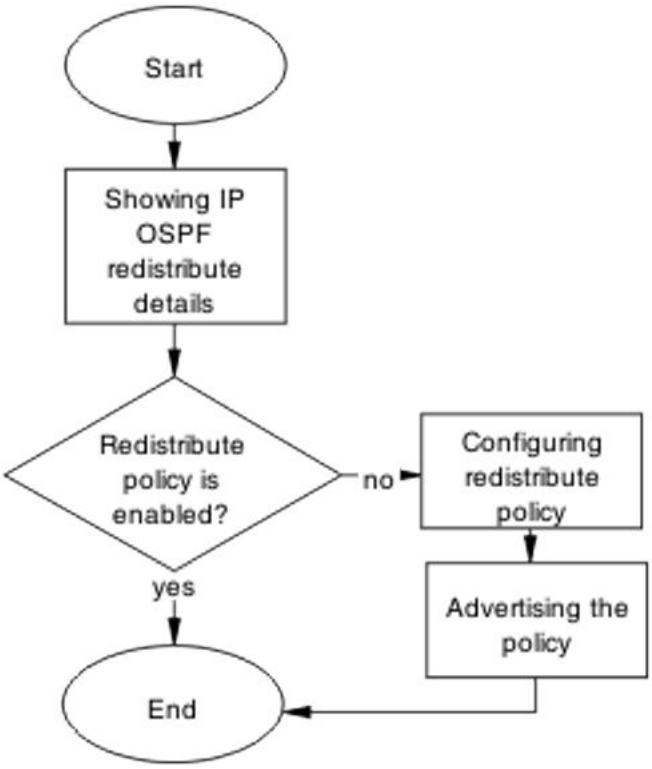



**Figure 111: Advertise external route**

## Showing IP OSPF redistribute

### About this task

Display the routing table information.

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

### Procedure

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

## Configuring Redistribute Policy

### About this task

Redistribute external routes into OSPF network.

### Procedure

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

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

Ensure that routes are learned between devices under test.

