Troubleshooting Avaya Ethernet Routing Switch 4000 Series

Release 5.7
NN47205-700
Issue 05.02
April 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. “Software” means Avaya’s computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products, pre-installed , or remotely accessed on hardware products, and any upgrades, updates, bug fixes, or modified versions thereto. “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. “Instance” means a single copy of the Software executing at a particular time: (i) on one physical machine; or (ii) on one deployed software virtual machine (“VM”) or similar deployment.

Licence types

Designated System(s) License (DS). End User may install and use each copy or an Instance of the Software only on a number of Designated Processors up to the number indicated in the order. Avaya may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, Instance, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

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/

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

The *Avaya Ethernet Routing Switch 4000 Series Troubleshooting* guide describes the diagnostic tools and utilities available with the Avaya Ethernet Routing Switch 4000 Series to help you troubleshoot operational and configuration issues. This document guides you through some common problems, to achieve a first tier solution to these situations, and advises you what information to compile prior to troubleshooting or calling Avaya for help.

You can configure and display files, view and monitor port statistics, trace a route, run loopback and ping tests, test the switch, and view the address resolution table. Although the diagnostic tools and utilities described are available with both the Avaya Command Line Interface (ACLI) and Enterprise Device Manager (EDM), this document focuses on using ACLI to demonstrate most of the troubleshooting tasks. You can access ACLI through either a direct console connection to the switch or by using the Telnet or SSH protocols to connect to the switch remotely.

Related resources

Documentation

For a list of the documentation for this product, see *Documentation Reference for Avaya Ethernet Routing Switch 4000 Series*, NN47205–101.

Training

Ongoing product training is available. For more information or to register, see http://avaya-learning.com/.

Enter the course code in the **Search** field and click **Go** to search for the course.

Course code	Course title
8D00020E	Stackable ERS and VSP Products Virtual Campus Offering

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.

Searching a document collection

On the Avaya Support website, you can download the documentation library for a specific product and software release to perform searches across an entire document collection. For example, you can perform a single, simultaneous search across the collection to quickly find all occurrences of a particular feature. Use this procedure to perform an index search of your documentation collection.

Before you begin

- Download the documentation collection zip file to your local computer.
- You must have Adobe Acrobat or Adobe Reader installed on your computer.

Procedure

1. Extract the document collection zip file into a folder.
2. Navigate to the folder that contains the extracted files and open the file named <*product_name_release*>.pdx, for example, ers4000_5.7x.pdx.

3. In the Search dialog box, select the option **In the index named <*product_name_release*>.pdx**.
4. Enter a search word or phrase.
5. Select any of the following to narrow your search:
    - Whole words only
    - Case-Sensitive
    - Include Bookmarks
    - Include Comments
6. Click **Search**.
   The search results show the number of documents and instances found. You can sort the search results by Relevance Ranking, Date Modified, Filename, or Location. The default is Relevance ranking.

Support

Visit the Avaya Support website at [xref to:http://support.avaya.com] for the most up-to-date documentation, product notices, and knowledge articles. You can also search for notices, release notes, downloads, user guides, 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 sections detail what is new in *Troubleshooting Avaya Ethernet Routing Switch 4000 Series*, NN47205-700 for Release 5.7.

Features

See the following sections for information about features changes:

SLA Monitor

The Service Level Agreement (SLA) Monitor feature is implemented phase-wise on the ERS 4000 series switch. In Release 5.6, the phase 1 implementation included the feature, SLA Monitor on the ERS 4000 series switch and supported only non-secure agent-server communication.

In Release 5.7, phase 2 implementation ensures a secure SLA Monitor agent-server communication through certificate-based authentication and encrypted agent-server communication. Also, SLA Monitor agent can perform QoS tests in the absence of SLA Monitor server using the platform CLI.

For more information about SLA Monitor agent, see:

- *Configuring System Monitoring on Avaya Ethernet Routing Switch 4000 Series*, NN47205-502.
- Troubleshooting SLA Monitoring on page 225

802.3at LLDP based discovery

ERS 4000 Series PWR+ devices support the IEEE 802.3at-2009 standard for an Link Layer Discovery Protocol (LLDP) configuration with a Powered Device (PD). The LLDP support for PoE+ is added by extending the existing standard LLDP DOT3 Power via MDI TLV defined by the IEEE 802.1ab with the new fields and values defined in the IEEE 802.3at-2009 standard. Information for power negotiation between PD and Power Sourcing Equipment (PSE) is described in Power via MDI, which is an optional 802.1AB TLV.

The PoE PD communicates through the Data Link Layer (DLL) classification instead of Physical Layer (high power mode). Hence, the PoE+ capable devices can deliver power greater than 15.4 watts for each port.

You can configure the PoE PD detection type (802.3at or 802.3at_and_legacy) to support a DLL classification for communication. The Data Link Layer classification provides finer power resolution and the ability for PSE and PD to participate in dynamic power allocation. The allocated power to the PD can change one or more times during PD operation.

For more information, see:

- *Configuring VLANs, Spanning Tree, and Multi-Link Trunking on Avaya Ethernet Routing Switch 4000 Series*, NN47205-501.
- LLDP based discovery on page 161

Change RADIUS Password

You can allow the users to change RADIUS account passwords when they expire. Note:

Note:

Change RADIUS password is available only in secure software builds.

You can enable or disable the Change RADIUS password feature. By default, this feature is disabled. When Change RADIUS password feature is enabled, the server reports the password expiry and system prompts you to create a new password.

For more information, see

- *Configuring Security on Avaya Ethernet Routing Switch 4000 Series*, NN47205-505.
- Changing RADIUS password on page 118

Link-state tracking

Link-state tracking (LST) binds the link state of multiple interfaces to create redundancy in the network. For more information about LST, see:

- *Configuring Systems on Avaya Ethernet Routing Switch 4000 Series*, NN47205-500.
- Link-state tracking on page 164

Run scripts

According to Avaya best practices for converged solutions, you can use the scripts to configure the parameters for an Avaya stackable Ethernet Switch. The scripts can be executed in a default or verbose mode.

In the automated or non-verbose mode, the switch is configured using predetermined parameter values. In the verbose mode, the script guides you to configure the parameters where the values must be provided as inputs when the script is executed.

In this release, run scripts are available in non-verbose and verbose mode for IP Office, and verbose mode for Link Layer Discovery Protocol (LLDP) and Auto Detect Auto Configuration (ADAC).

For more information, see:

- *Configuring Systems on Avaya Ethernet Routing Switch 4000 Series*, NN47205-500.
- Run scripts on page 163

Block subsequent MAC authentication

Prior to Release 5.7, in Multiple Host with Multiple Authentication (MHMA) mode, if a station successfully authenticates, the switch places the port in the RADIUS-assigned VLAN that corresponds to the login credentials of that station. If a second station properly authenticates on that same port, the switch ignores the RADIUS-assigned VLAN and the user is placed in the same VLAN as the first successfully authenticated station, creating a potential security risk. This feature enhancement gives the administrator the option of either using the current implementation or a separate option that blocks subsequent MAC authentications if the RADIUS-assigned VLAN is different than the first authorized station VLAN.

For more information, see:

- *Configuring Security on Avaya Ethernet Routing Switch 4000 Series*, NN47205-505.
- Block subsequent MAC authentication on page 160

Fail Open VLAN Continuity mode

The Fail Open VLAN Continuity mode feature introduces a new mode of operation for EAP/NEAP clients when the RADIUS server(s) become unreachable.

For more information, see:

- *Configuring Security on Avaya Ethernet Routing Switch 4000 Series*, NN47205-505.
- 802.1 x Fail Open Continuity Mode on page 118

NEAP Not Member of VLAN

The NEAP Not Member of VLAN feature ensures that ports configured with RADIUS Non-EAP authentication are assigned to at least one VLAN to make authentication possible for Non-EAP clients.

For more information, see:

- *Configuring Security on Avaya Ethernet Routing Switch 4000 Series*, NN47205-505.
- Non-EAP not a member of a VLAN on page 159

Syslog Support for 802.1X/EAP/NEAP/UBP

Syslog messages for the various states of 802.1X/EAP/NEAP/UBP authentications are introduced to allow more thorough troubleshooting.

Logged messages include:

- time of authentication
- MAC authentication success/failure
- IP address associated with MAC authentication
- VLAN and UBP policy assignment

For more information, see:

- *Configuring Security on Avaya Ethernet Routing Switch 4000 Series*, NN47205-505.
- System logs on page 33

Trace Support for 802.1X

The trace feature is a troubleshooting feature that provides detailed information about errors and events on the device. Use this feature to understand the cause of an error and take action to resolve it. The trace command supports 802.1X/EAP in four levels for each module or application apart from supporting various other applications (OSPF, RIP, SMLT, IPMC, IGMP, and PIM) from previous releases. All the previous levels of trace are supported (Very Terse, Terse, Verbose, and Very Verbose). If higher levels are requested, more information is displayed.

For more information, see:

- *Configuring Security on Avaya Ethernet Routing Switch 4000 Series*, NN47205-505.
- Using Trace on page 159

RSPAN

Remote Switch Port ANalyzer (RSPAN), also known as Remote Port Mirroring, enhances port mirroring by enabling mirrored traffic to be sent to one or more switches or stacks on the network using an intermediate VLAN for forwarding the mirrored traffic.

For more information, see

- *Configuring System Monitoring on Avaya Ethernet Routing Switch 4000 Series*, NN47205-502.
- RSPAN on page 27
- RSPAN commands on page 28

SPBM

Shortest Path Bridging MAC (SPBM) is a next generation virtualization technology that revolutionizes the design, deployment and operations of Ethernet networks. SPBM enables massive scalability while simultaneously reducing the complexity of the network.

Avaya networking products allow virtualization services at both layer 2 and layer 3, referred to as L2VSN and L3VSN. The Avaya Ethernet Switch 4800 is capable of providing L2VSN support connecting traditional Ethernet networks to an SPBM enabled network core, the ERS 4800 functions as a Backbone Edge Bridge. The 5.7 release introduces L2VSN capabilities to the ERS 4800 product, whereas SPBM support is exclusive to the ERS 4800 and stacks of ERS 4800. The L3 (e.g. OSPF) features of the ERS 4800 cannot be supported simultaneously with SPBM, they are mutually exclusive.

Avaya ERS 4800 Series supports the IEEE 802.1aq standard of SPBM, which allows for larger Layer 2 topologies and permits faster convergence.

Note:

SPBM is not supported on the ERS 4500 series or hybrid stacks of ERS 4500 and ERS 4800.

For more information, see:

- *Configuring Avaya VENA Fabric Connect on Avaya Ethernet Routing Switch 4000 Series*, NN47205-507.
- Troubleshooting SPBM on page 215

Chapter 3: Troubleshooting planning

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

First, use the *Documentation Reference for Avaya Ethernet Routing Switch 4000 Series*, NN47205–101 to familiarize yourself with the documentation set, so you know where to get information as you need it.

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

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

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

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

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

Chapter 4: Troubleshooting tools

This section describes available troubleshooting tools and their applications.

Port mirroring

Avaya Ethernet Routing Switch 4000 Series switches have a port mirroring feature that helps you to monitor and analyze network traffic. The port mirroring feature supports both ingress (incoming traffic) and egress (outgoing traffic) port mirroring. After port mirroring is enabled, the ingress or egress packets of the mirrored (source) port are forwarded normally and a copy of the packets is sent from the mirrored port to the mirroring (destination) port. Although you can configure Avaya Ethernet Routing Switch 4000 Series to monitor both ingress and egress traffic, some restrictions apply:

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

You can also monitor traffic for specified MAC addresses.

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

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

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

Port mirroring commands

See *Configuring System Monitoring on Avaya Ethernet Routing Switch 4000 Series*, NN47205-502 for port mirroring command information.

Use the port mirroring commands to assist in diagnostics and information gathering.

RSPAN

Remote Switch Port ANalyzer (RSPAN), also known as Remote Port Mirroring, enhances port mirroring by enabling mirrored traffic to be sent to one or more switches or stacks on the network using an intermediate VLAN for forwarding the mirrored traffic.

Considerations

- Switches must support RSPAN VLAN configuration and flood traffic within that VLAN as specified by the characteristics of an RSPAN VLAN.
- The RSPAN VLAN carries port mirroring and SPAN traffic between RSPAN source and destination sessions. All traffic in the RSPAN VLAN is flooded and no MAC address learning occurs on the RSPAN VLAN.
- RSPAN traffic may be terminated on a Avaya Switch supporting RSPAN.
- The maximum number of RSPAN vlans on a DUT is four
- Configure up to four RSPAN destination instances.
- You cannot use the same vlan or the same interface in another RSPAN instance.

Configuring ports

Install filters to enable port mirroring/ RSPAN source for MAC base modes (Asrc, Adst, AsrcBdst, AsrcBdstOrBsrcAdst, AsrcOrAdst) and port based modes (XrxYtx, XrxYtxOrYrxXtx) port-mirroring. If platform resource limits are reached, the application may not function in these modes. RSPAN only works for unicast traffic for port based modes.

Broadcast/Multicast/UUC traffic does not use hardware filters, it uses a group of workarounds that must be removed in order for RSPAN to work.

Note:

Port-mirroring shows incorrect source/dest mac for routed layer 3 traffic because mirroring is the last operation performed by the ASIC (after routing).

You cannot configure a port under the following conditions:

- A port has 802.1X enabled as an RSPAN destination port
- A port is a member of MLT/DMLT/LAG as an RSPAN destination port
- A port is a member of MLT/DMLT/LAG as a port mirroring/RSPAN source because this functionality has never been implemented for the classic PMT and there is a restriction which does not allow you to configure a MLT/DMLT/LAG port as MTP.
- A port cannot be configured as an RSPAN destination or Mirror To Port (MTP) if it is an RSPAN source / mirrored port for another instance.
- You cannot configure allow-traffic option and RSPAN because the port must be in a enabled and disabled state at the same time.

VLAN considerations

- If a RSPAN VLAN is used in a PMT RSPAN instance, it cannot be deleted. The RSPAN instance must be deleted first.
- RSPAN destination port cannot be removed from the RSPAN VLAN while involved in the RSPAN instance.
- RSPAN destination port membership cannot be changed unless the instance is deleted first.
- A SPBM B-VLAN or spbm-switchedUni VLAN can not be a RSPAN VLAN.
- A RSPAN VLAN cannot be set as a management VLAN.
- Mapping of an RSPAN VLAN over an SPB ISID and transport over an SPB cloud is not supported.

RSPAN commands

Use the RSPAN commands to assist in diagnostics and information gathering.

See *Configuring System Monitoring on Avaya Ethernet Routing Switch 4000 Series*, NN47205-502 for RSPAN command information.

Port statistics

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

For more information regarding port statistics and commands, see *Configuring System Monitoring on Avaya Ethernet Routing Switch 4000 Series*, NN47205-502.

Stack loopback testing

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

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

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

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

For more detail regarding stack loopback testing, see *Configuring System Monitoring on Avaya Ethernet Routing Switch 4000 Series*, NN47205-502.

Stack health check

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

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

For detailed information about stack health check, see *Configuring System Monitoring on Avaya Ethernet Routing Switch 4000 Series*, NN47205-502.

Stack Forced Mode

The Avaya Ethernet Routing Switch 4000 Series may enter Stack Forced Mode (if configured as such) after a stack of two units breaks into one or two standalone switches. The Stack Forced Mode operation allows the standalone device that comes out of a broken stack of two to be managed using the previous stack IP address. After a stack of two fails, you have access to a device without the need of a standalone IP address.

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

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

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

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

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

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

. The

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

represents the device MAC address.

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

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

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

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

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

   ```
   Forced-Stack Mode: Disabled

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

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

   ```
   Forced-Stack Mode: Enabled

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

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

   ```
   Forced-Stack Mode: Enabled

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

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

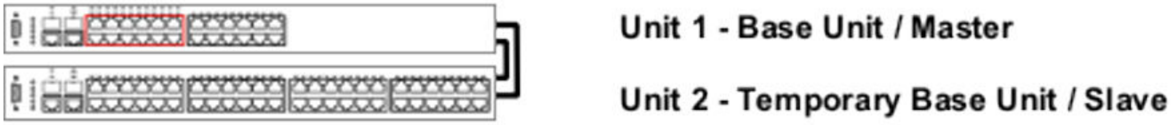

Unit 1 - Base Unit / Master
Unit 2 - Temporary Base Unit / Slave

Figure 1: Forced stack mode example setup

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

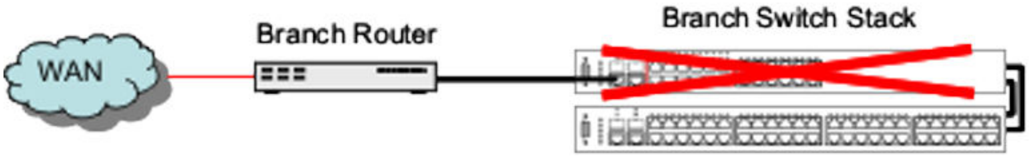


Figure 2: Remote Branch Office - Failure Scenario 1

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

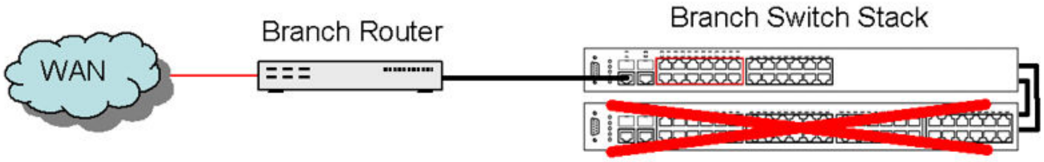


Figure 3: Remote Branch Office - Failure Scenario 2

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

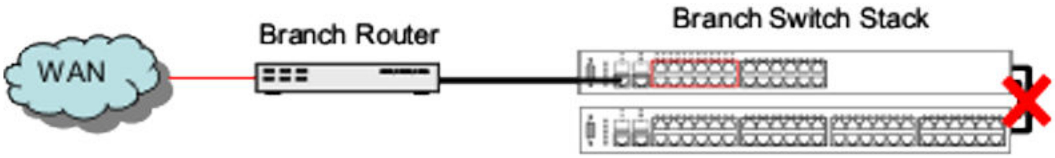


Figure 4: Remote Branch Office – Failure Scenario 3

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

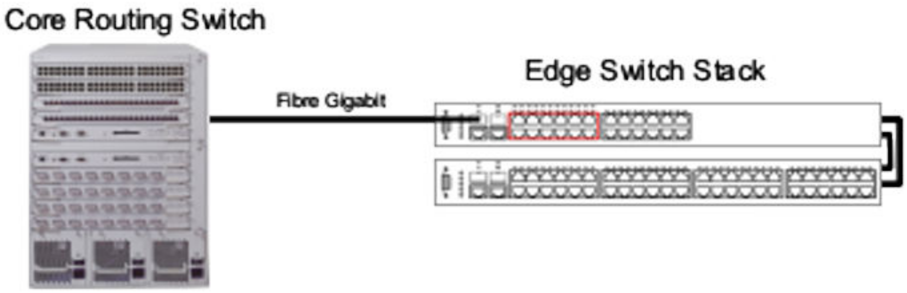


Figure 5: Wiring Closet Deployment 1

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

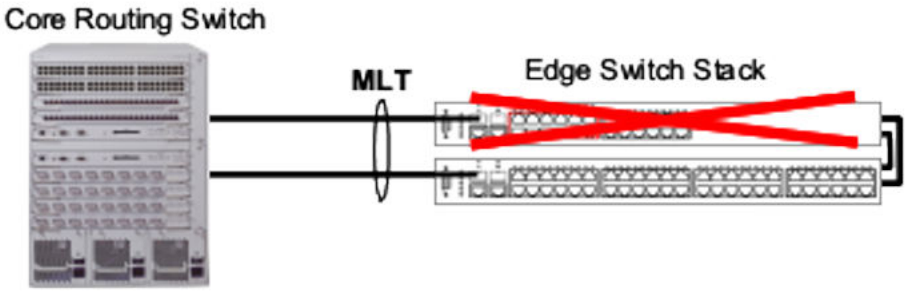


Figure 6: Wiring Closet Deployment 2 – Failure Scenario 1

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

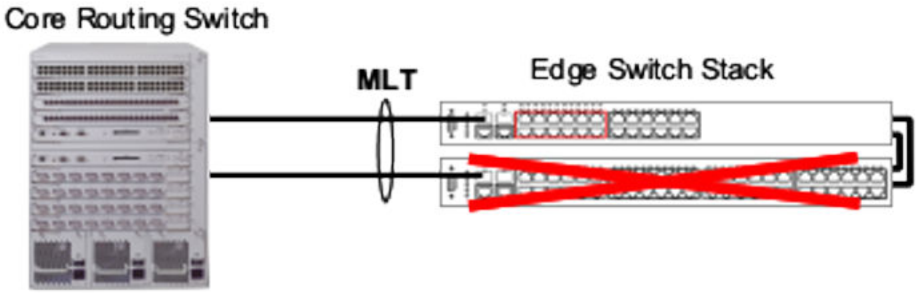


Figure 7: Wiring Closet Deployment 2 – Failure Scenario 2

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

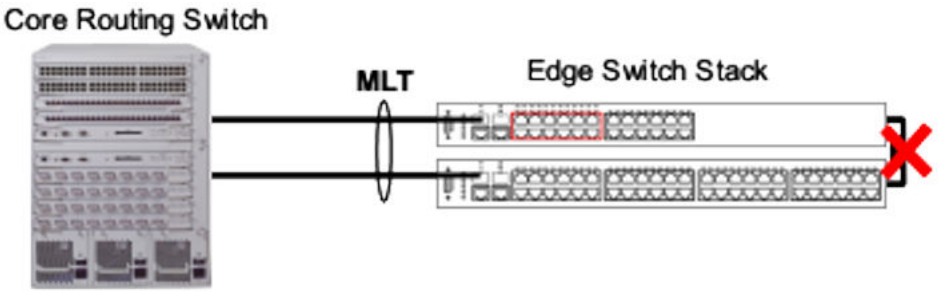


Figure 8: Wiring Closet Deployment 2 – Failure Scenario 3

System logs

You can use the syslog messaging feature of the Avaya Ethernet Routing Switch 4000 Series products to manage event messages. The Avaya Ethernet Routing Switch 4000 Series syslog software communicates with a server software component named syslogd that resides on your management workstation.

The daemon syslogd is a software component that receives and locally logs, displays, prints, or forwards messages that originate from sources that are internal and external to the workstation. For example, syslogd software concurrently handles messages received from applications running on the workstation, as well as messages received from an Avaya Ethernet Routing Switch 4000 Series device running in a network accessible to the workstation.

For more information about system logging, see *Configuring System Monitoring on Avaya Ethernet Routing Switch 4000 Series*, NN47205-502.

Syslog messages

Syslog messages for the various states of 802.1X/EAP/NEAP/UBP authentications are introduced to allow more thorough troubleshooting. Logged messages include:

- time of authentication
- MAC authentication success/failure
- IP address associated with MAC authentication
- VLAN and UBP policy assignment

Use the `show logging` command.

