AVAYA

Troubleshooting Avaya Ethernet Routing Switch 3500 Series

Release 5.2
NN47203-700
Issue 03.01
March 2014

Notice

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

Documentation disclaimer

“Documentation” means information published by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya may generally make available to users of its products and Hosted Services. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of documentation unless such modifications, additions, or deletions were performed by Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

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

Warranty

Avaya provides a limited warranty on Avaya hardware and software. 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 website: http://support.avaya.com or such successor site as designated by Avaya. Please note that if you acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to you by said Avaya Channel Partner and not by Avaya.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AVAYA CHANNEL PARTNER. 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 CHANNEL PARTNER; 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”).

Avaya grants you a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to you. “Designated Processor” means a single stand-alone computing device. “Server” means a Designated Processor that hosts a software application to be accessed by multiple users.

Heritage Nortel Software

“Heritage Nortel Software” means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software currently available for license from Avaya is the software contained within the list of Heritage Nortel Products located at http://support.avaya.com/LicenseInfo/ under the link “Heritage Nortel Products”, or such successor site as designated by Avaya. For Heritage Nortel Software, Avaya grants Customer a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or (in the event the applicable Documentation permits installation on non-Avaya equipment) for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

Copyright

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

Third Party Components

“Third Party Components” mean certain software programs or portions thereof included in the Software or Hosted Service may contain software (including open source software) distributed under third party agreements (“Third Party Components”), which contain terms regarding the rights to use certain portions of the Software (“Third Party Terms”). As required, information regarding distributed Linux OS source code (for those Products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the Documentation or on Avaya’s website at: http://support.avaya.com/Copyright or such successor site as designated by Avaya. You agree to the Third Party Terms for any such Third Party Components

Preventing Toll Fraud

“Toll Fraud” is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of Toll Fraud associated with your system and that, if Toll Fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya Toll Fraud intervention

If you suspect that you are being victimized by Toll Fraud and you need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: http://support.avaya.com or such successor site as designated by Avaya. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Trademarks

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: http://support.avaya.com, or such successor site as designated by Avaya.

Contact Avaya Support

See the Avaya Support website: http://support.avaya.com for Product or Hosted Service notices and articles, or to report a problem with your Avaya Product or Hosted Service. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: http://support.avaya.com (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

Contents

Chapter 1: Introduction

Purpose of this document

This document describes common problems and error messages and the techniques to resolve them.

Related resources

Documentation

For a list of the documentation for this product, see *Documentation Roadmap Reference for Avaya Ethernet Routing Switch 3500 Series*, NN47203-101.

Training

Ongoing product training is available. For more information or to register, you can access the Web site at http://avaya-learning.com.

Avaya Mentor videos

Avaya Mentor videos provide technical content on how to install, configure, and troubleshoot Avaya products.

About this task

Videos are available on the Avaya Support website, listed under the video document type, and on the Avaya-run channel on YouTube.

- To find videos on the Avaya Support website, go to http://support.avaya.com, select the product name, and select the *videos* checkbox to see a list of available videos.
- To find the Avaya Mentor videos on YouTube, go to http://www.youtube.com/AvayaMentor and perform one of the following actions:
    - Enter a key word or key words in the Search Channel to search for a specific product or topic.
    - Scroll down Playlists, and click the name of a topic to see the available list of videos posted on the site.

Note:

Videos are not available for all products.

Support

Visit the Avaya Support website at http://support.avaya.com for the most up-to-date documentation, product notices, and knowledge articles. You can also search for release notes, downloads, and resolutions to issues. Use the online service request system to create a service request. Chat with live agents to get answers to questions, or request an agent to connect you to a support team if an issue requires additional expertise.

Chapter 2: New in this release

The following hardware and software features are new in Avaya Ethernet Routing Switch (ERS) 3500 Series Release 5.2:

ERS 3500 hardware

The following table lists and describes the new hardware supported in Release 5.2:

Hardware	Description
Modules	
Avaya Ethernet Routing Switch 3549GTS	48 10/100/1000 non-PoE and 2 shared SFP, plus 1 1/10 Gigabit SFP+ port, plus 2 rear dual mode/stacking ports.
Avaya Ethernet Routing Switch 3549GTS-PWR+	48 10/100/1000 802.3at PoE+ and 2 shared SFP, plus 1 1/10 Gigabit SFP+ port, plus 2 rear dual mode/stacking ports.

ERS 3500 software features

The following software features are new for ERS 3500 Series Release 5.2:

- Avaya Energy Saver
- SLAMon enhancements
- Simple Loop Protection Protocol (SLPP) Guard
- Unified authentication
- Flash History
- Static LACP Key to Trunk ID binding

Other changes

See the following sections for information about changes that are not feature-related.

Document title change

In Release 5.2, the title of this document changed from *Avaya Ethernet Routing Switch 3500 Series Troubleshooting*, NN47203-700 to *Troubleshooting Avaya Ethernet Routing Switch 3500 Series*, NN47203-700.

Chapter 3: Introduction

Use this document to help you troubleshoot the Avaya Ethernet Routing Switch 3500 Series.

This document:

- Describes the diagnostic tools and utilities available for troubleshooting the Avaya Ethernet Routing Switch 3500 Series products using 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 3500 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 3500 Series network topologies. Other tools are more general in their application and can be used to diagnose and monitor ingress and egress traffic.

Chapter 4: Troubleshooting planning

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

1. Use the *Avaya Ethernet Routing Switch 3500 Series — Documentation Roadmap* , NN47203–101 to familiarize yourself with the documentation set, so you know where to get information when you need it.

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

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

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

  - A good practice is to store the details of all **key contacts**, such as support contacts, support numbers, engineer details, and telephone and fax numbers. Having this information available during troubleshooting saves you time.

4. Understand the normal network behavior so you can be more effective at troubleshooting problems.

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

Chapter 5: Troubleshooting fundamentals

This section describes available troubleshooting tools and their applications.

Port mirroring

Avaya Ethernet Routing Switch 3500 Series switches have a port mirroring feature that helps you to monitor and analyze network traffic. The port mirroring feature supports both ingress (incoming traffic) and egress (outgoing traffic) port mirroring. When port mirroring is enabled, the ingress or egress packets of the mirrored (source) port are forwarded normally and a copy of the packets is sent from the mirrored port to the mirroring (destination) port.

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

Port mirroring limitations

The Ethernet Routing Switch 3500 Series supports port mirroring in the following three modes:

- ingress mode (XRX or ->Port X)
- egress mode (XTX or Port X ->)
- ingress and egress mode (XRX or XTX or <->Port X)

There are limitations to the egress mode. As a standalone unit or in a stack, port-mirroring mode XTX mirrors egress traffic on the mirrored port, but does not mirror control packets generated by the switch. The monitor port does not receive copies of the generated control packets that egress from the mirrored port.

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

Note:

Stacking is not available in Release 5.0.

Port mirroring commands

See *Avaya Ethernet Routing Switch 3500 Series-Configuration — System Monitoring*, NN47203–501 for port mirroring command information. Use the port mirroring commands to assist in diagnostics and information gathering.

Port statistics

Use port statistics commands to display information on received and transmitted packets at the ports. The ingress and egress counts occur at the MAC layer.

For more information regarding port statistics and commands, see *Avaya Ethernet Routing Switch 3500 Series-Configuration — System Monitoring*, NN47203–501.

System logs

You can use the syslog messaging feature of the Ethernet Routing Switch 3500 Series products to manage event messages. The syslog software on the 3500 Series switch communicates with a server software component called syslogd that resides on your management workstation.

The daemon syslogd is a software component that receives and locally logs, displays, prints, or forwards messages that originate from sources that are internal and external to the workstation. For example, syslogd software concurrently handles messages received from applications running on the workstation, as well as messages received from an Ethernet Routing Switch 3500 Series device running in a network accessible to the workstation.

For more information about system logging, see *Avaya Ethernet Routing Switch 3500 Series-Configuration — System Monitoring*, NN47203–501.

Remote logging

As part of configuring system logging, you can specify remote logging parameters. This involves configuring a remote syslog address, enabling remote logging and configuring the remote logging level.

For more information, see *Avaya Ethernet Routing Switch 3500 Series - Configuration — System Monitoring*, NN47203–501.

Software Exception Log

This feature allows an administrator to see the software exceptions generated in the switching system. The software exception log provides a method for capturing software faults in the SYSLOG application as critical customer messages. The CLI allows you to display and clear the last software exceptions generated in the system. For more information, see *Avaya Ethernet Routing Switch 3500 Series-Configuration — System Monitoring,* NN47203–501.

Show environmental

You can use this feature to display environmental information about the operation of the switch. The information includes power supply status, fan status, and switch system temperature. For more information, see *Avaya Ethernet Routing Switch 3500 Series - Configuration — System Monitoring*, NN47203–501.

ASCII Config Generator (ACG)

The primary goal of the ASCII Configurator Generator (ACG) is to provide the users of the Ethernet Routing Switch 3500 Series with a tool that lets them easily modify the configuration of a particular switch.

ACG generates an ASCII configuration file which reproduces the behaviour of the current binary configuration file. The user can also rely on this function to maintain backup configurations, as well as use it as a reliable method for debugging the current configuration of a switch.

For more information, see *Avaya Ethernet Routing Switch 3500 Series — Getting Started*, NN47203–301.

CPU and Memory Utilization

The CPU and Memory Utilization feature provides data for CPU and memory utilization. You can view CPU utilization information for the past 10 seconds (s), 1 minute (min), 10 minutes (min), 1 hour (hr), 24 hours (hr), or since system startup. The switch displays CPU utilization as a percentage. With CPU utilization information you can see how the CPU was used during a specific time interval.

The memory utilization provides information about the percentage of the dynamic memory currently used by the system. The switch displays memory utilization in terms of the lowest percentage of dynamic memory available since system startup.

No configuration is required for this display-only feature. For more information, see *Avaya Ethernet Routing Switch 3500 Series - Configuration — System Monitoring*, NN47203–501.

SNMP trap enhancements

With SNMP management, you can configure SNMP traps to automatically generate notifications globally, or on individual ports. These notifications can report conditions such as an unauthorized access attempt or changes in port operating status. All notifications are enabled on individual interfaces by default.

The Avaya Ethernet Routing Switch 3500 Series supports both industry-standard SNMP traps, as well as private Avaya enterprise traps. SNMP trap notification-control provides a generic mechanism for the trap generation control that works with any trap type.

For more information, see *Avaya Ethernet Routing Switch 3500 Series - Configuration — Security*, NN47203–504.

SNMP Trap list web page in EDM

You can use Enterprise Device Manager (EDM) MIB Web page to query SNMP objects on the switch. For more information, see *Avaya Ethernet Routing Switch 3500 Series - Configuration — System Monitoring*, NN47203–501.

Remote monitoring (RMON) (RFC1757) per port Statistics History Alarm and Events

Remote Monitoring (RMON) MIB is an interface between the RMON agent on an Ethernet Routing Switch 3500 Series switch and an RMON management application, such as Enterprise Device Manager. The RMON agent defines objects that are suitable for the management of any type of network, but some groups are targeted for Ethernet networks in particular.

The RMON agent continuously collects statistics and proactive monitors switch performance. You can view this data through A\CLI and EDM.

RMON has three major functions:

- creating and displaying alarms for user-defined events
- gathering cumulative statistics for Ethernet interfaces
- tracking a history of statistics for Ethernet interfaces

For more information on RMON per port Statistics, History, Alarms and Events, see *Avaya Ethernet Routing Switch 3500 Series - Configuration — System Monitoring*, NN47203–501.

Avaya knowledge and solution engine

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

Chapter 6: General diagnostic tools

The Avaya Ethernet Routing Switch 3500 Series device has diagnostic features available through 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.

The command line interface is accessed through either a direct console connection to the switch or by using the Telnet or SSH protocols to connect to the switch remotely.

ACLI command modes

ACLI command modes provide different levels of authority for operation.

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

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

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

The command modes are as follows:

- `User EXEC mode :`

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

- `Privileged EXEC mode`:

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

- `Global configuration mode`:

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

- `Interface configuration mode`:

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

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

For more information about the ACLI command modes, see *Avaya Ethernet Routing Switch 3500 Series — Fundamentals*. NN47203–102.

Chapter 7: Initial troubleshooting

The types of problems that typically occur with networks involve connectivity and performance. Using the Open System Interconnection (OSI) network architecture layers, and checking each in sequential order, is usually best when troubleshooting. For example, confirm that the physical environment, such as the cables and module connections, is operating without any failures before moving up to the network and application layers.

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

Gather information

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

- **Default and current configuration of the switch.** To obtain this information, use the `show running-config` command.
- **System status.** Obtain this information using the show sys-info command. Output from the command displays technical information about system status and information about the hardware, software, and switch operation. For more detail, use the `show tech` command.
- **Information about past events.** To obtain this information, review the log files using the `show logging` command.
- The **software version** that is running on the device. To obtain this information, use the `show sys-info` or `show system verbose` command to display the software version.
- **A network topology diagram.** Get an accurate and detailed topology diagram of your network that shows the nodes and connections. Your planning and engineering function should have this diagram.
- **Recent changes.** Find out about recent changes or upgrades to your system, your network, or custom applications (for example, has configuration or code been changed). Get the date and time of the changes, and the names of the persons who made them.

Get a list of events that occurred prior to the trouble, such as an upgrade, a LAN change, increased traffic, or installation of new hardware.

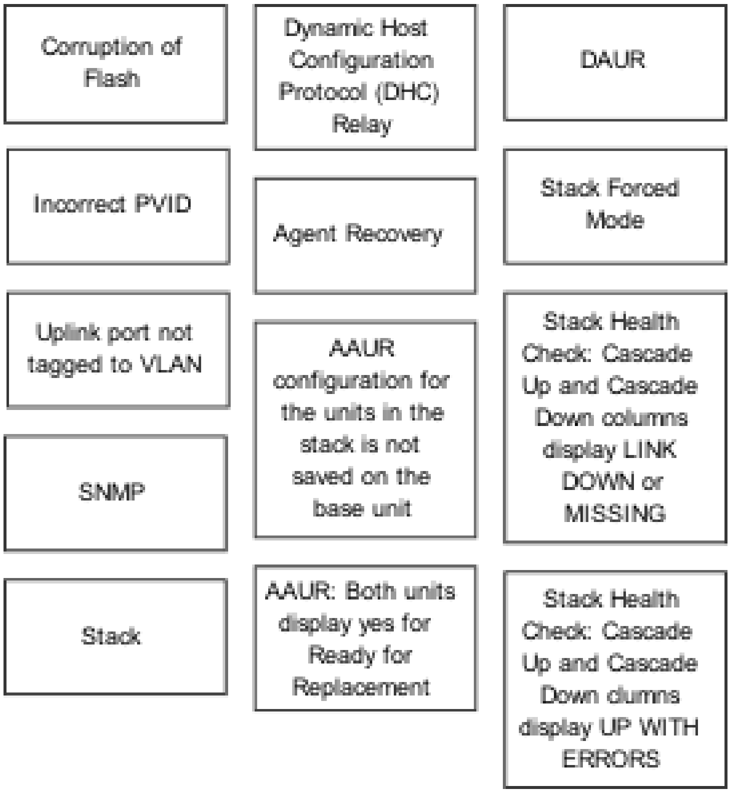
- **Connectivity information.** When connectivity problems occur, get information on at least five working source and destination IP pairs and five IP pairs with connectivity issues. To obtain this information, use the following commands:
    - **`show tech`**
    - **`show running-config`**
    - **`show port-statistics <port>`**

Chapter 8: Emergency recovery trees

An Emergency Recovery Tree (ERT) is designed to quickly guide you through some common failures and solutions, by providing a quick reference for troubleshooting without procedural detail.

Emergency recovery trees

The following work flow shows the ERTs included in this section. Each ERT describes steps to correct a specific issue; the ERTs are not dependant upon each other.



Corruption of Flash

Incorrect PVID

Uplink port not tagged to VLAN

SNMP

Stack

Dynamic Host Configuration Protocol (DHC) Relay

Agent Recovery

AAUR configuration for the units in the stack is not saved on the base unit

AAUR: Both units display yes for Ready for Replacement

DAUR

Stack Forced Mode

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

Stack Health Check: Cascade Up and Cascade Down clumns display UP WITH ERRORS

Figure 1: Emergency Recovery Trees

Corruption of flash

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

For assistance with tasks in the Corruption of Flash Emergency Recovery Tree, see

- Locating the switch console ports on page 57
- Using the Diagnostics Menu on page 58

Corruption of flash recovery tree

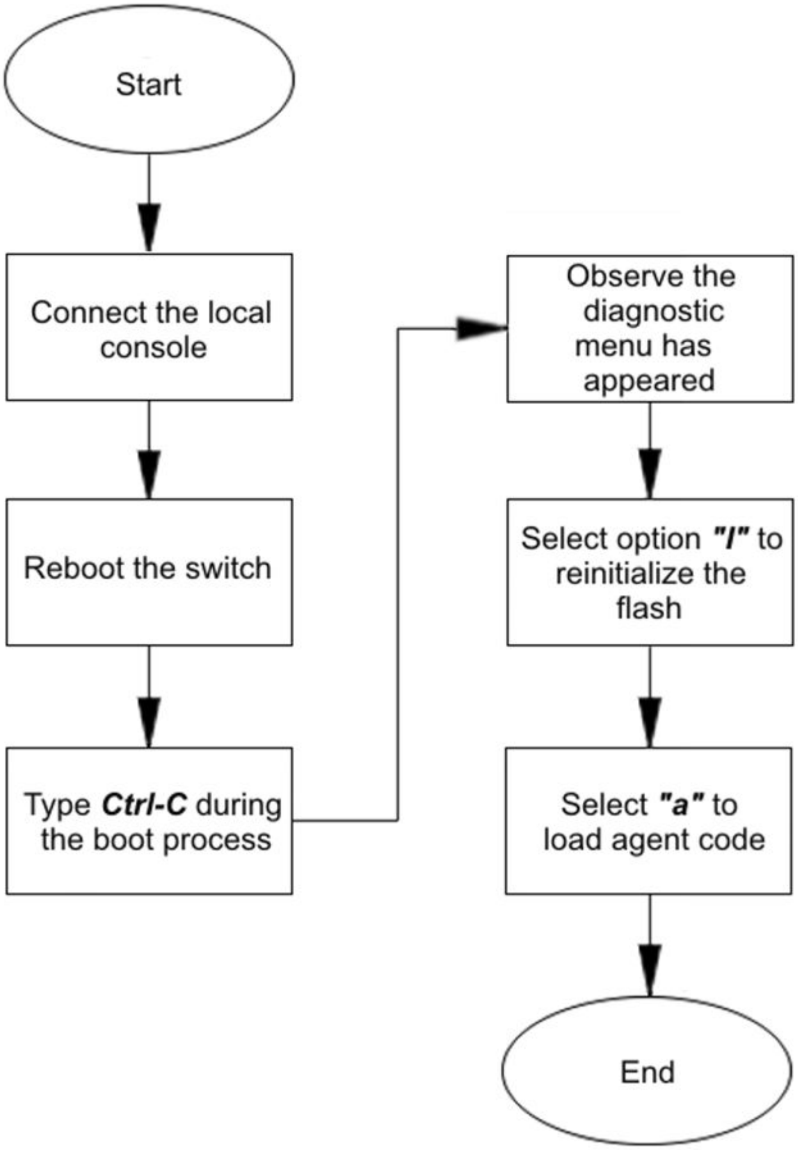

Start
Connect the local console
Reboot the switch
Type ***Ctrl-C*** during the boot process
Observe the diagnostic menu has appeared
Select option ***"I"*** to reinitialize the flash
Select ***"a"*** to load agent code
End

Figure 2: Corruption of flash recovery tree

Incorrect Port VLAN Identifier (PVID)

Port VLAN identifier (PVID) is a classification mechanism that associates a port with a specific VLAN. For example, a port with a PVID of 3 (PVID=3) assigns all untagged frames received on this port to VLAN 3.

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

For examples that show how to check the PVID of ports, and how to make PVID corrections, see

- Example Checking PVID of ports on page 59
- Example VLAN Interface VLAN IDs on page 60

Incorrect PVID recovery tree

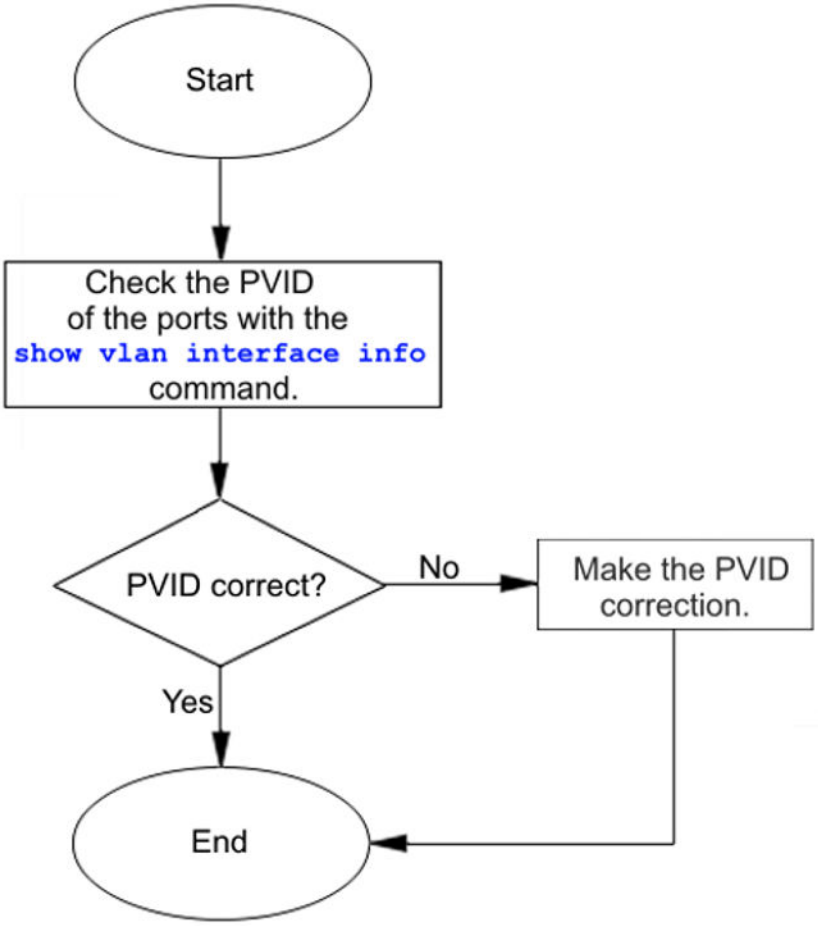

Start
Check the PVID of the ports with the show vlan interface info command.
PVID correct?
No
Make the PVID correction.
Yes
End

Figure 3: Incorrect PVID recovery tree

Uplink ports not tagged to VLAN

When an ERS 3500 series switch is connected to an ERS 8600 series switch or another Avaya Ethernet series switch, and devices in a VLAN on the ERS 8600 series switch are not able to communicate with devices at the ERS 3500 series switch in the same VLAN, then it is likely that the uplink ports are not tagged to the VLAN on the ERS 3500 series switch.