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

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

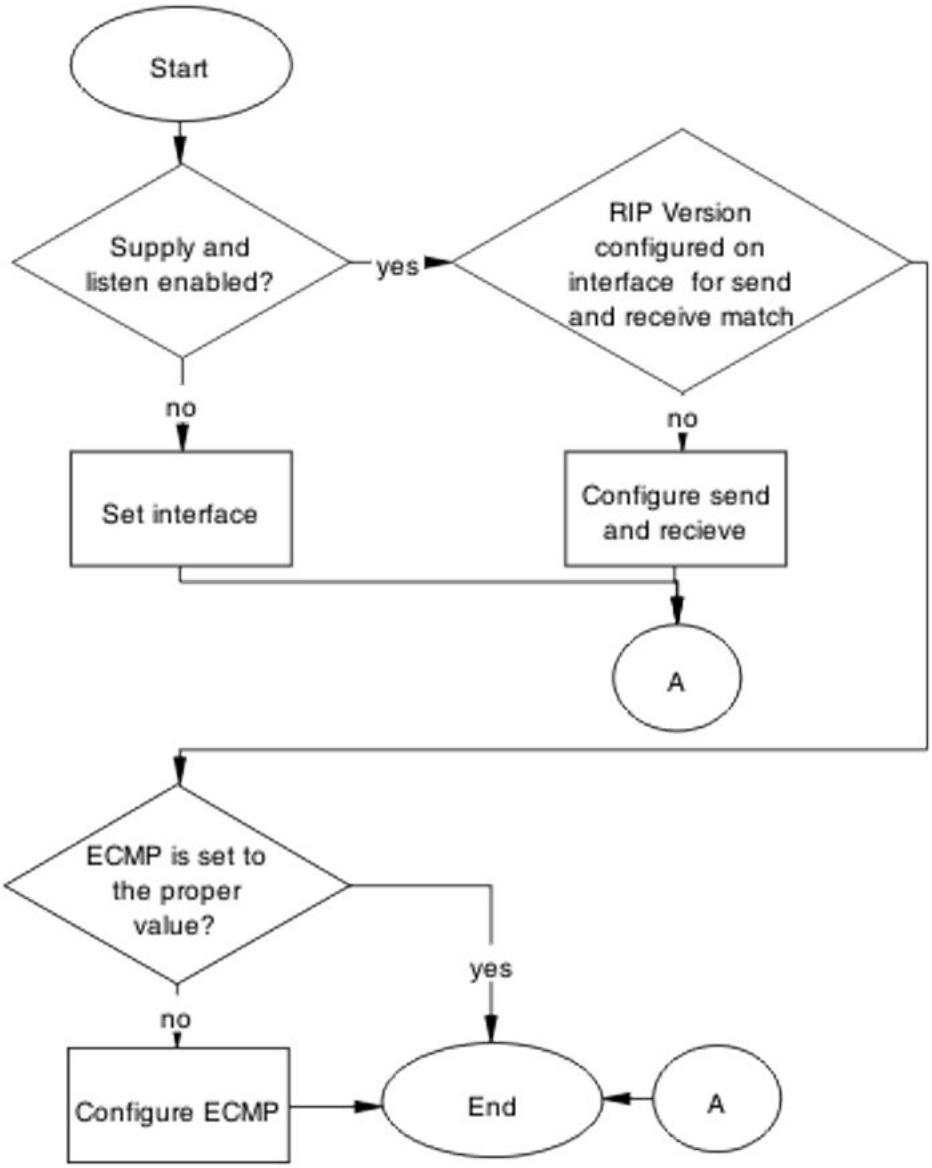



**Figure 112: RIP Packets exchanged between device under test (DUT) but no routes are learned**

## 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.

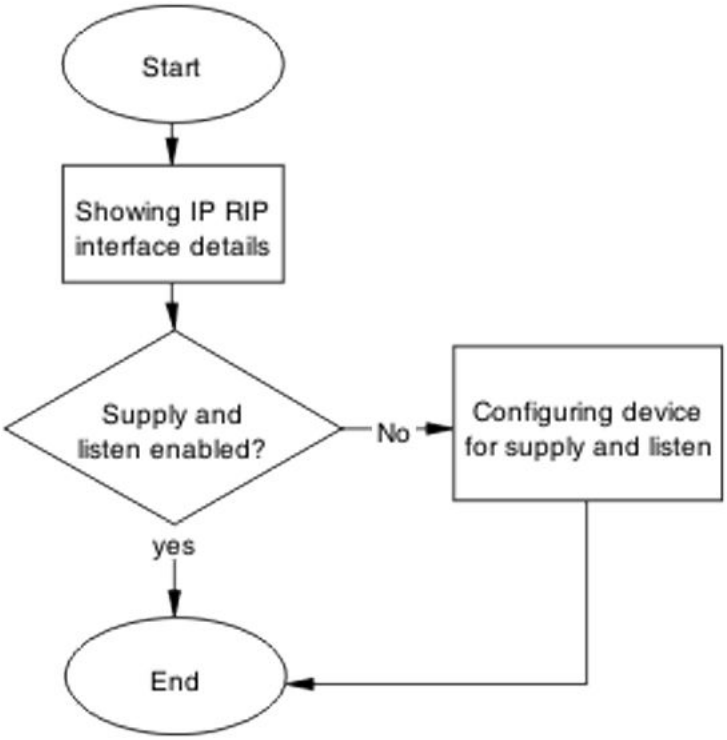



**Figure 113: Set interface**

## Showing RIP IP interface

### About this task

Display the RIP interface information.

### Procedure

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

## Configuring device for supply and listen

### About this task

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

### Procedure

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

# Configure send and receive

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

## Task flow: Configure send and receive

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

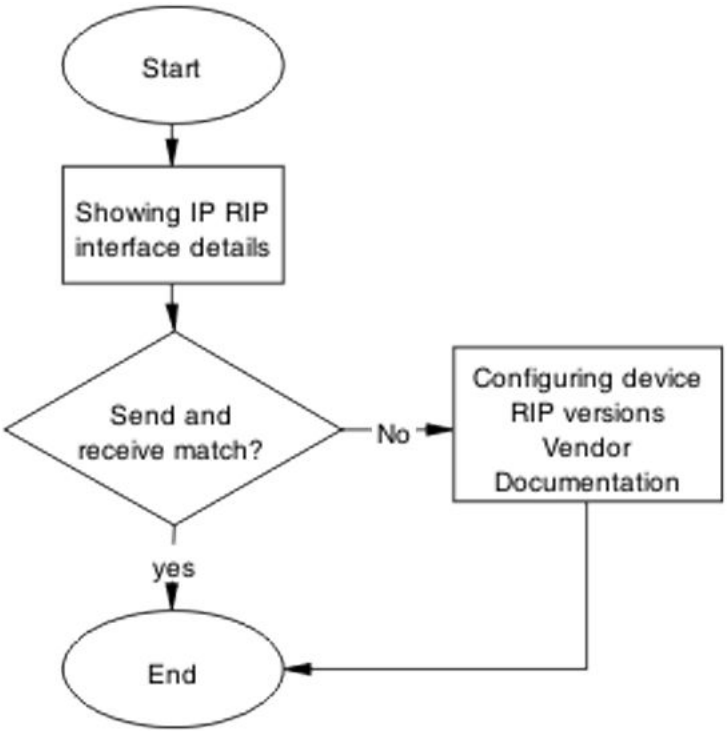



**Figure 114: Configure send and receive**

## Showing RIP IP interface

### About this task

Display the RIP interface information

### Procedure

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

## Configuring device RIP versions

### About this task

Configure the device to send and receive RIP packets.

### Procedure

1. Use the **`show ip rip interface`** command to display the interface information.

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

# Configure ECMP

Set ECMP to proper value.

## Task flow: Configure ECMP

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

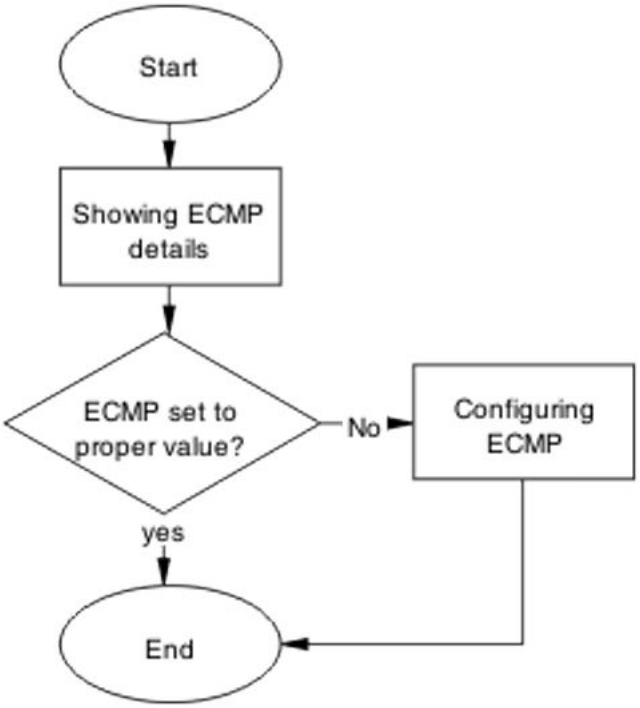



**Figure 115: Configure ECMP**

## Showing ECMP details

### About this task

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

### Procedure

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

## Configuring ECMP

### About this task

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

**Prerequisites:**

An ECMP license is required to enable this feature.