```
4526T-PWR+(config)#sh logging
Type Time                           Idx  Src Message
---- ------------------------------ ---- --- -------
I    00:00:00:15                    1        Web server starts service on port 8
0.
I    00:00:00:17                   2        Successfully loaded configuration files
from block 1
```

Backup config file

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

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

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

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

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

The following messages are loaded to the engineering log menu:

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

ASCII download log enhancement

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

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

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

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

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

CPU and memory utilization

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

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

This feature is supported by both ACLI and Web-based management. For more information about the feature, see *Configuring System Monitoring on Avaya Ethernet Routing Switch 4000 Series*, NN47205-502.

Show commands

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

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

Address Resolution Protocol

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

⚠ **Caution:**

Every time an IP interface or link goes up, the driver for that interface will typically send a gratuitous ARP to preload the ARP tables of all other local hosts. A gratuitous ARP will tell us that host just has had a link up event, such as a link bounce, a machine just being rebooted or you are just configuring the interface up. If you see multiple gratuitous ARPs from the same host frequently, it can be an indication of bad Ethernet hardware or cabling resulting in frequent link bounces.

Dynamic ARP inspection

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

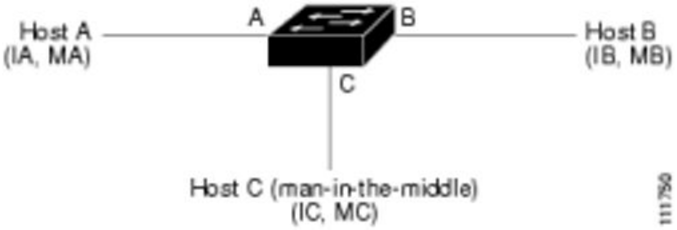


Figure 9: Dynamic ARP inspection

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

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

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

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

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

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

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

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

The following ACLI commands are used for Dynamic ARP Inspection:

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

MAC Flush

The Avaya Ethernet Routing Switch 4000 Series Release 5.3 supports MAC Flush. MAC Flush is a direct way to flush out MAC addresses from the MAC table. If the Layer 2 Forwarding Database (FDB) appears corrupted, you can:

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

- per VLAN

- across the whole switch

The following ACLI commands are used for MAC Flush:

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

MLT/DMLT trunk

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

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

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

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

- DHCP Snooping
- IP Source Guard
- Dynamic ARP Inspection

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

- `send_bsaiArpPacketDroppedOnUntrustedPort_trap`

  - generated when there is an invalid IP/MAC binding
- `send_bsSourceGuardReachedMaxIpEntries_trap`

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

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

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

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

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

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

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

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

- bsDhcpSnoopingBindingTableFull
- bsDhcpSnoopingTrap
- bsaiArpPacketDroppedOnUntrustedPort
- bsSourceGuardReachedMaxIpEntries
- bsSourceGuardCannotEnablePort

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

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

Dynamic Host Configuration Protocol Relay (DHCP) relay

The Avaya Ethernet Routing Switch 4000 Series supports static routes. In order for DHCP servers to talk to clients on different VLANs or subnets, the feature relays client requests to DHCP servers on different Layer 3 VLANs and a relay server replies back to the clients.

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

For more information about ACLI and Web-based management of DHCP relay, see *Configuring IP Routing and Multicast on Avaya Ethernet Routing Switch 4000 Series*, NN47205-506.

Auto Unit Replacement

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

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

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

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

Beginning with Release 5.5, you can remove entries from the Automatic Unit Replacement (AUR) cache. You can use this enhancement to remove the MAC address for a non-operational stack switch from the AUR address cache. A non-operational switch is a unit that is not present in the stack or is in an unknown restore state.

With this enhancement, you can also display MAC address and operational status information for all switches in a stack.

When you remove the MAC address for a non-operational stack switch from the AUR address cache, information about switch hardware type and configuration is maintained on the base unit switch. When the same non-operational switch or a replacement unit is inserted into the stack, AUR performs a hardware type match, and because the switch MAC address was erased, AUR is performed on the inserted switch.

If you attempt to remove the MAC address for an operational switch from the AUR address cache, the base unit switch displays an error message, and the MAC address is not removed.

For more information about AUR, see Configuring Systems on Avaya Ethernet Routing Switch 4000 Series, NN47205-500.

Diagnostic Auto Unit Replacement (DAUR)

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

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

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

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

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

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

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

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

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

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

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

You may encounter the following situations:

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

  transfer is stopped and a serious error message is logged on the Release 5.3 master unit. A manual download must be performed for both the diagnostic and agent images.

  - If the agent image on the added unit is Release 5.2 with the Release 5.2.0.1 diagnostic, then both images support DAUR and the Release 5.2 diagnostic supports images greater than 6M. The new added unit does not join the stack. A diagnostic update is first performed and then, because the agent images are different, an agent update is performed and the switch reboots. The switch joins the stack after reboot .

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

- A stack with Release 5.1 or 5.0 software and the Release 5.1 or 5.0 diagnostic image
  - If the agent image on the added unit is Release 5.2 with the Release 5.2.0.1 diagnostic image, the new added unit does not join stack because the stack does not support DAUR. A diagnostic upgrade or downgrade is not performed and, because agent images are different, an agent downgrade is performed and the switch reboots. The switch joins the stack after reboot .

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

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

Stack master image and diagnostic version	Slave image diagnostic version	Expected behavior
	Software 5.2_non SSH/SSH Diagnostic 5.1	Because the diagnostic and agent images are different, DAUR upgrades the diagnostic image, and then AAUR transfers the agent. AAUR and DAUR reboot the unit. The unit joins the stack after the reboot.
	Software 5.2_non SSH/SSH Diagnostic 5.2	AAUR performs the agent image transfer and reboots the unit. The unit joins the stack after the reboot.