Use the **`show vlan interface info`** command to see if ports are tagged or untagged:

- **Untagged frame**: a frame that carries no VLAN tagging information in the frame header.
- **Tagged frame:** a frame that contains the 32–bit 802.1q field (VLAN tag) and identifies the frame as belonging to a specific VLAN.
- **Untagged member:** a port configured as an untagged member of a specific VLAN. When an untagged frame exits the switch through an untagged member port, the frame header remains unchanged. When a tagged frame exits the switch through an untagged member port, the tag is stripped and the tagged frame is changed to an untagged frame.
- **Tagged member:** a port configured as a tagged member of a specific VLAN. When an untagged frame exits the switch through a tagged member port, the frame header changes to include the 32–bit tag associated with the ingress port PVID. When a tagged frame exits the switch through a tagged member port, the frame header remains unchanged. The original VLAN ID (VID) remains.

An example using the **`show vlan interface info`** command is provided in Example Checking PVID of ports on page 59.

To ensure that the uplink port(s) are tagged and a member of ALL of the configured VLANs, use the **`show vlan interface vids`** command. An example using the **`show vlan interface vids`** command is provided in Example VLAN Interface VLAN IDs on page 60.

Correct errors by adding missing VLANs to affected uplink ports. Refer to Tagging options on page 61.

Uplink ports not tagged to VLAN recovery tree

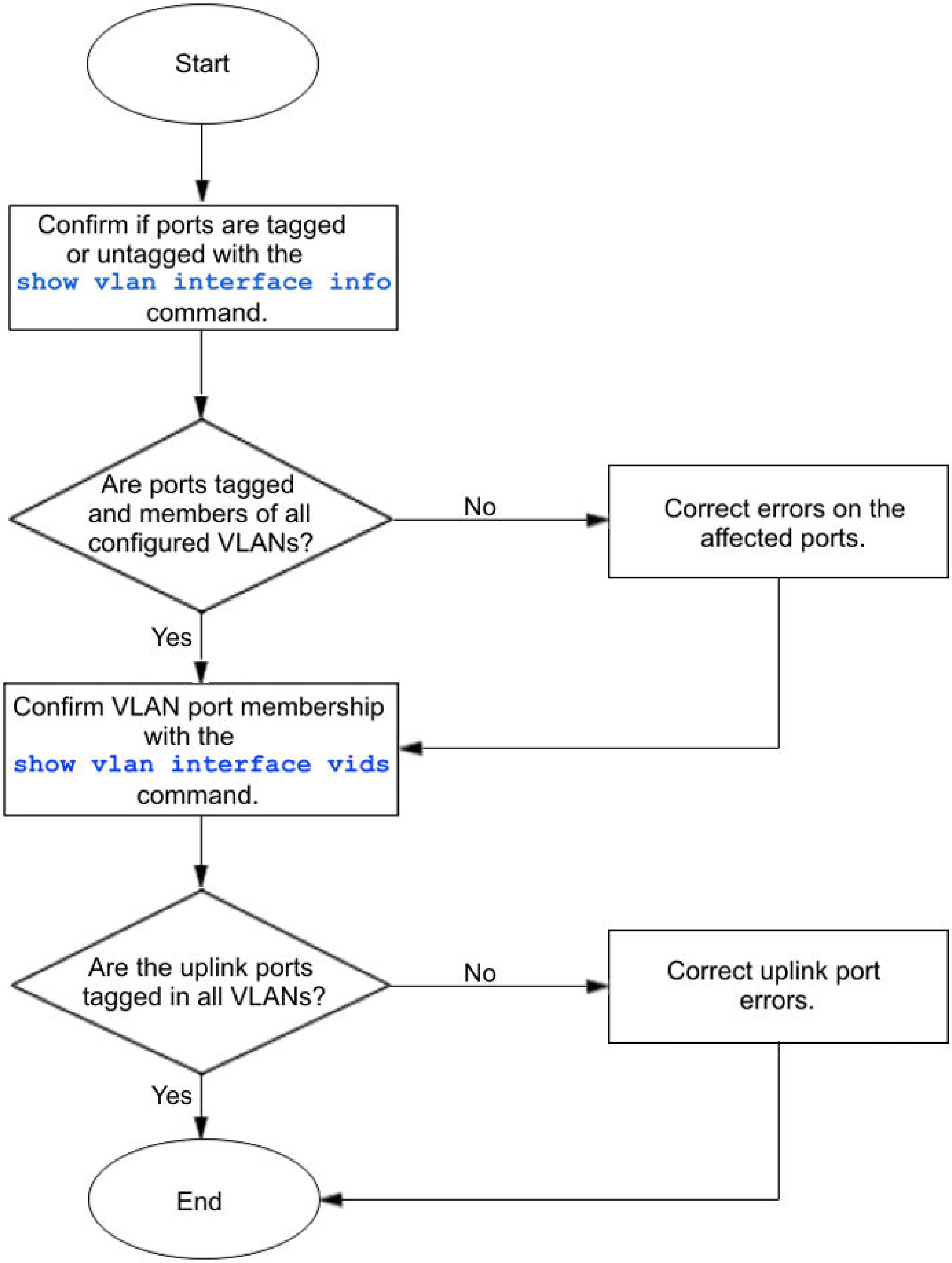

Start
Confirm if ports are tagged or untagged with the show vlan interface info command.
Are ports tagged and members of all configured VLANs?
No
Correct errors on the affected ports.
Yes
Confirm VLAN port membership with the show vlan interface vids command.
Are the uplink ports tagged in all VLANs?
No
Correct uplink port errors.
Yes
End

Figure 4: Uplink ports not tagged to VLAN recovery tree

SNMP

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

SNMP recovery tree

About this task

The following figures show the SNMP recovery tree.

Procedure

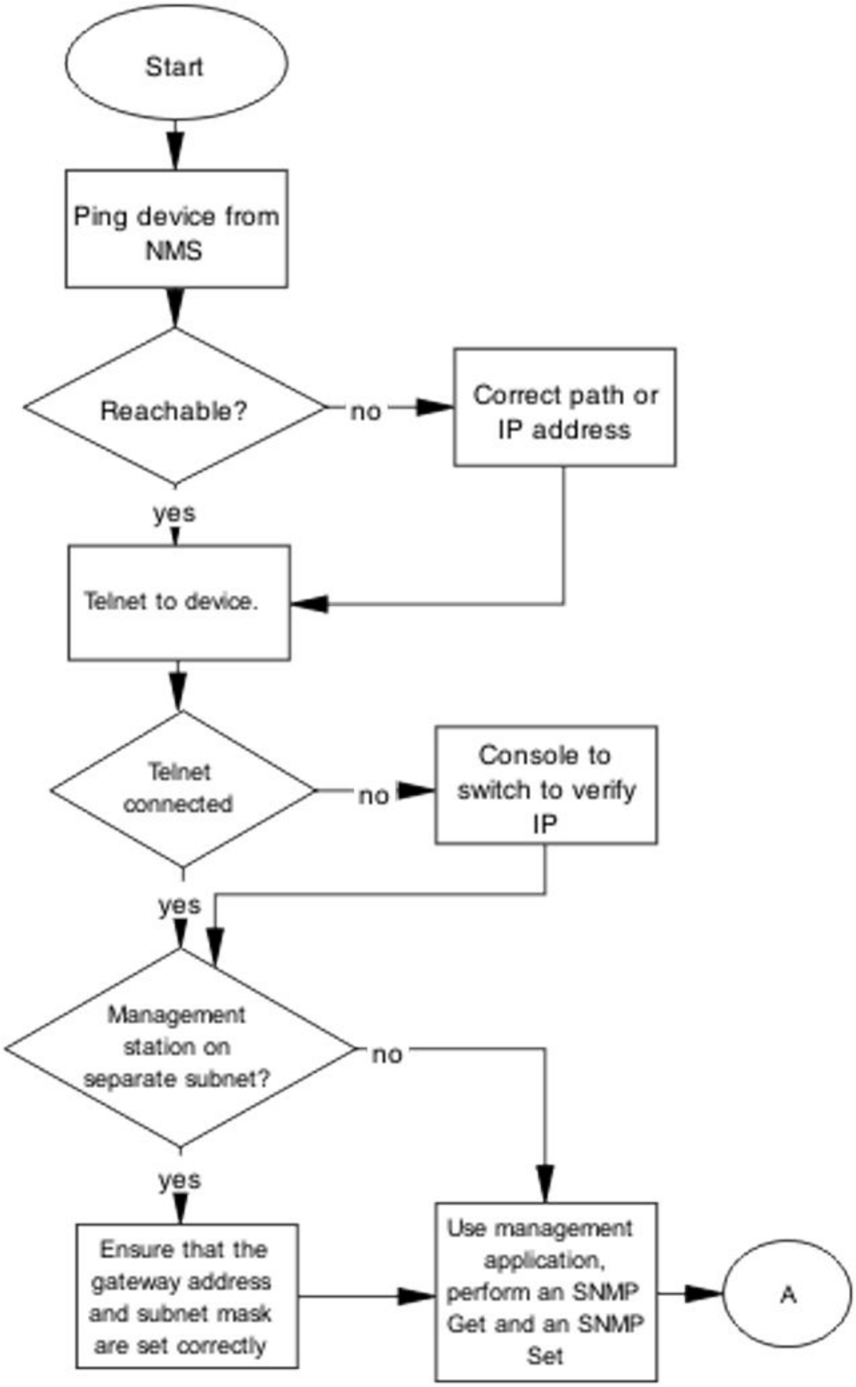

Start
Ping device from NMS
Reachable?
no
Correct path or IP address
yes
Telnet to device.
Telnet connected
no
Console to switch to verify IP
yes
Management station on separate subnet?
no
yes
Ensure that the gateway address and subnet mask are set correctly
Use management application, perform an SNMP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

Figure 5: SNMP part 1

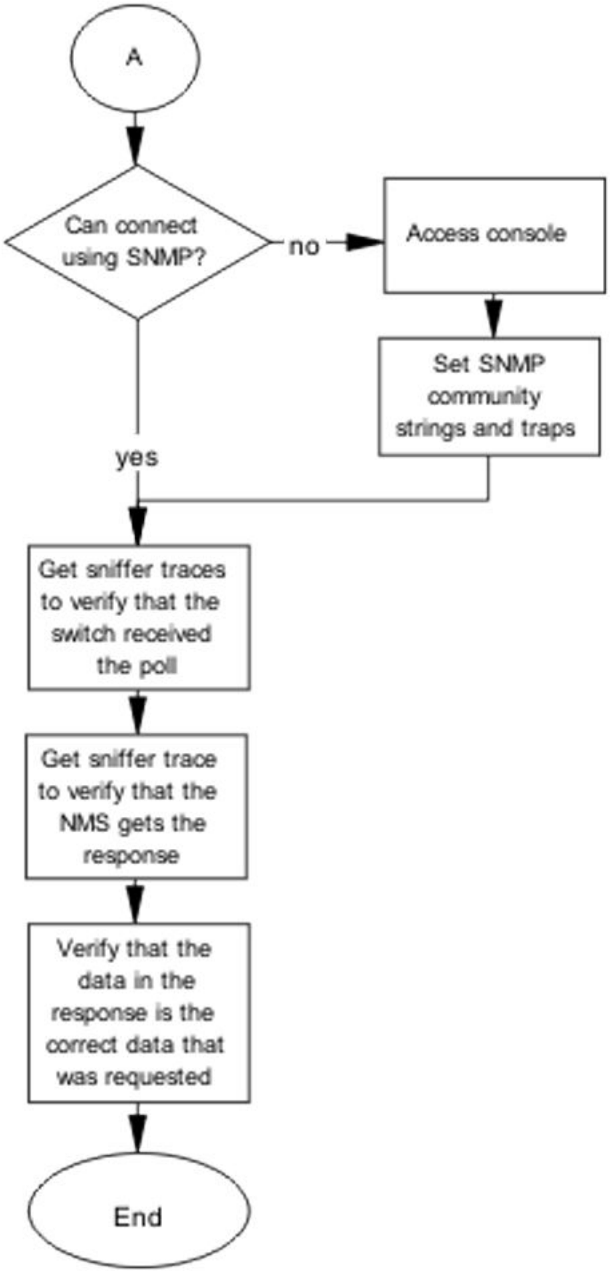

A
Can connect using SNMP?
no
Access console
Set SNMP community strings and traps
yes
Get sniffer traces to verify that the switch received the poll
Get sniffer trace to verify that the NMS gets the response
Verify that the data in the response is the correct data that was requested
End

Figure 6: SNMP part 2

Stack

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

Several situation may cause stacking problems, for example:

- No units have a base switch set to the on position.
- Multiple units have the Base Unit Select switch to the Base position. Only ONE switch in a stack configuration must have the Base Unit Select switch set to this position.
- Cable incorrectly inserted into the corresponding Cascade Up or Cascade Down port..

Stack recovery tree

About this task

The following figures show the stack recovery tree.

Procedure

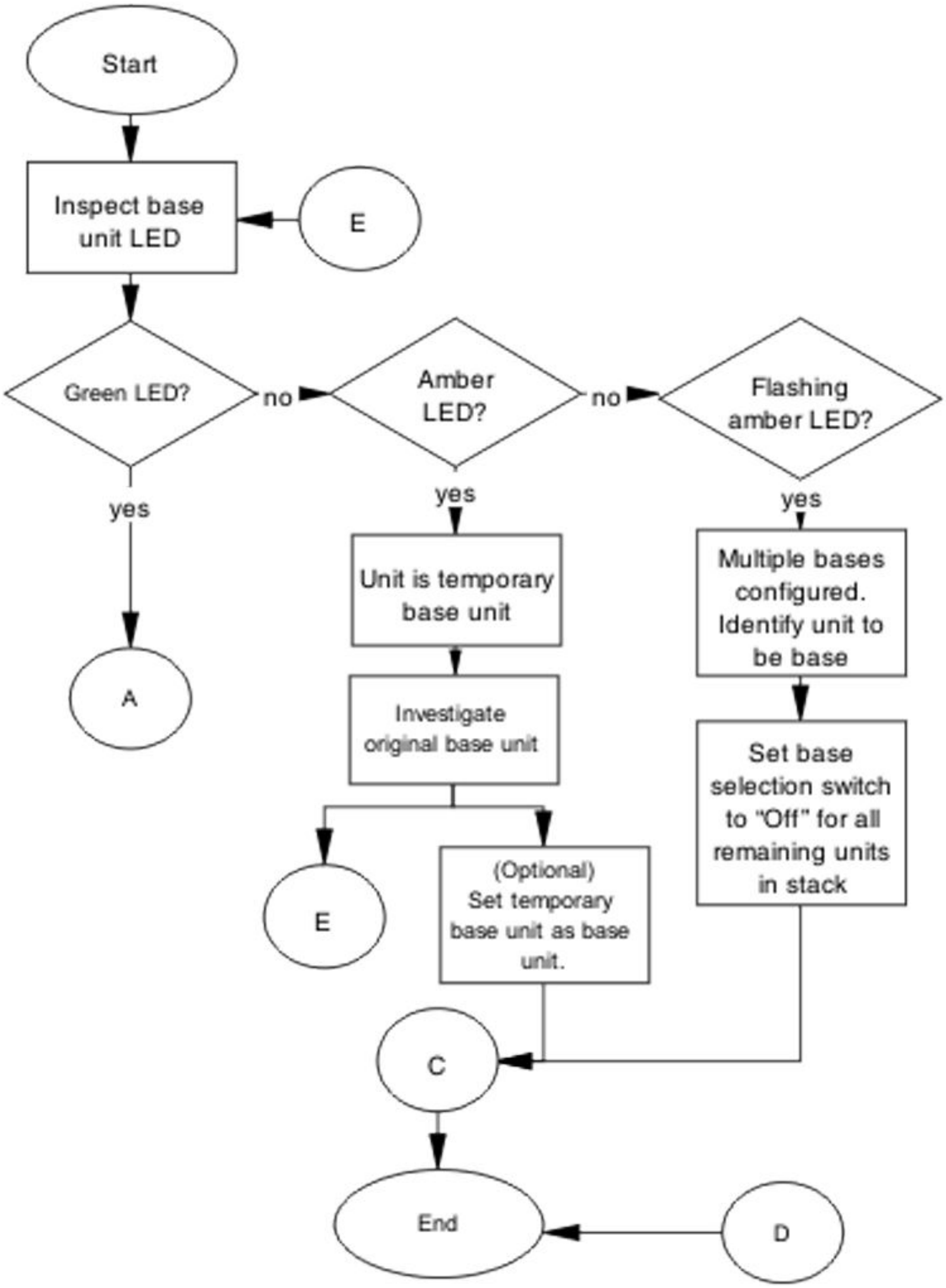

Start
Inspect base unit LED
E
Green LED?
no
Amber LED?
no
Flashing amber LED?
yes
yes
yes
A
Unit is temporary base unit
Investigate original base unit
E
(Optional) Set temporary base unit as base unit.
Multiple bases configured. Identify unit to be base
Set base selection switch to "Off" for all remaining units in stack
C
End
D

Figure 7: Stack part 1

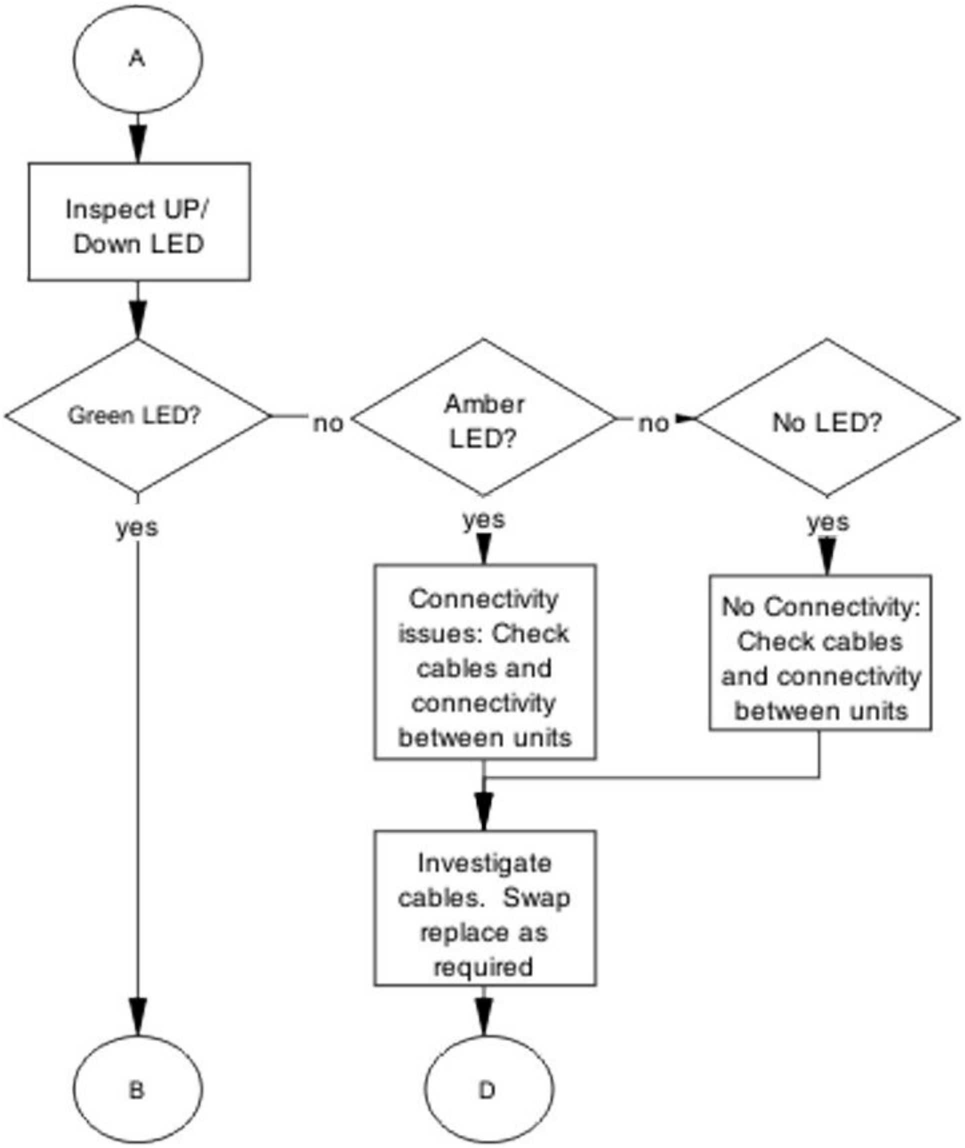

A
Inspect UP/ Down LED
Green LED?
no
Amber LED?
no
No LED?
yes
yes
yes
Connectivity issues: Check cables and connectivity between units
No Connectivity: Check cables and connectivity between units
Investigate cables. Swap replace as required
B
D