### Procedure

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

# RIP routes are learned-deleted learned again

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

# Task flow: RIP routes are learned-deleted learned again

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

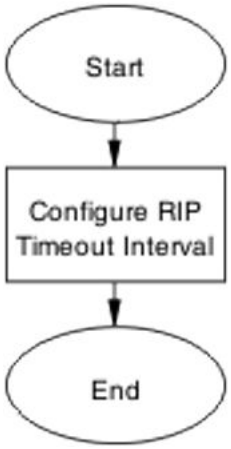



**Figure 116: RIP routes are learned-deleted learned again**

# Configuring RIP timeout interval

### About this task

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.

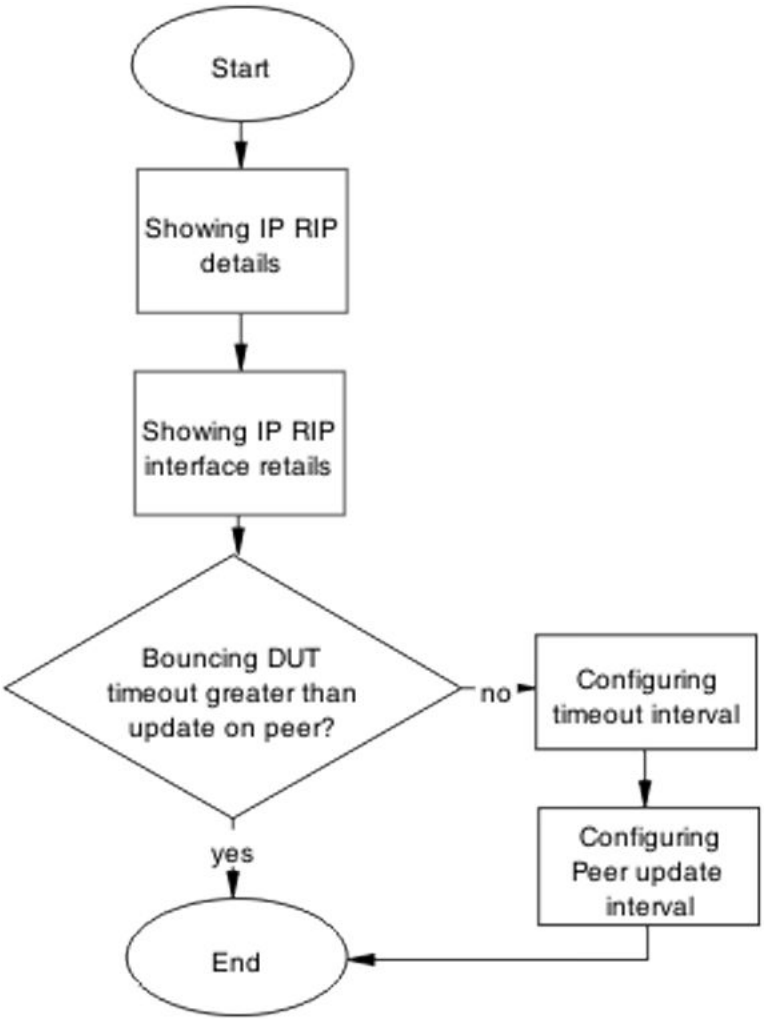



**Figure 117: Configure RIP timeout interval**

## Showing IP RIP

### About this task

Display the IP RIP information to observe the timeout intervals.

### Procedure

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

## Showing RIP IP interface

### About this task

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

### Procedure

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

## Configuring timeout Interval

### About this task

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

### Procedure

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

## Configuring peer update interval

### About this task

Configure the peer update timeout interval.

### Procedure

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

6. Use the **`show ip rip`** command to review the current settings.

# RIP routes learned with increasing cost

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

## Work flow: RIP routes learned with increasing cost

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

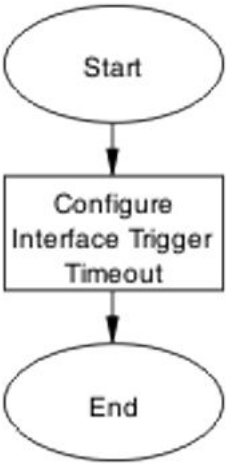



**Figure 118: RIP routes learned with increasing cost**

## Configure interface trigger timeout

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

### Task flow: Configure interface trigger timeout

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

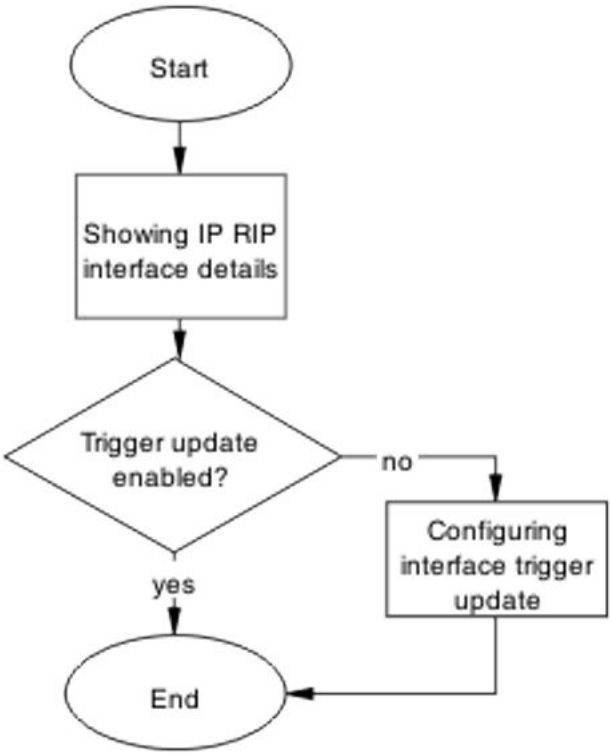



**Figure 119: Configure interface trigger timeout**

## Showing IP RIP interface

### About this task

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

### Procedure

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

## Configuring interface trigger update

### About this task

Change the trigger update to enabled.

### Procedure

1. Use the **`enable`** command to enter User Executive mode.

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

# SMLT routing issue

Ensure that the SMLT is routing packets properly.