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

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

  – message logged after a stand-alone unit sends a DAUR request
- `Informational: DAUR - Info: Start receive image`

  – message logged after the unit starts to receive an image
- `Serious: DAUR - Warning: Diag image check sum ERROR`

  – message logged after the checksum for the receive image is not the same as the master’s checksum
- `Informational: DAUR - Info: Diag transfer finished`

  – message logged after the image is properly transferred and programmed to flash.
- `Serious: AAUR - Warning: unsupported image size. Please update image manually`

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

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

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

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

  – message logged after a unit receives a request for DAUR transfer and it starts transfer.
- `Informational: DAUR - Info: Diag transfer finished`

  – message logged after the image is properly transferred.
- `Informational: DAUR - Info: Slave refuse transfer`

– message logged when a slave unit refuses diagnostic transfer.

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

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

Multicast behavior

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

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

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

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

IPv6

IPv6 provides dual-stack configuration that allows both IPv4 and IPv6 protocol stacks to run simultaneously. Release 5.7 supports IPv6 for management purposes only.

Running IPv6 is optional. Release 5.7 provides a maximum of one IPv6 interface for the management VLAN only. The IPv6 interface must be enabled on the management VLAN and IPv6 globally enabled on the IPv6 stack.

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

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

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

For detailed information about IPv6, see Configuring Systems on Avaya Ethernet Routing Switch 4000 Series, NN47205-500.

Light Emitting Diode (LED) display

The Avaya Ethernet Routing Switch 4000 Series displays diagnostic and operation information through the LEDs on the unit. Familiarize yourself with the interpretation of the LEDs on the 4000 series device. See the technical document *Installing Avaya Ethernet Routing Switch 4000 Series*, NN47205-300 for detailed information regarding the interpretation of the LEDs.

Avaya Knowledge and Solution Engine

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

Chapter 5: General diagnostic tools

The Avaya Ethernet Routing Switch 4000 Series device has diagnostic features available through DM, ACLI, and Web-based Management. You can use these diagnostic tools to help you troubleshoot operational and configuration issues. You can configure and display files, view and monitor port statistics, trace a route, run loopback and ping tests, test the switch fabric, and view the address resolution table.

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

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

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

ACLI command modes

ACLI provides the following command modes:

- User EXEC
- Privileged EXEC
- Global Configuration
- Interface Configuration
- Router Configuration
- Application Configuration

Mode access is determined by access permission levels and password protection.

If no password is set, you can enter ACLI in User EXEC mode and use the `enable` command to move to the next level (Privileged EXEC mode). However, if you have read-only access, you cannot progress beyond User EXEC mode, the default mode. If you have read-write access you can progress from the default mode through all of the available modes.

With sufficient permission, you can use the rules in the following table to move between the command modes.

Table 1: ACLI command modes

Command mode and sample prompt	Entrance commands	Exit commands

User EXEC
`4548GT-PWR>`
	No entrance command, default mode	`exit`
		or
		`logout`

Privileged EXEC
`4548GT-PWR#`
	`enable`	`exit`
		or
		`logout`

Global Configuration
`4548GT-PWR(config)#`
	`configure terminal`	mode, enter:
		`end`
		or
		`exit`
		To exit ACLI completely, enter:
		`logout`

Interface Configuration
`4548GT-PWR(config-if)#`
You can configure the following interfaces:
• Ethernet
• VLAN
	From Global Configuration mode: To configure a port, enter: `interface ethernet <port number>`
	To configure a VLAN, enter: `interface vlan <vlan number>`
		To return to Global Configuration mode, enter:
		`Exit`
		To return to Privileged EXEC mode, enter:
		`end`
		To exit ACLI completely, enter:
		`logout`

Router Configuration `4548GT-(configrouter)#` You can configure the following routers: • RIP • OSPF • VRRP • ISIS	From Global or Interface Configuration mode: To configure RIP, enter `router rip`. To configure OSPF, enter `router ospf`. To configure VRRP, enter `router vrrp`. To configure IS-IS, enter `router isis`.	To return to Global Configuration mode, enter `exit`. To return to Privileged EXEC mode, enter `end`. To exit ACLI completely, enter `logout`.
Application Configuration `4850GT-(config-app)`	From Global, Interface or Router Configuration mode, enter `application`.	To return to Global Configuration mode, enter `exit`. To return to Privileged EXEC mode, enter `end`. To exit ACLI completely, enter `logout`.

Chapter 6: Initial troubleshooting

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

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

Gather information

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

- **Default and current configuration of the switch**. To obtain this information, use the **`show running-config`** command.
- **System status**. Obtain this information using the **`show sys-info`** command. Output from the command displays technical information about system status and information about the hardware, software, and switch operation. For more detail, use the **`show tech`** command.
- **Information about past events**. To obtain this information, review the log files using the **`show logging`** command.
- **Information about the FLASH boot image, agent image, or diagnostic image version**. To obtain this information for a single unit or from the base unit, use the **show flash** command. To obtain this information from a specified unit in the stack, use the **show flash unit <1-8>** command.
- The **software version** that is running on the device. To obtain this information, use the **`show sys-info`** or **`show system verbose`** command to display the software version that is running on all devices.
- A **`network topology diagram`**: Get an accurate and detailed topology diagram of your network that shows the nodes and connections. Your planning and engineering function should have this diagram.
- **`Recent changes`**: Find out about recent changes or upgrades to your system, your network, or custom applications (for example, has configuration or code been changed). Get the date and time of the changes, and the names of the persons who made them.

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

- **`Connectivity information`**: To help troubleshoot connectivity problems, you should always provide source and destination IP pairs to facilitate in troubleshooting. Ten pairs is a good rule of thumb (five working pairs and five pairs with connectivity issues). Use the following commands to get connectivity information:
    - **`show tech`**
    - **`show running-config`**
    - **`show port-statistics <port>`**

Chapter 7: Emergency recovery trees

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

Emergency recovery trees

About this task

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.

Procedure

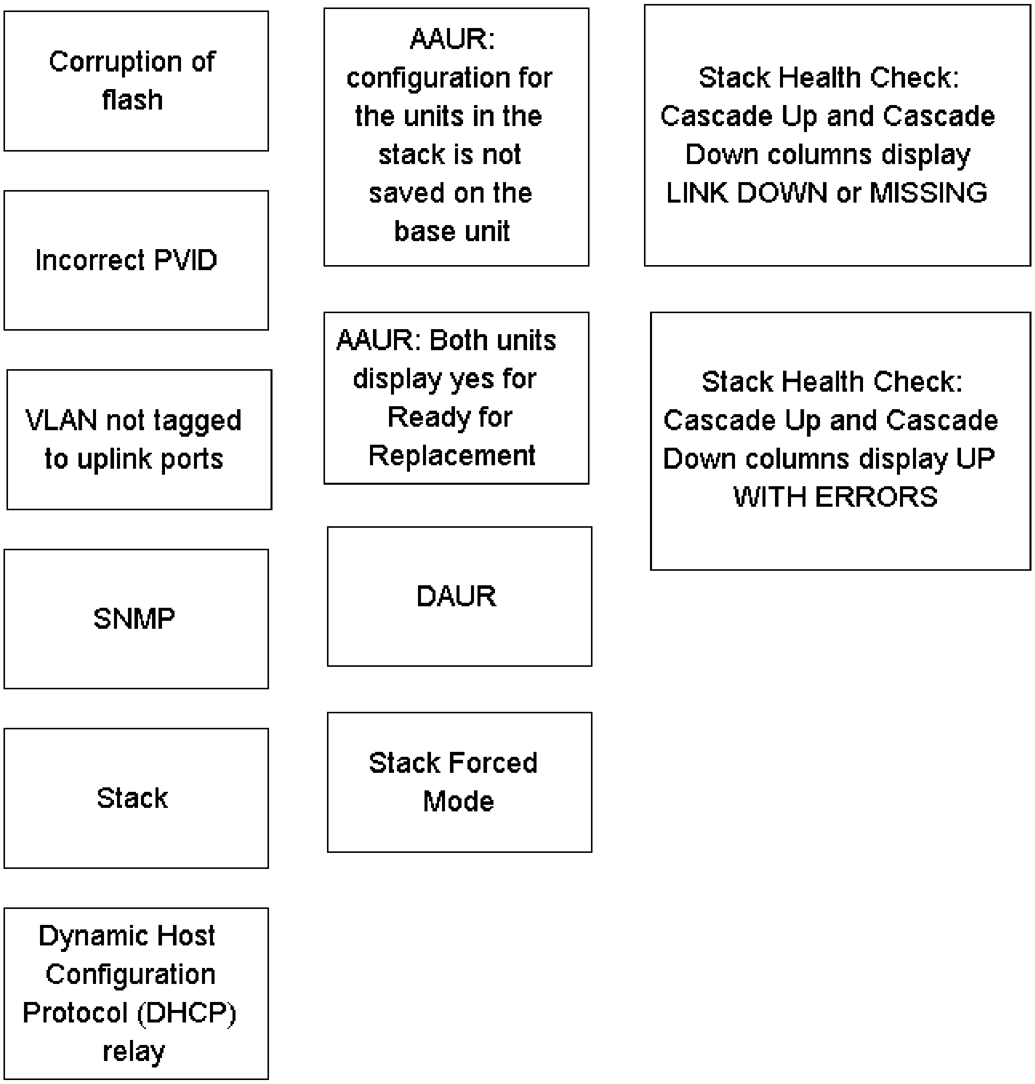

Corruption of flash
Incorrect PVID
VLAN not tagged to uplink ports
SNMP
Stack
Dynamic Host Configuration Protocol (DHCP) relay
AAUR: configuration for the units in the stack is not saved on the base unit
AAUR: Both units display yes for Ready for Replacement
DAUR
Stack Forced Mode
Stack Health Check: Cascade Up and Cascade Down columns display LINK DOWN or MISSING
Stack Health Check: Cascade Up and Cascade Down columns display UP WITH ERRORS

Figure 10: Emergency recovery trees

Navigation

- Corruption of flash on page 55
- Incorrect PVID on page 56
- VLAN not tagged to uplink ports on page 57

- SNMP on page 60
- Stack on page 62
- Dynamic Host Configuration Protocol (DHCP) relay on page 68