Figure 8: Stack part 2

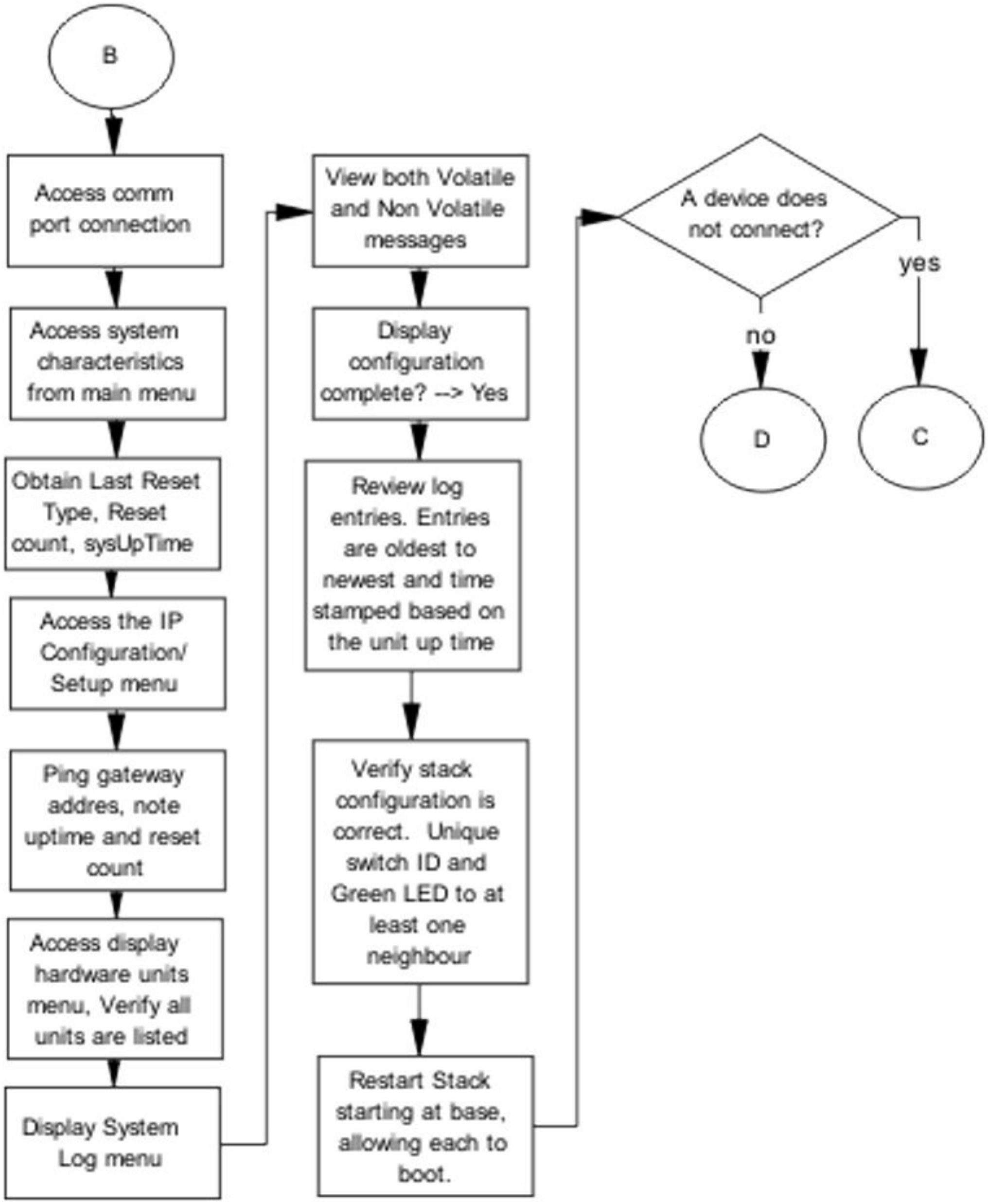

B
Access comm port connection
Access system characteristics from main menu
Obtain Last Reset Type, Reset count, sysUpTime
Access the IP Configuration/ Setup menu
Ping gateway addres, note uptime and reset count
Access display hardware units menu, Verify all units are listed
Display System Log menu
View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

Figure 9: Stack part 3

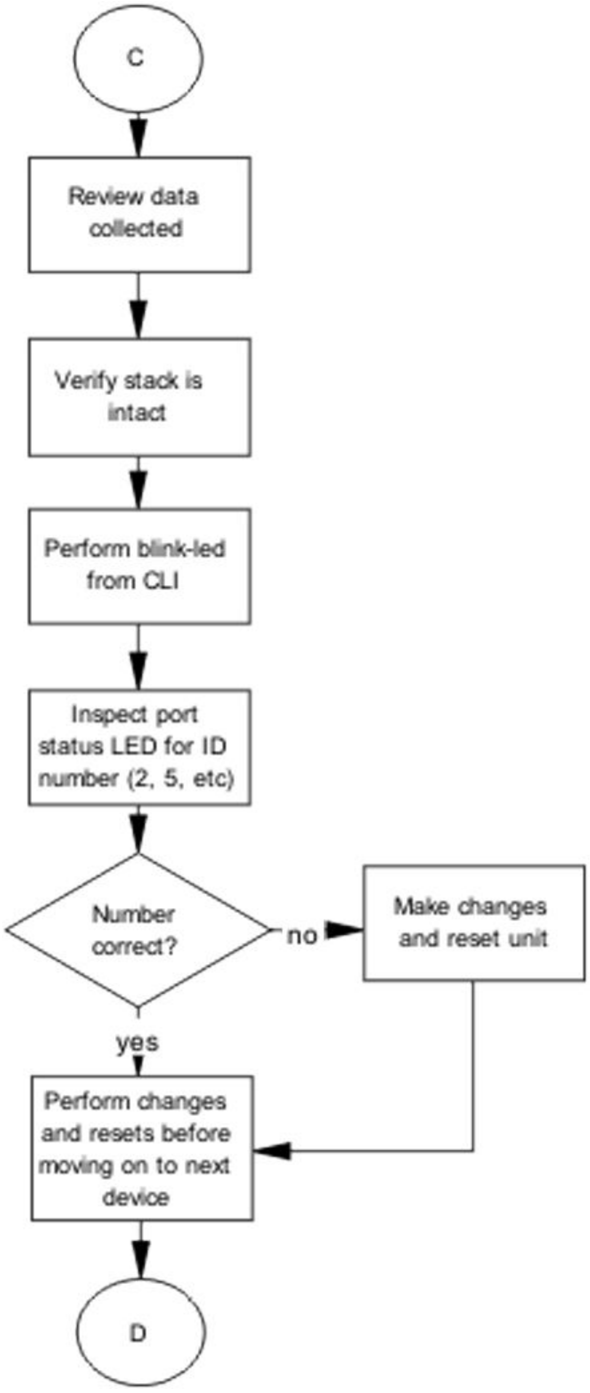

C
Review data collected
Verify stack is intact
Perform blink-led from CLI
Inspect port status LED for ID number (2, 5, etc)
Number correct?
no
Make changes and reset unit
yes
Perform changes and resets before moving on to next device
D

Figure 10: Stack part 4

Dynamic Host Configuration Protocol (DHCP) relay

DHCP and DHCP relay errors are often on the client-side of the communication. In the situation where the DHCP server is not on the same subnet as the client, the DHCP relay configuration may be at fault. If the DHCP snooping application is enabled, then problems may occur if this is improperly configured. For example, the ports that provide connection to the network core or DHCP server are not set as trusted for DHCP snooping.

DHCP recovery tree

About this task

The following figure shows the DHCP relay recovery tree.

Procedure

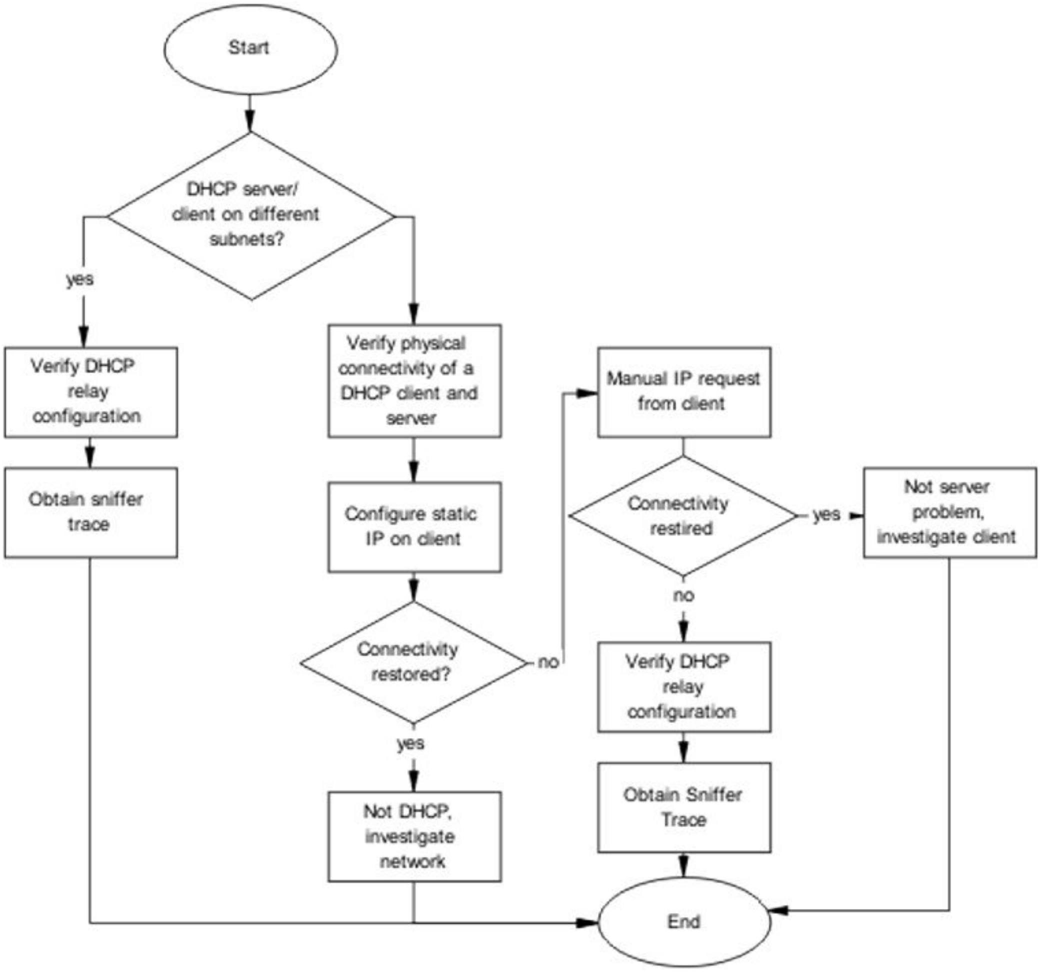

Start
DHCP server/ client on different subnets?
yes
Verify DHCP relay configuration
Obtain sniffer trace
Verify physical connectivity of a DHCP client and server
Configure static IP on client
Connectivity restored?
no
yes
Not DHCP, investigate network
Manual IP request from client
Connectivity restired
yes
Not server problem, investigate client
no
Verify DHCP relay configuration
Obtain Sniffer Trace
End

Figure 11: DHCP

Agent Recovery

In some cases during a software upgrade, the switch turns off before the software agent has been completely written to flash. This may be due to a power outage. In this case, the switch will report an error such as `Agent code verification fails!!`

Units exhibiting the symptoms should NOT be returned through the Return Merchandise Authorization (RMA). They should be corrected in the field.

For assistance with tasks shown in the Agent Recovery emergency recovery tree, see

- Locating the switch console ports on page 57
- Using the Diagnostics Menu on page 58

Agent Recovery Emergency Recovery Tree

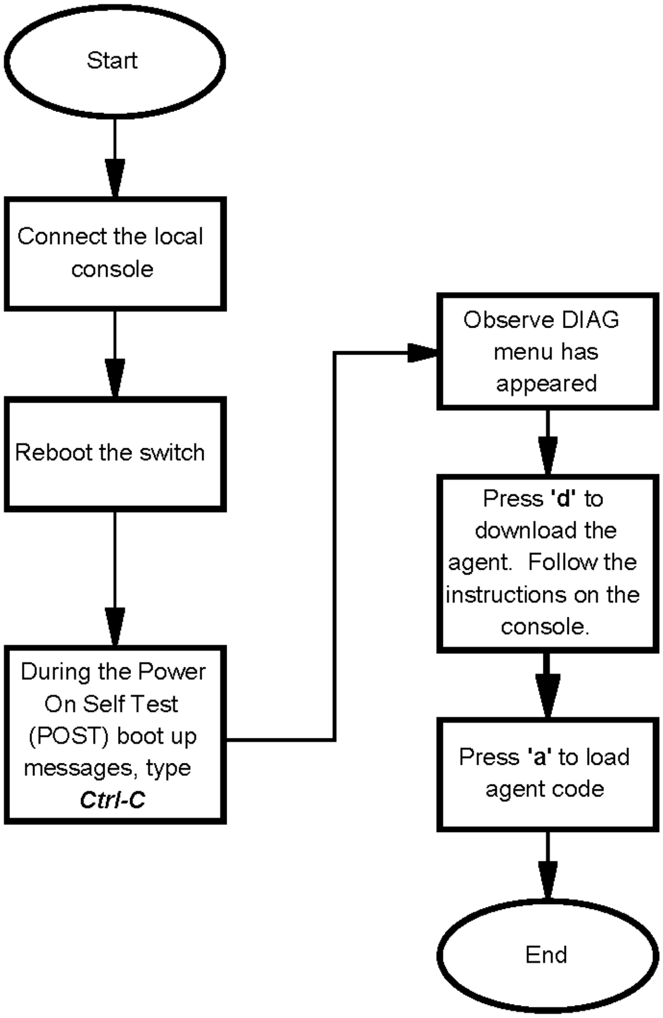

Start
Connect the local console
Reboot the switch
During the Power On Self Test (POST) boot up messages, type ***Ctrl-C***
Observe DIAG menu has appeared
Press **'d'** to download the agent. Follow the instructions on the console.
Press **'a'** to load agent code
End

Figure 12: Agent Recovery Emergency Recovery Tree

AAUR: configuration for the units in the stack is not saved on the base unit

Use the recovery tree in this section if configuration for the units in the stack is not saved on the base unit. The typical scenario is that configuration for a unit in a stack is not saved on the base unit because the AUR Auto-Save is disabled. You can manually save the configuration of a non–base unit to the base unit regardless of the state of the AUR feature.

Configuration for the units in the stack is not saved on the base unit recovery tree

About this task

The following figure shows the recovery tree to save configuration for the units in the stack to the base unit. Check that AUR is enabled. If AUR is not enabled, either save the configuration manually or enable AUR.

Procedure

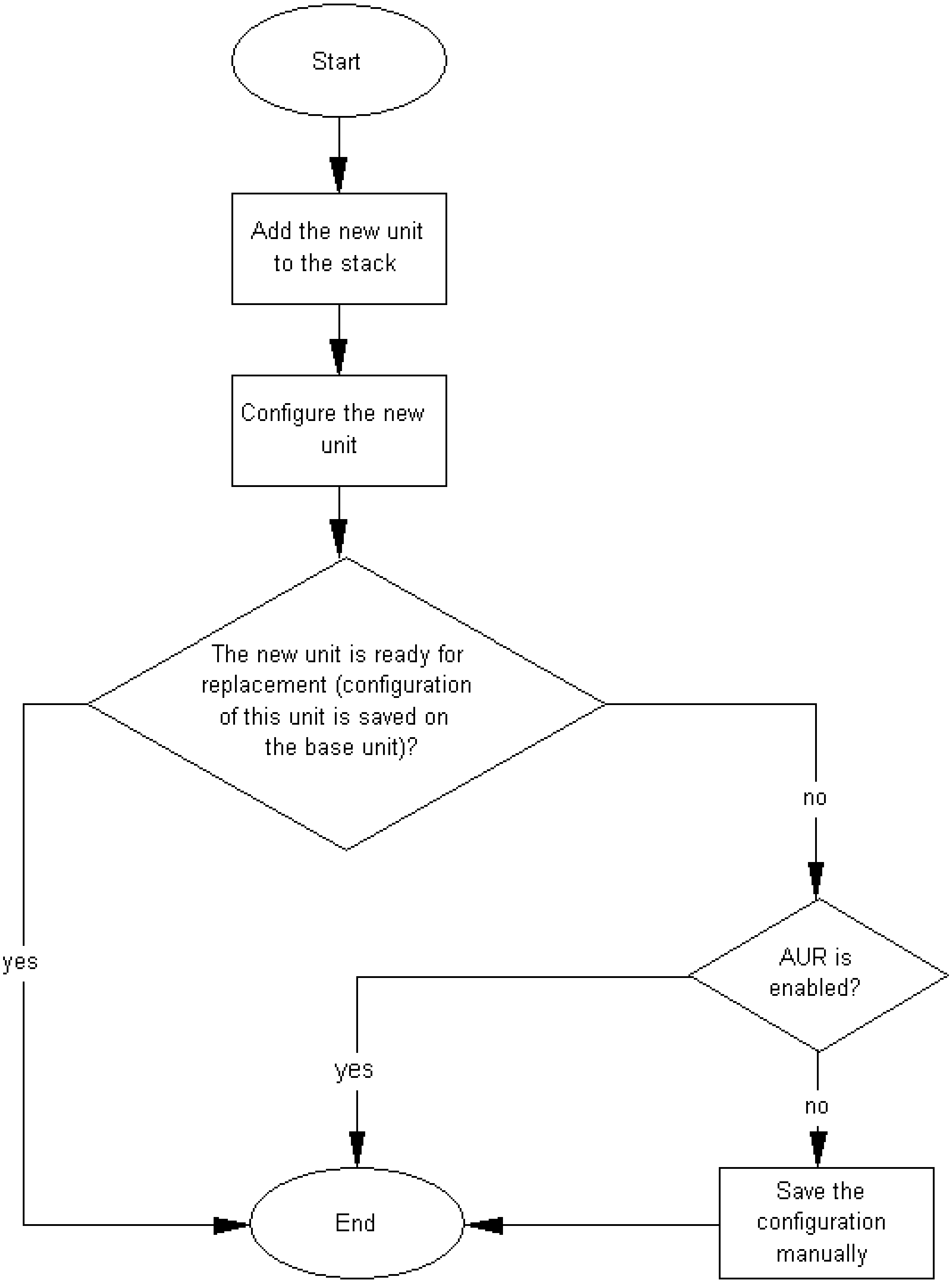

Start
Add the new unit to the stack
Configure the new unit
The new unit is ready for replacement (configuration of this unit is saved on the base unit)?
no
yes
AUR is enabled?
yes
no
Save the configuration manually
End

Figure 13: Configuration for the units in the stack is not saved on the base unit

AAUR: Both units display yes for Ready for Replacement

Use the recovery tree in this section if both units in a stack of two display "yes" for "Ready for Replacement".

Both units display yes for Ready for Replacement recovery tree

About this task

In a stack of two units, you enter the **`show stack auto-unit-replacement`** command and both units display as ready for replacement (only the non–base unit should be ready for replacement in a stack of two units). The following figure shows the recovery tree to correct the issue.

Procedure

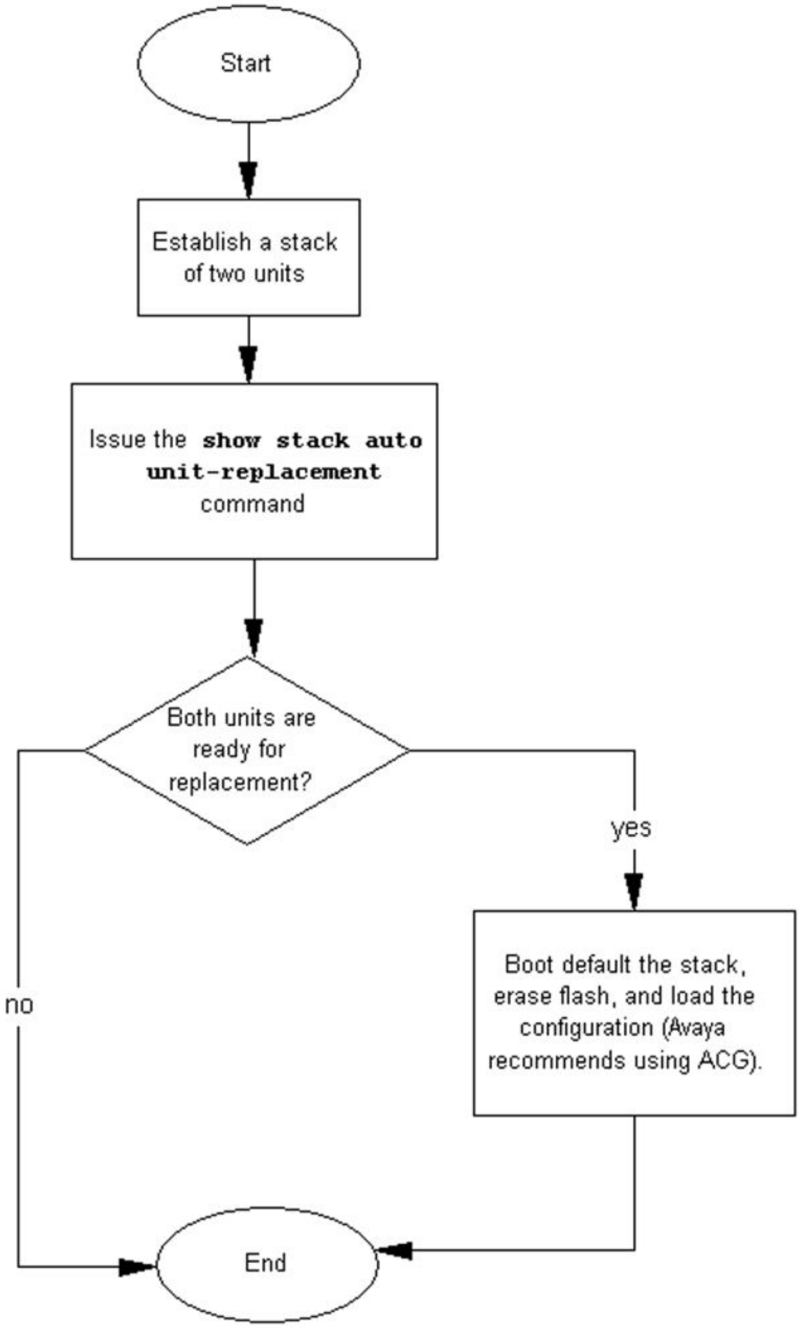

Start
Establish a stack of two units
Issue the **show stack auto unit-replacement** command
Both units are ready for replacement?
yes
no
Boot default the stack, erase flash, and load the configuration (Avaya recommends using ACG).
End

Figure 14: Both units display yes for Ready for Replacement

DAUR

If you add a new unit to a stack, and the units have different diagnostic images, the new unit should start to copy the diagnostic image from the existing stack. Use the recovery tree in this section if the new unit fails to copy the diagnostic image.