## Work flow: SMLT routing issue

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

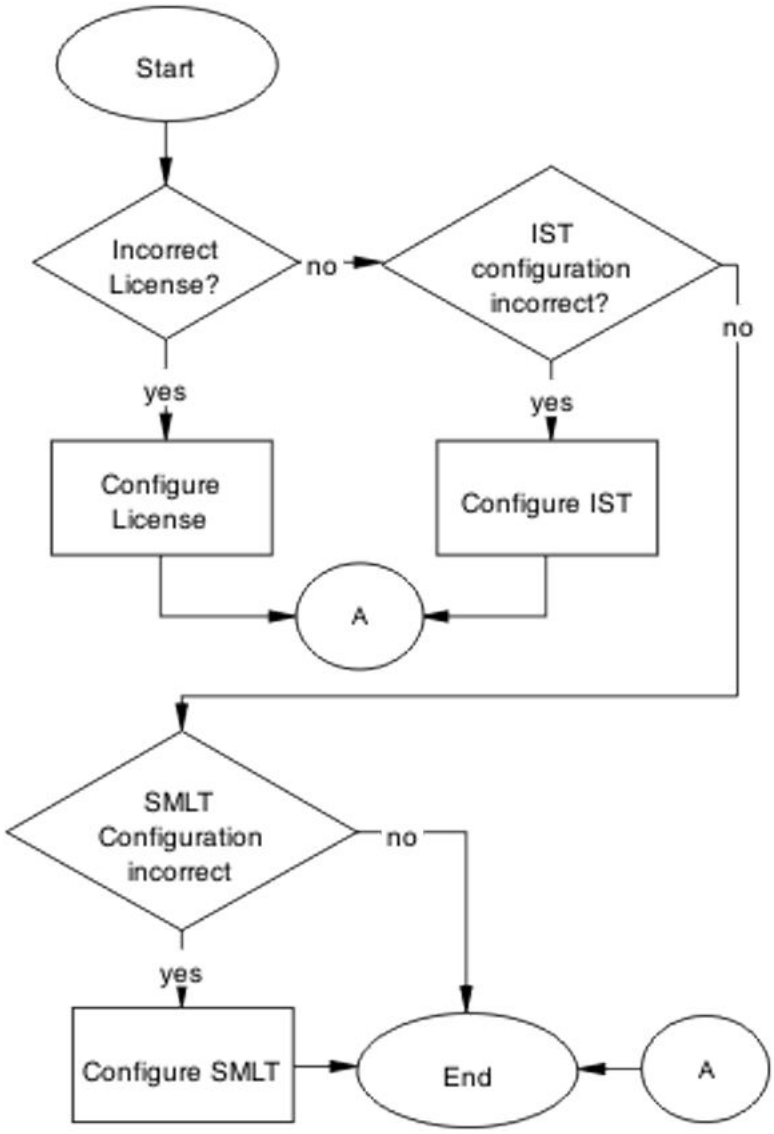



**Figure 120: SMLT routing issue**

# 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.

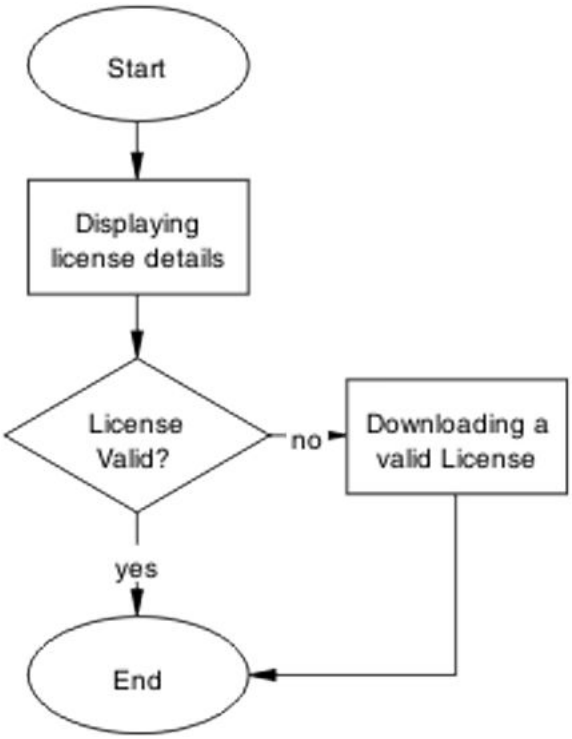



**Figure 121: Configure license**

## Displaying license details

### About this task

View license information about the edge and aggregation devices.

### Procedure

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

## Downloading a valid license

### About this task

Download the valid license to the switch.

Refer to document *Avaya Ethernet Routing Switch 5000 Series Getting Started* ( NN47200-303) 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.