- AAUR: configuration for the units in the stack is not saved on the base unit on page 69
- AAUR: Both units display yes for Ready for Replacement on page 72
- DAUR on page 74
- Stack Forced Mode on page 76
- Stack Health Check: Cascade Up and Cascade Down columns display LINK DOWN or MISSING on page 77
- Stack Health Check: Cascade Up and Cascade Down columns display UP WITH ERRORS on page 80

Corruption of flash

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

Corruption of flash recovery tree

About this task

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

Procedure

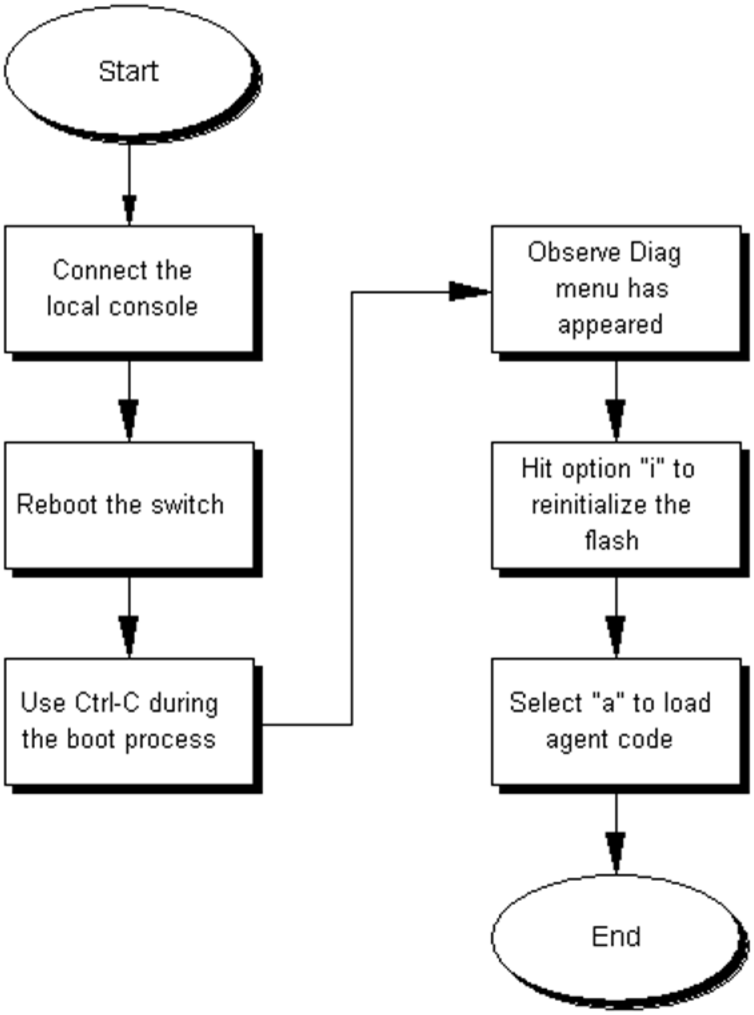

Start
Connect the local console
Reboot the switch
Use Ctrl-C during the boot process
Observe Diag menu has appeared
Hit option "i" to reinitialize the flash
Select "a" to load agent code
End

Figure 11: Corruption of flash

Incorrect PVID

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

Incorrect PVID recovery tree

About this task

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

Procedure

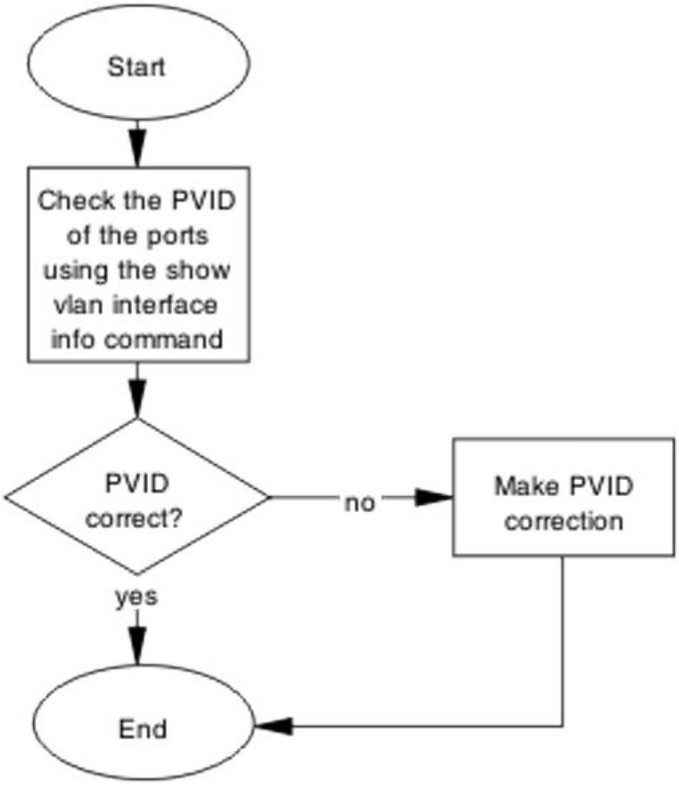

Start
Check the PVID of the ports using the show vlan interface info command
PVID correct?
no
Make PVID correction
yes
End

Figure 12: Incorrect PVID

VLAN not tagged to uplink ports

After a 4000 Series switch is connected to an 8600 Series switch and devices in a VLAN on the 8600 Series switch are unable to communicate with devices at the 4000 Series switch in the same VLAN, then it is likely that the uplink ports are not tagged to the VLAN on the 4000 Series switch.

VLAN not tagged to uplink ports recovery tree

About this task

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

Procedure

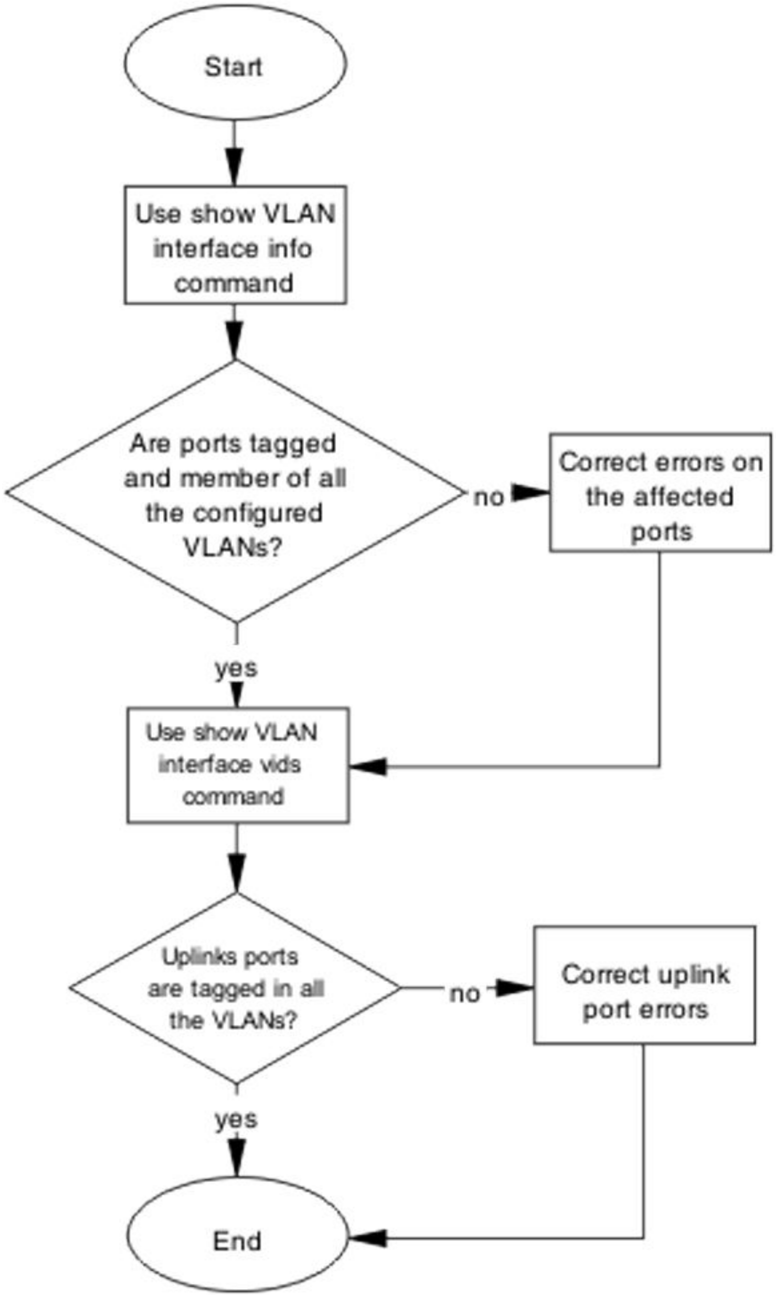

Start
Use show VLAN interface info command
Are ports tagged and member of all the configured VLANs?
no
Correct errors on the affected ports
yes
Use show VLAN interface vids command
Uplinks ports are tagged in all the VLANs?
no
Correct uplink port errors
yes
End

Figure 13: VLAN not tagged to uplink ports

SNMP

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

SNMP recovery tree

About this task

The following figures show the SNMP recovery tree.

Procedure

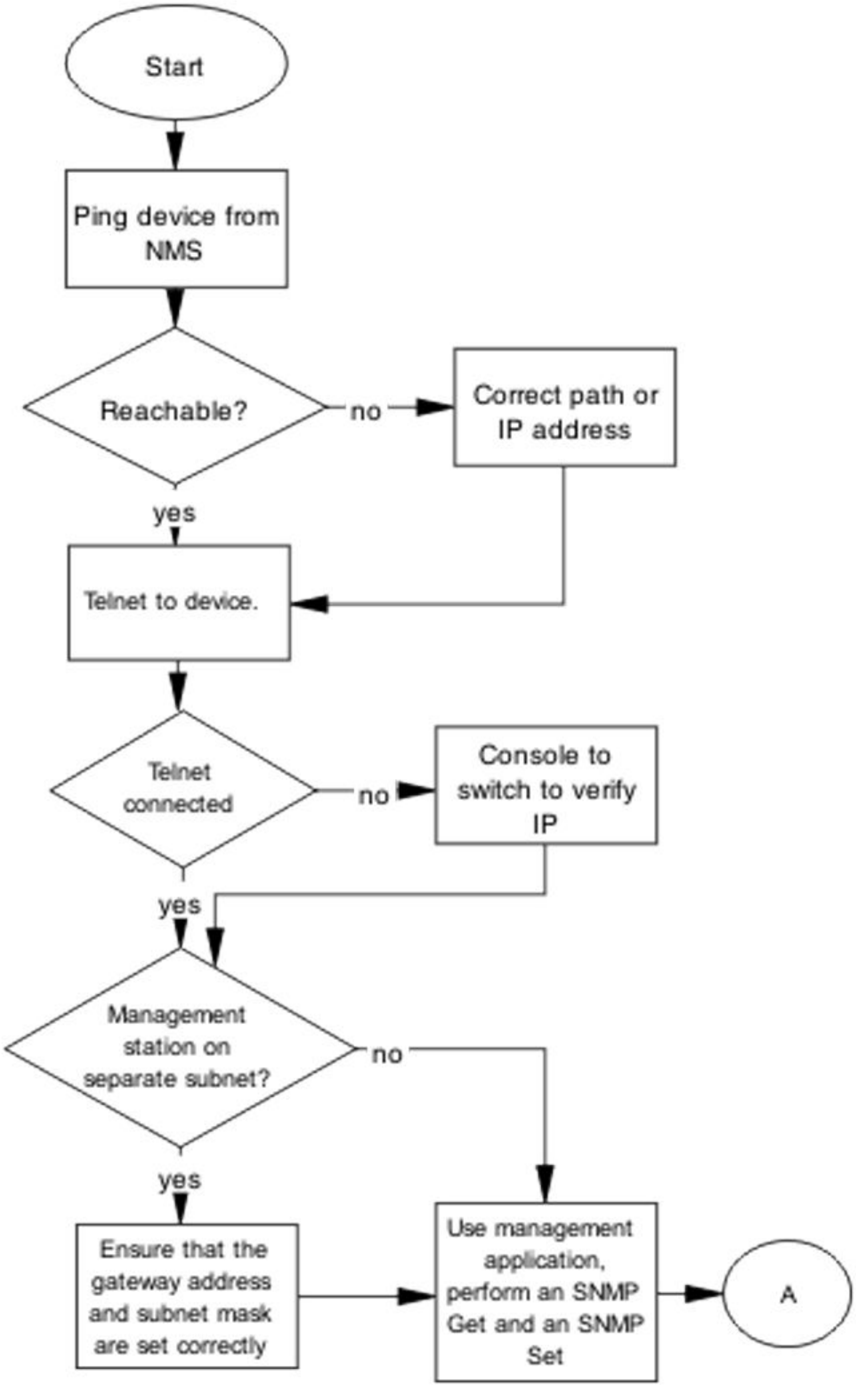

Start
Ping device from NMS
Reachable?
no
Correct path or IP address
yes
Telnet to device.
Telnet connected
no
Console to switch to verify IP
yes
Management station on separate subnet?
no
yes
Ensure that the gateway address and subnet mask are set correctly
Use management application, perform an SNMP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

Figure 14: SNMP part 1

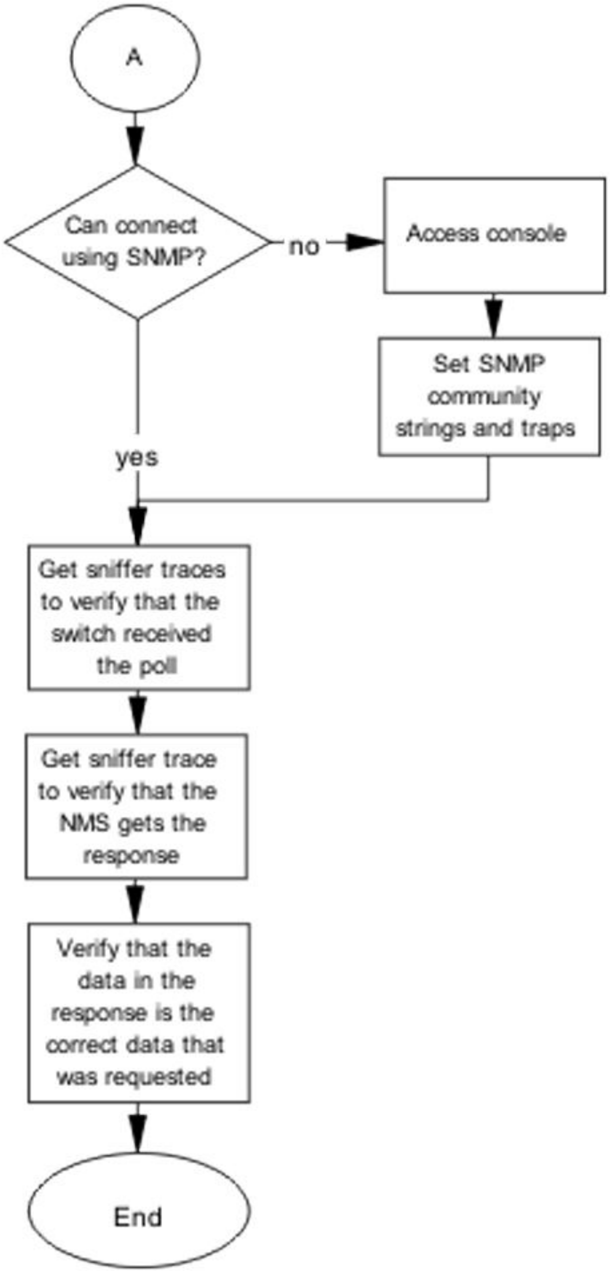

A
Can connect using SNMP?
no
Access console
Set SNMP community strings and traps
yes
Get sniffer traces to verify that the switch received the poll
Get sniffer trace to verify that the NMS gets the response
Verify that the data in the response is the correct data that was requested
End

Figure 15: SNMP part 2

Stack

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

Several situation may cause stacking problems, for example:

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

Stack recovery tree

About this task

The following figures show the stack recovery tree.

Procedure

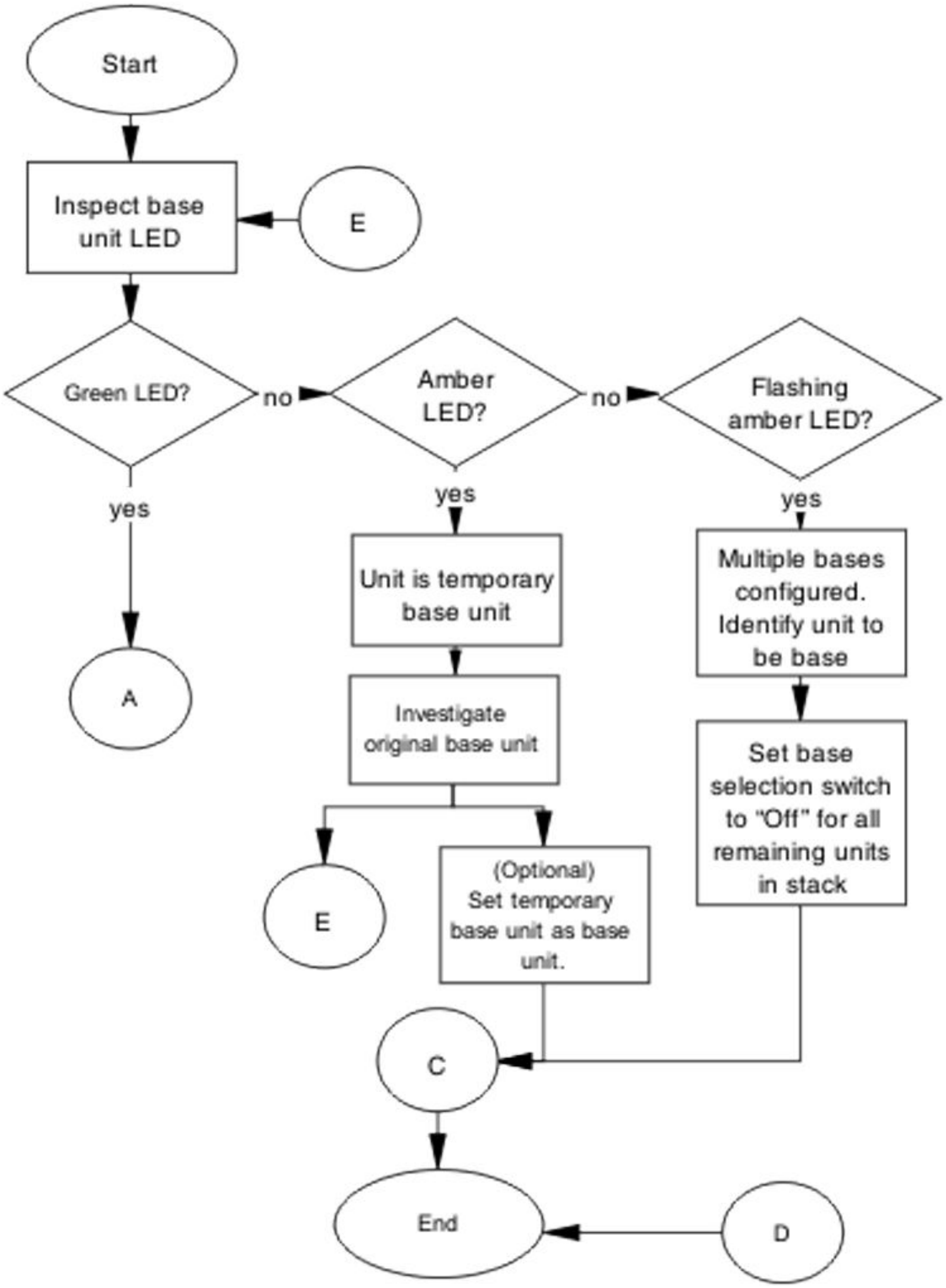

Start
Inspect base unit LED
E
Green LED?
no
Amber LED?
no
Flashing amber LED?
yes
yes
yes
A
Unit is temporary base unit
Investigate original base unit
E
(Optional) Set temporary base unit as base unit.
Multiple bases configured. Identify unit to be base
Set base selection switch to "Off" for all remaining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

Figure 16: Stack part 1

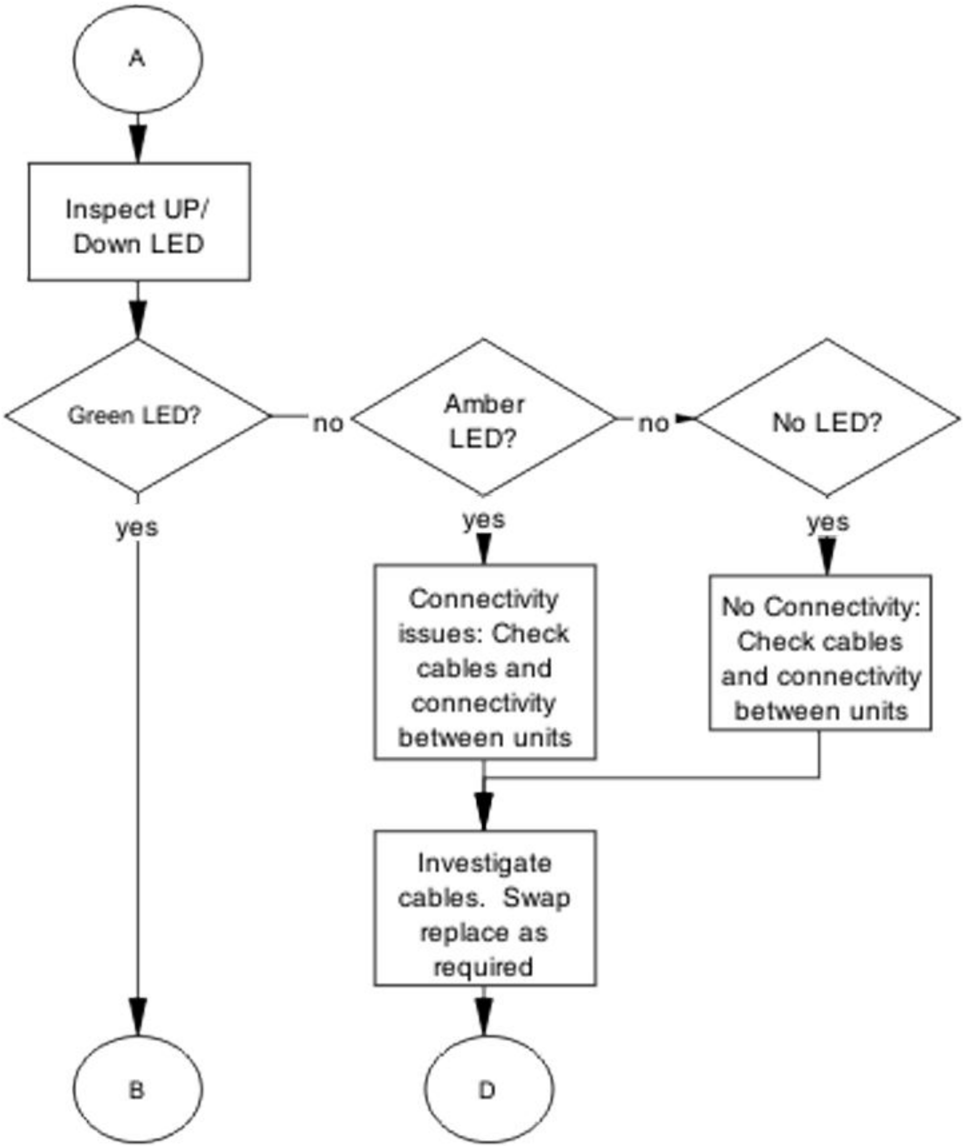

A
Inspect UP/ Down LED
Green LED?
no
Amber LED?
no
No LED?
yes
yes
yes
Connectivity issues: Check cables and connectivity between units
No Connectivity: Check cables and connectivity between units
Investigate cables. Swap replace as required
B
D

Figure 17: Stack part 2

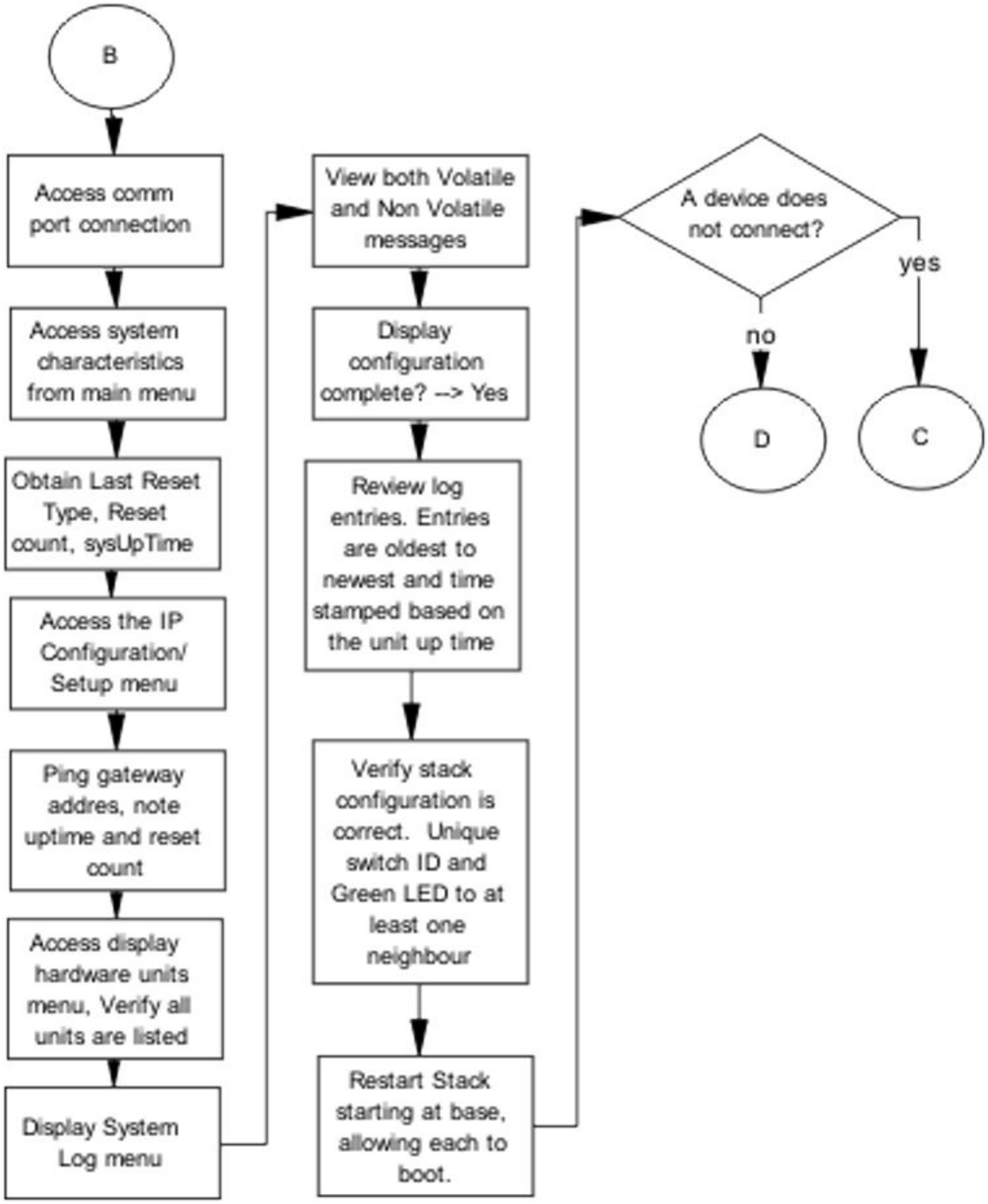

B
Access comm port connection
Access system characteristics from main menu
Obtain Last Reset Type, Reset count, sysUpTime
Access the IP Configuration/ Setup menu
Ping gateway addres, note uptime and reset count
Access display hardware units menu, Verify all units are listed
Display System Log menu
View 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?
yes
no
D
C

Figure 18: Stack part 3

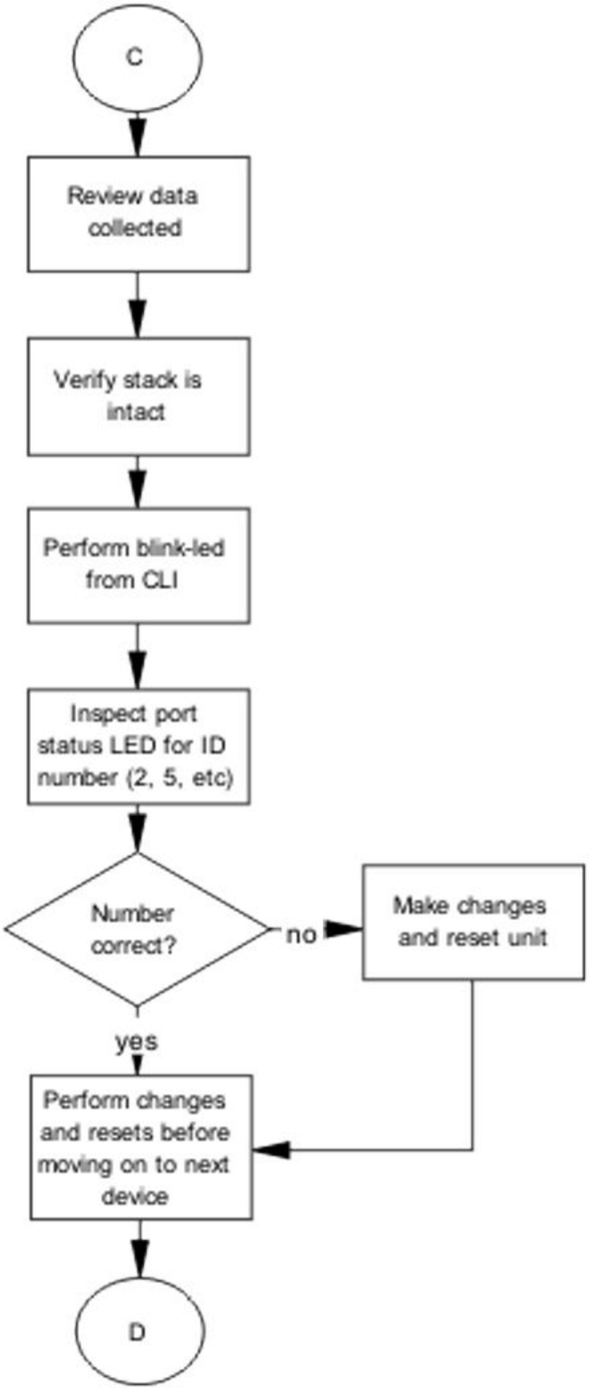

C
Review data collected
Verify stack is intact
Perform blink-led from CLI
Inspect port status LED for ID number (2, 5, etc)
Number correct?
no
Make changes and reset unit
yes
Perform changes and resets before moving on to next device
D

Figure 19: 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

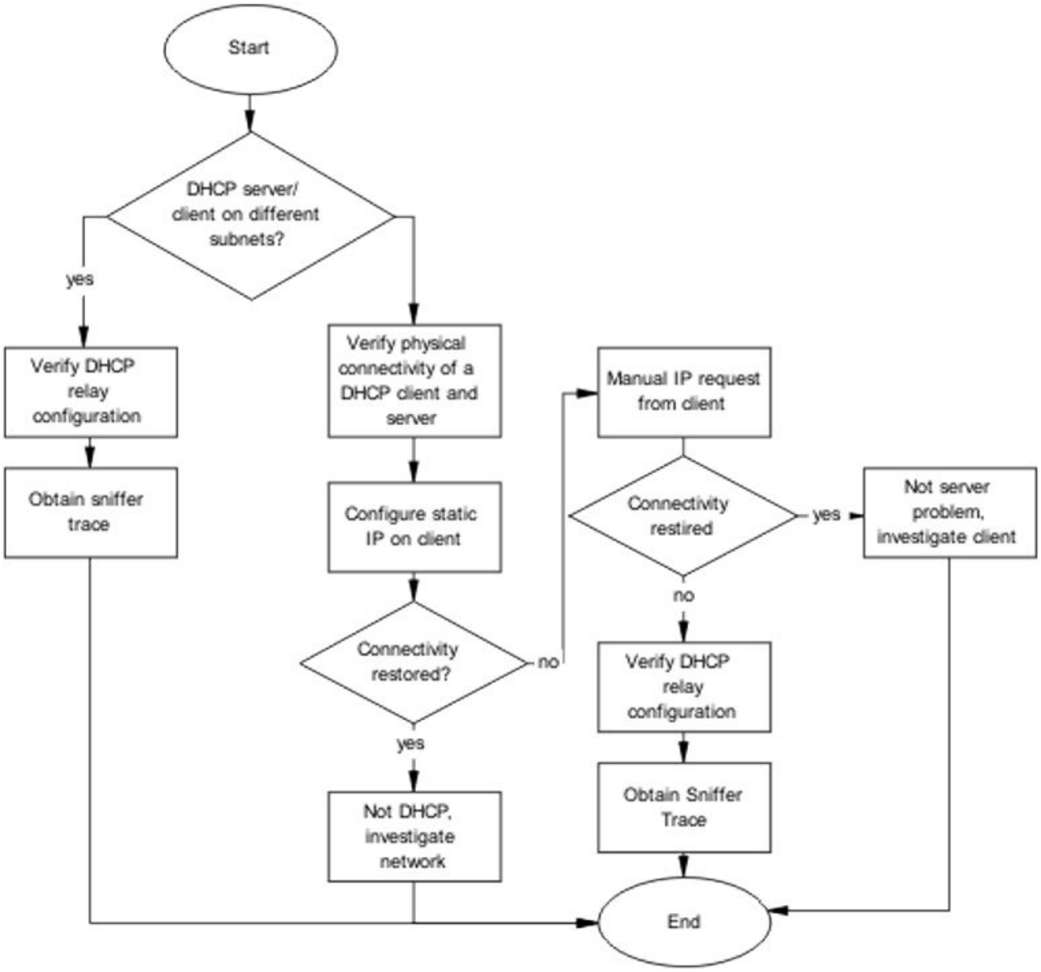

Start
DHCP server/ client on different subnets?
yes
Verify DHCP relay configuration
Obtain sniffer trace
Verify physical connectivity of a DHCP client and server
Configure static IP on client
Connectivity restored?
no
yes
Not DHCP, investigate network
Manual IP request from client
Connectivity restired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

Figure 20: DHCP

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

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

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

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

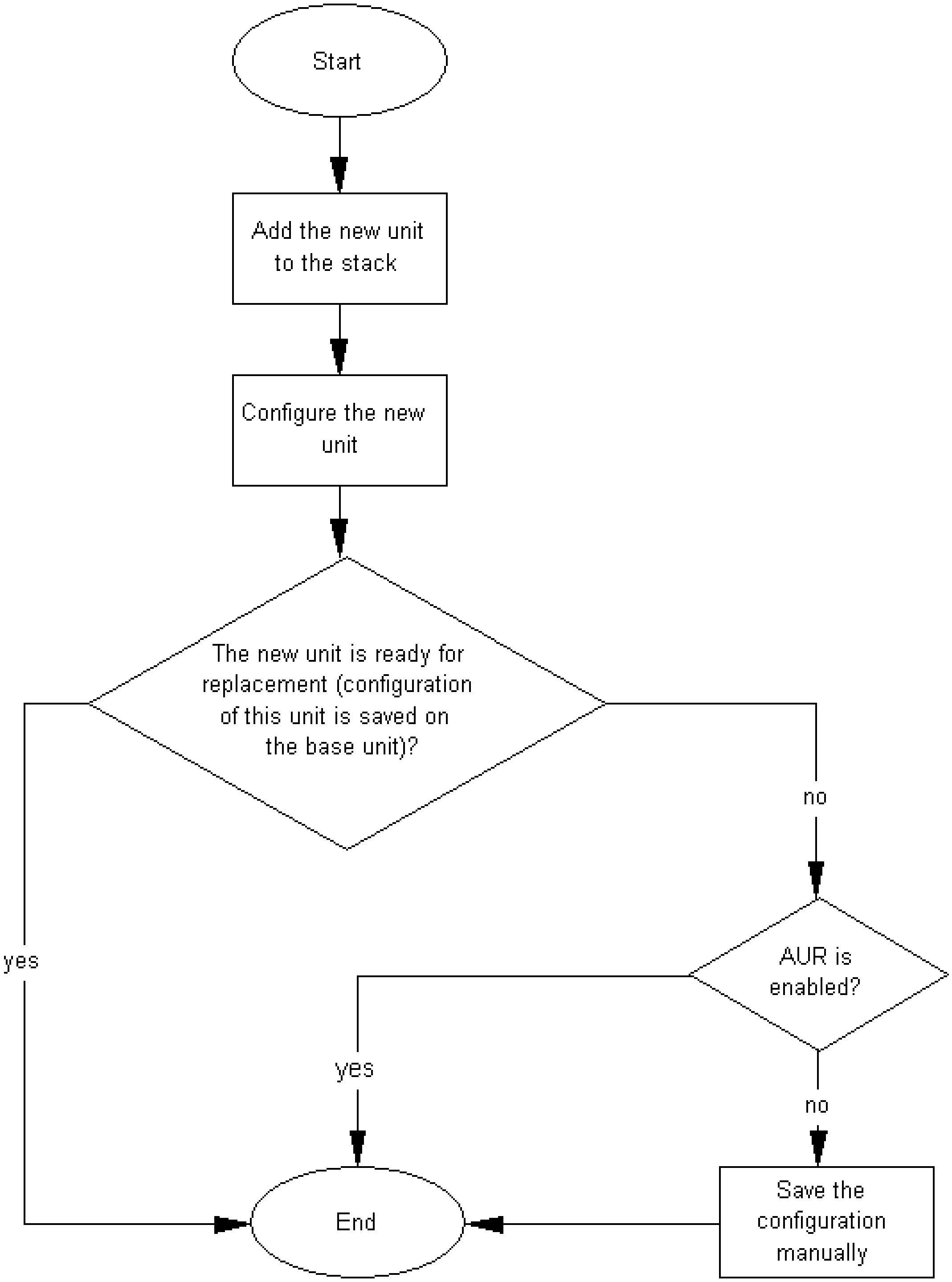

Start
Add the new unit to the stack
Configure the new unit
The new unit is ready for replacement (configuration of this unit is saved on the base unit)?
no
yes
AUR is enabled?
yes
no
Save the configuration manually
End

Figure 21: 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

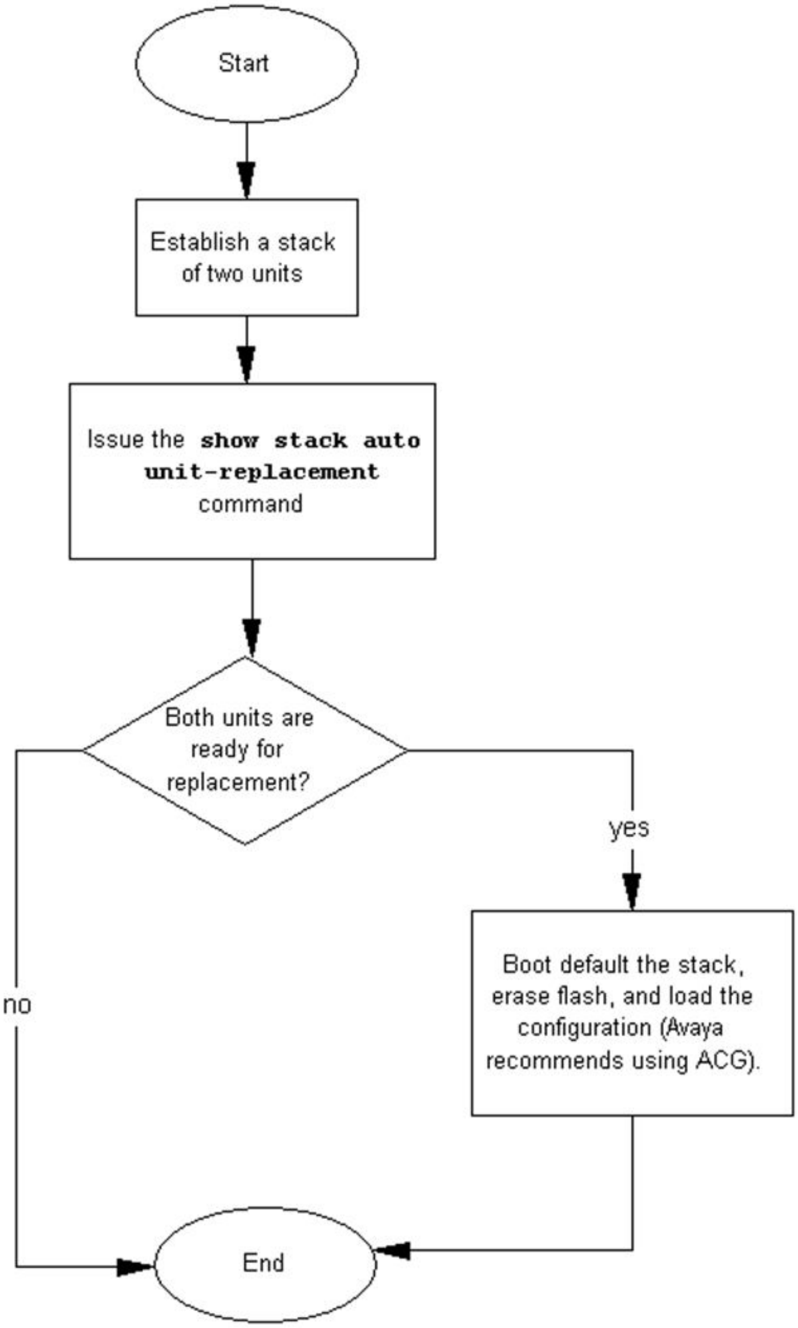

Start
Establish a stack of two units
Issue the **show stack auto unit-replacement** command
Both units are ready for replacement?
yes
no
Boot default the stack, erase flash, and load the configuration (Avaya recommends using ACG).
End

Figure 22: 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

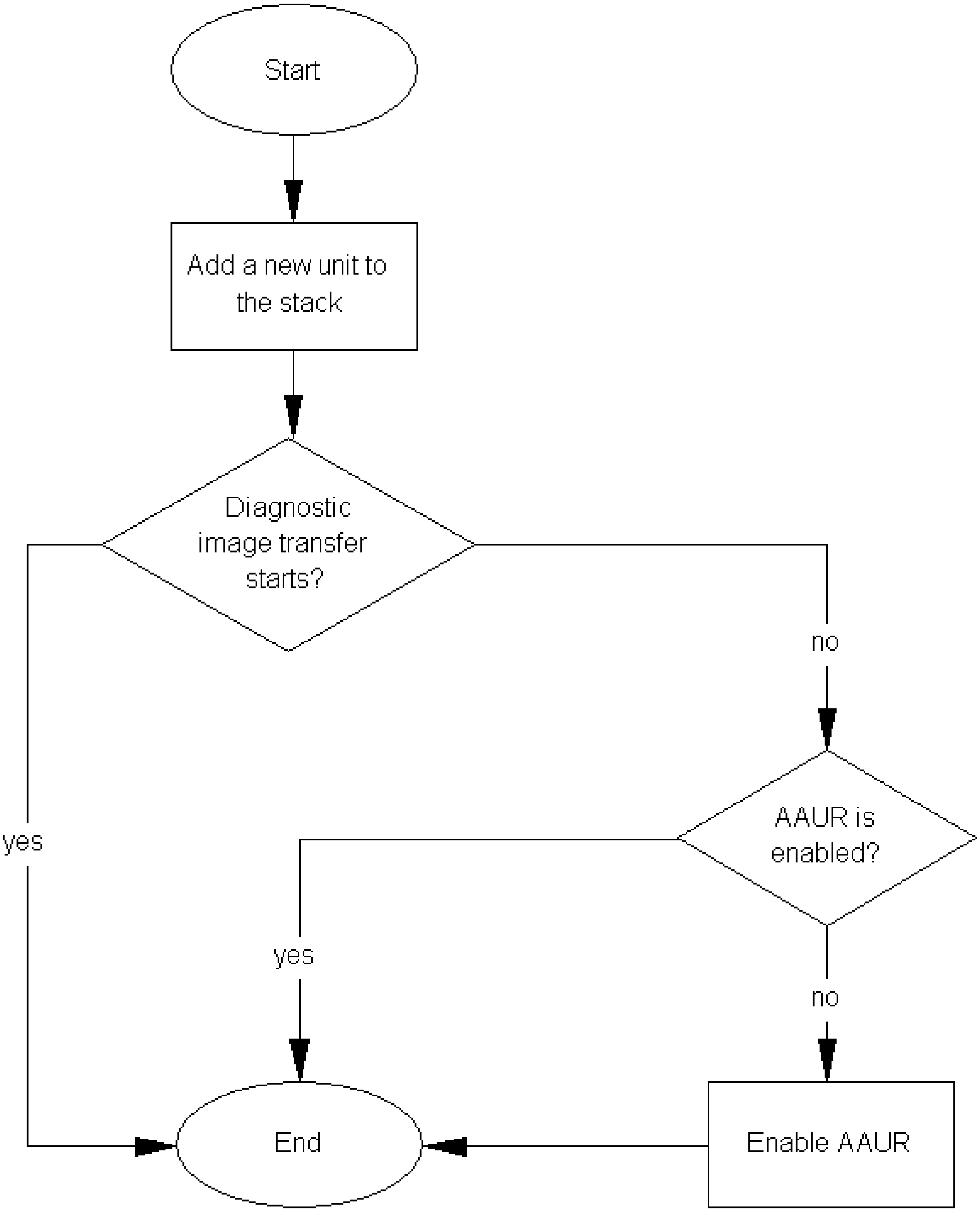

Start
Add a new unit to the stack
Diagnostic image transfer starts?
no
yes
AAUR is enabled?
yes
no
End
Enable AAUR

Figure 23: Diagnostic image transfer does not start

Stack Forced Mode

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

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

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

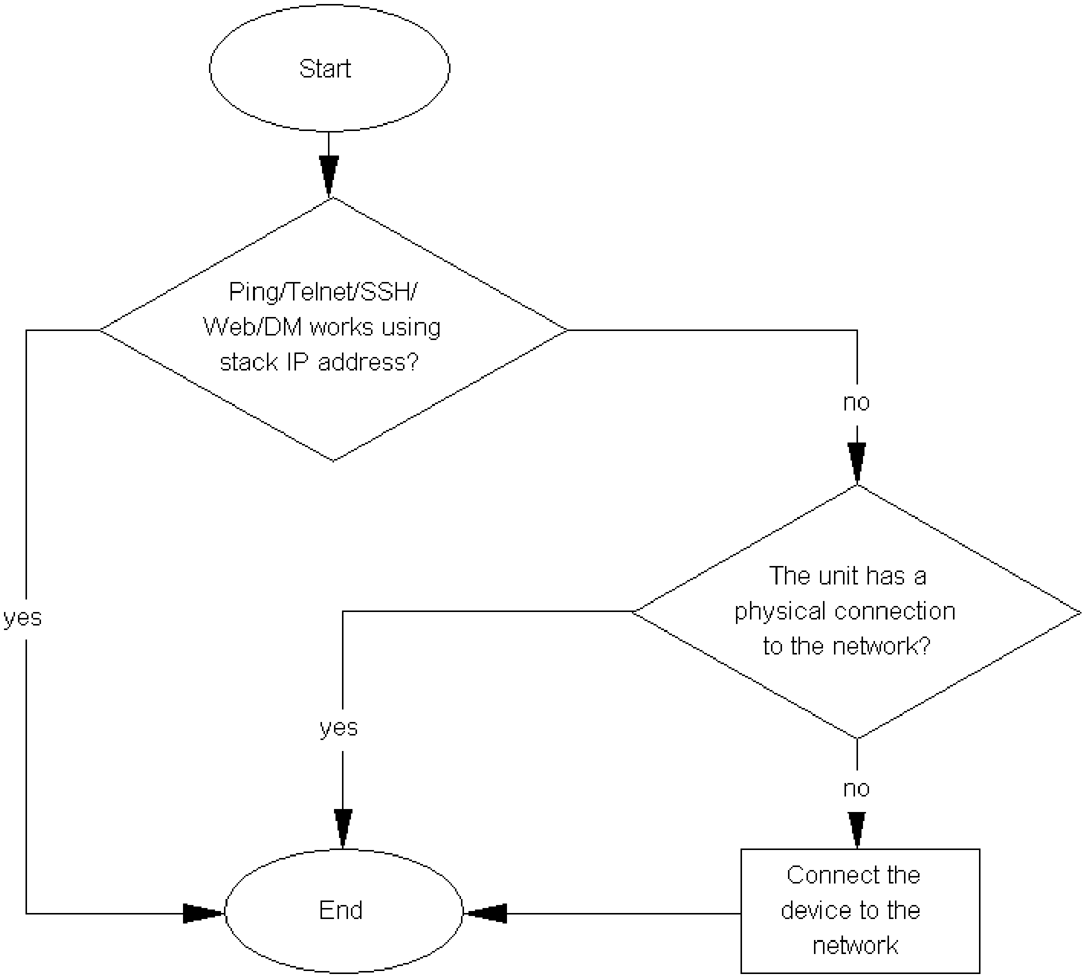

Start
Ping/Telnet/SSH/ Web/DM works using stack IP address?
no
yes
The unit has a physical connection to the network?
yes
no
End
Connect the device to the network

Figure 24: Ping/Telnet/SSH/Web/DM do not work when you use the stack IP address

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

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

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

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

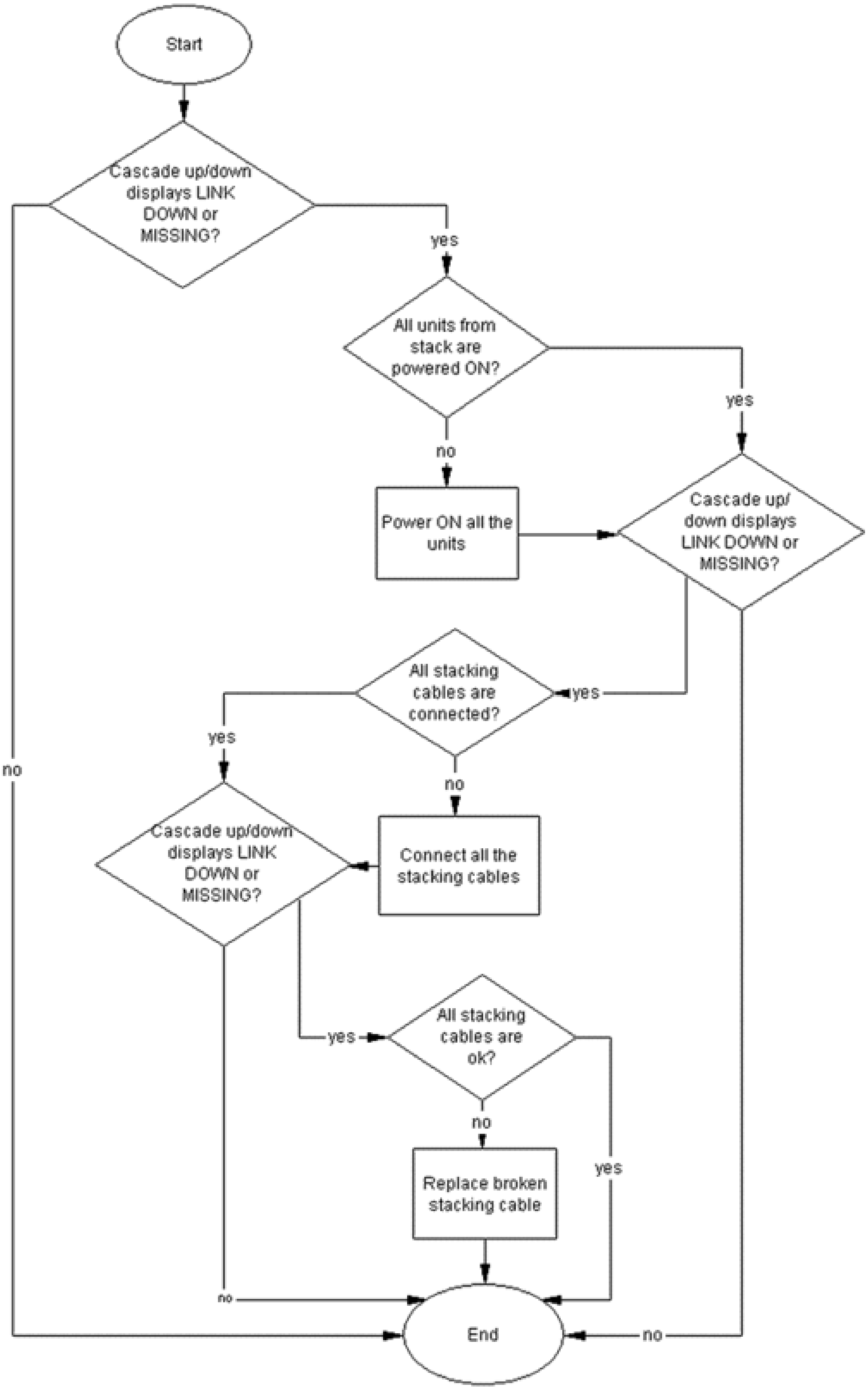

Start
Cascade up/down displays LINK DOWN or MISSING?
yes
no
All units from stack are powered ON?
yes
no
Power ON all the units
Cascade up/ down displays LINK DOWN or MISSING?
All stacking cables are connected?
yes
yes
no
Cascade up/down displays LINK DOWN or MISSING?
Connect all the stacking cables
yes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

Figure 25: Stack Health Check: Cascade Up and Cascade Down columns display LINK DOWN or MISSING

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

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

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

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

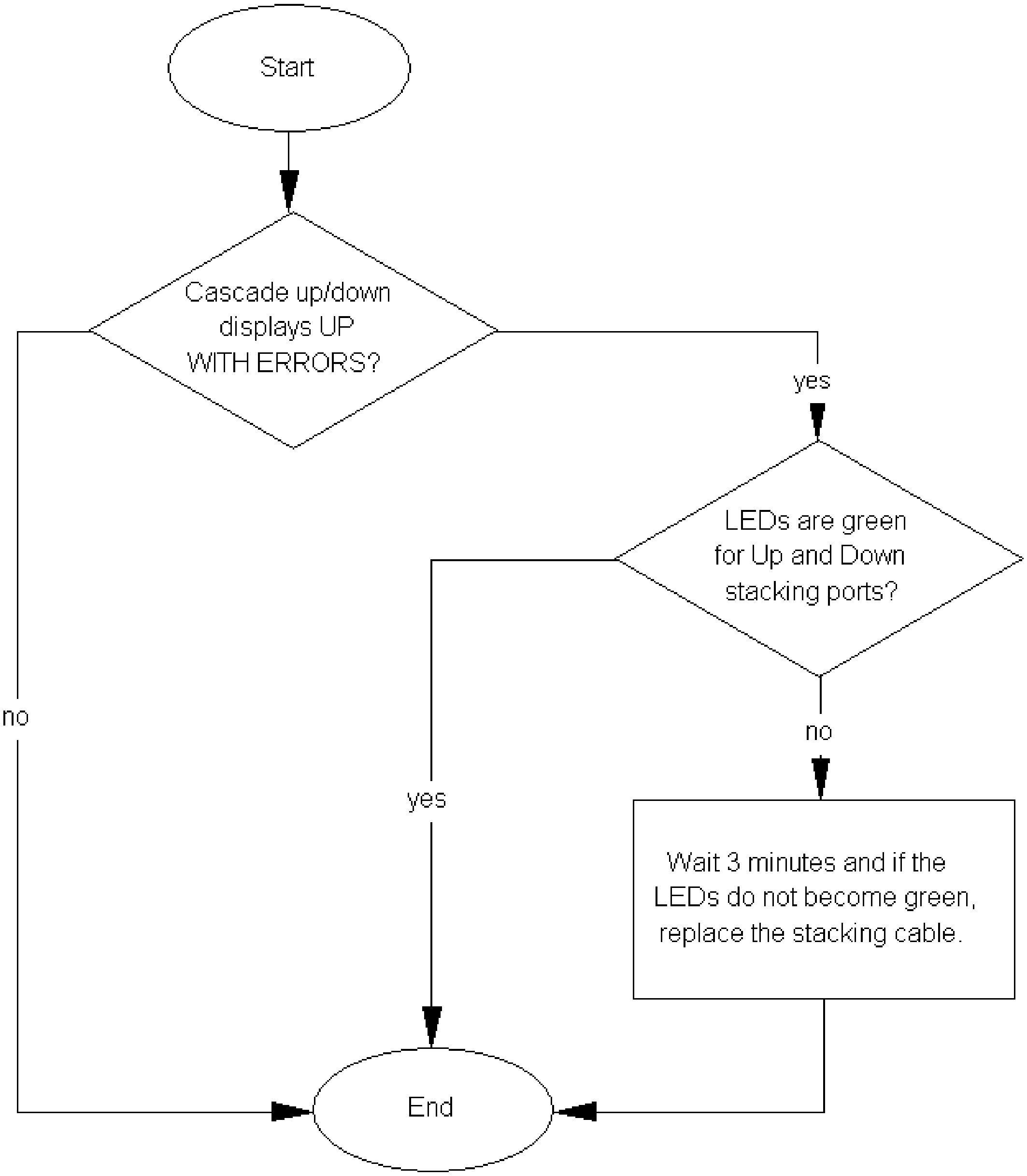

Start
Cascade up/down displays UP WITH ERRORS?
yes
no
LEDs are green for Up and Down stacking ports?
yes
no
Wait 3 minutes and if the LEDs do not become green, replace the stacking cable.
End

Figure 26: Stack Health Check: Cascade Up and Cascade Down columns display UP WITH ERRORS

Chapter 8: General troubleshooting of hardware

Use this section for hardware troubleshooting specific to the Avaya Ethernet Routing Switch 4000 Series.

Work flow: General troubleshooting of hardware

About this task

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

Procedure

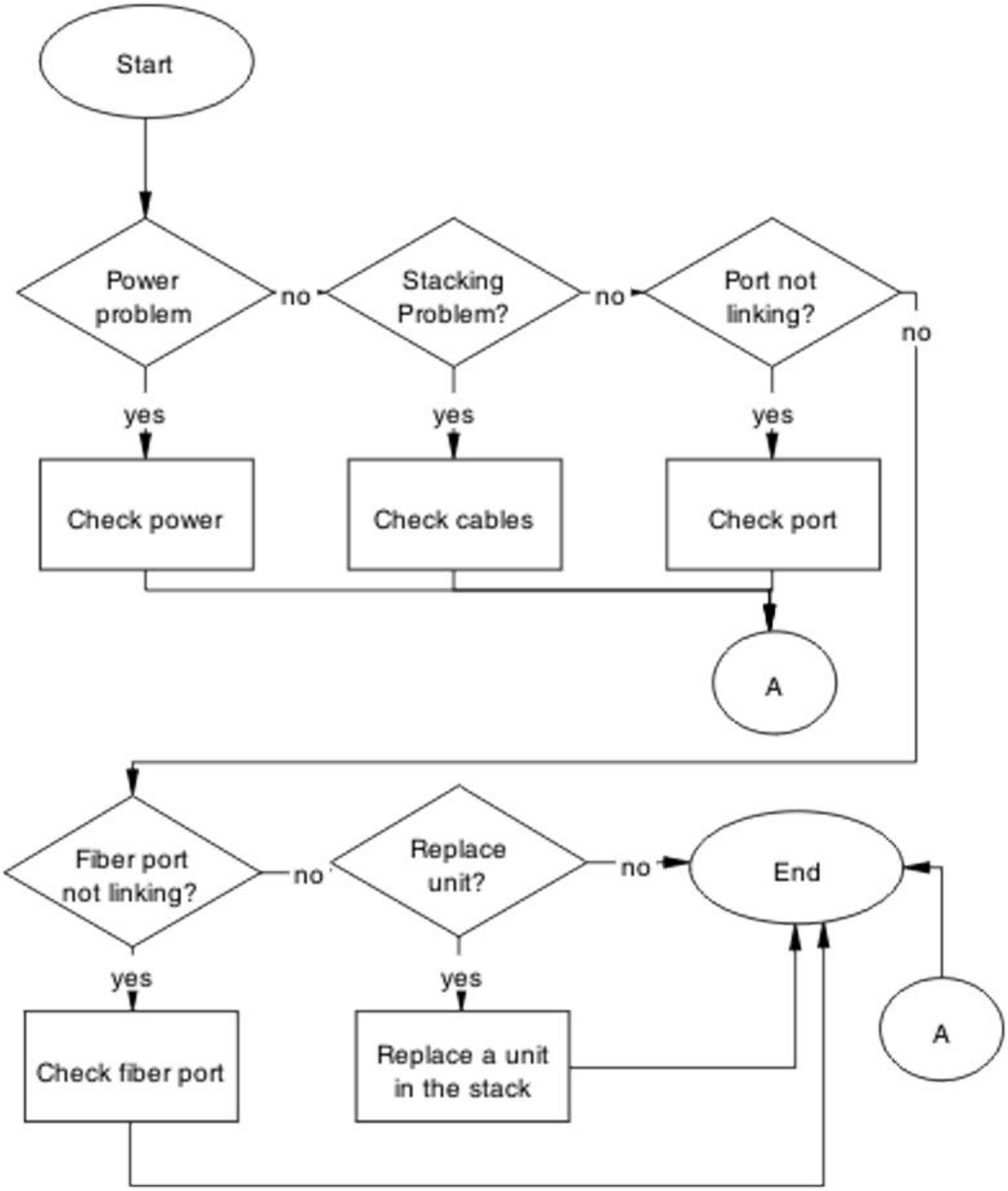


Figure 27: General troubleshooting of hardware

Check power

Confirm power is being delivered to the device. The Avaya Ethernet Routing Switch 4000 Series utilizes a universal Power Supply Unit (PSU) that operates with voltages between 90v and 260v AC.

Task flow: Check power

About this task

The following task flow assists you to confirm that the Avaya Ethernet Routing Switch 4000 Series device is powered correctly.

Procedure

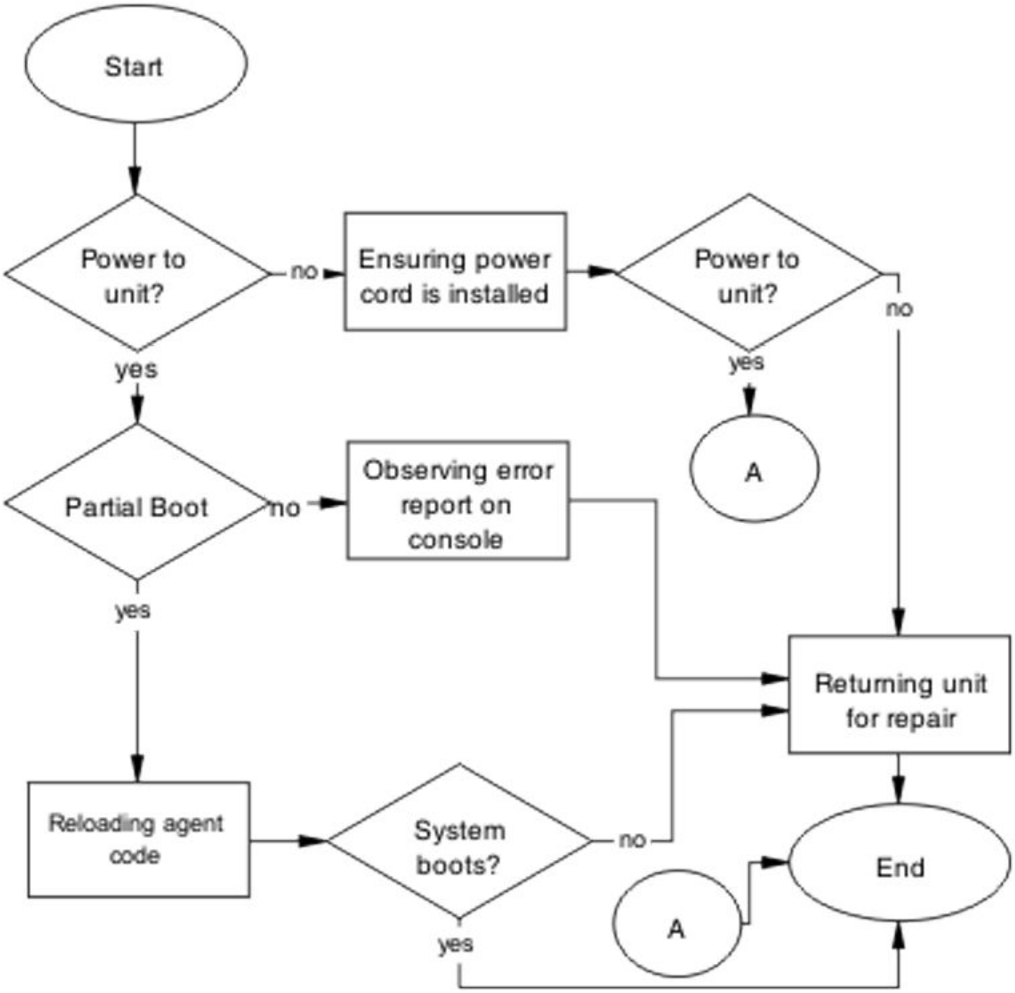


Figure 28: Check power