Diagnostic image transfer does not start recovery tree

About this task

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

Procedure

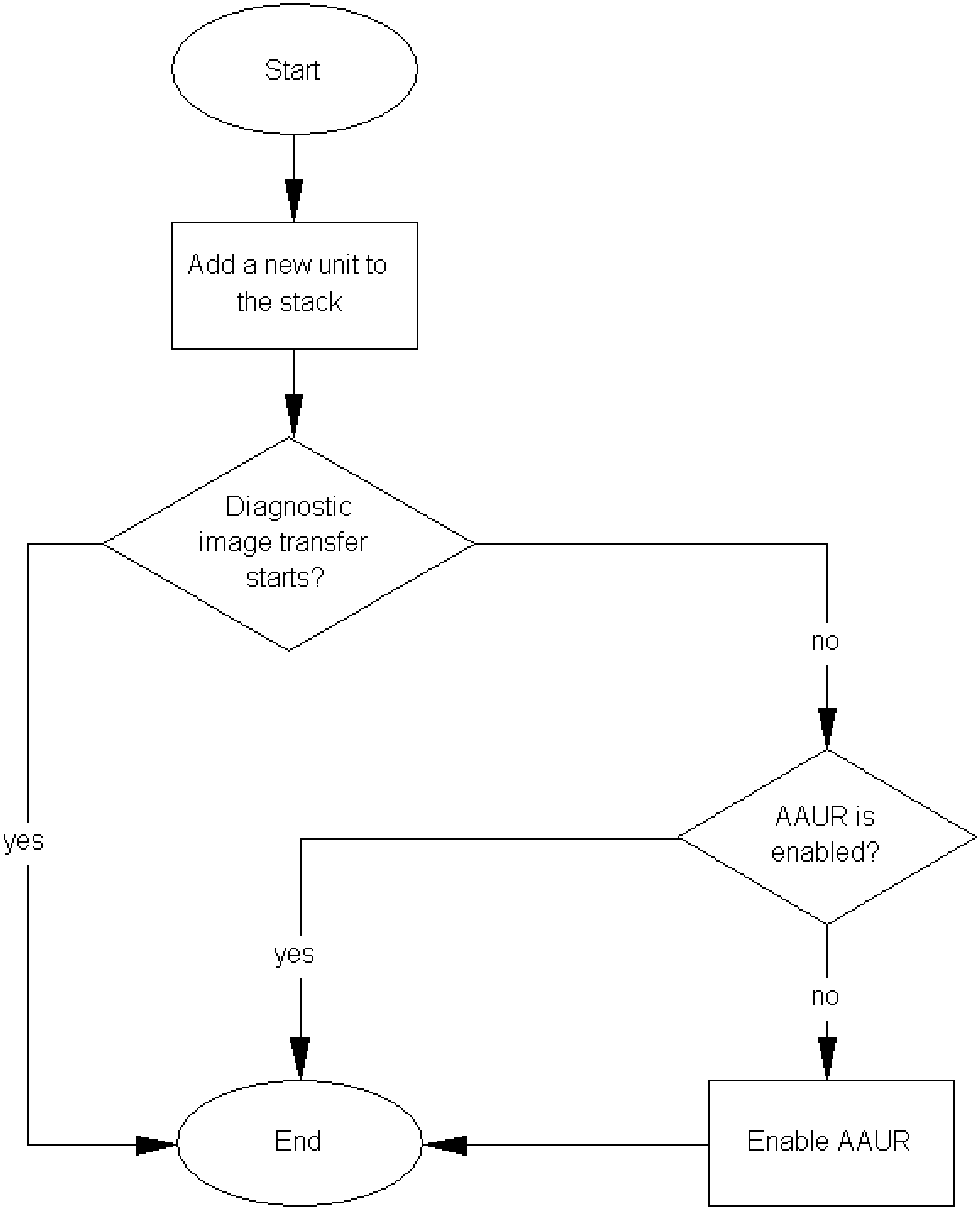

Start
Add a new unit to the stack
Diagnostic image transfer starts?
no
yes
AAUR is enabled?
yes
no
End
Enable AAUR

Figure 15: Diagnostic image transfer does not start

Stack Forced Mode

If you enable the Stack Forced Mode feature and a stack of two units breaks, the standalone switch that results from that broken stack of two is managed using the previous stack IP address. Use the recovery tree in this section if you cannot access the standalone switch using the stack IP address.

You cannot access a switch at the stack IP address using ping, Telnet, SSH, Web, or EDM recovery tree

About this task

If you cannot access a standalone switch in a broken stack of two units, even though you had enabled the Stack Forced Mode feature, check that the standalone device still has a physical connection to the network. The following figure shows the recovery tree for this scenario.

Procedure

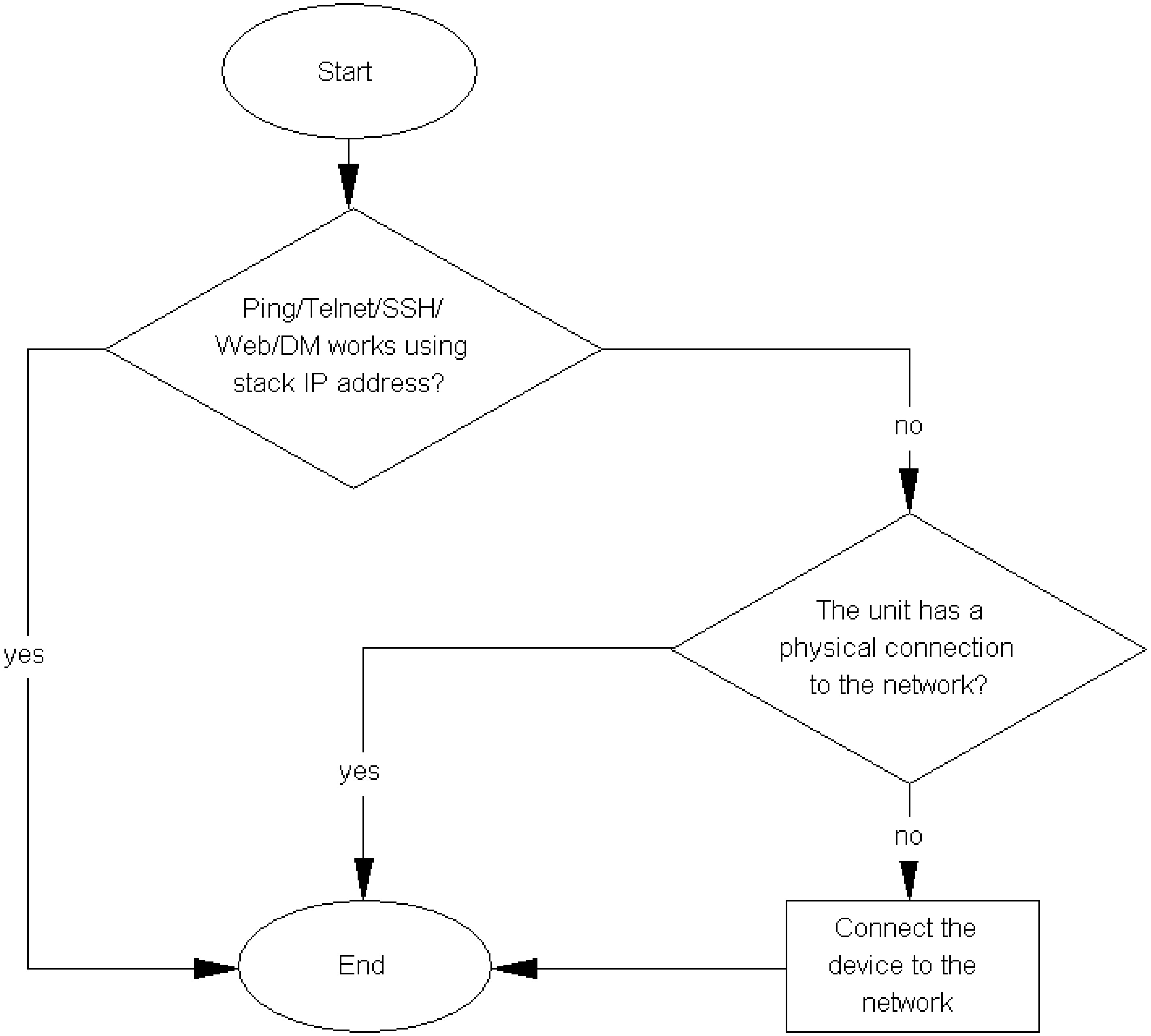

Start
Ping/Telnet/SSH/Web/DM works using stack IP address?
no
yes
The unit has a physical connection to the network?
yes
no
Connect the device to the network
End

Figure 16: Ping/Telnet/SSH/Web/EDM do not work when you use the stack IP address

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

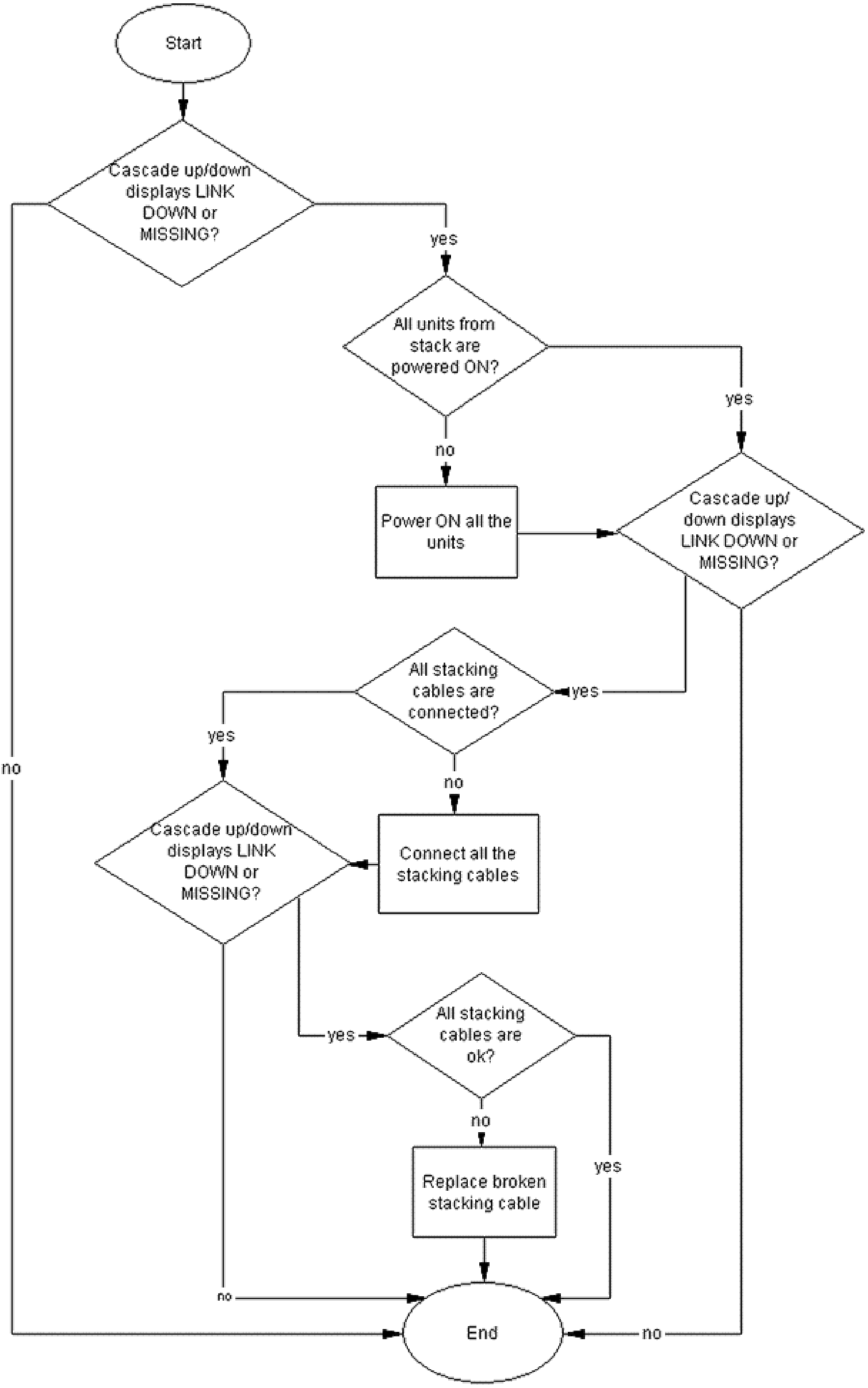
Use the recovery tree in this section if the output from the switch displays "LINK DOWN" or "MISSING" in the Cascade Up or Cascade Down columns when you issue the **`show stack health`** command.

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

About this task

The following figure shows the recovery tree to use if the output from the switch displays "LINK DOWN" or "MISSING" in the Cascade Up or Cascade Down columns when you issue the **`show stack health`** command.

Procedure


Start
Cascade up/down displays LINK DOWN or MISSING?
yes
no
All units from stack are powered ON?
yes
no
Power ON all the units
Cascade up/ down displays LINK DOWN or MISSING?
yes
no
All stacking cables are connected?
yes
no
Connect all the stacking cables
Cascade up/down displays LINK DOWN or MISSING?
yes
no
All stacking cables are ok?
no
yes
Replace broken stacking cable
End

DOWN or MISSING

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

Use the recovery tree in this section if the switch displays “UP WITH ERRORS” in the Cascade Up and Cascade Down columns when you issue the `show stack health` command.

Cascade Up and Cascade Down columns display UP WITH ERRORS recovery tree

About this task

The following figure shows the recovery tree to use if the output from the switch displays "UP WITH ERRORS" in the Cascade Up and Cascade Down columns when you issue the `show stack health` command.

Procedure

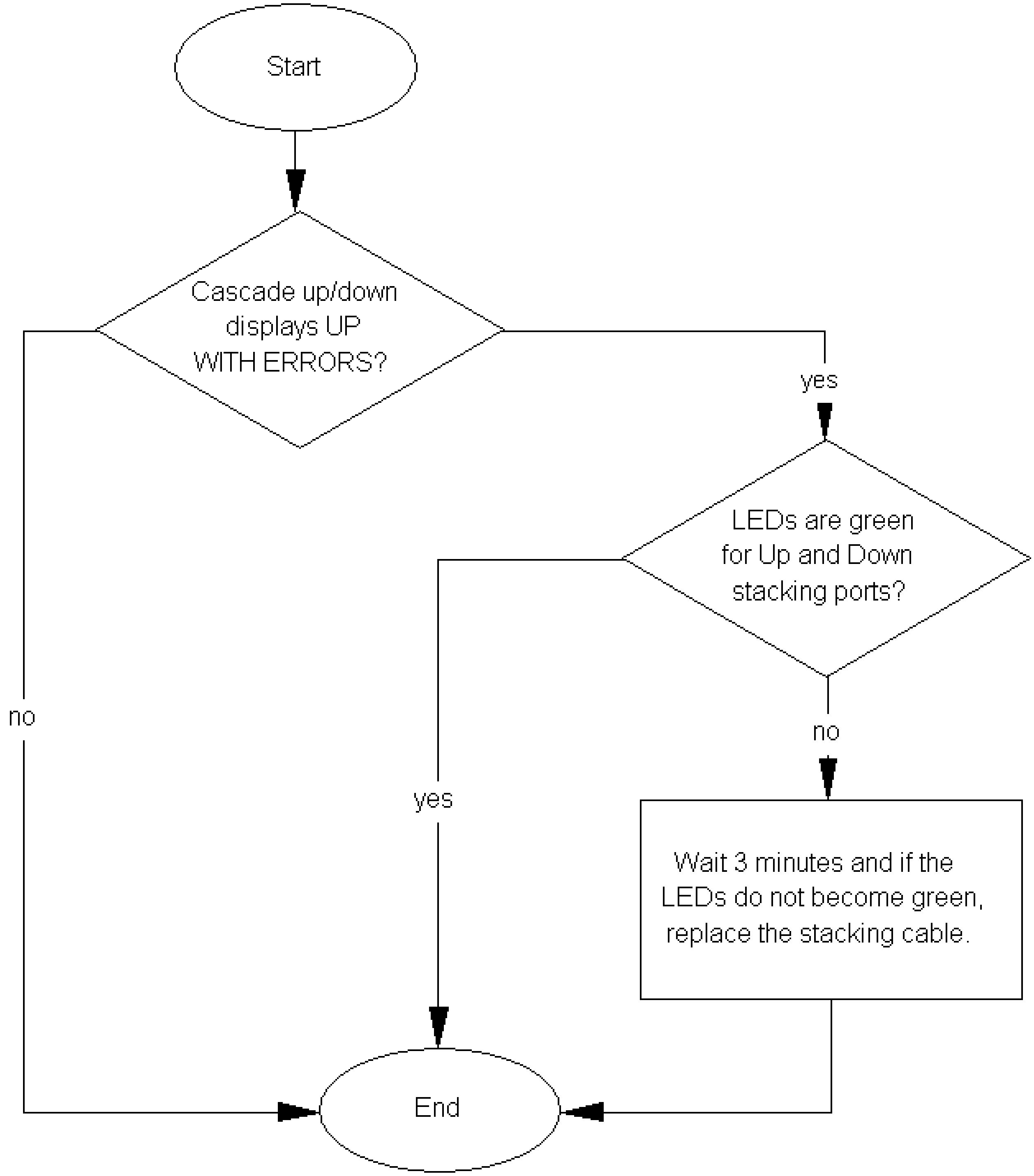
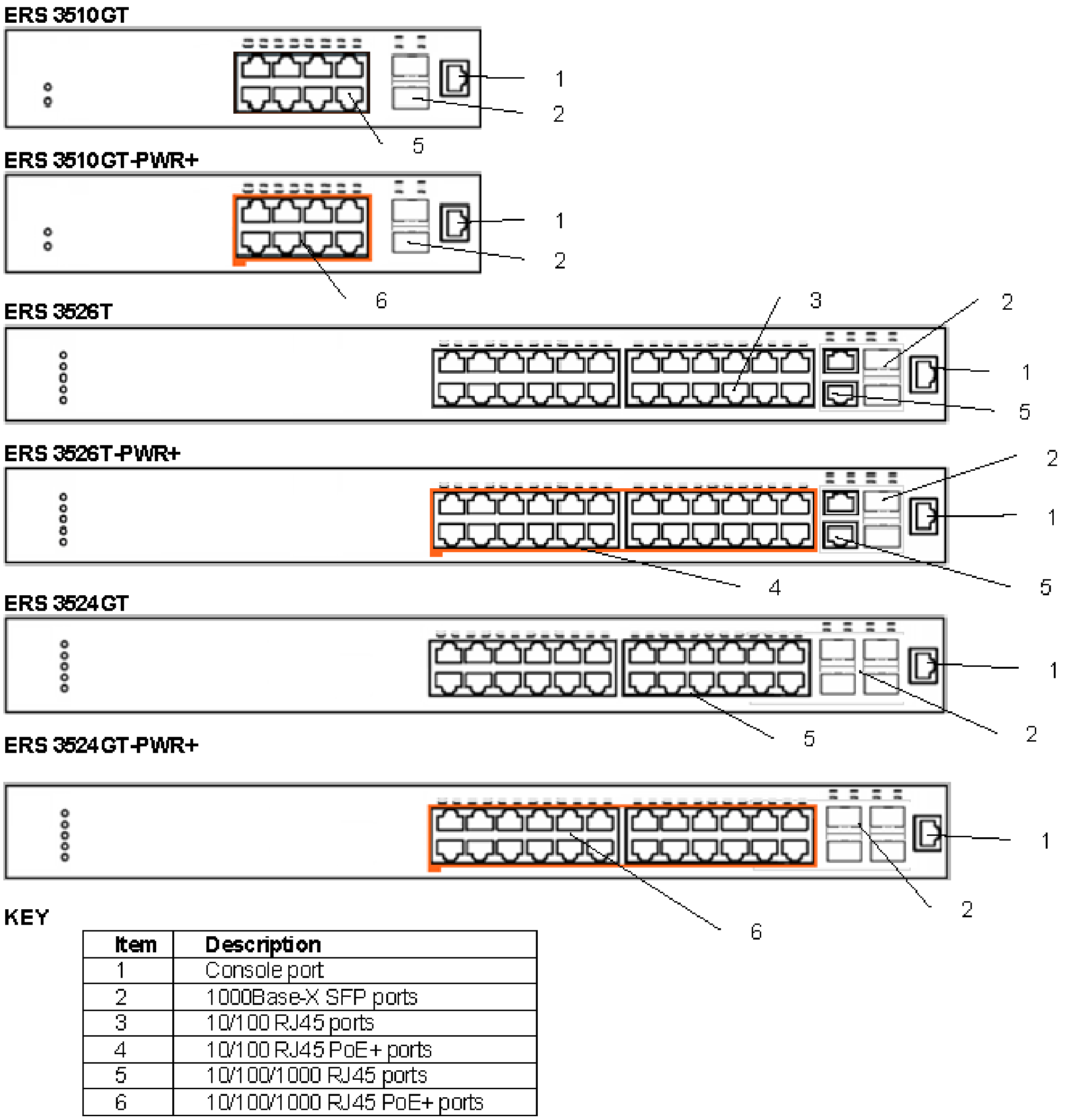

Start
Cascade up/down displays UP WITH ERRORS?
yes
no
LEDs are green for Up and Down stacking ports?
yes
no
Wait 3 minutes and if the LEDs do not become green, replace the stacking cable.
End

Figure 18: Stack Health Check: Cascade Up and Cascade Down columns display UP WITH ERRORS

Locating the switch console ports

The following figure identifies the ports on the ERS 3500 switches:



KEY

Item	Description
1	Console port
2	1000Base-X SFP ports
3	10/100 RJ45 ports
4	10/100 RJ45 PoE+ ports
5	10/100/1000 RJ45 ports
6	10/100/1000 RJ45 PoE+ ports

Figure 19: ERS 3500 Series switch console ports

Using the Diagnostics Menu

On power up, the Power-On Self Tests (POST) are executed and the following is displayed:

```
Test 111     DDRAM Walking 1/0s           -PASSED
Test 112     DDRAM Byte/Word/Long         -PASSED
Test 113     DDRAM Power-of-2             -PASSED
Test 121     ROM Config                   -PASSED
Test 151     FANs Status                  -PASSED
Test 207     XGS SWITCH Registers         -PASSED
Test 221     PHYs Register                -PASSED
Test 271     Ports Internal Loopback      -PASSED
```

If an error is found, the test reports FAILED and an error message is displayed and stored in the Error Log. The Error Log may contain up to 10 POST (or Burn-In) errors. Use the 'e' — **`show errors`** command in the Press menu or the Manufacturing **`SHOWLOG`** command to display errors. Clear errors using the **`INITLOG`** command.