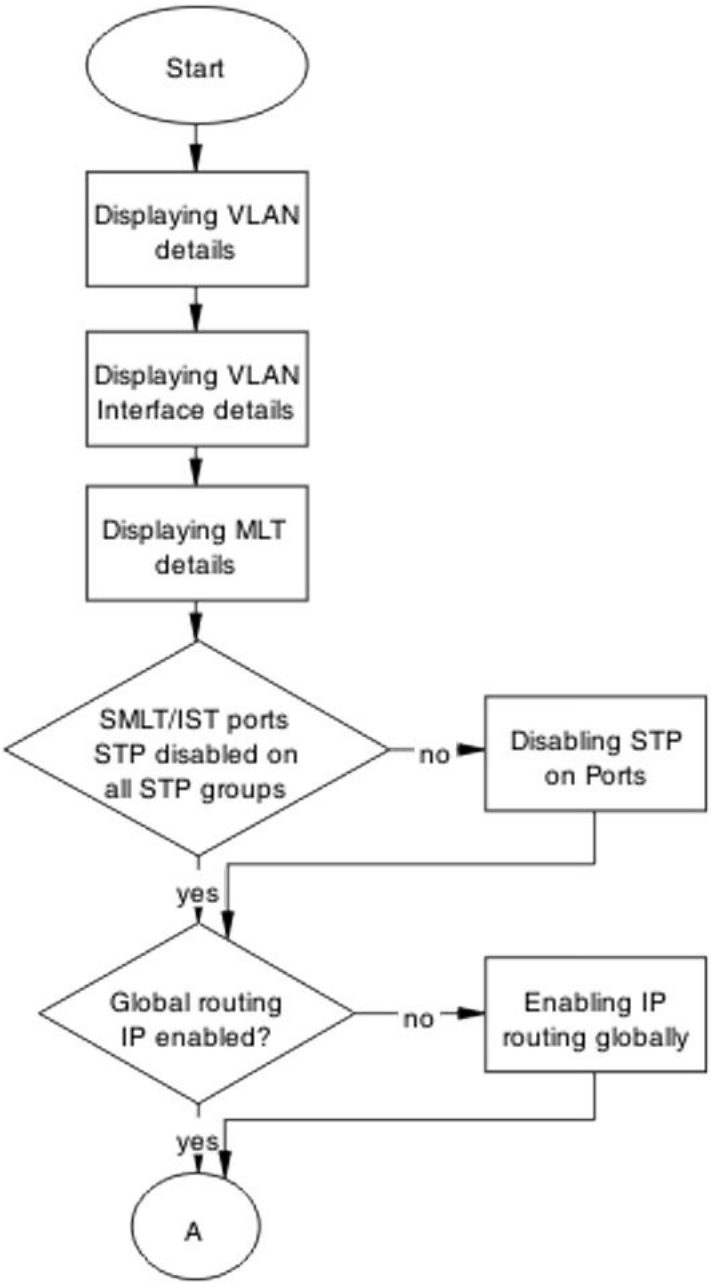



**Figure 122: Configure IST part 1**

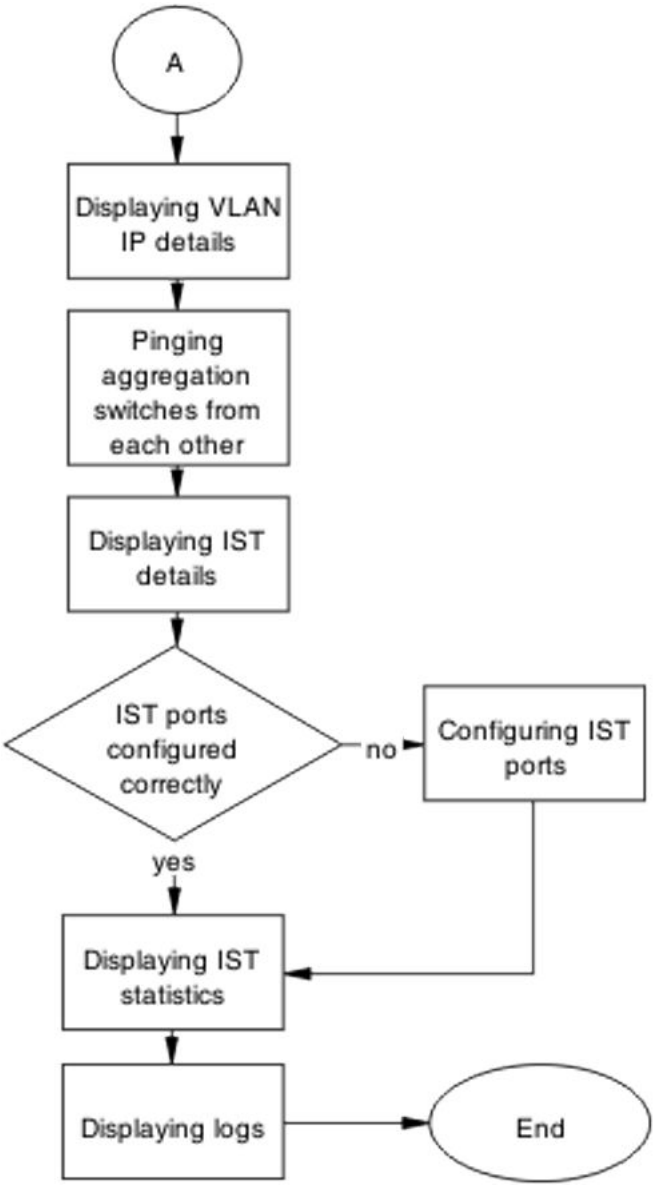



**Figure 123: Configure IST part 2**

## Displaying VLAN details

### About this task

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

### Procedure

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

## Displaying VLAN interface details

### About this task

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

### Procedure

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

## Displaying MLT details

### About this task

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

### Procedure

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

## Disabling STP on ports

### About this task

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

### Procedure

1. Use the **show spanning-tree port** command to display the spanning-tree participation for ports.

2. Observe the displayed information.

## Enabling IP routing globally

### About this task

View the IP routing information

### Procedure

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

## Displaying VLAN IP details

### About this task

Display the VLAN IP information.

### Procedure

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

## Pinging aggregation switches from each other

### About this task

Test the IP connection between two switches.

### Procedure

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

## Configuring IST ports

### About this task

View the IST configuration and operational mode.

### Procedure

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

## Displaying IST statistics

### About this task

Check the counters between two aggregate switches for messages.

### Procedure

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

## Displaying logs

### About this task

Check the logging to see possible messages related to IST.

### Procedure

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

# Configure SMLT

Configure SMLT to ensure it is functioning correctly.

## Task flow: Configure SMLT

The following task flow assists you to properly configure SMLT.