Result

Navigation

- Ensuring the power cord is installed on page 87
- Observing an error report on the console on page 87
- Reloading the agent code on page 87
- Returning the unit for repair on page 88

Ensuring the power cord is installed

About this task

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

See the technical document *Installing Avaya Ethernet Routing Switch 4000 Series*, NN47205-300 for power cord standards and details.

Observing an error report on the console

About this task

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

Procedure

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

Reloading the agent code

About this task

Reload the agent code on the Avaya Ethernet Routing Switch 4000 Series device to eliminate corrupted or damaged code that causes a partial boot of the device.

⚠ **Caution:**

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

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

Procedure

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

2. See *Release Notes for Avaya Ethernet Routing Switch 4000 Series*, NN47205-400 for information about software installation.

Replacing the power cord

About this task

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

Procedure

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

Returning the unit for repair

About this task

Return a unit to Avaya for repair.

Contact Avaya for return instructions and RMA information.

Check cables

Confirm the stacking cables are correctly connected. Review the *Installing Avaya Ethernet Routing Switch 4000 Series*, NN47205-300 stacking section for cable requirements.

Task flow: Check cables

About this task

The following task flow assists you to confirm the stacking cables on the Avaya Ethernet Routing Switch 4000 Series device are installed correctly.

Procedure

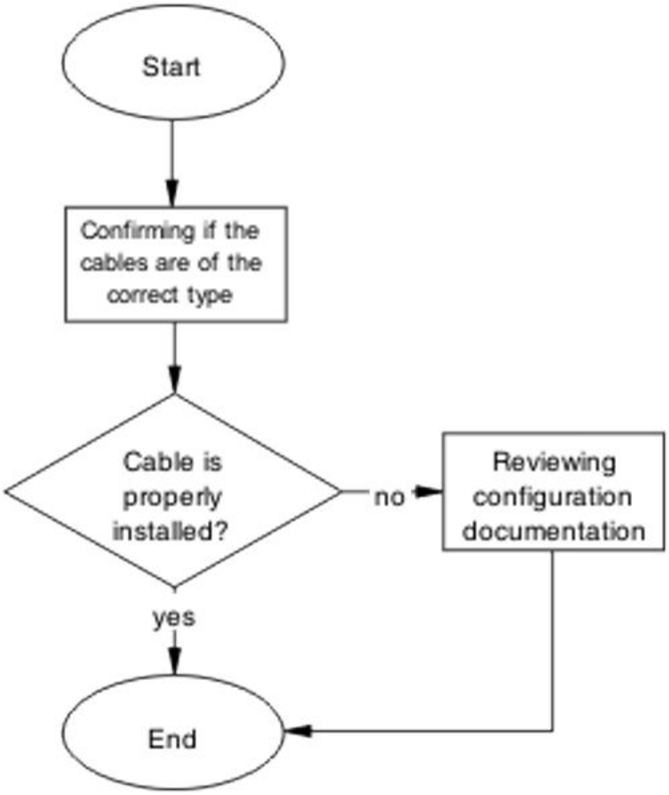

Start
Confirming if the cables are of the correct type
Cable is properly installed?
no
Reviewing configuration documentation
yes
End

Figure 29: Check cables

Result

Navigation

- Confirming if the cables are the correct type on page 89
- Reviewing stacking configuration documentation on page 90

Confirming if the cables are the correct type

About this task

To create a stack connection, order the appropriate Avaya Ethernet Routing Switch 4000 Series cascade cables to ensure fail-safe stacking. A 1.5 foot stacking cable is included with the switch. For stacking three or more units (maximum eight units in a stack), order the 5-foot (1.5 m), 10-foot (3.0 m), 14-foot (4.3 m), or 16.4-foot (4.9 m) cables as applicable.

Reviewing stacking configuration documentation

About this task

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

Review the stacking procedure and diagram for your stack configuration (cascade up or down) in the stacking section of *Installing Avaya Ethernet Routing Switch 4000 Series*, NN47205-300.

Check port

Confirm that the port and the Ethernet cable connecting the port are in proper configuration.

Task flow: Check port

About this task

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

Procedure

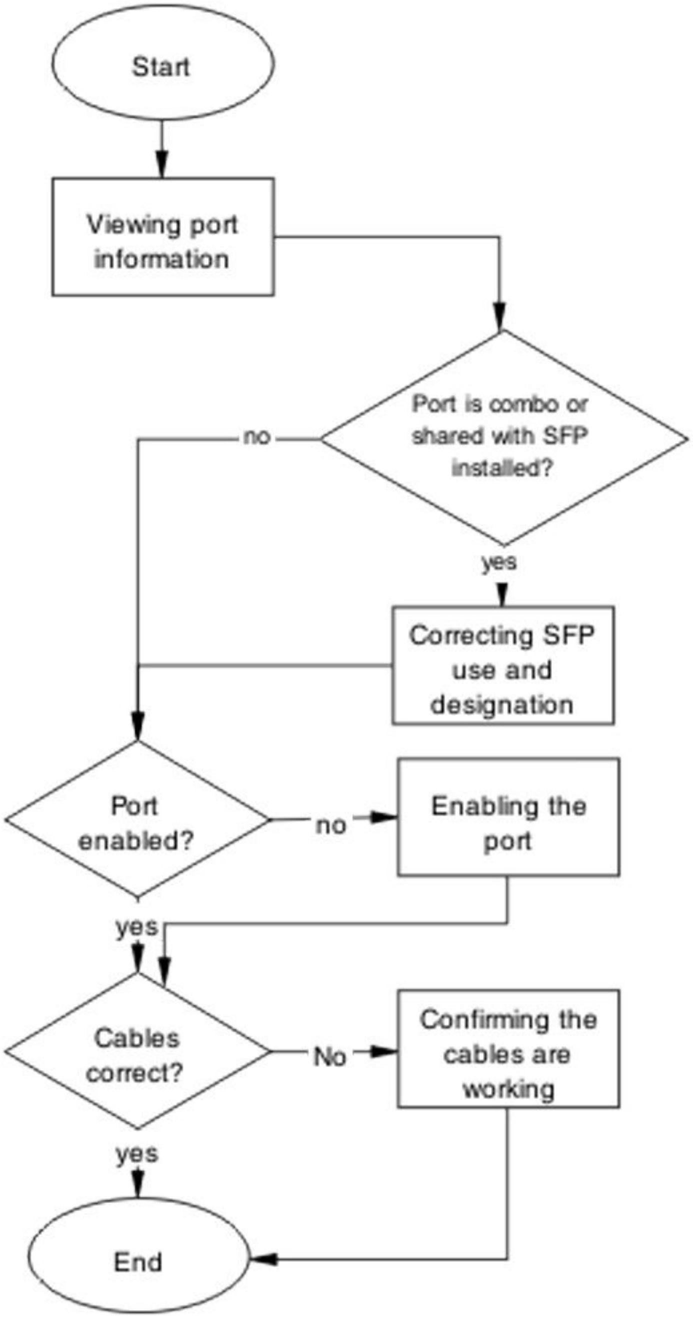

Start
Viewing port information
Port is combo or shared with SFP installed?
no
yes
Correcting SFP use and designation
Port enabled?
no
Enabling the port
yes
Cables correct?
No
Confirming the cables are working
yes
End

Figure 30: Check port

Result

Navigation

- Viewing port information on page 92
- Correcting SFP use and designation on page 92
- Enabling the port on page 92
- Confirming the cables are working on page 93

Viewing port information

About this task

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

Procedure

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

Correcting SFP use and designation

About this task

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

For complete information about SFP transceiver use and designation, see *Installing Transceivers and Optical Components on Avaya Ethernet Routing Switch 4000 Series*, NN47205-301.

Enabling the port

About this task

Enable the port.

Procedure

1. Go to interface specific mode using the **`interface ethernet <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

About this task

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

Procedure

1. Go to interface specific mode using the **`interface ethernet <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

About this task

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

Procedure

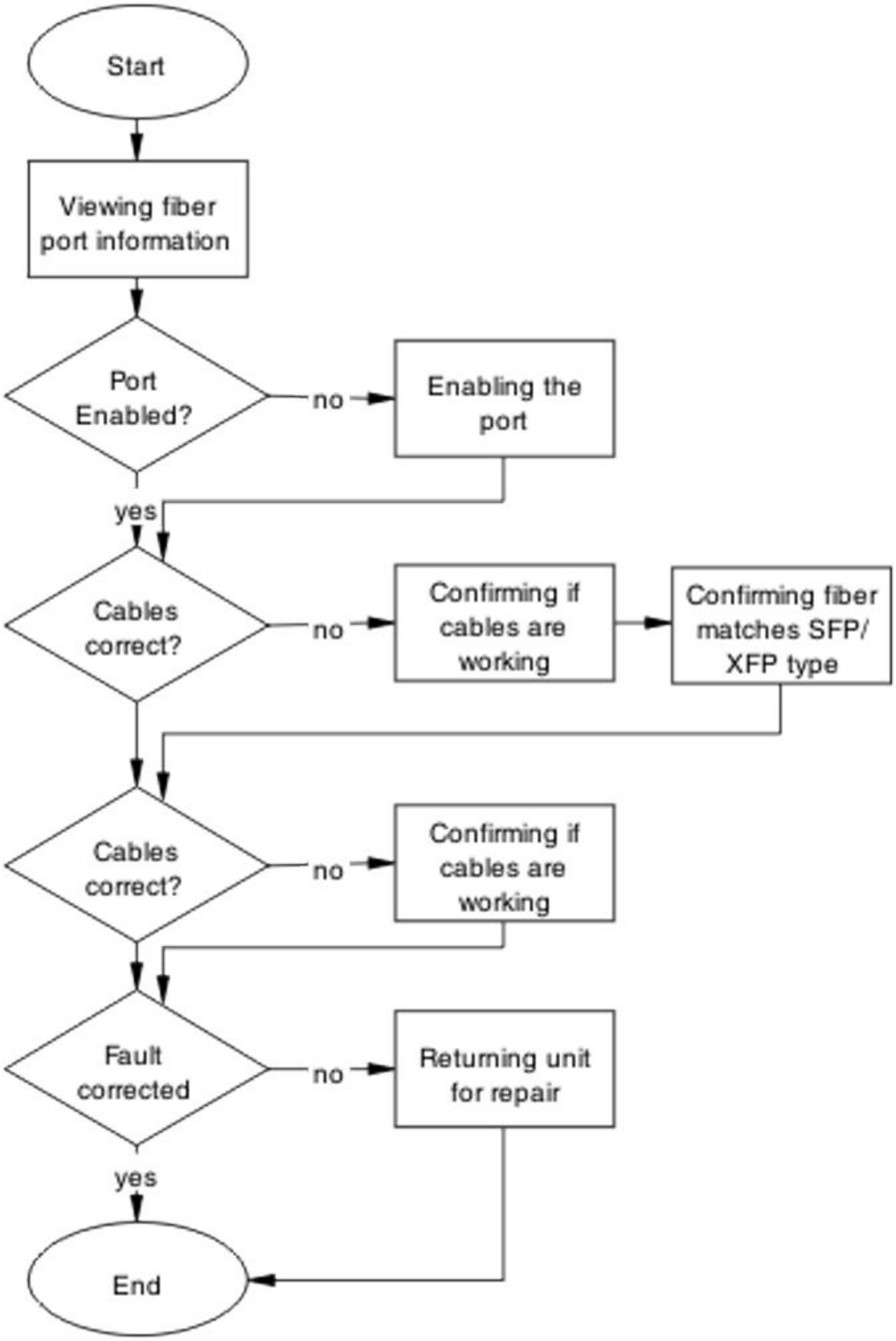

Start
Viewing fiber port information
Port Enabled?
no
Enabling the port
yes
Cables correct?
no
Confirming if cables are working
Confirming fiber matches SFP/ XFP type
Cables correct?
no
Confirming if cables are working
Fault corrected
no
Returning unit for repair
yes
End

Figure 31: Check fiber port

Result

Navigation

- Viewing fiber port information on page 95
- Enabling the port on page 95
- Confirming if cables are working on page 95
- Confirming fiber matches SFP/XFP type on page 96
- Returning the unit for repair on page 96

Viewing fiber port information

About this task

Review the port information to ensure the port is enabled.

Procedure

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

Enabling the port

About this task

Ensure the port on the Avaya Ethernet Routing Switch 4000 Series device is enabled.

Procedure

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

Confirming if cables are working

About this task

Confirm that the cables are working on the port.

Procedure

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

Confirming fiber matches SFP/XFP type

About this task

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

Procedure

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

Returning the unit for repair

About this task

Return unit to Avaya for repair.

Contact Avaya for return instructions and RMA information.

Replace a unit in the stack

Remove the defective unit and insert the replacement.

⚠ **Caution:**

Due to physical handling of the device and your physical proximity to electrical equipment, review and adhere to all safety instructions and literature included with the device and in *Installation Job Aid (English) for Avaya Ethernet Routing Switch 4000 Series*, NN47205-303.

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

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

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

Important:

If the stack is only of two switches, the remaining switch enters Stack Forced Mode if that feature is enabled. Review the section Stack Forced Mode on page 29regarding this feature.

Important:

Different versions of the software and diagnostic images have different behaviors for the software and diagnostic images. Review the section Diagnostic Auto Unit Replacement (DAUR) on page 42 regarding DAUR and its expected results.

Task flow: Replace a unit in the stack

About this task

The following task flow assists you to replace one of the Avaya Ethernet Routing Switch 4000 Series devices in a stack. This is only appropriate if old software is used or AAUR is disabled. If AAUR is available (and it is turned on by default in such cases), then the procedures to verify software are not required.

Procedure

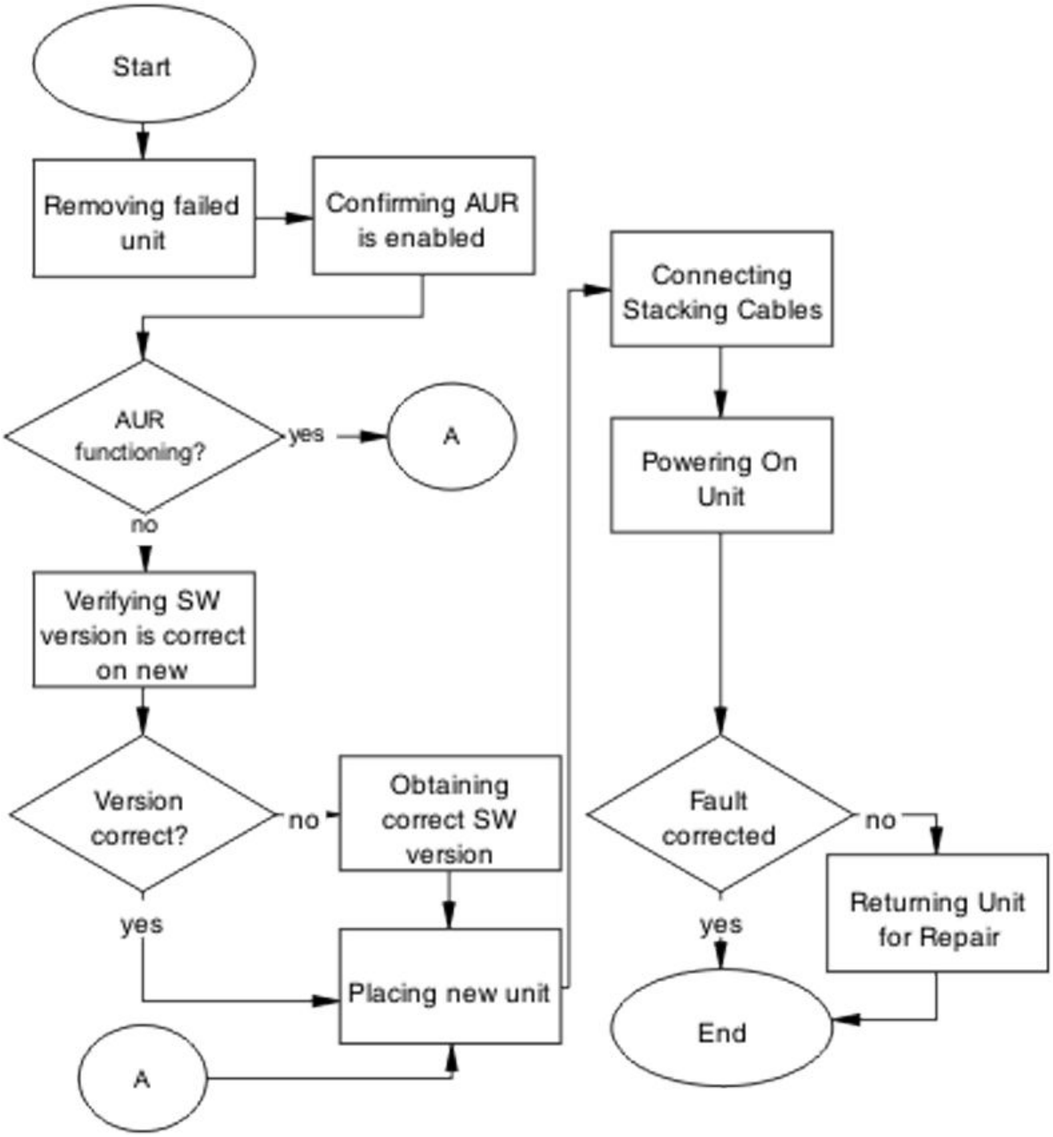

Start
Removing failed unit
Confirming AUR is enabled
AUR functioning?
yes
A
no
Verifying SW version is correct on new
Version correct?
no
Obtaining correct SW version
yes
Placing new unit
A
Connecting Stacking Cables
Powering On Unit
Fault corrected
no
Returning Unit for Repair
yes
End

Figure 32: Replace a unit in the stack

Result

Navigation

- Removing a failed unit on page 99
- Confirming AUR is enabled on page 99
- Verifying the software version is correct on the new device on page 100
- Obtaining the correct software version on page 100
- Placing a new unit on page 101

- Connecting stacking cables on page 101
- Powering on the unit on page 101
- Returning the unit for repair on page 102

Removing a failed unit

About this task

Remove the failed unit from the stack.

Procedure

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

Confirming AUR is enabled

About this task

Confirm AUR is enabled in the stack.

Procedure

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

Removing a MAC address from the AUR cache

About this task

Remove the MAC address for a non-operational stack switch from the AUR address cache.

Procedure

1. Enter the `show stack auto-unit-replacement mac-addresses` command to display the MAC addresses and operational status for all switches within a stack.
2. Enter the `stack auto-unit-replacement remove-mac-address unit <1-8>` command to remove the MAC address.