If you type `CTRL-C` on the console during the power-up or reset sequence, the Diagnostics display the following break message:

```
       >>Break Recognized - Wait . .
```

After Diagnostics finish initializing, the “Press” menu is displayed:

```
Press 'a'   to run Agent Code
Press 'd'   to download agent/diag/bootloader code
Press 'e'   to display Errors
Press 'i'   to initialize config flash
Press 'p'   to run POST tests
Press 'r'   to reset the box.
```

<table>
<tr><th>If you press . . .</th><th>Result</th></tr>
<tr><td>a</td><td>Diagnostics executes the Agent code (if present):
<pre>
Starting Agent Version: 5.0.0.xxx
Decompressing the image   done,
Initializing . . . .
</pre></td></tr>
<tr><td>d</td><td>The following information is required:
<pre>
Enter Port Number   [<all>]:
Enter Speed: 10, 100 or 1G   [100]:
Enter Local IP Address   [0.0.0.0]:
Enter Server IP Address   [0.0.0.0]:
Enter Subnet Mask   [255.255.255.0]:
Enter Filename:
</pre></td></tr>
<tr><td>e</td><td>The POST test errors are re-displayed:
<pre>
System Resets   =   1.
Burn-In Loops   =   0.
Burn-In Errors   = DISABLED
Default Baud   =   9600

Error Log:
</pre></td></tr>
</table>

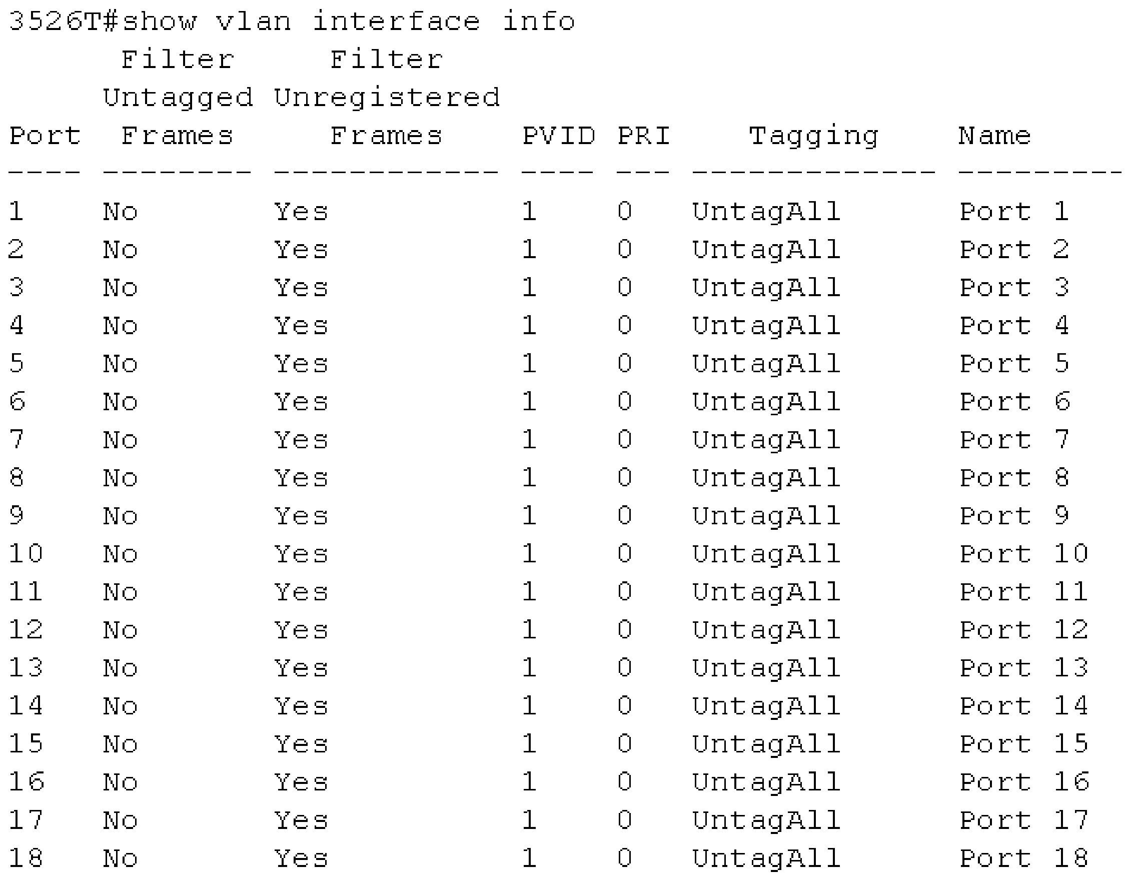
If you press . . .	Result

	`Bad Port Mask   = 00000000`
	`Loop Test Error Description:`
	`<errors>`

i	The flash config/log area is initialized. This area is used by the Agent code.
p	The POST tests are executed again.
r	Resets the switch

Example Checking PVID of ports

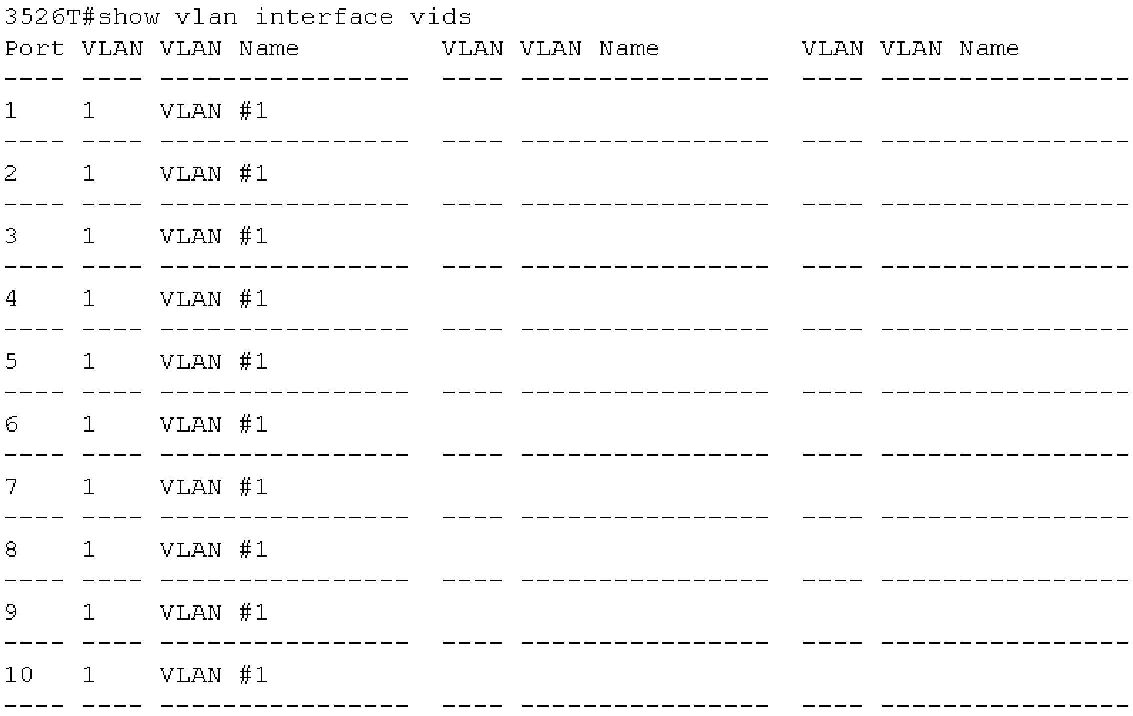
The following figure shows output from the **`show vlan interface info`** command.



```
3526T#show vlan interface info
      Filter     Filter
     Untagged Unregistered
Port  Frames     Frames     PVID PRI    Tagging     Name
---- -------- ------------ ---- --- ------------- ---------
1    No       Yes          1    0   UntagAll      Port 1
2    No       Yes          1    0   UntagAll      Port 2
3    No       Yes          1    0   UntagAll      Port 3
4    No       Yes          1    0   UntagAll      Port 4
5    No       Yes          1    0   UntagAll      Port 5
6    No       Yes          1    0   UntagAll      Port 6
7    No       Yes          1    0   UntagAll      Port 7
8    No       Yes          1    0   UntagAll      Port 8
9    No       Yes          1    0   UntagAll      Port 9
10   No       Yes          1    0   UntagAll      Port 10
11   No       Yes          1    0   UntagAll      Port 11
12   No       Yes          1    0   UntagAll      Port 12
13   No       Yes          1    0   UntagAll      Port 13
14   No       Yes          1    0   UntagAll      Port 14
15   No       Yes          1    0   UntagAll      Port 15
16   No       Yes          1    0   UntagAll      Port 16
17   No       Yes          1    0   UntagAll      Port 17
18   No       Yes          1    0   UntagAll      Port 18
```

Example VLAN Interface VLAN IDs

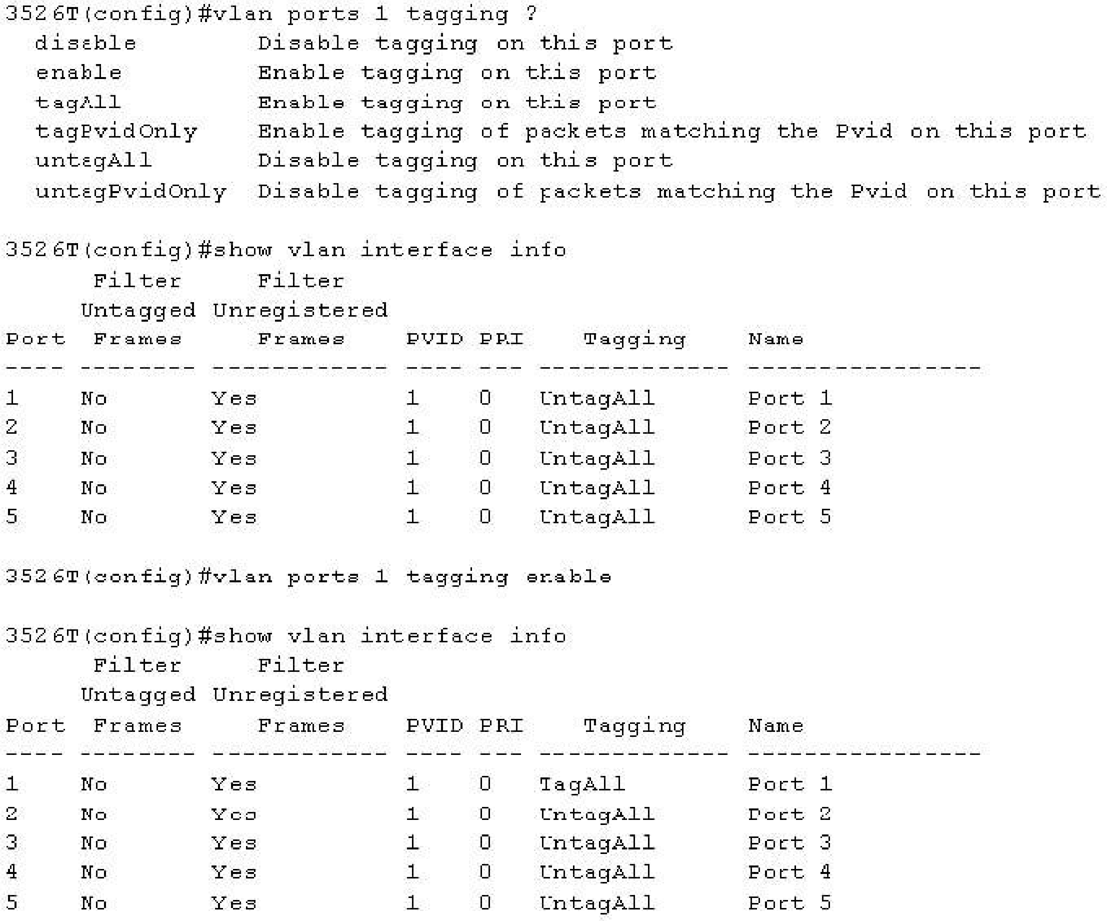
The following figure provides example output from the **`show vlan interface vids`** command.



```
3526T#show vlan interface vids
Port VLAN VLAN Name         VLAN VLAN Name         VLAN VLAN Name
---- ---- ----------------  ---- ----------------  ---- ----------------
1    1    VLAN #1
---- ---- ----------------  ---- ----------------  ---- ----------------
2    1    VLAN #1
---- ---- ----------------  ---- ----------------  ---- ----------------
3    1    VLAN #1
---- ---- ----------------  ---- ----------------  ---- ----------------
4    1    VLAN #1
---- ---- ----------------  ---- ----------------  ---- ----------------
5    1    VLAN #1
---- ---- ----------------  ---- ----------------  ---- ----------------
6    1    VLAN #1
---- ---- ----------------  ---- ----------------  ---- ----------------
7    1    VLAN #1
---- ---- ----------------  ---- ----------------  ---- ----------------
8    1    VLAN #1
---- ---- ----------------  ---- ----------------  ---- ----------------
9    1    VLAN #1
---- ---- ----------------  ---- ----------------  ---- ----------------
10   1    VLAN #1
---- ---- ----------------  ---- ----------------  ---- ----------------
```

Tagging options

Use the commands and outputs in this example to assist in adding missing VLANs to affected uplink ports.



```
3526T(config)#vlan ports 1 tagging ?
  disable         Disable tagging on this port
  enable          Enable tagging on this port
  tagAll          Enable tagging on this port
  tagPvidOnly     Enable tagging of packets matching the Pvid on this port
  untagAll        Disable tagging on this port
  untagPvidOnly   Disable tagging of packets matching the Pvid on this port

3526T(config)#show vlan interface info
       Filter      Filter
      Untagged Unregistered
Port  Frames      Frames     PVID PRI    Tagging     Name
---- -------- ------------ ---- --- ------------- ----------------
1     No       Yes          1    0   UntagAll      Port 1
2     No       Yes          1    0   UntagAll      Port 2
3     No       Yes          1    0   UntagAll      Port 3
4     No       Yes          1    0   UntagAll      Port 4
5     No       Yes          1    0   UntagAll      Port 5

3526T(config)#vlan ports 1 tagging enable

3526T(config)#show vlan interface info
       Filter      Filter
      Untagged Unregistered
Port  Frames      Frames     PVID PRI    Tagging     Name
---- -------- ------------ ---- --- ------------- ----------------
1     No       Yes          1    0   TagAll        Port 1
2     No       Yes          1    0   UntagAll      Port 2
3     No       Yes          1    0   UntagAll      Port 3
4     No       Yes          1    0   UntagAll      Port 4
5     No       Yes          1    0   UntagAll      Port 5
```

Chapter 9: Troubleshooting hardware

Use this section for hardware troubleshooting specific to the Ethernet Routing Switch 3500 Series.

Work flow Troubleshooting hardware

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

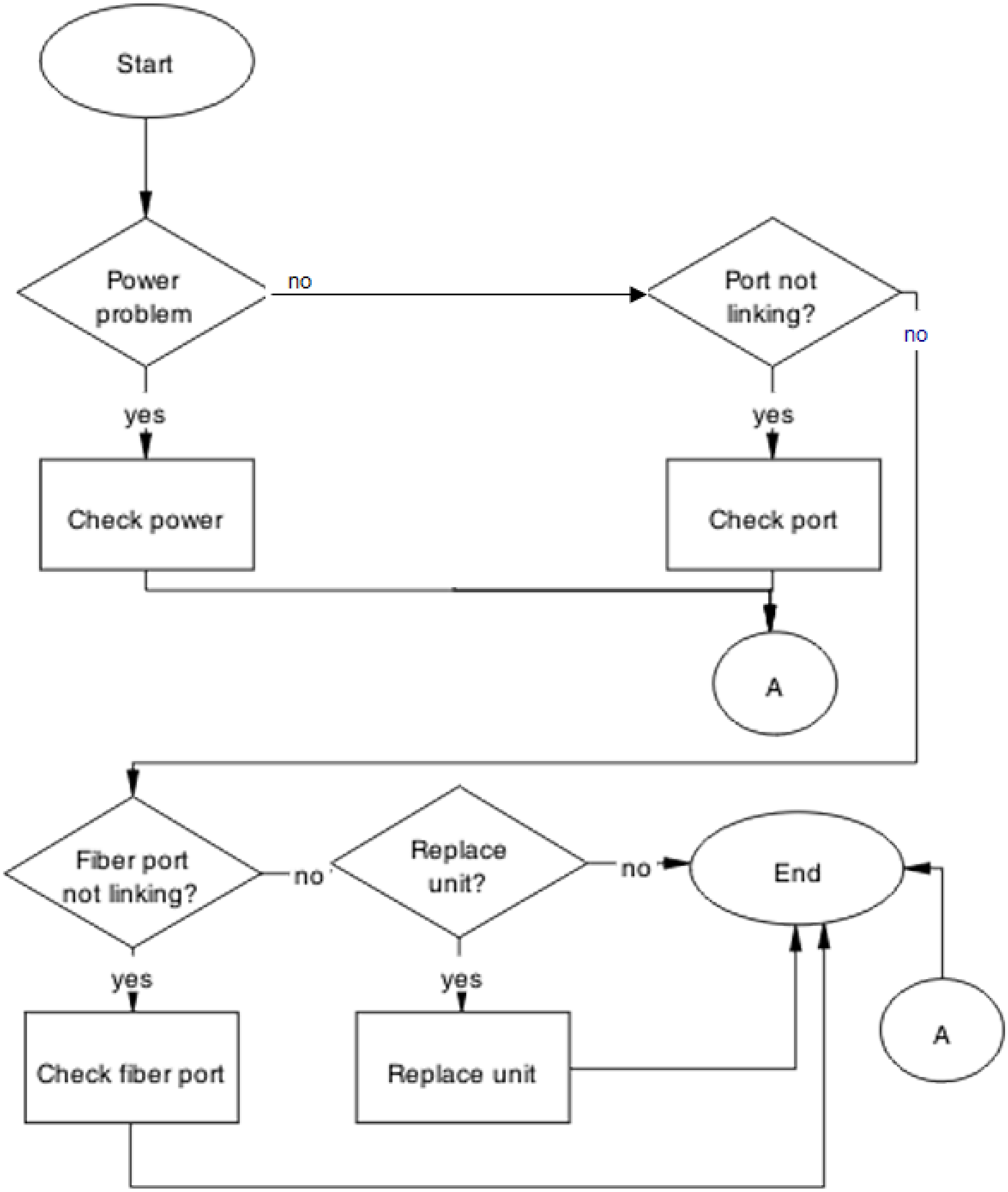


Figure 20: Troubleshooting hardware

Check power

Confirm power is being delivered to the device.

Task flow Check power

The following task flow assists you to confirm that the Ethernet Routing Switch 3500 Series device is powered correctly.

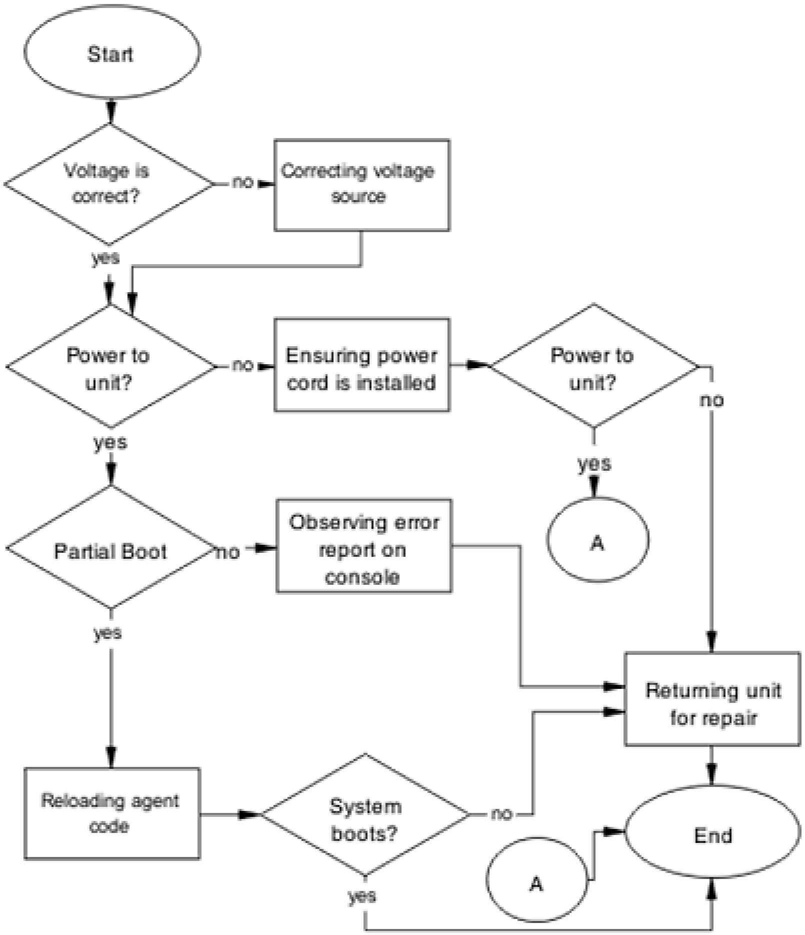


Figure 21: Check power

Correcting voltage source

Confirm the power cord is connected to the appropriate voltage source.

Ensuring power cord is installed

Confirm the power cord is properly installed for the device. All power cords are to be firmly seated.

Observing error report on console

Check the message that is sent to the console after a failure.