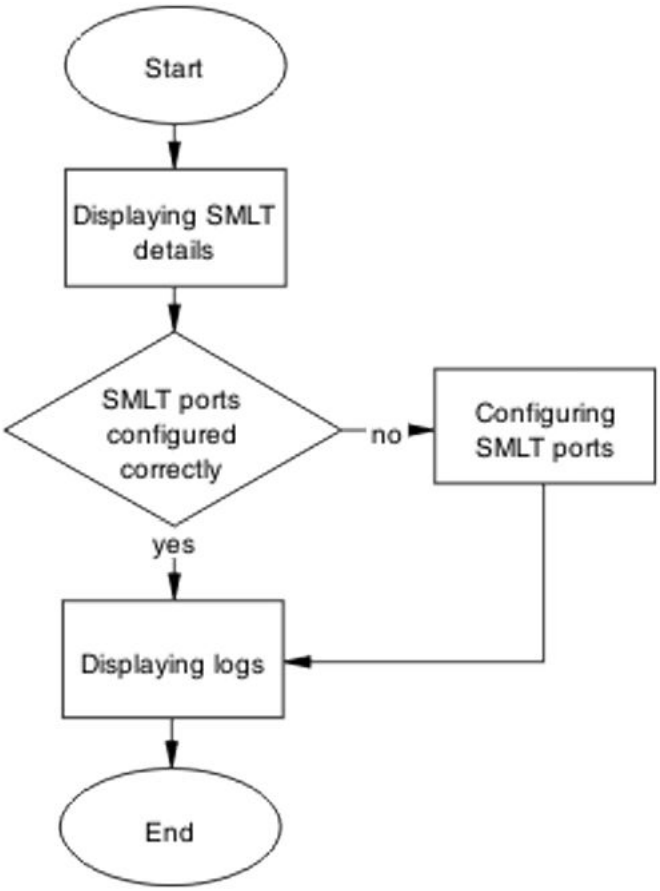



**Figure 124: Configure SMLT**

## Displaying SMLT details

### About this task

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

### Procedure

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

### Configuring SMLT ports

#### About this task

Configure the SMLT on the ports.

#### Procedure

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

### Displaying logs

#### About this task

Check the logging to see possible messages related to SMLT.

#### Procedure

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

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

Correct a Virtual Rack to be master or backup.