3. Enter the `show stack auto-unit-replacement mac-addresses` command to verify that the MAC address for the non-operational switch is removed from the AUR address cache.

Verifying the software version is correct on the new device

About this task

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

Procedure

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

Obtaining the correct software version

About this task

Obtain and install the correct software version.

⚠ **Caution:**

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

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

Procedure

See *Release Notes for Avaya Ethernet Routing Switch 4000 Series*, NN47205-400 for software installation information.

Placing a new unit

About this task

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

Place the device in the stack in accordance with procedures outlined in *Installing Avaya Ethernet Routing Switch 4000 Series*, NN47205-300.

Connecting stacking cables

About this task

Reconnect the stacking cables to correctly stack the device.

Procedure

1. Review the stacking section in *Installing Avaya Ethernet Routing Switch 4000 Series*, NN47205-300 for cabling details.
2. Connect the cables in accordance with physical stack requirements.

Powering on the unit

About this task

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

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

Procedure

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

Returning the unit for repair

About this task

Return the unit to Avaya for repair.

Contact Avaya for return instructions and RMA information.

Chapter 9: Troubleshooting ADAC

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

ADAC clarifications

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

You must manually create a VLAN to be used as the voice VLAN and then set this VLAN as the ADAC voice VLAN using the command **adac voice-vlan x**.

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 cannot detect phones using the LLDP detection mechanism.

Work flow: Troubleshooting ADAC

About this task

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

Procedure

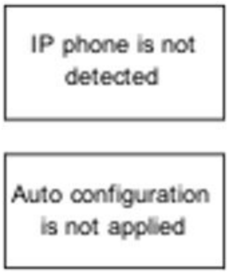


Figure 33: Troubleshooting ADAC

IP phone is not detected

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

Work flow: IP phone not detected

About this task

The following work flow assists you to resolve detection issues.

Procedure

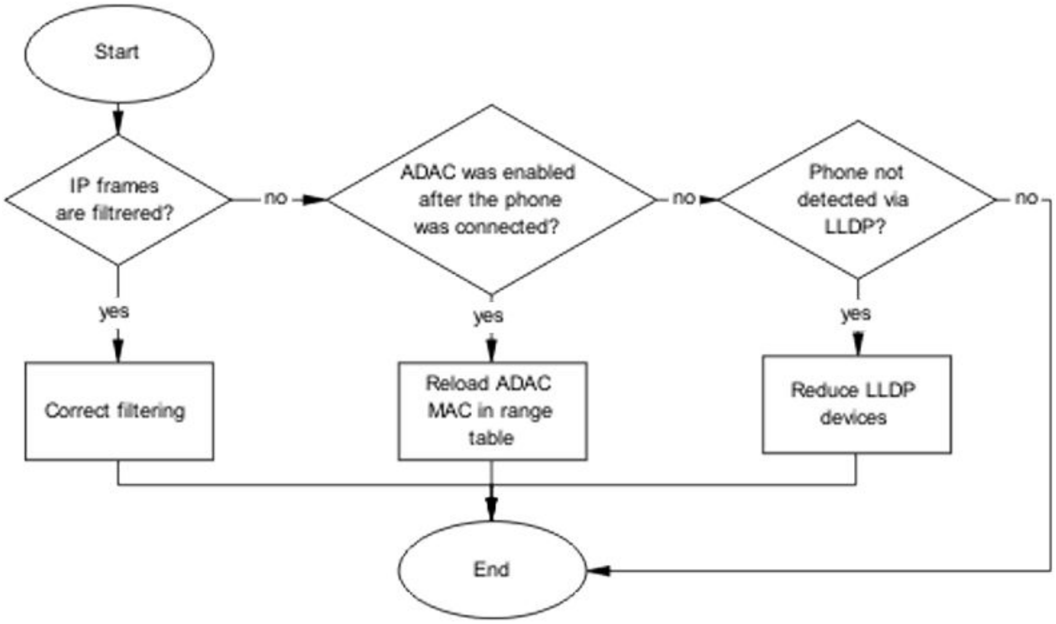

Start
IP frames are filtrered?
no
yes
Correct filtering
ADAC was enabled after the phone was connected?
no
yes
Reload ADAC MAC in range table
Phone not detected via LLDP?
no
yes
Reduce LLDP devices
End

Figure 34: IP phone not detected

Correct filtering

Configure the VLAN filtering to allow ADAC.

Task flow: Correct filtering

About this task

The following task flow assists you to correct the filtering.

Procedure

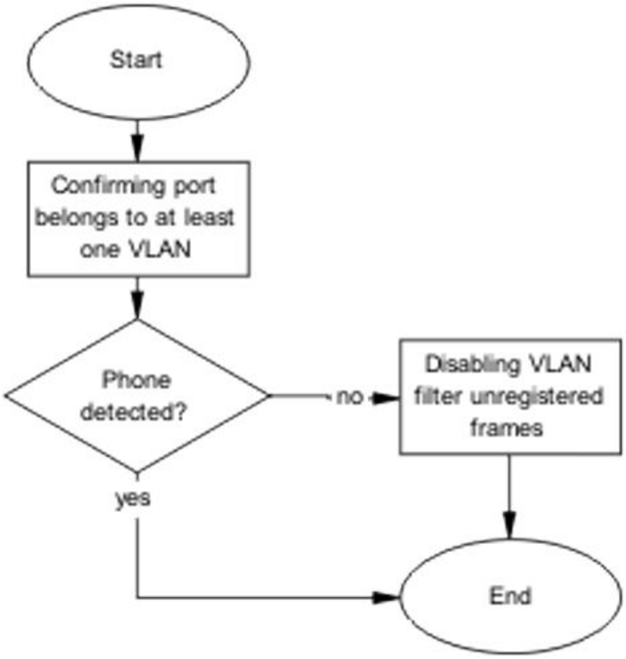

Start
Confirming port belongs to at least one VLAN
Phone detected?
no
Disabling VLAN filter unregistered frames
yes
End

Figure 35: Correct filtering

Confirming port belongs to at least one VLAN

About this task

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

Procedure

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

About this task

Change the unregistered frames filtering of the VLAN.

Procedure

1. Use the **`vlan ports <port> filter-unregistered-frames disable`** 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

About this task

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

Procedure

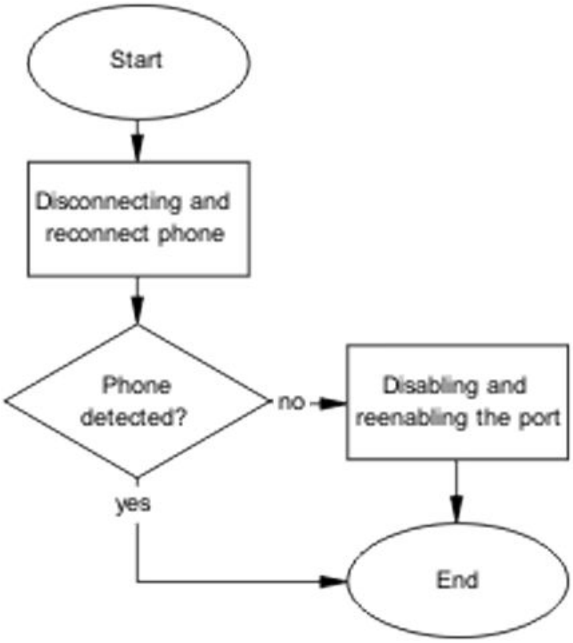

Start
Disconnecting and reconnect phone
Phone detected?
no
Disabling and reenabling the port
yes
End

Figure 36: Reload ADAC MAC in range table

Disconnecting and reconnecting phone

About this task

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

Procedure

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

Disabling and enabling the port

About this task

Disable ADAC on the port and then enable it to detect the phone. After disabling and re-enabling the port administratively, the MAC addresses already learned on the respective port are aged out.

Procedure

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

About this task

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

Procedure

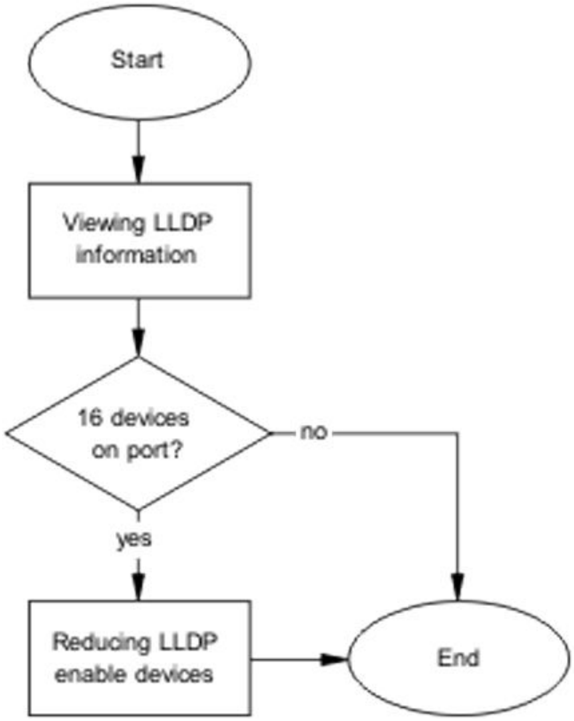


Figure 37: Reduce LLDP devices

Viewing LLDP information

About this task

Display the LLDP devices that are connected to a port.

Procedure

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

About this task

Reduce the number of LLDP devices on the system.

Procedure

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

About this task

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

Procedure

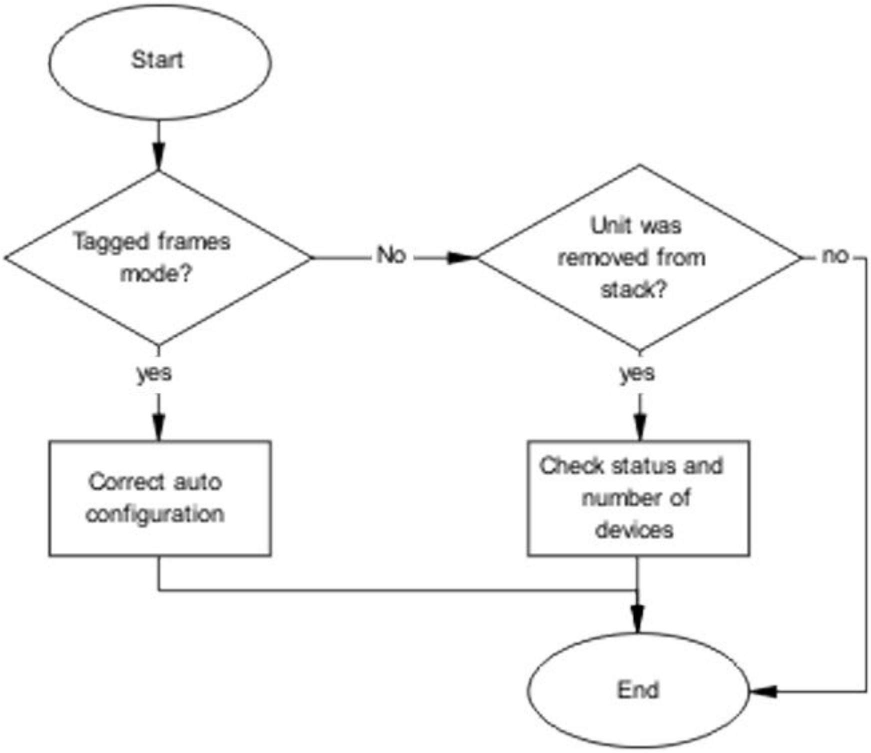

Start
Tagged frames mode?
No
yes
Unit was removed from stack?
no
yes
Correct auto configuration
Check status and number of devices
End

Figure 38: 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

About this task

The following task flow assists you to correct auto configuration.

Procedure

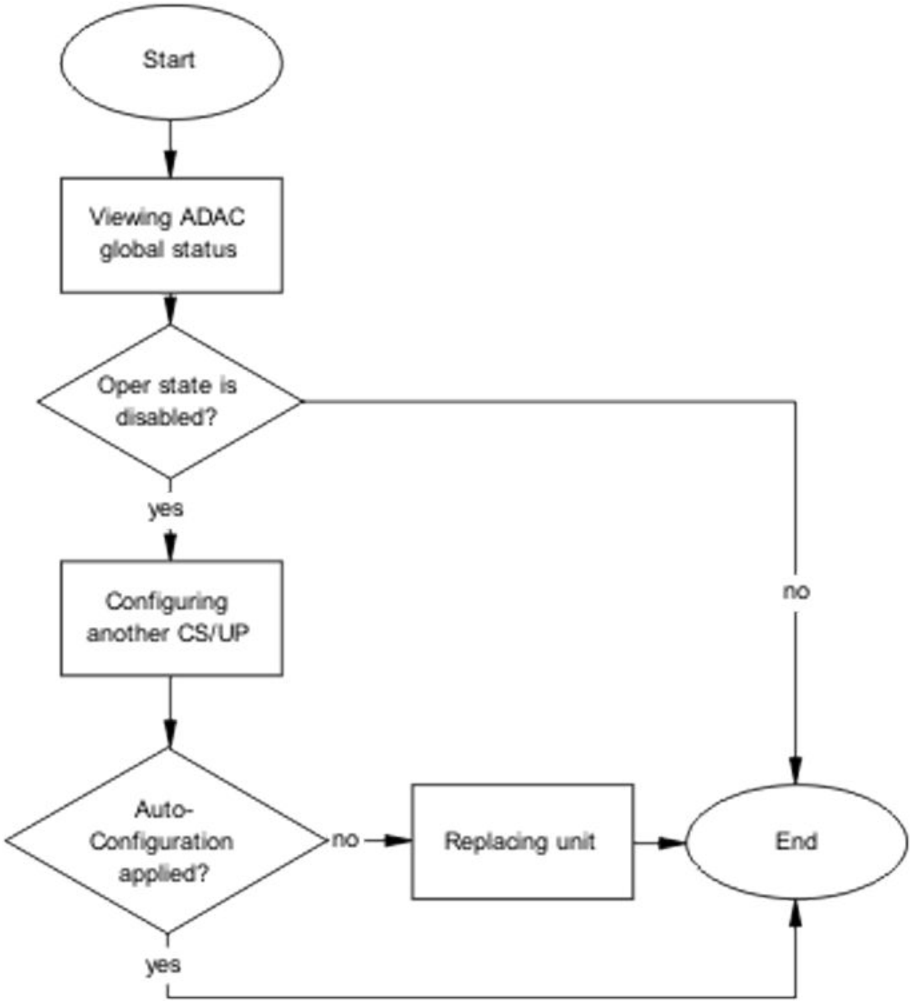

Start
Viewing ADAC global status
Oper state is disabled?
yes
no
Configuring another CS/UP
Auto-Configuration applied?
no
Replacing unit
End
yes

Figure 39: Correct auto configuration

Viewing ADAC global status

About this task

Display the global status of ADAC.

Procedure

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

About this task

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

Procedure

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

Replacing the unit

About this task

Replace the unit to replicate configuration if AUR is enabled.

Procedure

1. Follow the replacement guidelines in Configuring Systems on Avaya Ethernet Routing Switch 4000 Series, NN47205-500.
2. Refer to the unit replacement section in the Troubleshooting Hardware section of this document.

Check status and number of devices

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

Task flow: Check status and number of devices

About this task

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

Procedure

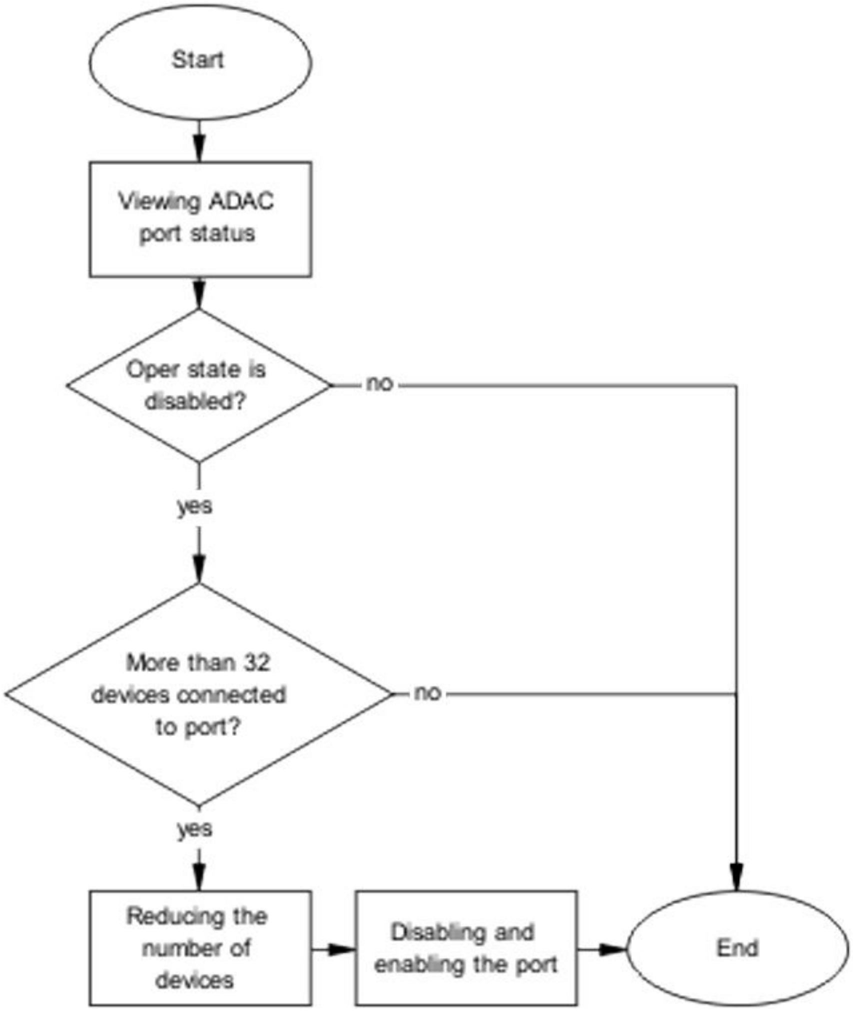

Start
Viewing ADAC port status
Oper state is disabled?
no
yes
More than 32 devices connected to port?
no
yes
Reducing the number of devices
Disabling and enabling the port
End

Figure 40: Check status and number of devices

Viewing ADAC port status

About this task

Display the status of ADAC on the port.

Procedure

1. Use the **`show adac in <port>`** command to display the ADAC information for the port.

2. Note if the oper state is disabled and the number of devices connected.

Reducing the number of devices

About this task

Reduce the number of LLDP devices on the system.

Procedure

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

Disabling and enabling the port

About this task

Administratively disable and enable the port to initialize the configuration.

Procedure

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

Chapter 10: Troubleshooting authentication

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

Work flow: Troubleshooting authentication

About this task

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

Procedure

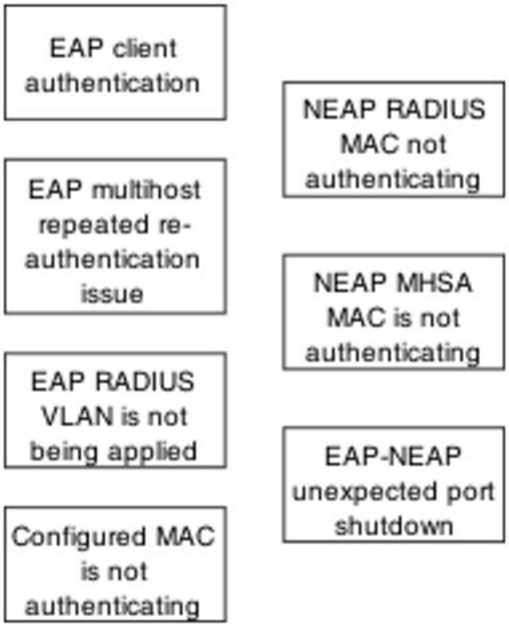

EAP client authentication
EAP multihost repeated re-authentication issue
EAP RADIUS VLAN is not being applied
Configured MAC is not authenticating
NEAP RADIUS MAC not authenticating
NEAP MHSA MAC is not authenticating
EAP-NEAP unexpected port shutdown

Figure 41: Troubleshooting authentication

Change RADIUS password

Before you begin

- Enable MS-CHAPv2 encapsulation on the switch in order to change the RADIUS password. Follow the steps in *Configuring Security on Avaya Ethernet Routing Switch 4000 Series* NN47205-505.
- Use this feature in conjunction with password fallback. Follow the steps in *Configuring Systems on Avaya Ethernet Routing Switch 4000 Series* NN47205-500.
- Ensure the RADIUS server is configured properly. Follow the steps in *Configuring Systems on Avaya Ethernet Routing Switch 4000 Series* NN47205-500.

Note:

If the server is not reachable after waiting one to two minutes to try again, use the following command:`radius reachability use-radius`.

About this task

The feature is used to validate RADIUS credentials to allow CLI, Telnet, and SSH access to the switch. Change the password using one of two methods:

- Enter one of the following commands:`cli password serial radius` or `cli password telnet radius`. If the password has expired, you are prompted to enter and confirm a new password.
- Enter new CLI command described in the procedure below.

Procedure

Enter the following CLI command:`cli password change`

Example