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

Reloading agent code

Reload the agent code on the Ethernet Routing Switch 3500 Series device to eliminate corrupted or damaged code that causes a partial boot of the device.

⚠ **Caution:**

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

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

1. Use the show sys-info command to view the software version.
2. See *Avaya Ethernet Routing Switch 3500 Series Release 5.0 Release Notes* (NN47203-400) for information about software installation.

Returning unit for repair

Return unit to Avaya for repair.

Contact Avaya for return instructions and RMA information.

Check port

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

Task flow Check port

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

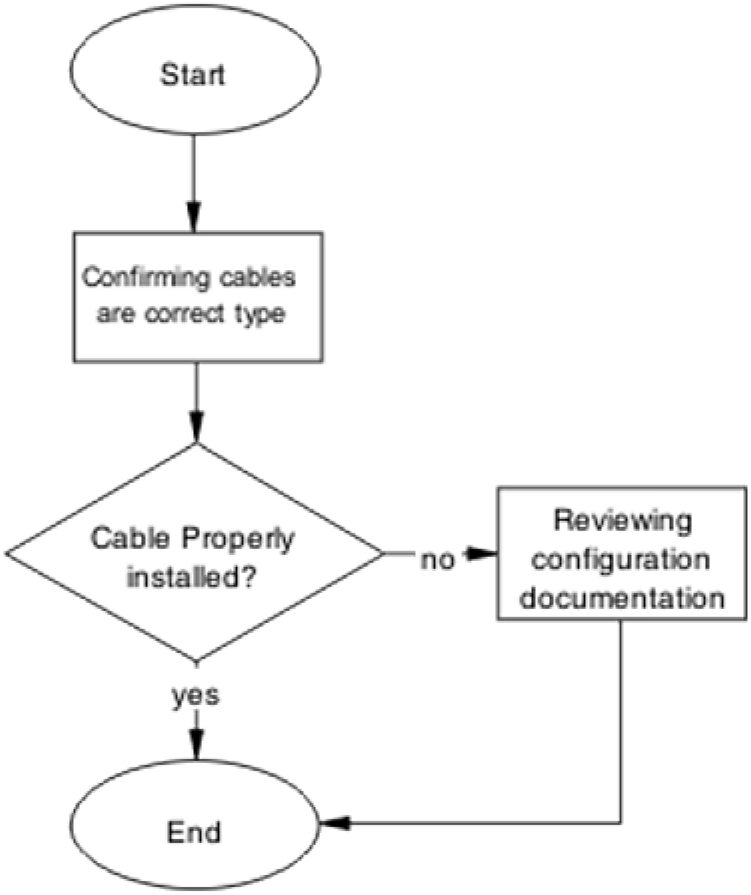

Start
Confirming cables are correct type
Cable Properly installed?
no
Reviewing configuration documentation
yes
End

Figure 22: Check port

Viewing port information

Review the port information to ensure that the port is enabled.

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

Enabling the port

Enable the port.

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

Confirming the cables are working

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

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

Check fiber port

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

Task flow Check fiber port

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

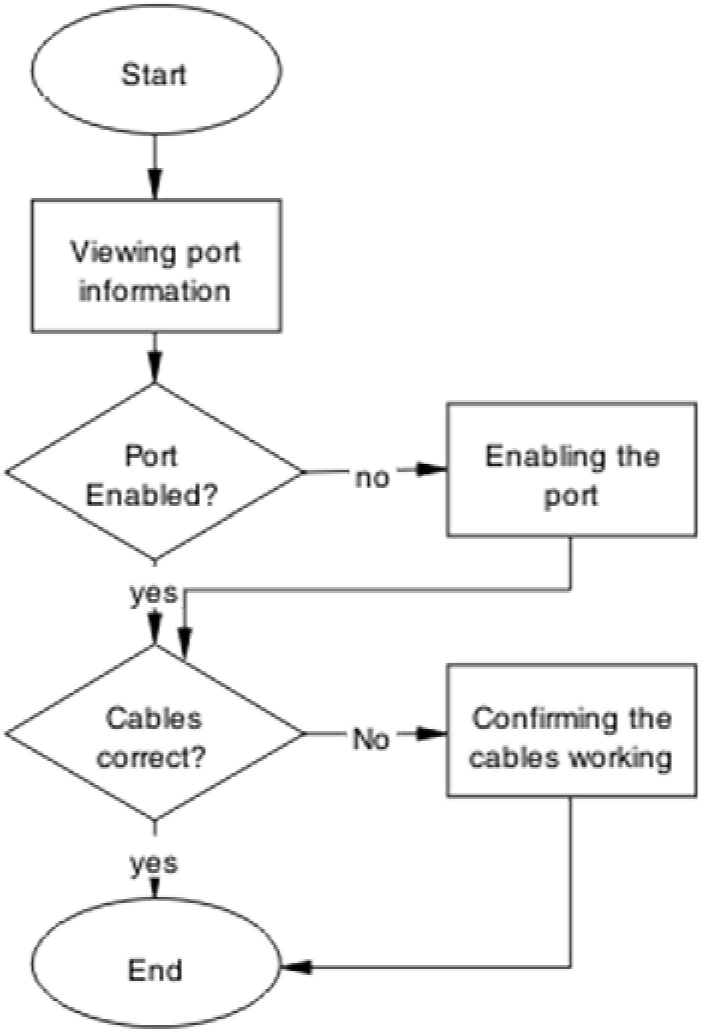


Figure 23: Check fiber port

Viewing fiber port information

Review the port information to ensure the port is enabled.

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

Enabling the port

Ensure the port on the Ethernet Routing Switch 3500 series device is enabled.

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

Confirming cables are working

Confirm that the cables are working on the port.

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

Returning unit for repair

Return unit to Avaya for repair.

Contact Avaya for return instructions and RMA information.

Replace unit

Remove defective unit and insert the replacement.

⚠ **Caution:**

Due to physical handling of the device and your physical proximity to electrical equipment, review and adhere to all safety instructions and literature included with device and in *Avaya Ethernet Routing Switch 3500 Series – Regulatory Information* (NN47203-100).

Verifying software version is correct on new device

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

1. Connect the new device to the console.
2. Use the `show sys-info` command to view the software version.

Powering on the unit

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

Prerequisites

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

Note:

Stacking is not available in Release 5.0.

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

Returning unit for repair

Return unit to Avaya for repair.

Contact Avaya for return instructions and RMA information.

Chapter 10: Troubleshooting ADAC

Automatic Detection and Automatic Configuration (ADAC) can encounter detection and configuration errors that can be easily corrected.

ADAC clarifications

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

You do not manually create a VLAN to be used as the voice VLAN and then try to set this VLAN as the ADAC voice VLAN using the command `adac voice-vlan x`. ADAC automatically creates the voice VLAN when needed. You only have to reserve or set the VLAN number used by ADAC with the `adac voice-vlan x` command.

After the VLAN number is reserved as the ADAC voice VLAN using the `adac voice-vlan x` command, even if the ADAC administrative status is disabled or ADAC is in UTF mode, the VLAN number cannot be used by anyone else in regular VLAN creation.

If you enable the LLDP detection mechanism for telephony ports, then LLDP itself has to be enabled on the switch. Otherwise, ADAC does not detect phones.

Work flow Troubleshooting ADAC

The following work flow assists you to identify the type of problem you are encountering.

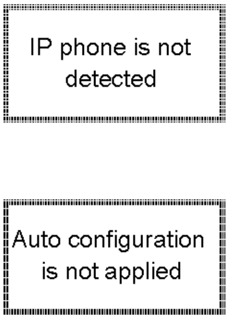


Figure 24: Troubleshooting ADAC

IP phone is not detected

Correct an IP phone that is not being detected by ADAC.

Work flow IP phone not detected

The following work flow assists you to resolve detection issues.

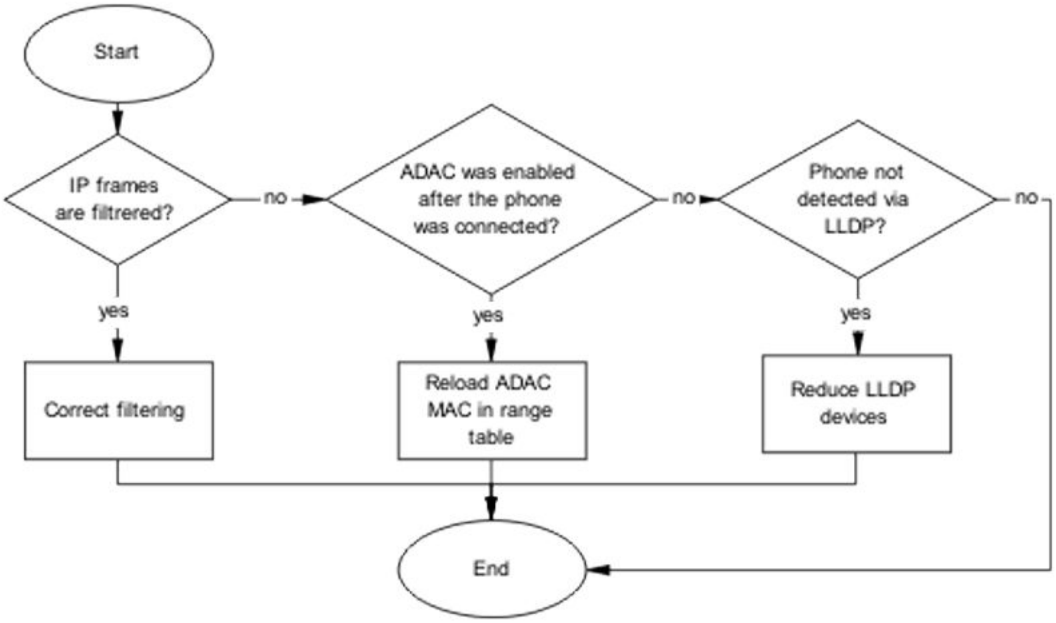

Start
IP frames are filtrered?
no
yes
Correct filtering
ADAC was enabled after the phone was connected?
no
yes
Reload ADAC MAC in range table
Phone not detected via LLDP?
no
yes
Reduce LLDP devices
End

Figure 25: IP phone not detected

Correct filtering

Configure the VLAN filtering to allow ADAC.

Task flow Correct filtering

The following task flow assists you to correct the filtering.

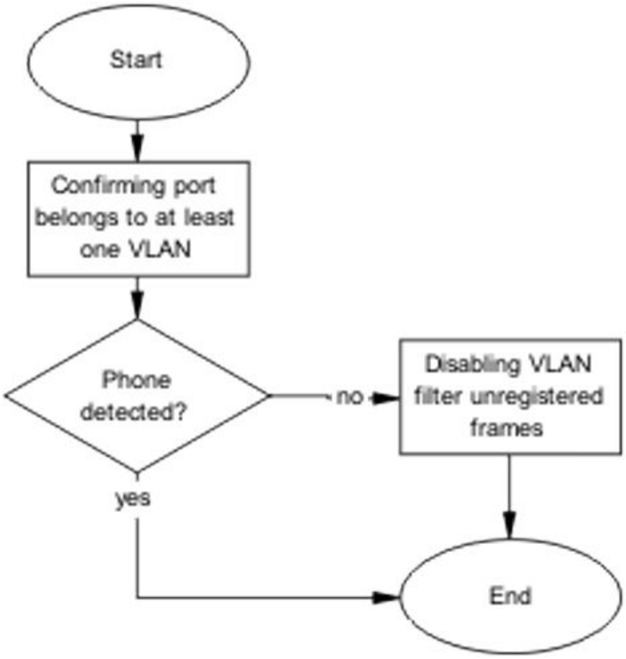

Start
Confirming port belongs to at least one VLAN
Phone detected?
no
Disabling VLAN filter unregistered frames
yes
End

Figure 26: Correct filtering

Confirming port belongs to at least one VLAN

View information to ensure that the port belongs to a VLAN.

1. Use the show vlan interface info <port> command to view the details.
2. Note the VLANs listed with the port.

Disabling the VLAN filtering of unregistered frames

Change the unregistered frames filtering of the VLAN.

1. Use the `vlan ports <port> filter-unregistered-frames enable` command to view the details.
2. Ensure no errors after command execution.

Reload ADAC MAC in range table

Ensure the ADAC MAC address is properly loaded in the range table.

Task flow Reload ADAC MAC in range table

The following task flow assists you to place the ADAC MAC address in the range table.

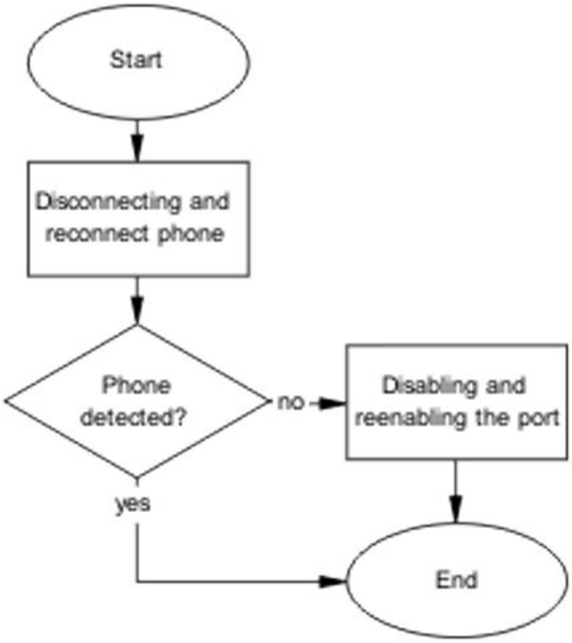

Start
Disconnecting and reconnect phone
Phone detected?
no
Disabling and reenabling the port
yes
End

Figure 27: Reload ADAC MAC in range table

Disconnecting and reconnecting phone

Remove the phone and the reconnect it to force a reload of the MAC address in the range table.

1. Follow local procedures to disconnect the phone.
2. Follow local procedures to reconnect the phone.

Disabling and enabling the port

Disable ADAC on the port and then enable it to detect the phone. When disable and reenable the port administratively, the MAC addresses already learned on the respective port are aged out.

1. Use the `no adac enable <port>` command to disable ADAC.
2. Use the `adac enable <port>`command to enable ADAC.

Reduce LLDP devices

Reduce the number of LLDP devices. More than 16 devices may cause detection issues.

Task flow Reduce LLDP devices

The following task flow assists you to reduce the number of LLDP devices on the system.

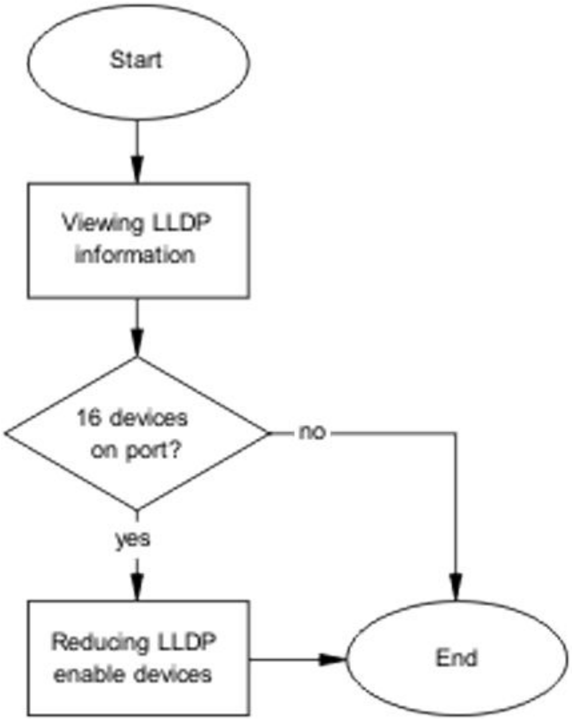


Figure 28: Reduce LLDP devices

Viewing LLDP information

Display the LLDP devices that are connected to a port.

1. Use the `show lldp port 1 neighbor` command to identify the LLDP devices.
2. Note if there are more than 16 LLDP-enabled devices on the port.

Reducing LLDP enabled devices

Reduce the number of LLDP devices on the system.

1. Follow local procedures and SOPs to reduce the number of devices connected.
2. Use the `show adac in <port>` command to display the ADAC information for the port to ensure there are less than 16 devices connected.

Auto configuration is not applied

Correct some common issues that may interfere with auto configuration of devices.

Task flow Auto configuration is not applied

The following task flow assists you to solve auto configuration issues.

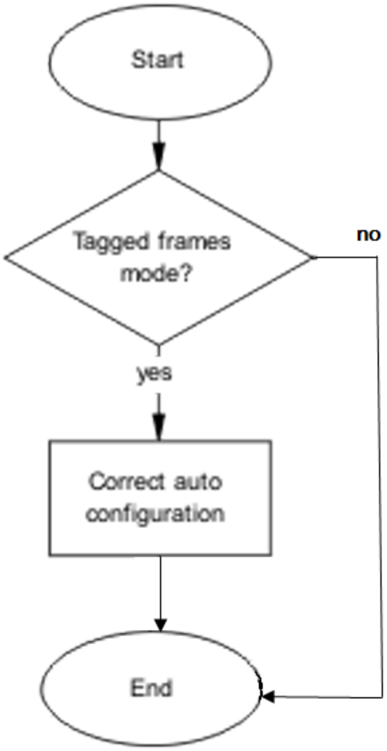


Figure 29: Auto configuration is not applied

Correct auto configuration

Tagged frames mode may be causing a problem. In tagged frames mode, everything is configured correctly, but auto configuration is not applied on a telephony port.

Task flow Correct auto configuration

The following task flow assists you to correct auto configuration.

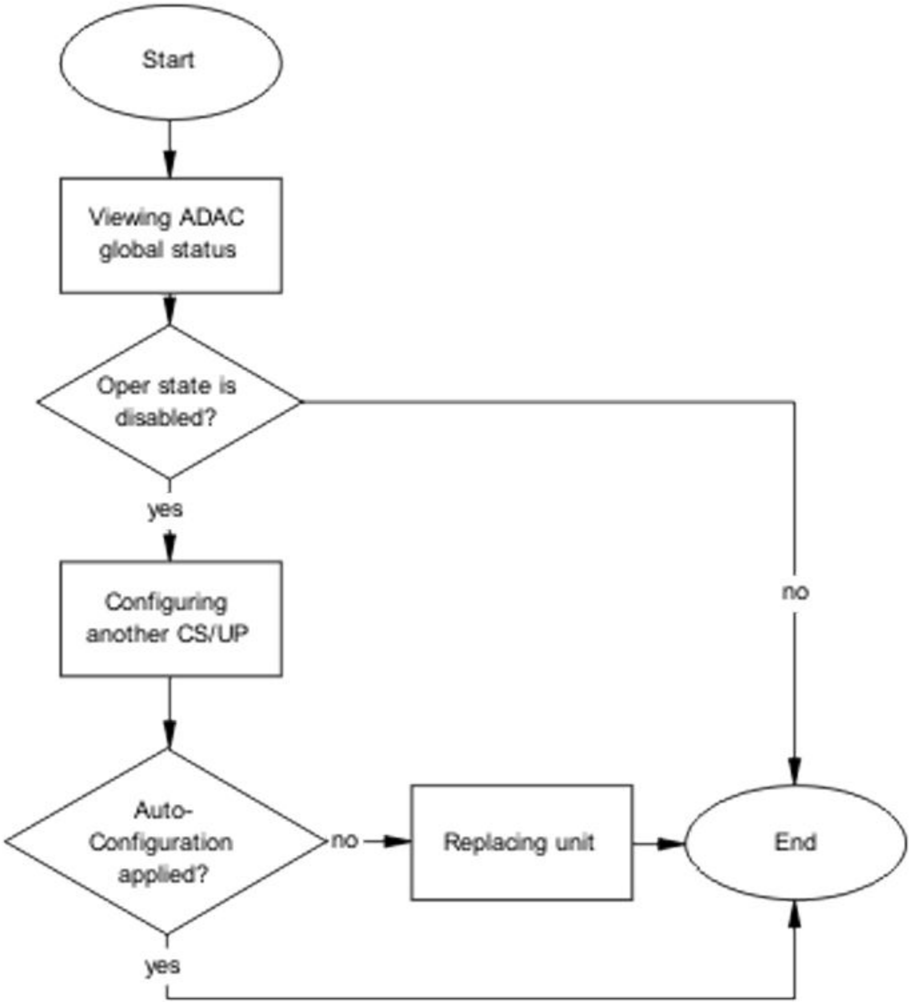

Start
Viewing ADAC global status
Oper state is disabled?
yes
no
Configuring another CS/UP
Auto-Configuration applied?
no
Replacing unit
End
yes

Figure 30: Correct auto configuration

Viewing ADAC global status

Display the global status of ADAC.

1. Use the `show adac` command to display the ADAC information.
2. Note if the oper state is showing as disabled.

Configuring another call server and uplink port

Configuring another call server and uplink port can assist the auto configuration.

1. Use the `adac uplink-port <port>` command to assign the uplink port.
2. Use the `adac call-server-port <port>` command to assign the call server port.

Chapter 11: Troubleshooting authentication

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

Work flow Troubleshooting authentication

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

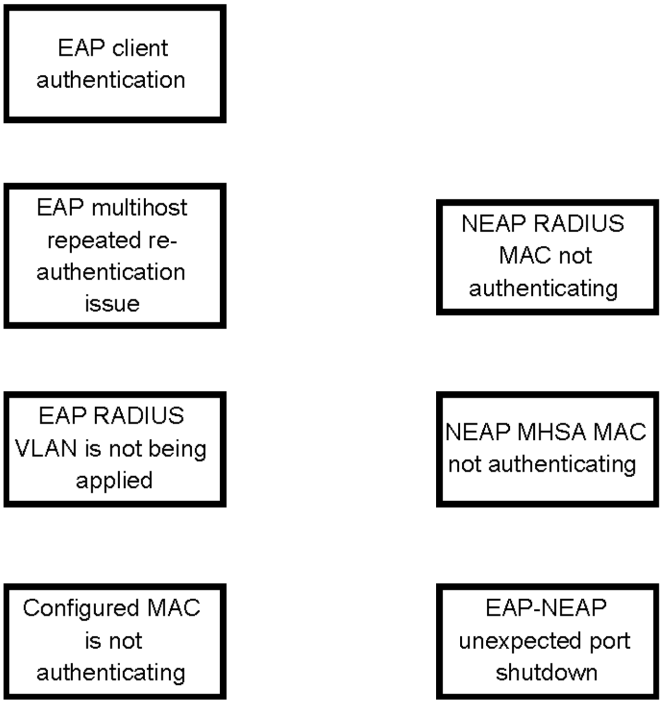

EAP client authentication
EAP multihost repeated re-authentication issue
NEAP RADIUS MAC not authenticating
EAP RADIUS VLAN is not being applied
NEAP MHSA MAC not authenticating
Configured MAC is not authenticating
EAP-NEAP unexpected port shutdown

Figure 31: Troubleshooting authentication

EAP client authentication

This section provides troubleshooting guidelines for the EAP and non-EAP features on the Ethernet Routing Switch 3500 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.