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

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

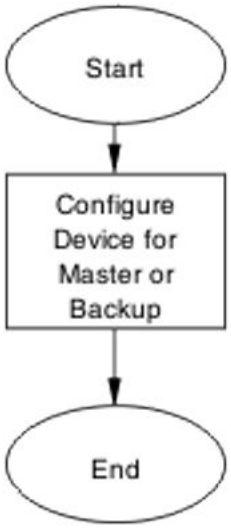



**Figure 125: VR is stuck in initialize state when it should be master or backup**

# 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.

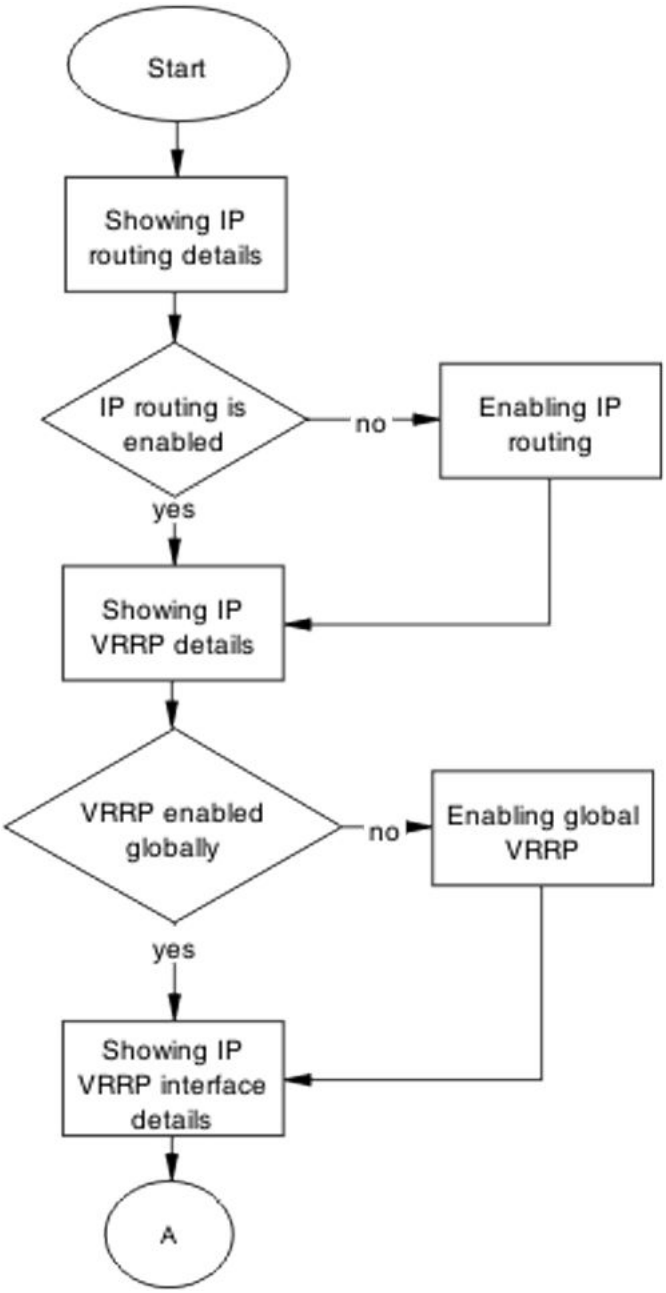



**Figure 126: Configure device for master or backup part 1**

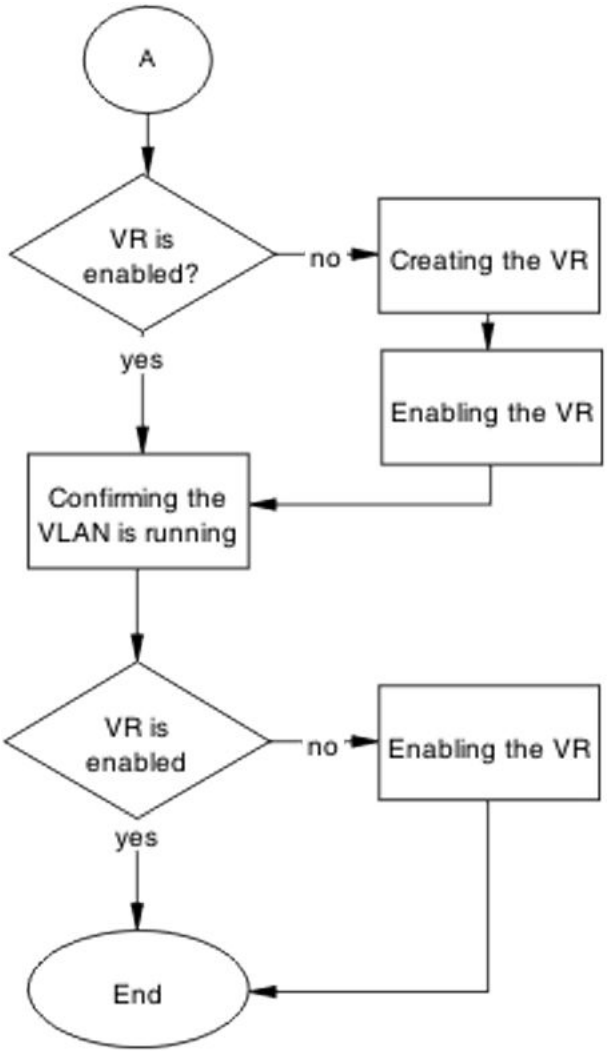



**Figure 127: Configure device for master or backup part 2**

## Showing IP routing details

### About this task

Verify that IP routing is enabled.

### Procedure

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

## Enabling IP routing

### About this task

IP routing is to be globally enabled on the switch.

### Procedure

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

## Showing IP VRRP details

### About this task

Verify that VRRP is enabled globally.

### Procedure

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

## Enabling global VRRP

### About this task

This procedure assists you to enable VRRP globally.

### Procedure

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

## Showing IP VRRP interface details

### About this task

Verify that the VR itself is enabled.

### Procedure

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

## Creating the VR

### About this task

The following procedure assists you to create a VR.

### Procedure

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

## Enabling the VR

### About this task

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

### Procedure

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

## Confirming VLAN is running

### About this task

Verify that the VR itself is enabled.

### Procedure

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

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

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

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

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

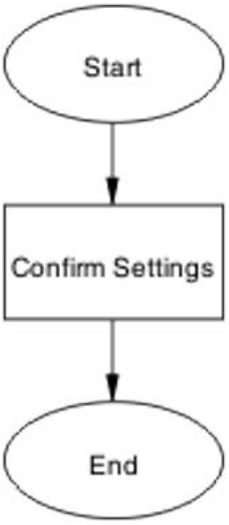



**Figure 128: VR stuck in master state when it should be backup (more than one master is present in a VR)**

## 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.

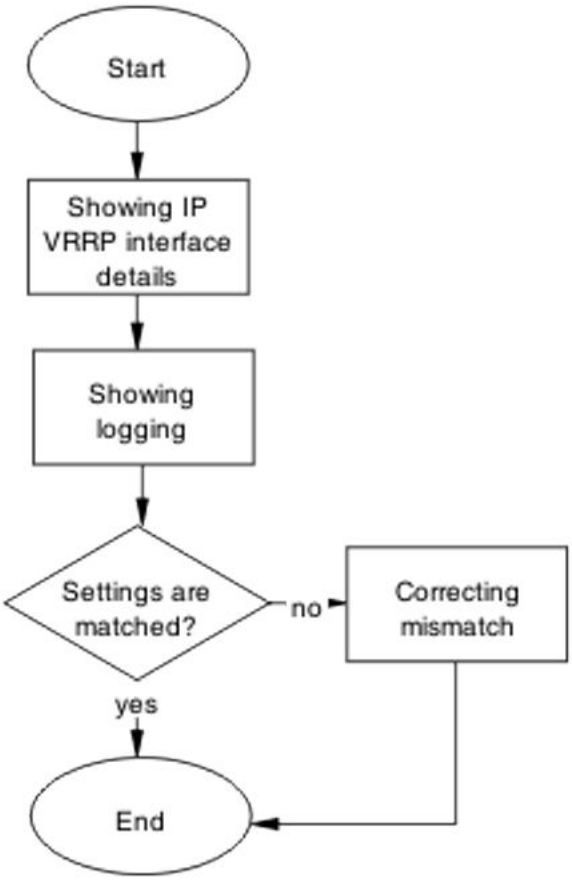



**Figure 129: Confirm settings**

## Showing IP VRRP interface details

### About this task

Verify critical information for the VRRP interface.

### Procedure

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

### Showing logging

#### About this task

Obtain log messages for the device.

#### Procedure

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

### Correcting mismatch

#### About this task

Configure the VRRP interface eliminate the mismatch.