```
4826GTS(config)#cli password change
Changing password for user: admin-test
Enter old password              : **********
Enter New Password           : ********
Re-enter New Password      : ********
```

Troubleshooting Fail Open VLAN Continuity Mode

The Fail Open VLAN Continuity Mode feature introduces a new mode of operation for EAP/NEAP clients when the RADIUS server(s) become unreachable.

From Release 5.7 onwards, when Fail Open VLAN Continuity Mode is enabled, if the RADIUS client does not receive any response from RADIUS server, the EAP or Non-EAP MACs are not flushed. The RADIUS reachability is triggered, and the port is moved or copied to Fail Open VLAN.

Display Fail Open VLAN continuity mode status

```
4xxx(config)#show eapol multihost
[...]
Fail Open VLAN:  Enabled
Fail Open VLAN ID:  1000
Fail Open VLAN Continuity Mode:  Enabled
```

Verify functionality

Verify Fail Open VLAN Continuity Mode is functioning properly by using syslog when the RADIUS server is down and a client is reauthenticated.

```
4xxx(config)#show logging sort-reverse
[...]
I    00:00:29:57                   43       No Response from RADIUS Server port 14
mac 1c:bd:b9:e5:cb:42, FOV continuity activated; RADIUS Reachability Triggered
[...]
```

Limitations

It is recommended that the RADIUS Reachability to be set on Use RADIUS.

If Use ICMP is used and the RADIUS server is reachable, but the RADIUS Server Service is stopped, an ICMP packet is sent for every authentication. If there are many EAP/Non-EAP clients in the setup, this flood with ICMP packets can be disturbing. This is a corner case and can be avoided using RADIUS packets for reachability, as recommended, or starting RADIUS Server Service if Use ICMP is used for reachability. This situation appears because with Fail Open Continuity Mode enabled, the RADIUS Reachability mechanism is triggered when no response is received from the RADIUS Server.

EAP client authentication

This section provides troubleshooting guidelines for the EAP and NEAP features on the Avaya Ethernet Routing Switch 4000 Series devices.

Work flow: EAP client is not authenticating

About this task

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

Procedure

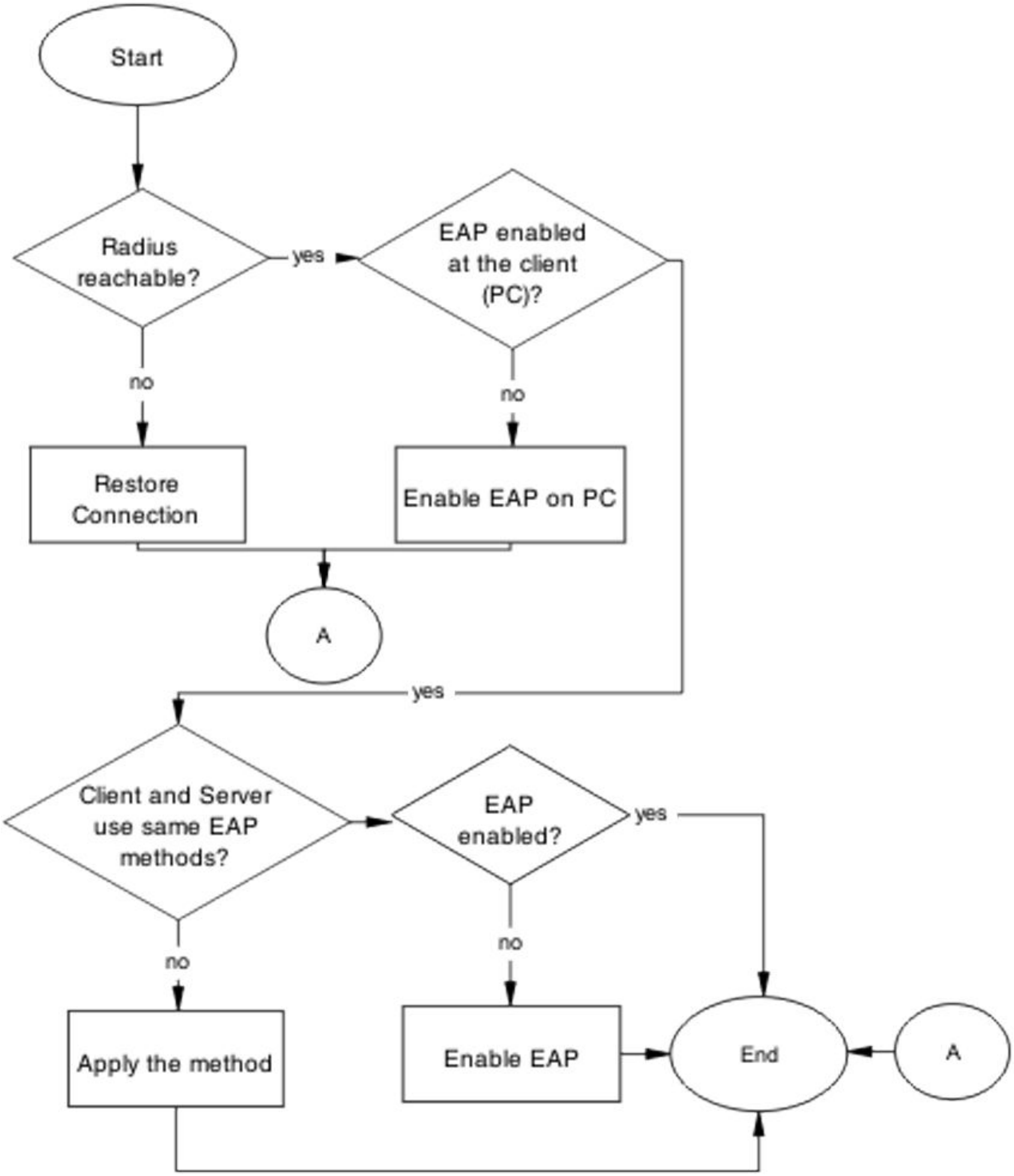


Figure 42: EAP client is not authenticating

Restore RADIUS connection

Ensure that the RADIUS server has connectivity to the device.

Task flow: Restore RADIUS connection

About this task

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

Procedure

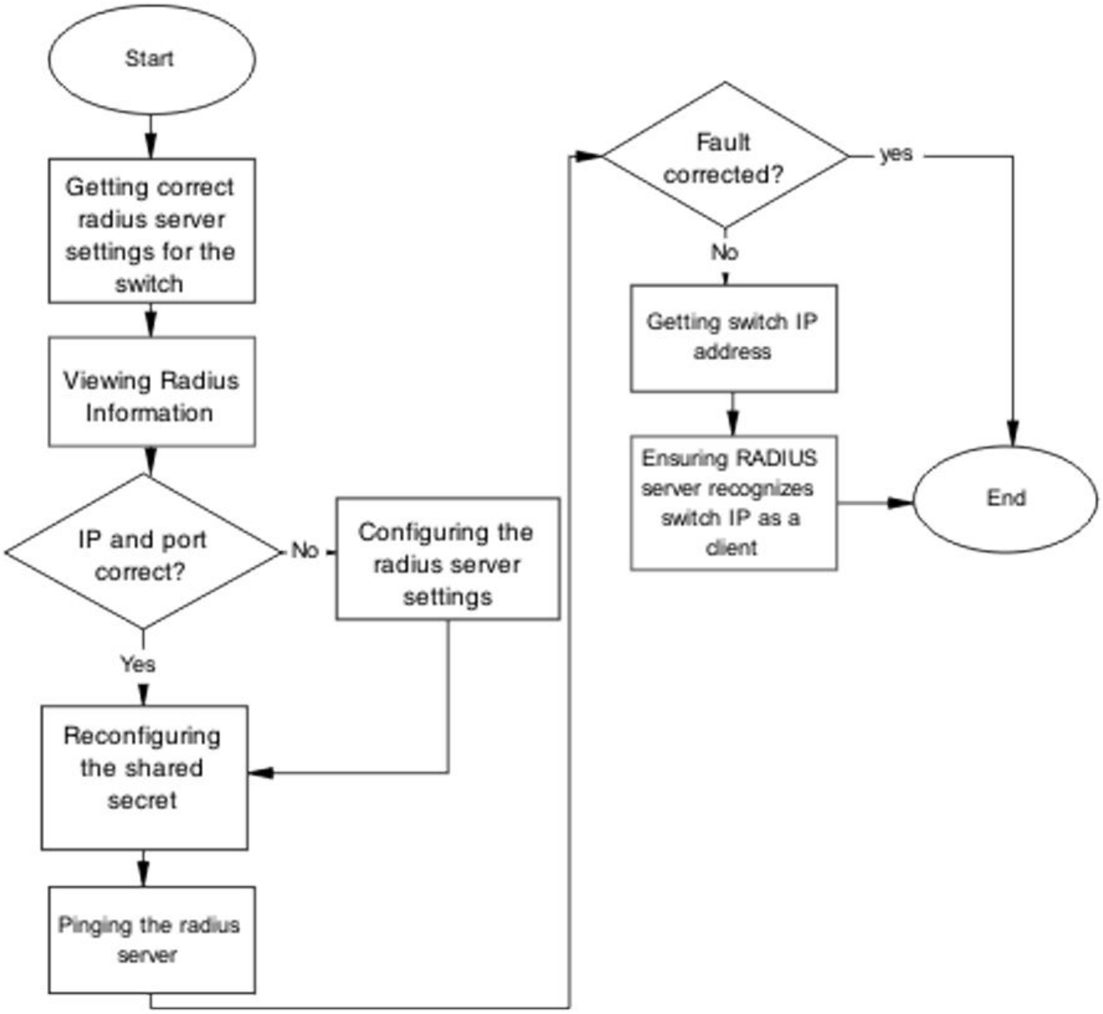

Start
Getting correct radius server settings for the switch
Viewing Radius Information
IP and port correct?
No
Configuring the radius server settings
Yes
Reconfiguring the shared secret
Pinging the radius server
Fault corrected?
yes
No
Getting switch IP address
Ensuring RADIUS server recognizes switch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

Figure 43: Restore RADIUS connection

Getting correct RADIUS server settings for the switch

About this task

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

Procedure

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

Viewing RADIUS information

About this task

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

Procedure

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

Configuring the RADIUS server settings

About this task

The RADIUS server settings must be correct for the network.

Follow vendor documentation to set the RADIUS server settings.

Reconfiguring the shared secret

About this task

Reset the shared secret in case there was any corruption.

Procedure

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

Pinging the RADIUS server

About this task

Ping the RADIUS server to ensure connection exists.

Procedure

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

Enable EAP on the PC

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

Task flow: Enable EAP on the PC

About this task

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

Procedure

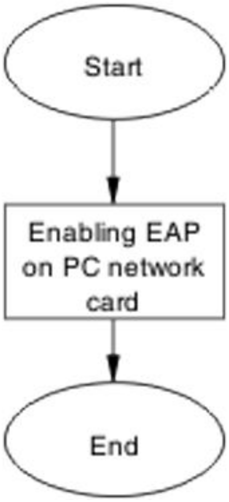


Figure 44: Enable EAP on the PC

Enabling EAP on PC network card

About this task

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

Procedure

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

About this task

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

Procedure

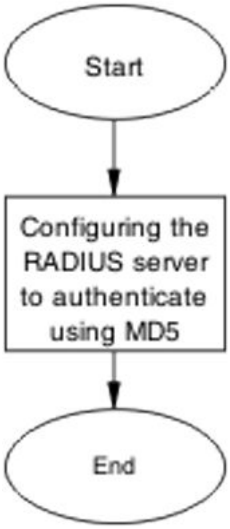


Figure 45: Apply the method

Configuring the RADIUS server

About this task

Configure the RADIUS server to authenticate using MD5.

Procedure

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 4000 Series device.

Task flow: Enable EAP globally

About this task

The following task flow assists you to enable EAP globally on the Avaya Ethernet Routing Switch 4000 Series device.

Procedure

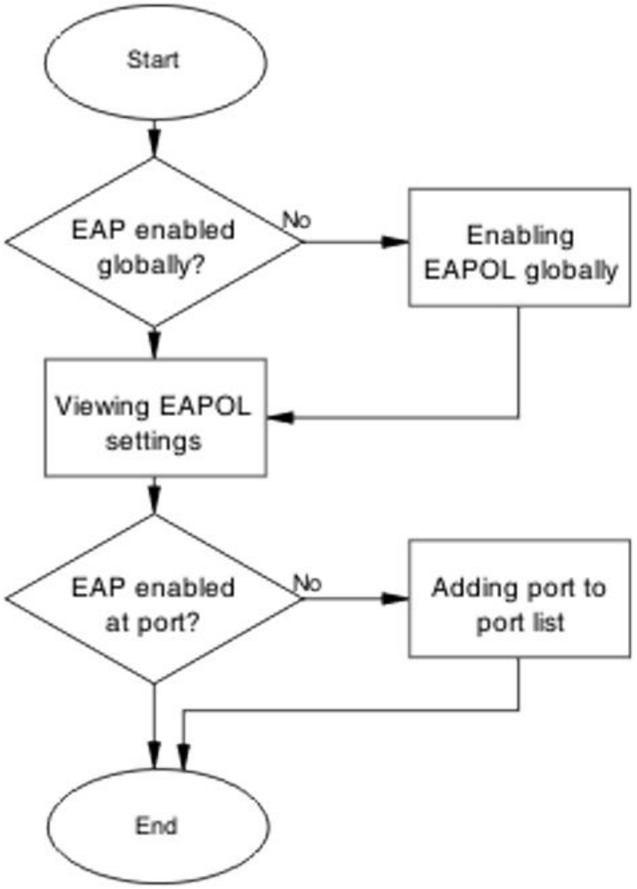


Figure 46: Enable EAP globally

Enabling EAP globally

About this task

Enable EAP globally on the Avaya Ethernet Routing Switch 4000 Series device.

Procedure

1. Use the **`eapol enable`** command to enable EAP globally on the Avaya Ethernet Routing Switch 4000 Series device.
2. Ensure that there are no errors after command execution.

Viewing EAPOL settings

About this task

Review the EAPOL settings to ensure EAP is enabled.

Procedure

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

Setting EAPOL port administrative status to auto

About this task

Set the EAPOL port administrative status to auto.

Procedure

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

EAP multihost repeated re-authentication issue

Eliminate the multiple authentication of users.

Task flow: EAP multihost repeated re-authentication issue

About this task

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

Procedure

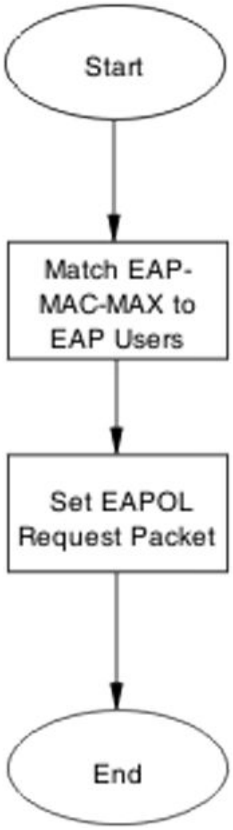


Figure 47: EAP multihost repeated re-authentication issue

Match EAP-MAC-MAX to EAP users

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

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

About this task

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

Procedure

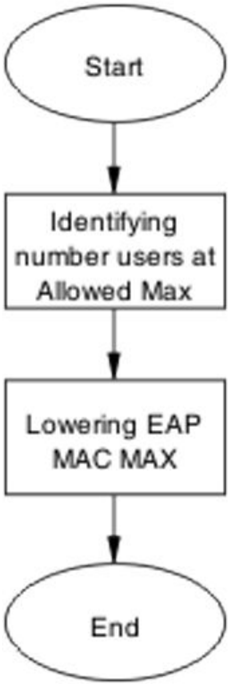


Figure 48: Match EAP-MAC-MAX to EAP users

Identifying number of users at allowed max

About this task

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

Procedure

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

Lowering EAP max MAC

About this task

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

Procedure

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

About this task

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

Procedure

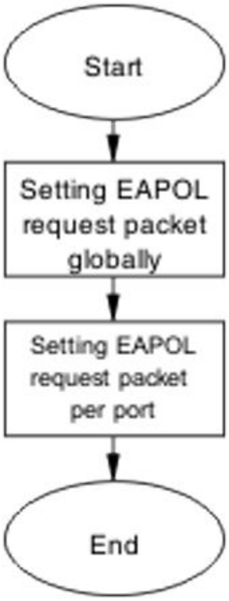

Start
Setting EAPOL request packet globally
Setting EAPOL request packet per port
End

Figure 49: Set EAPOL request packet

Setting EAPOL request packet globally

About this task

Globally change the EAPOL request packet from multicast to unicast.

Procedure

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

Setting EAPOL request packet for a port

About this task

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

Procedure

1. Enter the Interface Configuration mode.

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

EAP RADIUS VLAN is not being applied

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

Work flow: EAP RADIUS VLAN is not being applied

About this task

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

Procedure

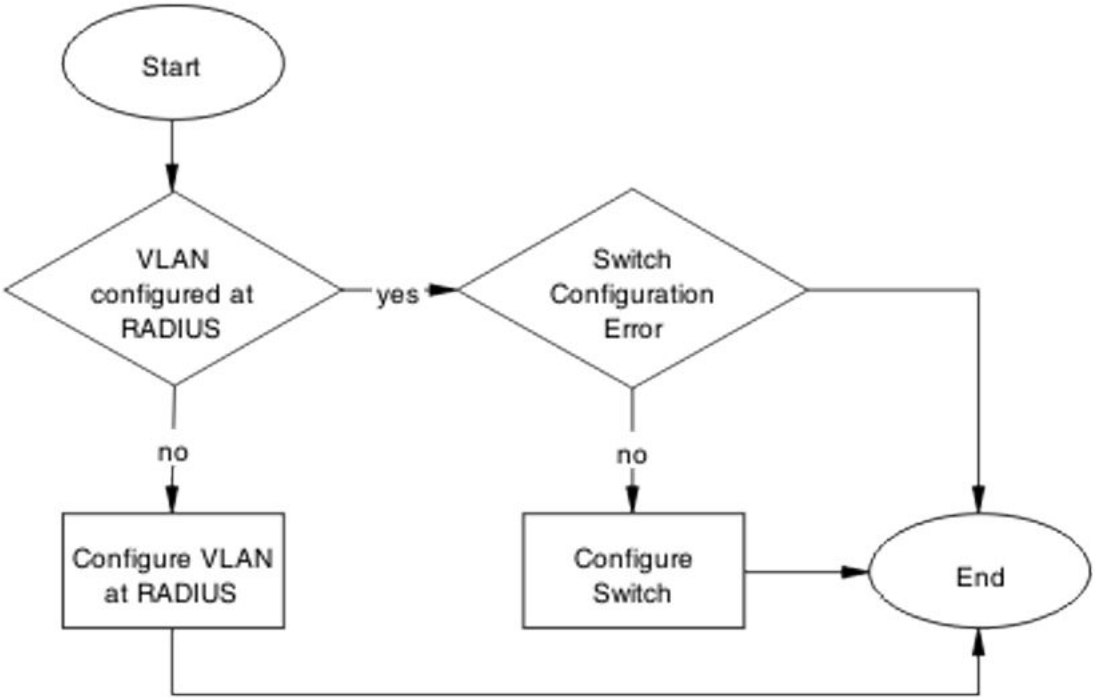


Figure 50: EAP Radius VLAN is not being applied

Configure VLAN at RADIUS

Correct any discrepancies in VLAN information at the RADIUS server.

Task flow: Configure VLAN at RADIUS

About this task

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

Procedure

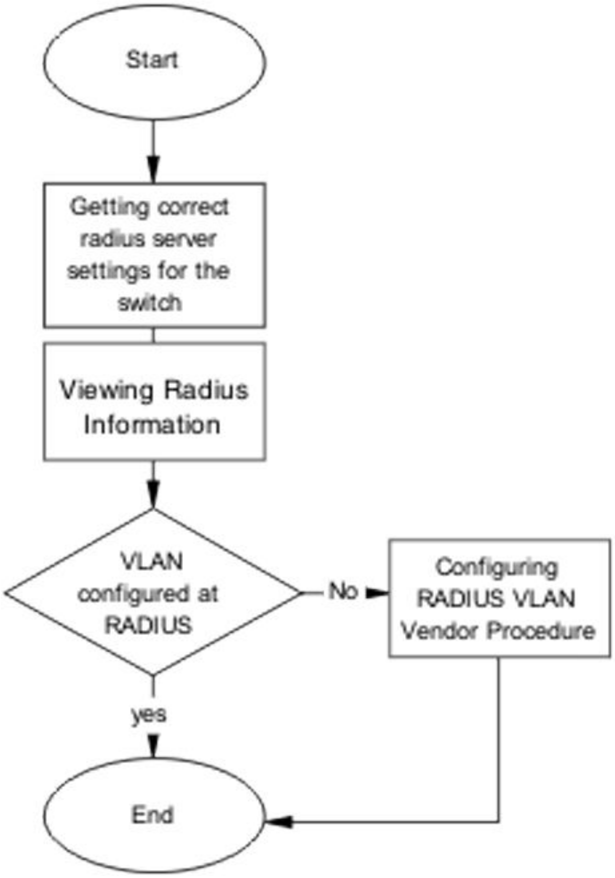

Start
Getting correct radius server settings for the switch
Viewing Radius Information
VLAN configured at RADIUS
No
Configuring RADIUS VLAN Vendor Procedure
yes
End

Figure 51: Configure VLAN at RADIUS

Getting correct RADIUS server settings

About this task

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

Procedure

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

Viewing RADIUS information

About this task

Obtain the RADIUS information to identify its settings.

Use vendor documentation to obtain settings display.

Configuring RADIUS

About this task

Configure the RADIUS server with the correct VLAN information. Use vendor documentation to make the required changes.

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

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

Configure the switch

The VLAN must be configured correctly on the Avaya Ethernet Routing Switch 4000 Series device.

Task flow: Configure switch

About this task

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

Procedure

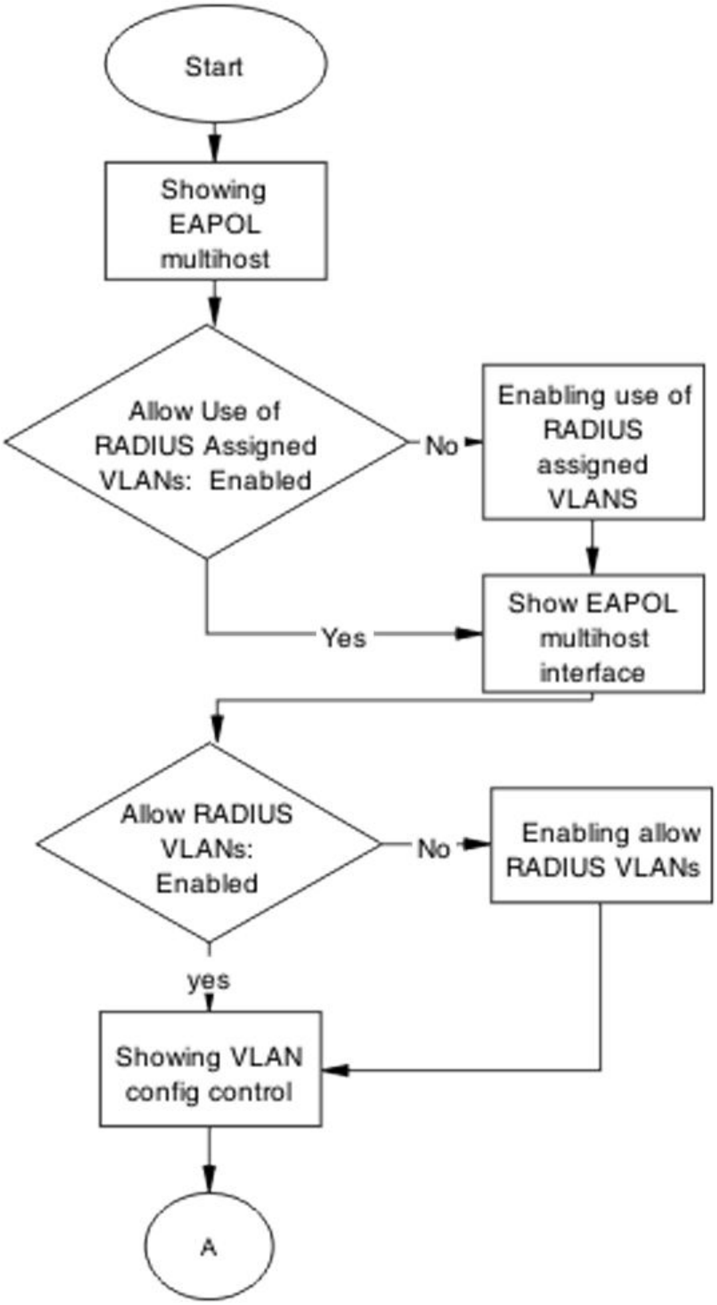

Start
Showing EAPOL multihost
Allow Use of RADIUS Assigned VLANs: Enabled
No
Enabling use of RADIUS assigned VLANS
Yes
Show EAPOL multihost interface
Allow RADIUS VLANs: Enabled
No
Enabling allow RADIUS VLANs
yes
Showing VLAN config control
A

Figure 52: Configure switch task part 1

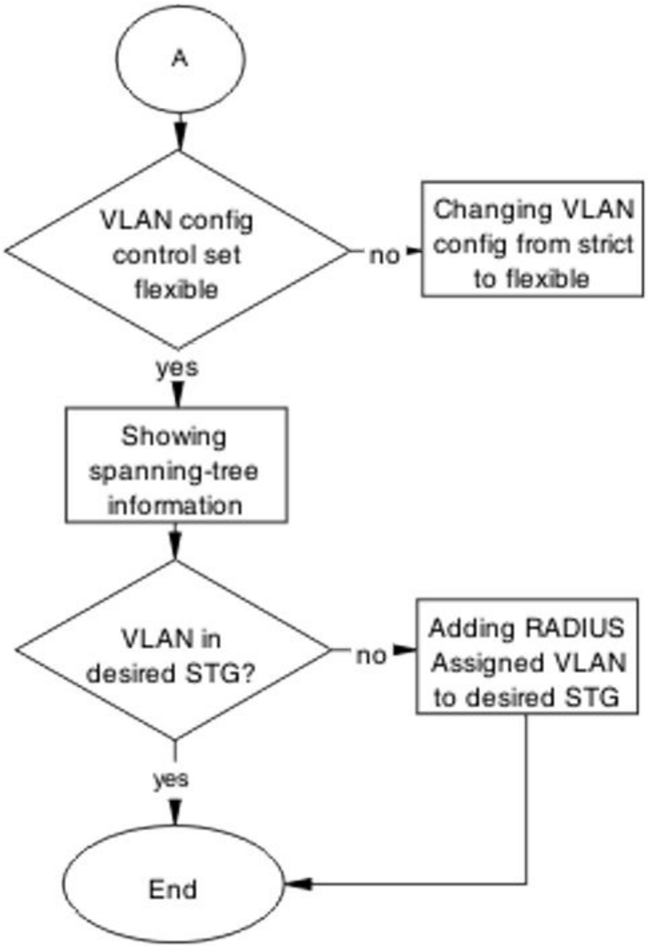

A
VLAN config control set flexible
no
Changing VLAN config from strict to flexible
yes
Showing spanning-tree information
VLAN in desired STG?
no
Adding RADIUS Assigned VLAN to desired STG
yes
End

Figure 53: Configure switch task part 2

Showing EAPOL multihost

About this task

Identify the EAPOL multihost information.

Procedure

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

Enabling use of RADIUS assigned VLANs

About this task

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

Procedure

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

About this task

Display the EAPOL interface information.

Procedure

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

Showing VLAN config control

About this task

Display the VLAN config control information.

Procedure

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

Changing VLAN config from strict to flexible

About this task

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

Procedure

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

Showing spanning tree

About this task

View the VLANs added to the desired STG.

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

Procedure

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

Adding RADIUS assigned VLAN to desired STG

About this task

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

Procedure

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

Configured MAC is not authenticating

Correct a MAC to allow authentication.

Work flow: Configured MAC is not authenticating

About this task

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

Procedure

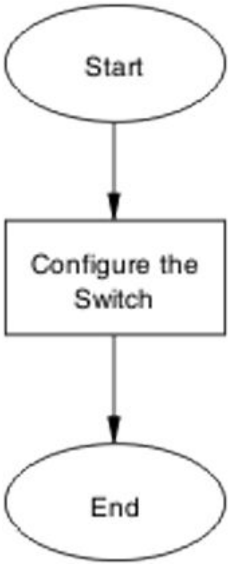


Figure 54: Configured MAC is not authenticating

Configure the switch

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

Task flow: Configure the switch

About this task

The following task flows assist you to ensure that the MAC is authenticating on the Avaya Ethernet Routing Switch 4000 Series device.

Procedure