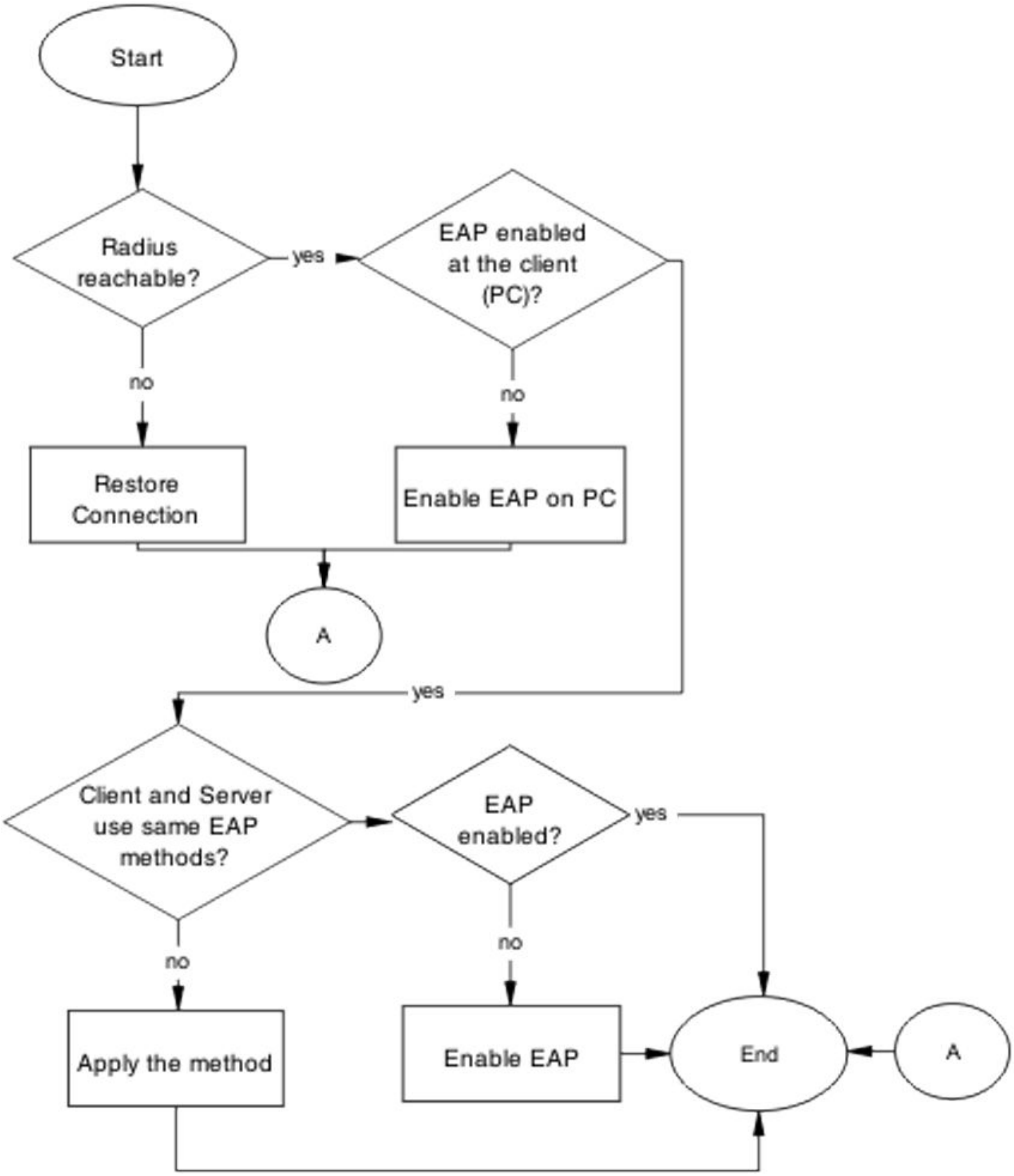


Figure 32: EAP client is not authenticating

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.

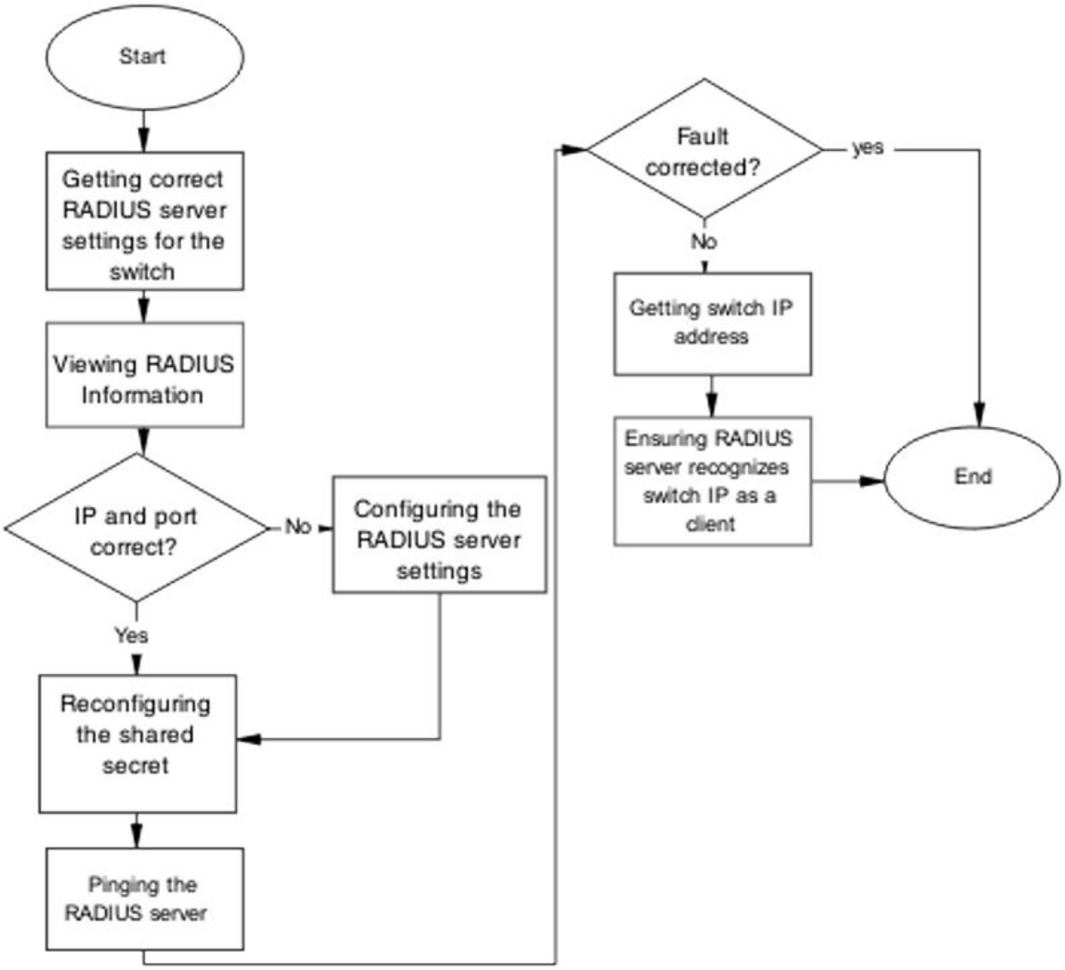

Start
Getting correct RADIUS server settings for the switch
Viewing RADIUS Information
IP and port correct?
No
Configuring the RADIUS server settings
Yes
Reconfiguring the shared secret
Pinging the RADIUS server
Fault corrected?
yes
No
Getting switch IP address
Ensuring RADIUS server recognizes switch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

Figure 33: Restore RADIUS connection

Getting correct RADIUS server settings for the switch

This section provides troubleshooting guidelines for obtaining the RADIUS server settings.

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

Viewing RADIUS information

Review the RADIUS server settings in the device. The default server port is 1812/UDP. Older servers may use 1645/UDP, and other older servers do not support UDP at all.

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

Configuring the RADIUS server settings

The RADIUS server settings must be correct for the network.

Follow vendor documentation to set the RADIUS server settings.

Reconfiguring the shared secret

Reset the shared secret in case there was any corruption.

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

Pinging the RADIUS server

Ping the RADIUS server to ensure connection exists.

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

Enable EAP on the PC

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

Task flow Enable EAP on the PC

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

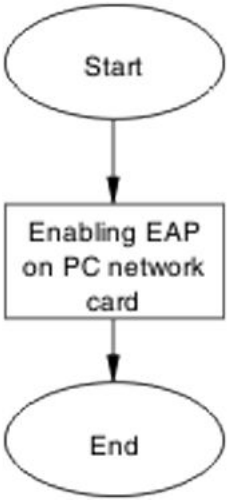


Figure 34: Enable EAP on the PC

Enabling EAP on PC network card

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

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

Apply the method

Ensure you apply the correct EAP method.

Task flow Apply the method

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

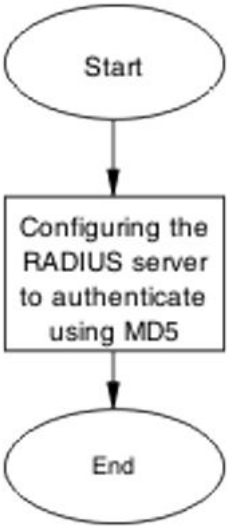


Figure 35: Apply the method

Configuring the RADIUS server

Configure the RADIUS server to authenticate using MD5.

1. Obtain network information for the RADIUS Server from Planning and Engineering.
2. Save the information for later reference.

Enable EAP globally

Enable EAP globally on the 3500 Series device.

Task flow Enable EAP globally

The following task flow assists you to enable EAP globally on the 3500 Series device.

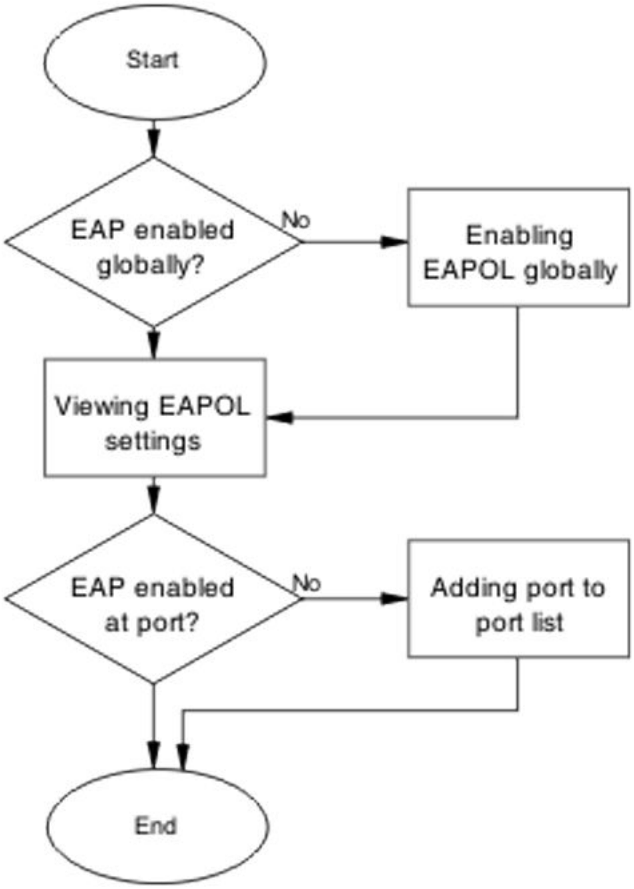


Figure 36: Enable EAP globally

Enabling EAP globally

Enable EAP globally on the Ethernet Routing Switch 3500 Series device.

1. Use the `eapol enable` command to enable EAP globally on the 3500 Series device.
2. Ensure that there are no errors after command execution.

Viewing EAPOL settings

Review the EAPOL settings to ensure EAP is enabled.

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

Setting EAPOL port administrative status to auto

Set the EAPOL port administrative status to auto.

1. Use the `eapol status auto` command to change the port status to auto.
2. Ensure that there are no errors after the command execution.

EAP multihost repeated re-authentication issue

Eliminate the multiple authentication of users.

EAP multihost repeated re-authentication issue

The following work flow assists you to determine the cause and solution of an EAP multihost that authenticates repeatedly.

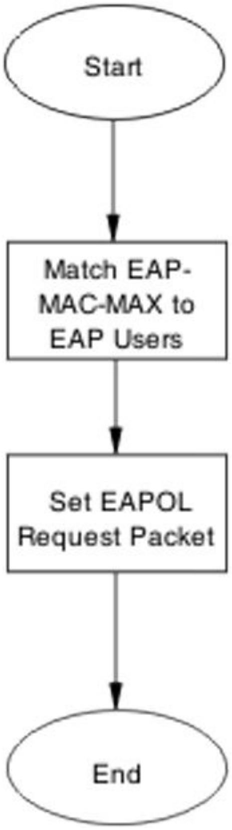


Figure 37: EAP multihost repeated re-authentication issue

Match EAP-MAC-MAX to EAP users

When the number of authenticated users reaches the allowed maximum, lower the eap-macmax to the exact number of EAP users that may soon enter to halt soliciting EAP users with multicast requests.

Identifying number of users at allowed max

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

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

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.

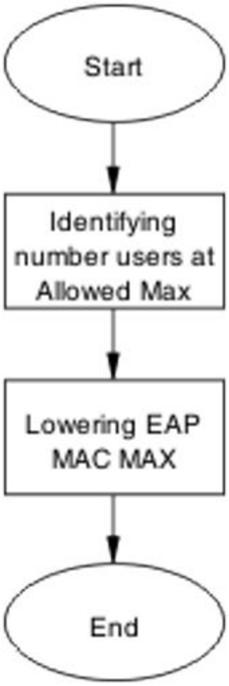


Figure 38: Match EAP-MAC-MAX to EAP users

Lowering EAP max MAC

Lower the eap-mac-max value to match the users.

1. Use the `eapol multihost eap-mac-max` command to set the mac-max value.
2. Ensure that there are no errors after execution.

Set EAPOL request packet

Change the request packet generation to unicast.

Task flow Set EAPOL request packet

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

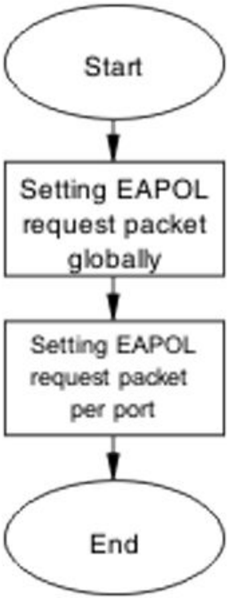

Start
Setting EAPOL request packet globally
Setting EAPOL request packet per port
End

Figure 39: Set EAPOL request packet

Setting EAPOL request packet globally

Globally change the EAPOL request packet from multicast to unicast.

1. Use the `eapol multihost eap-packet-mode unicast` command to set the EAPOL request packet to unicast.
2. Ensure that there are no errors after execution.

Setting EAPOL request packet for a port

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

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

EAP RADIUS VLAN is not being applied

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

Work flow EAP RADIUS VLAN is not being applied

The following work flow assists you to determine the cause and solution of the RADIUS VLAN not being applied.

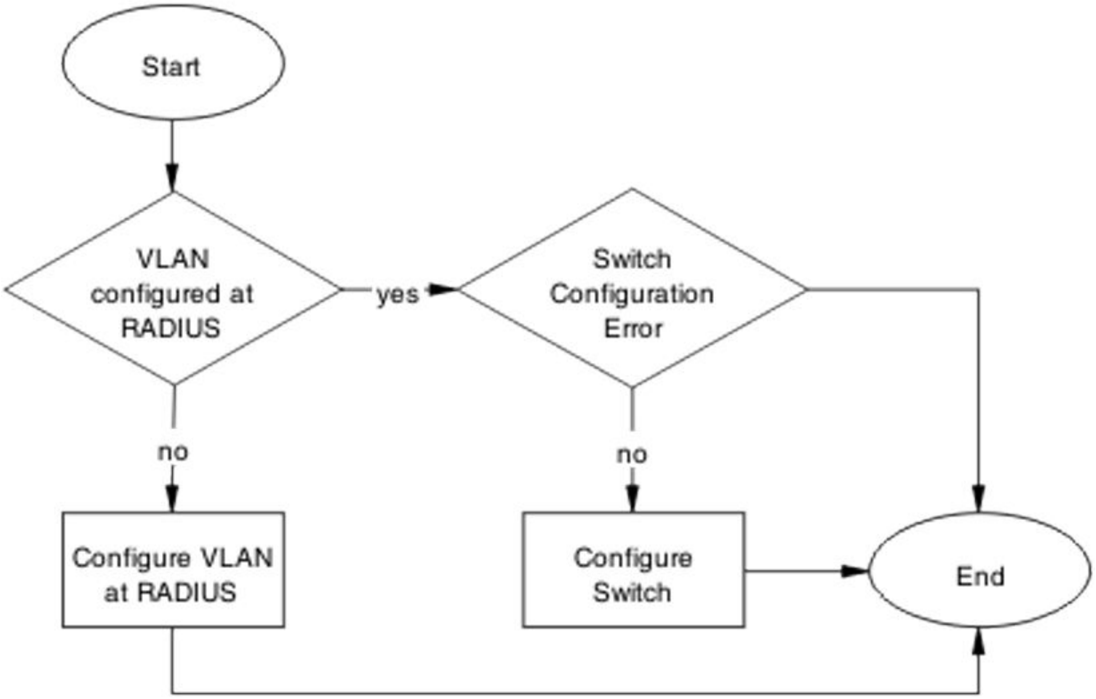


Figure 40: EAP RADIUS VLAN is not being applied

Configure VLAN at RADIUS

Correct any discrepancies in VLAN information at the RADIUS server.

Task flow Configure VLAN at RADIUS

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

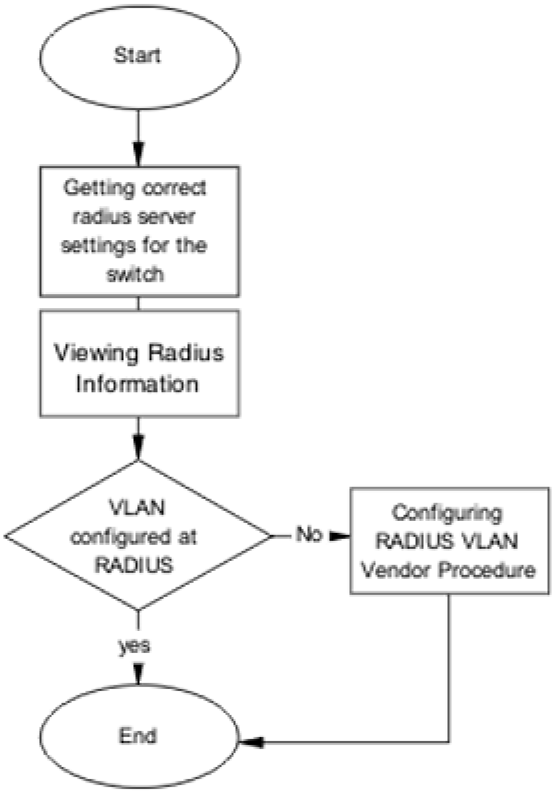

Start
Getting correct radius server settings for the switch
Viewing Radius Information
VLAN configured at RADIUS
No
Configuring RADIUS VLAN Vendor Procedure
yes
End

Figure 41: Configure VLAN at RADIUS

Getting correct RADIUS server settings

This section provides troubleshooting guidelines to obtain the correct RADIUS server settings.

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

Viewing RADIUS information

Obtain the radius information to identify its settings.

Use vendor documentation to obtain settings display.

Configuring RADIUS

Configure the RADIUS server with the correct VLAN information.

Use vendor documentation to make the required changes.

There are three attributes that the RADIUS server sends back to the NAS (switch) for RADIUSassigned VLANs. These attributes are the same for all RADIUS vendors:

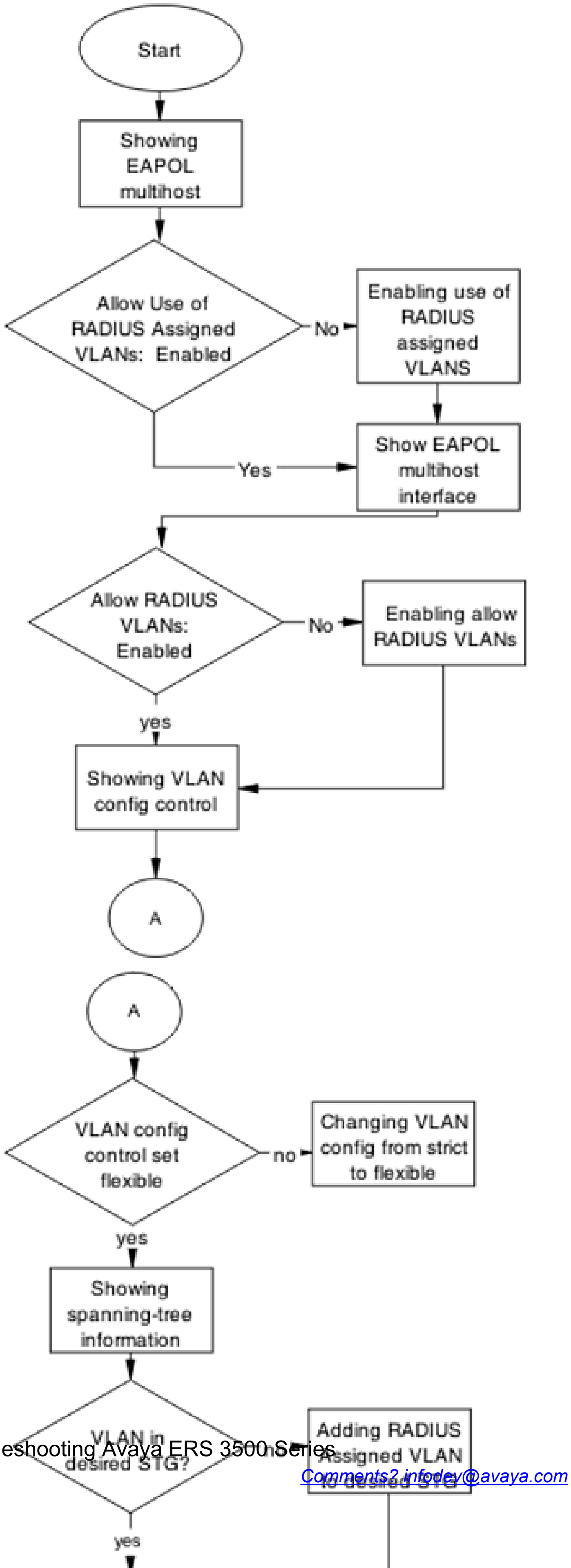
- Tunnel-Medium-Type – 802
- Tunnel-Pvt-Group-ID – <VLAN ID>
- Tunnel-Type – Virtual LANs (VLAN)

Configure switch

The VLAN must be configured correctly on the Ethernet Routing Switch 3500 Series device.