#### Procedure

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

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

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

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

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

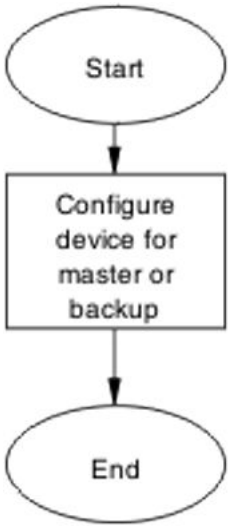



**Figure 130: VR is stuck in master state when it should be backup (no master is present in a VR)**

# 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.

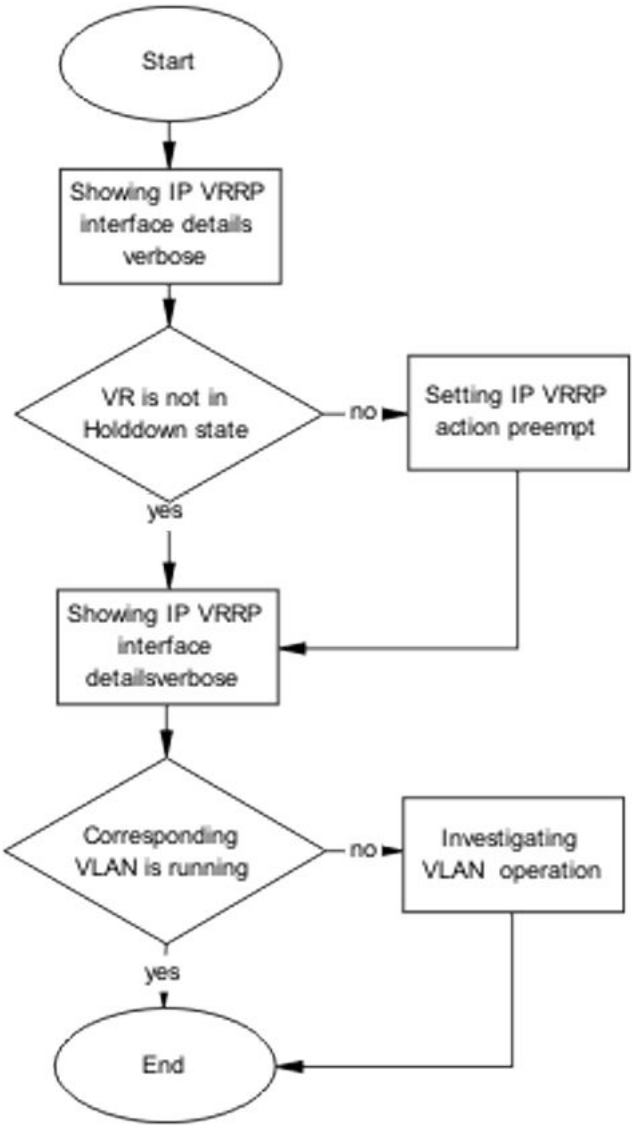



**Figure 131: Configure device for master or backup**

## Showing IP VRRP interface details verbose

### About this task

Verify critical information for the VRRP interface.

### Procedure

1. Use the command **`show ip vrrp interface verbose`**.
2. Verify VR is not in holddown state.

3. Verify that the corresponding VLAN is up for the critical IP feature is enabled and the critical IP address is set to one of the local L3 VLANs IP.

### Setting IP VRRP action preempt

#### About this task

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

#### Procedure

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

### Investigating VLAN operation

#### About this task

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

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

## Preempt mode is not working

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

## Work flow: Preempt mode is not working

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

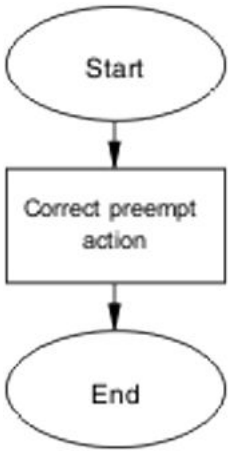



**Figure 132: Preempt mode is not working**

# 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.

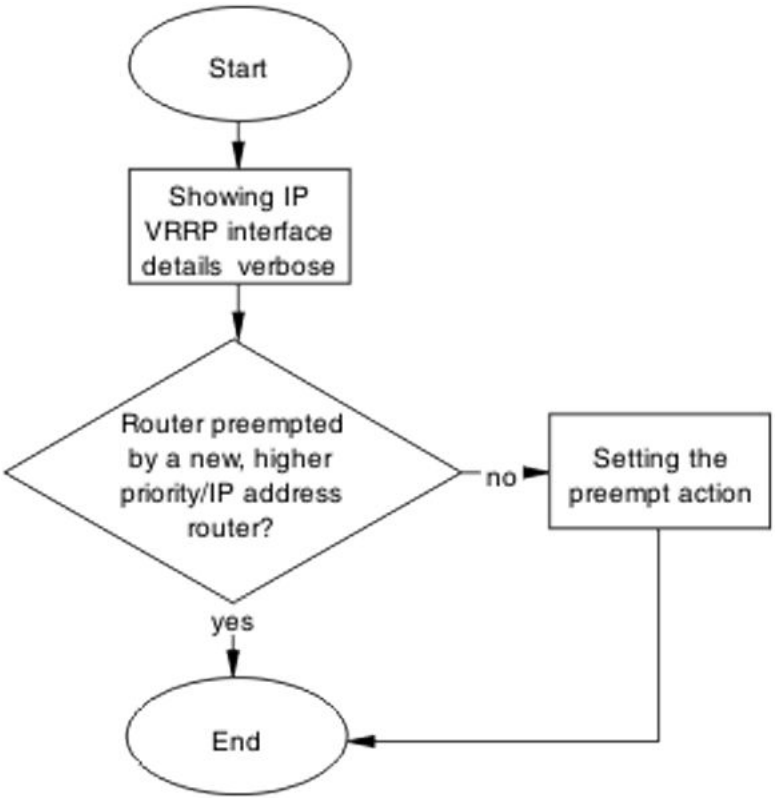



**Figure 133: Configure preempt action**

## Showing IP VRRP interface verbose

### About this task

Verify critical information for the VRRP interface.

### Procedure

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

## Setting the preempt action

### About this task

Configure the preempt for manual operation.

### Procedure

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

# Chapter 12: Common procedures

### About this task

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

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

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

## User Executive Mode

### About this task

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

### Procedure

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

## Privileged Exec Mode

### About this task

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

### Procedure

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

## Global Configuration Mode

### About this task

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

### Procedure

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

## Interface Configuration Mode

### About this task

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

### Procedure

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

5. The exit the ACLI completely, type the **logout** command.

# Router Configuration Mode

### About this task

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

### Procedure

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