Task flow Configure switch

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


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

Showing EAPOL multihost

Identify the EAPOL multihost information.

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

Enabling use of RADIUS assigned VLANs

Change the "allow RADIUS assigned VLAN" to "enable".

1. Use the `eapol multihost use-radius-assigned-vlan` command to allow the use of VLAN IDs assigned by RADIUS.
2. Ensure that there are no errors after execution.

Showing EAPOL multihost interface

Display the EAPOL interface information.

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

Showing VLAN config control

Display the VLAN config control information.

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

Changing VLAN config from strict to flexible

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

1. Use the `vlan config control flexible` command to set the VLAN config control to flexible.
2. Ensure that there are no errors after execution.

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.

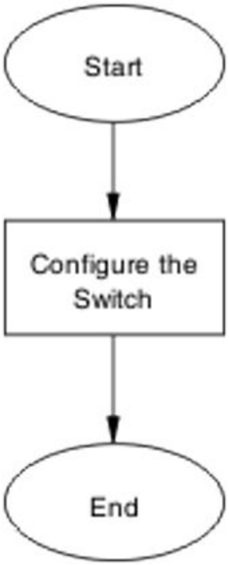


Figure 43: Configured MAC is not authenticating

Configure the switch

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

Task flow Configure the switch

The following task flow assists you to ensure the MAC is authenticating on the ERS 3500 Series device.

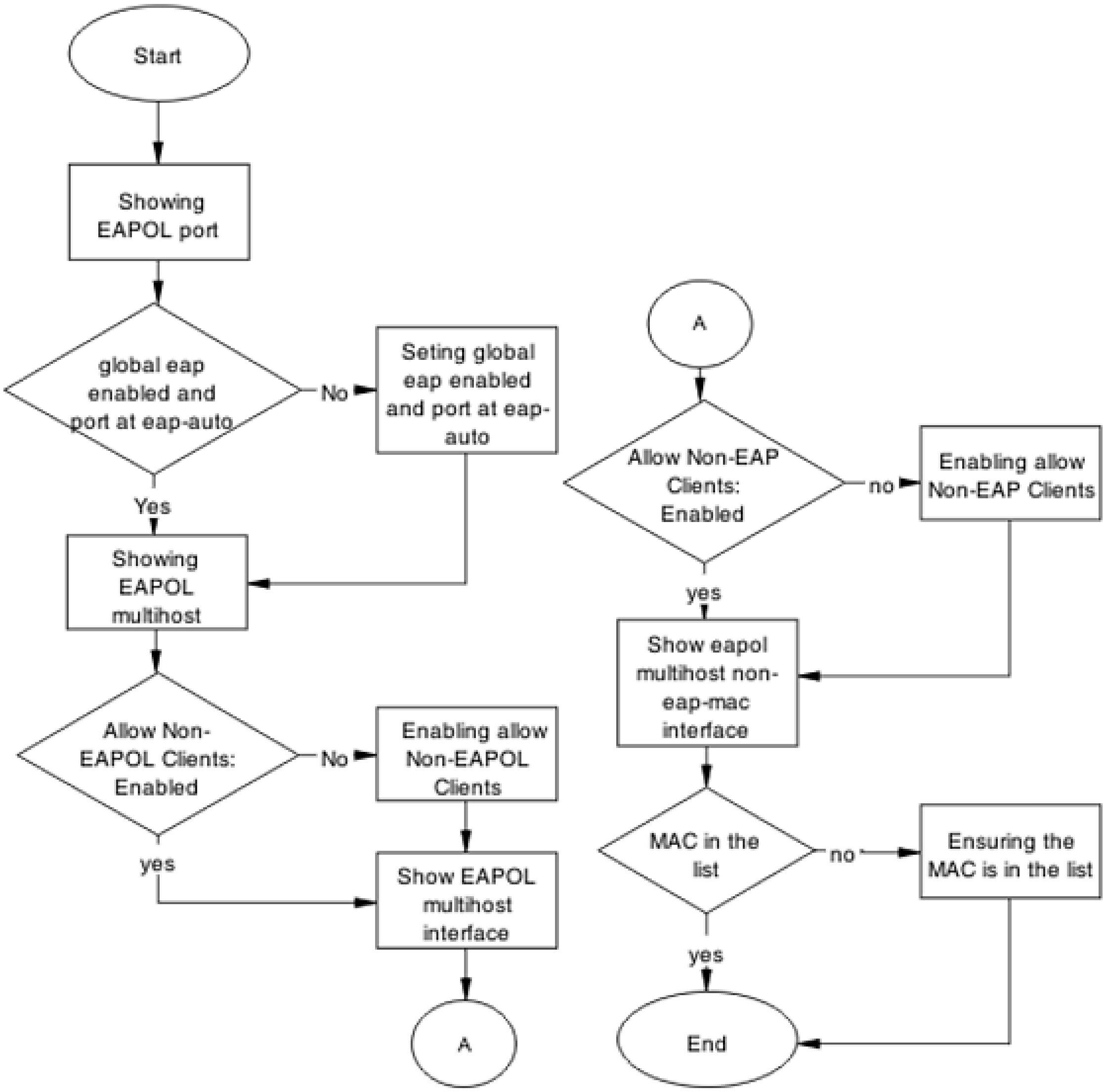

Start
Showing EAPOL port
global eap enabled and port at eap-auto
No
Seting global eap enabled and port at eap-auto
Yes
Showing EAPOL multihost
Allow Non-EAPOL Clients: Enabled
No
Enabling allow Non-EAPOL Clients
yes
Show EAPOL multihost interface
A
A
Allow Non-EAP Clients: Enabled
no
Enabling allow Non-EAP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

Figure 44: Configure the switch

Showing EAPOL port

Display the EAPOL port information

1. Use the `show eapol port <port>` command to display the port information.
2. Ensure that EAP is enabled globally, and that the port EAP status is set to auto.

Setting global EAP enabled and port at eap-auto

Make corrections to ensure that EAP is enabled globally, and that the port EAP status is set to auto.

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

Showing EAPOL multihost

Display the EAPOL multihost information.

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

Enabling allow non-EAPOL clients

Correct the non-EAPOL client attribute.

1. Use the `eapol multihost allow-non-eap-enable` command to allow non-EAPOL clients.
2. Ensure that there are no errors after execution.

Showing EAPOL multihost interface

Display the EAPOL multihost interface information.

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

Enabling multihost status and allow non-EAPOL clients

Correct the non-EAP client attribute.

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

Showing EAPOL multihost non-eap-mac interface

Display the EAPOL multihost interface information.

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

Ensuring MAC in the list

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

1. Use the `show eapol multihost non-eap-mac status` command to view MAC addresses.
2. Use the `eapol multihost non-eap-mac <H.H.H> <port>` command to add a MAC address to the list.

Non-EAP RADIUS MAC not authenticating

Correct a non-EAP RADIUS MAC that is not authenticating.

Work flow Non-EAP RADIUS MAC not authenticating

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

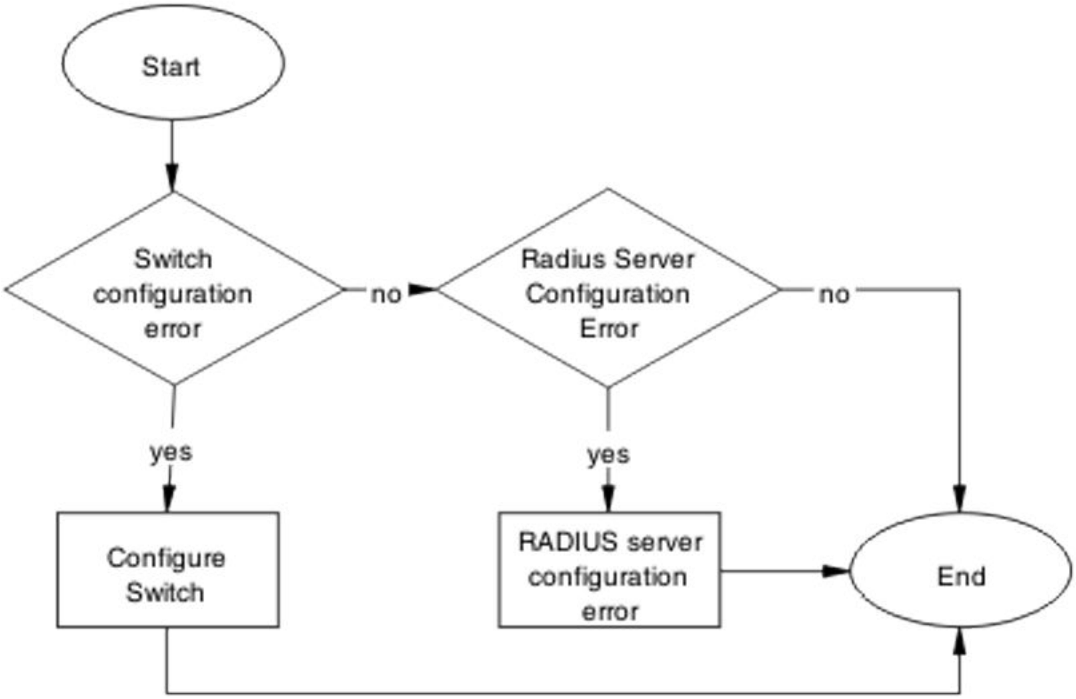

Start
Switch configuration error
no
Radius Server Configuration Error
no
yes
yes
Configure Switch
RADIUS server configuration error
End

Figure 45: Non-EAP RADIUS MAC not authenticating

Configure switch

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

Task flow Configure switch

The following task flow assists you to configure the ERS 3500 Series device to correct the RADIUS MAC issue.

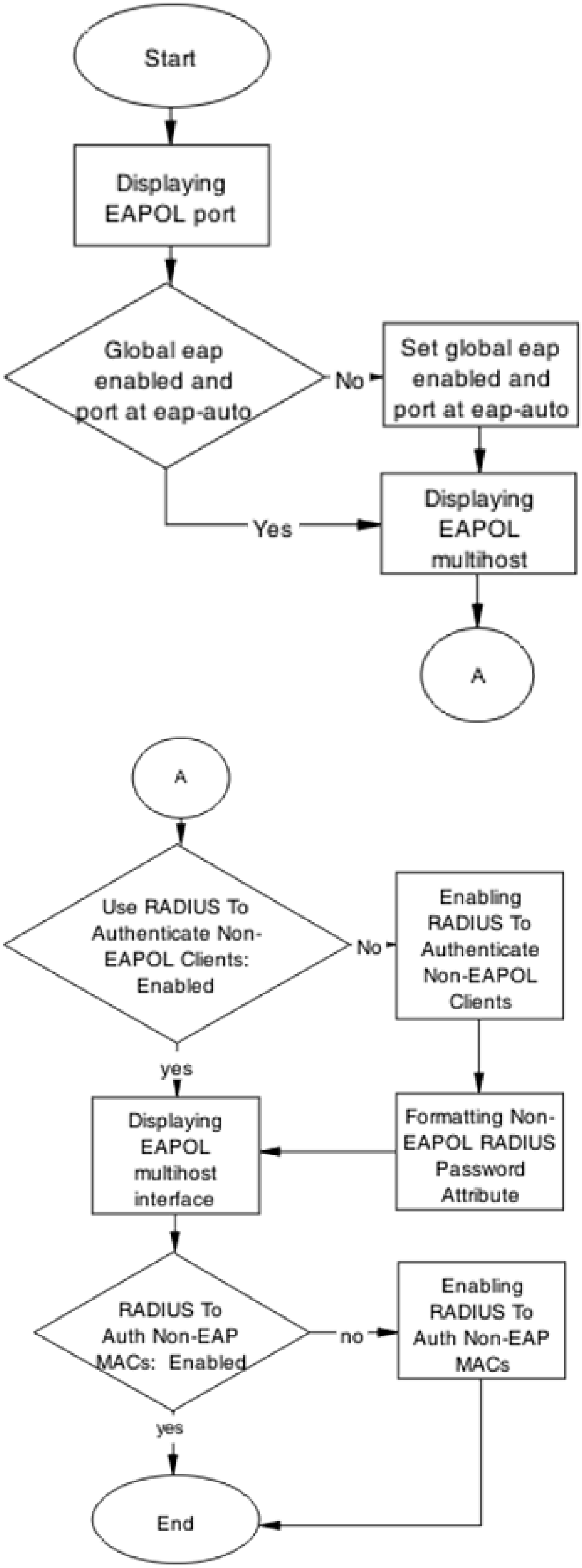

Start
Displaying EAPOL port
Global eap enabled and port at eap-auto
No
Set global eap enabled and port at eap-auto
Yes
Displaying EAPOL multihost
A
A
Use RADIUS To Authenticate Non-EAPOL Clients: Enabled
No
Enabling RADIUS To Authenticate Non-EAPOL Clients
yes
Displaying EAPOL multihost interface
Formatting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

Figure 46: Configure switch

Displaying EAPOL port

Review the EAPOL port information.

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

Setting global EAP enabled and port at eap-auto

Make corrections to ensure that EAP is enabled globally, and that the port EAP status is set to auto.

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

Displaying EAPOL multihost

Review the EAPOL multihost information.

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

     `IpAddr.MACAddr.PortNumber`

Enabling RADIUS to authenticate non-EAPOL clients

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

Apply changes to the RADIUS server using vendor documentation.

Formatting non-EAPOL RADIUS password attribute

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

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

Displaying EAPOL multihost interface

Review the EAPOL multihost information.

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

   Use RADIUS To Authenticate Non EAP MACs is enabled

Enabling RADIUS To Auth non-EAP MACs

Make the required changes on the RADIUS server to authenticate non-EAP clients. Apply changes to RADIUS server using vendor documentation.

RADIUS server configuration error

The RADIUS server requires that the correct MAC address and password for the 3500 Series device be configured.

Task flow RADIUS server configuration error

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

Start
Configuring MAC and password on RADIUS server
End

Figure 47: RADIUS server configuration error

Configuring MAC and password on RADIUS server

The RADIUS server requires that the MAC address and password for the 3500 Series device be correct. If it is incorrect, the 3500 Series device may not authenticate.

See the vendor documentation for the RADIUS server for details.

Non-EAP MHSA MAC is not authenticating

Ensure that the switch is configured correctly.

Work flow Non-EAP MHSA MAC is not authenticating

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

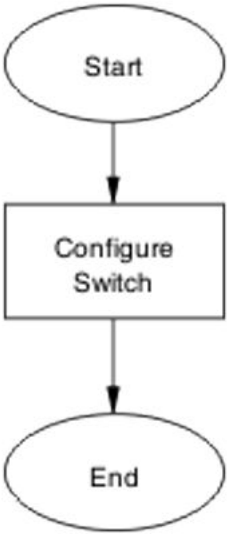


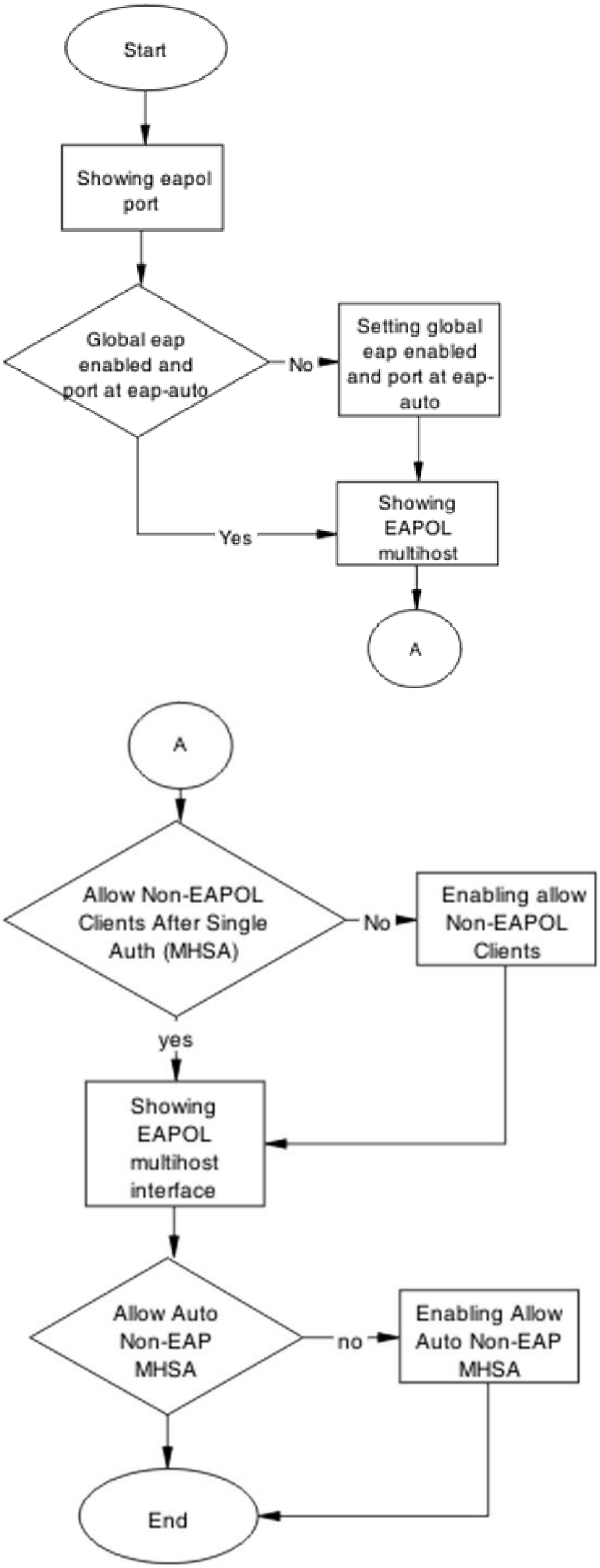
Figure 48: Non-EAP MHSA MAC is not authenticating

Configure switch

Configure the switch to enable MHSA.

Task flow Configure switch

The following task flow assists you to enable MHSA on the ERS 3500 Series device.


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

Showing EAPOL port

Review the EAPOL port information.

1. Enter the `show eapol port <port#>` command to display the information.
2. Ensure that global EAP is enabled and that the port status is eap-auto.

Showing EAPOL multihost

Review the EAPOL multihost information.

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

   Use RADIUS To Authenticate NonEAPOL Clients is enabled

Formatting non-EAPOL RADIUS password attribute

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

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

Enabling RADIUS to authenticate non-EAPOL clients

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

Apply changes to RADIUS server using vendor documentation.

Showing EAPOL multihost interface

Review the EAPOL multihost information.

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

   Allow Auto Non-EAP MHSA: Enabled

Enabling RADIUS to auth non-EAP MACs

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

Apply changes to RADIUS server using vendor documentation.

EAP–non-EAP unexpected port shutdown

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

Work flow EAP–non-EAP unexpected port shutdown

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

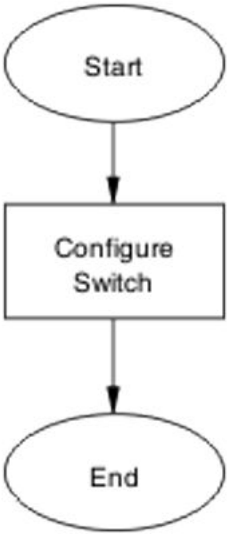


Figure 50: EAP — non-EAP unexpected port shutdown

Configure switch

Configure ports to allow more unauthorized clients.

Task flow Configure switch

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

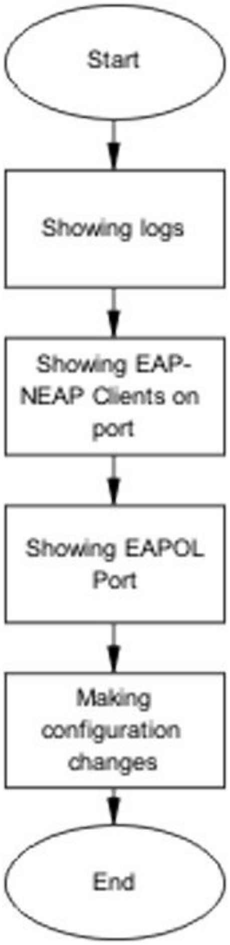

Start
Showing logs
Showing EAP-NEAP Clients on port
Showing EAPOL Port
Making configuration changes
End

Figure 51: Configure switch

Showing Logs

Display log information to provide additional information.

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

Showing EAP–non-EAP clients on port

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

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

Showing EAPOL port information

Display EAPOL port information for additional information.

1. Use the `show eapol port <port#>` command to display the port information.
2. Observe the log output and note any anomalies.

Making changes

This section provides troubleshooting guidelines for changing the EAP settings. It assists in the cleanup of old MAC addresses.

1. Use the `eapol status auto`command to change to eap-auto.
2. In the Interface Configuration Mode, use the `shut/no shut` commands.