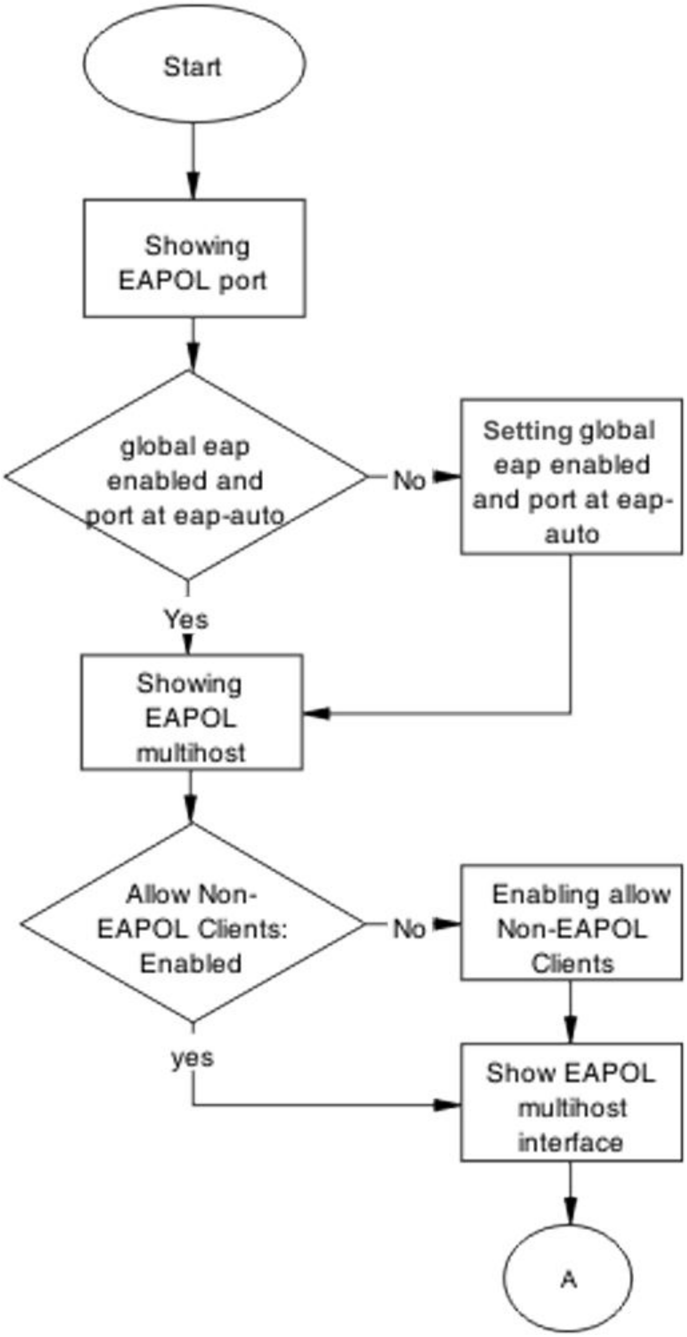

Start
Showing EAPOL port
global eap enabled and port at eap-auto
No
Setting global eap enabled and port at eap-auto
Yes
Showing EAPOL multihost
Allow Non-EAPOL Clients: Enabled
No
Enabling allow Non-EAPOL Clients
yes
Show EAPOL multihost interface
A

Figure 55: Configure the switch part 1

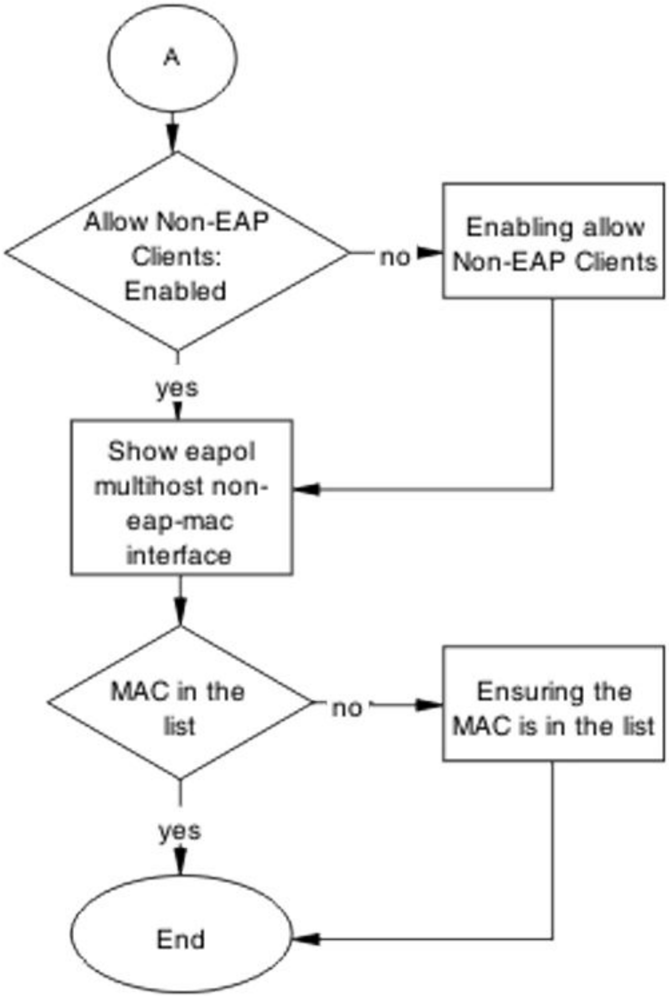

A
Allow Non-EAP Clients: Enabled
no
Enabling allow Non-EAP Clients
yes
Show eapol multihost non-eap-mac interface
MAC in the list
no
Ensuring the MAC is in the list
yes
End

Figure 56: Configure the switch part 2

Showing the EAPOL port

About this task

Display the EAPOL port information

Procedure

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

About this task

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

Procedure

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

Showing EAPOL multihost

About this task

Display the EAPOL multihost information.

Procedure

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

Enabling allow non-EAPOL clients

About this task

Correct the non-EAPOL client attribute.

Procedure

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

About this task

Display the EAPOL multihost interface information.

Procedure

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

About this task

Correct the non-EAP client attribute.

Procedure

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

About this task

Display the EAPOL multihost interface information.

Procedure

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

Ensuring MAC is in the list

About this task

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

Procedure

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

2. Use the `eapol multihost non-eap-mac <port> <H.H.H>` 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

About this task

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

Procedure

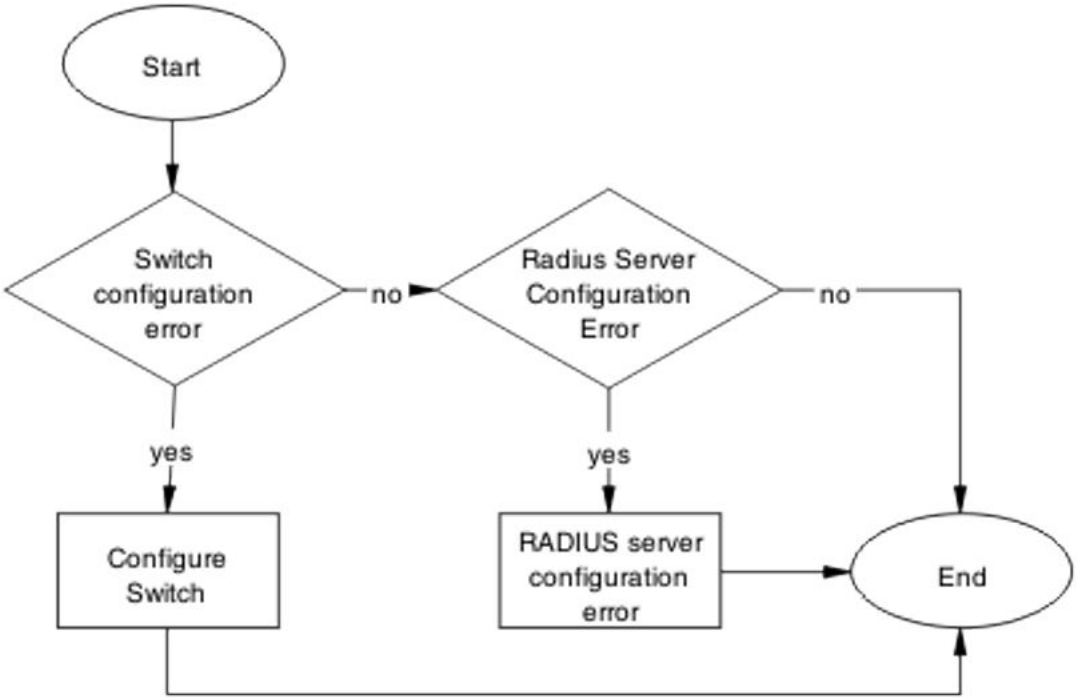

Start
Switch configuration error
no
Radius Server Configuration Error
no
yes
yes
Configure Switch
RADIUS server configuration error
End

Figure 57: NEAP RADIUS MAC not authenticating

Configure switch

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

Task flow: Configure switch

About this task

The following task flows assist you to configure the Avaya Ethernet Routing Switch 4000 Series device to correct the RADIUS MAC issue.

Procedure

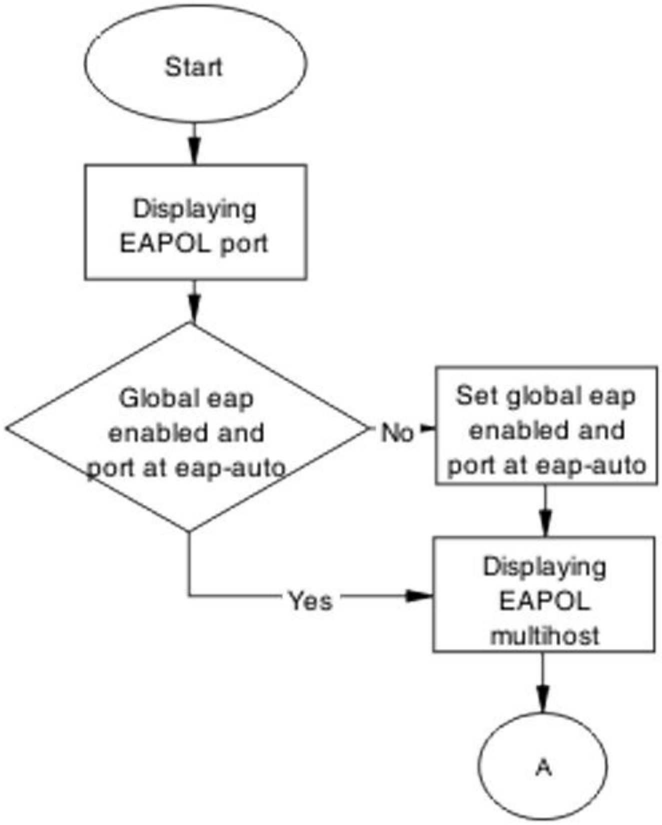

Start
Displaying EAPOL port
Global eap enabled and port at eap-auto
No
Set global eap enabled and port at eap-auto
Yes
Displaying EAPOL multihost
A

Figure 58: Configure switch part 1

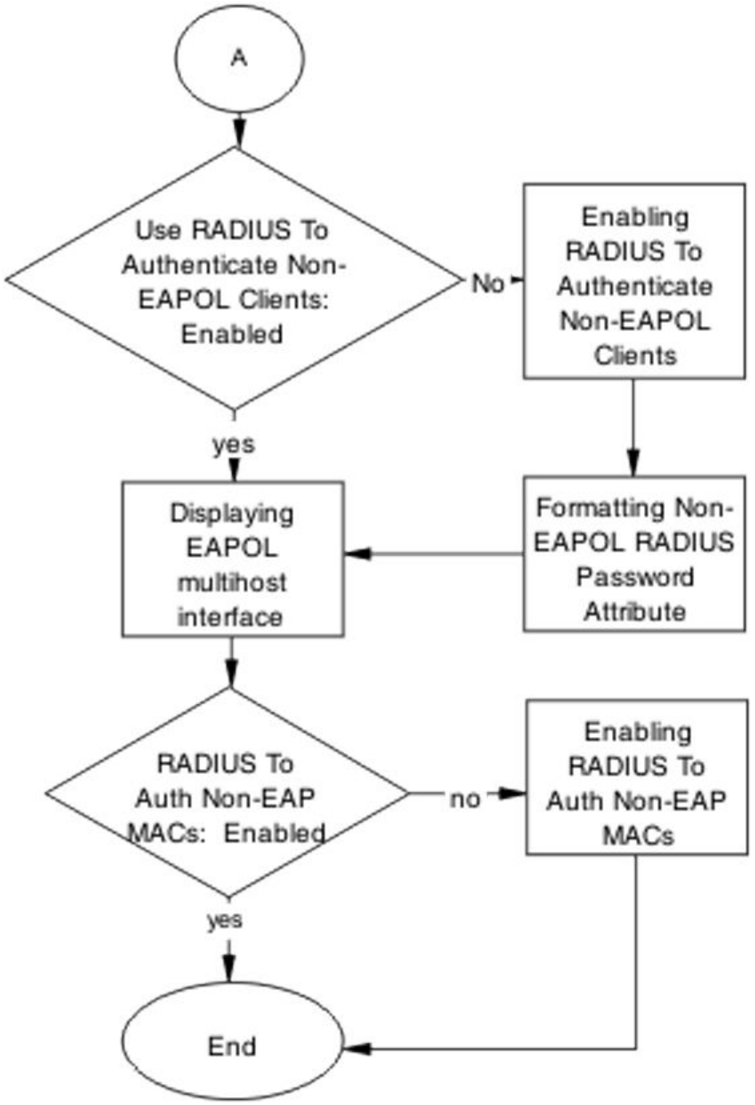

A
Use RADIUS To Authenticate Non-EAPOL Clients: Enabled
No
Enabling RADIUS To Authenticate Non-EAPOL Clients
yes
Displaying EAPOL multihost interface
Formatting Non-EAPOL RADIUS Password Attribute
RADIUS To Auth Non-EAP MACs: Enabled
no
Enabling RADIUS To Auth Non-EAP MACs
yes
End

Figure 59: Configure switch part 2

Result

Navigation

- Displaying the EAPOL port on page 149
- Setting global eap enabled and port at eap-auto on page 149
- Displaying EAPOL multihost on page 149
- Enabling RADIUS to authenticate non-EAPOL clients on page 150
- Formatting non-EAPOL RADIUS password attribute on page 150
- Displaying EAPOL multihost interface on page 150
- Enabling RADIUS To Auth non-EAP MACs on page 150

Displaying the EAPOL port

About this task

Review the EAPOL port information.

Procedure

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

Setting global eap enabled and port at eap-auto

About this task

Make required changes to enable EAP globally and to set the port status to auto.

Procedure

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

About this task

Review the EAPOL multihost information.

Procedure

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

Enabling RADIUS to authenticate non-EAPOL clients

About this task

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

Apply changes to the RADIUS server using vendor documentation.

Formatting non-EAPOL RADIUS password attribute

About this task

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

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

Displaying EAPOL multihost interface

About this task

Review the EAPOL multihost information.

Procedure

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

About this task

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

Apply any changes to the RADIUS server using vendor documentation.

RADIUS server configuration error

The RADIUS server requires that the correct MAC address and password for the Avaya Ethernet Routing Switch 4000 Series device be configured.

Task flow: RADIUS server configuration error

About this task

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

Procedure

Start
Configuring MAC and password on RADIUS server
End

Figure 60: RADIUS server configuration error

Configuring MAC and password on RADIUS server

About this task

The RADIUS server requires that the MAC and password for the Avaya Ethernet Routing Switch 4000 Series device be correct. If it is incorrect, the Avaya Ethernet Routing Switch 4000 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

About this task

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

Procedure

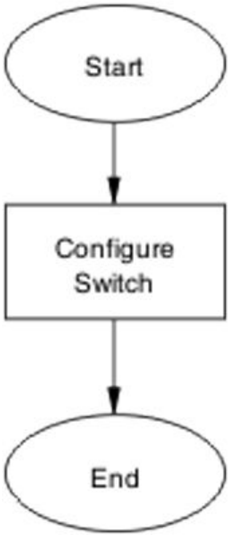


Figure 61: Non-EAP MHSA MAC is not authenticating

Configure switch

Configure the switch to enable MHSA.

Task flow: Configure switch

About this task

The following task flows assist you to enable MHSA on the Avaya Ethernet Routing Switch 4000 Series device.

Procedure

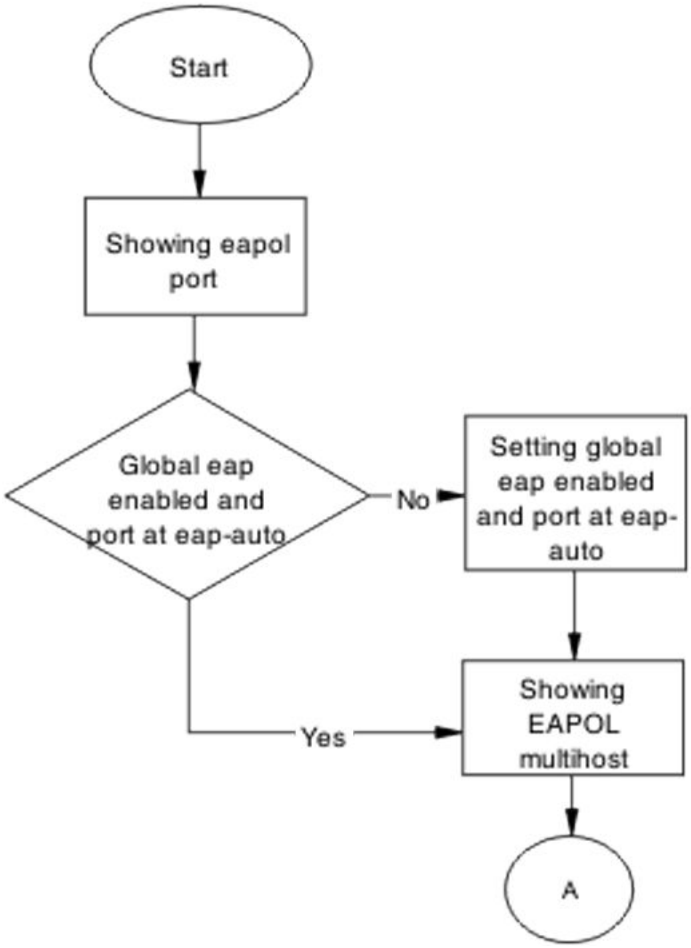

Start
Showing eapol port
Global eap enabled and port at eap-auto
No
Setting global eap enabled and port at eap-auto
Yes
Showing EAPOL multihost
A

Figure 62: Configure switch part 1

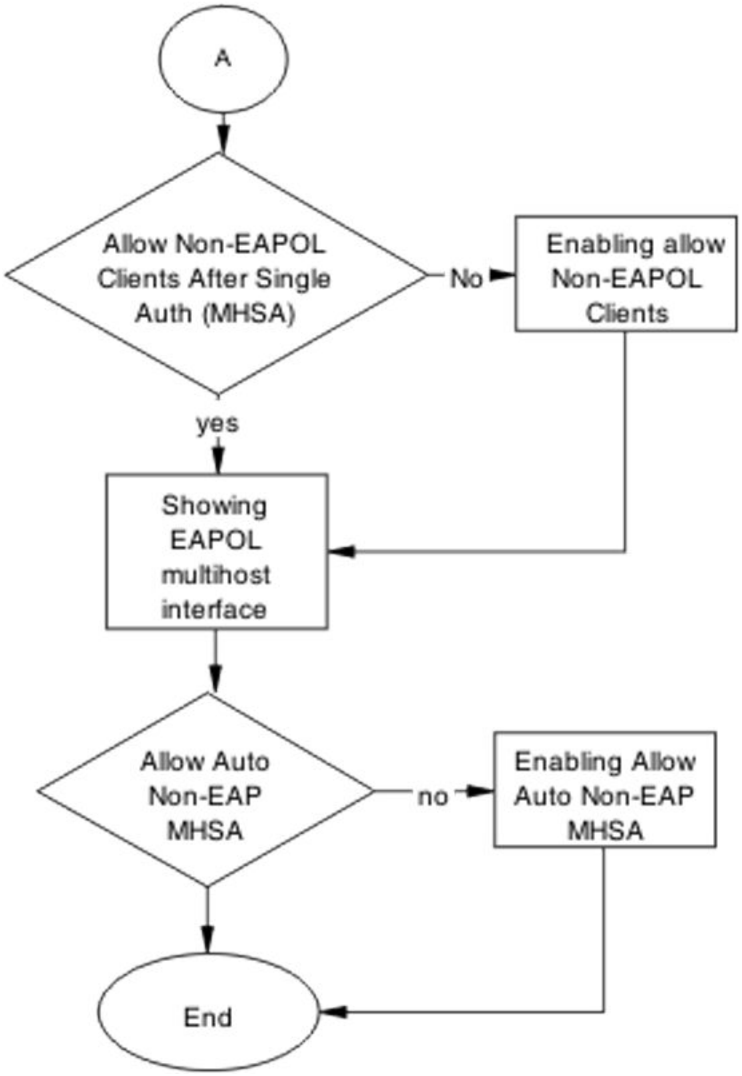

A
Allow Non-EAPOL Clients After Single Auth (MHSA)
No
Enabling allow Non-EAPOL Clients
yes
Showing EAPOL multihost interface
Allow Auto Non-EAP MHSA
no
Enabling Allow Auto Non-EAP MHSA
End

Figure 63: Configure switch part 2

Showing EAPOL port

About this task

Review the EAPOL port information.

Procedure

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

Setting global EAP enabled and port at eap-auto

About this task

Make the required changes to ensure that EAP is enabled globally and that the port status is set to auto.

Procedure

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

Showing EAPOL multihost

About this task

Review the EAPOL multihost information.

Procedure

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

Formatting non-EAPOL RADIUS password attribute

About this task

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

About this task

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

Apply changes to the RADIUS server using vendor documentation.

Showing EAPOL multihost interface

About this task

Review the EAPOL multihost information.

Procedure

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

About this task

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

Apply changes to the RADIUS server using vendor documentation.

EAP–non-EAP unexpected port shutdown

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

Work flow: EAP–non-EAP unexpected port shutdown

About this task

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

Procedure

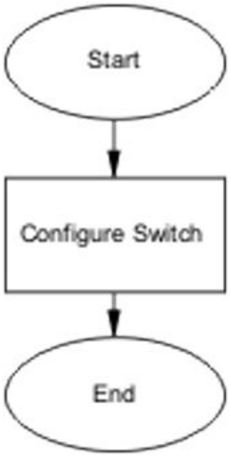


Figure 64: EAP-NEAP unexpected port shutdown

Configure switch

Configure ports to allow more unauthorized clients.

Task flow: Configure switch

About this task

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

Procedure

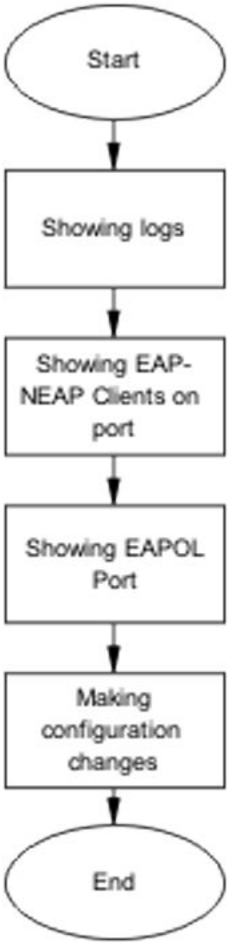

Start
Showing logs
Showing EAP-NEAP Clients on port
Showing EAPOL Port
Making configuration changes
End

Figure 65: Configure switch

Showing logs

About this task

Display log information to provide additional information.

Procedure

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

Showing EAP–non-EAP clients on port

About this task

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

Procedure

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

Showing EAPOL port information

About this task

Display EAPOL port information for additional information.

Procedure

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

Making changes

About this task

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

Procedure

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

Non-EAP is not a member of a VLAN

If no VLAN is pre-existing on the port, authentication cannot happen because a RADIUS request has not been sent by the switch. NEAP authentication will not occur for a port with no VLAN, but an EAP client on a similarly configured port can be authenticated.

Limitations

- Verify a port with Non-EAP authentication is assigned to at least one VLAN at all times.
- If Non-EAP is not member of a VLAN:
    - Enable Non-EAP authentication on a port that isn't in a VLAN.
    - The port already has Non-EAP authentication enabled, but you want to remove it from all vlans.

    In both cases, the port is added to vlan 1.
- The feature will not take action if vlan 1 and the previous vlan are in different stages.

Non-EAP freeform password

When you configure the RADIUS password, you can also use the following commands:

- `show eapol multihost non-eap-pwd-fmt`—this command shows the password fields and padding.
- `show eapol multihost non-eap-pwd-fmt key`—this command prints the key used. The password is printed in cleartext only when password security is not enabled. Otherwise, the password is printed as a string of asterisks.

Using Trace

Use trace to observe the status of a software module at a given time. Follow the steps in *Configuring System Monitoring on Avaya Ethernet Routing Switch 4000 Series* NN47205-502.

Note:

If the trace level is set to a higher level (3 or above), a large number of messages are displayed in CLI. This may cause subsequent commands to not be displayed properly, and the actions of those commands may be executed with a slight delay.

Block subsequent MAC authentication

This feature enhancement gives the administrator the option of either using the current implementation or a separate option that blocks subsequent MAC authentications if the RADIUS-assigned VLAN is different than the first authorized station VLAN.

Follow the steps in *Configuring Security on Avaya Ethernet Routing Switch 4000 Series* NN47205-505 to configure this feature.

Display Block subsequent MAC authentication status

Display Block subsequent MAC authentication status (global and per interface):

```
4xxx(config)#show eapol multihost [interface X]
[...]
Block Different RAV Auth:  Enabled
[...]
```

Verify Block subsequent MAC authentication

Verify Block subsequent MAC authentication works by using syslog after a client with invalid/missing vlan attribute tries to authenticate, or usage of radius assigned vlan is disabled.

```
4xxx(config)#show logging sort-reverse
[...]
I    00:00:56:59     89       EAP Mac AuthFail - Port: 14 MAC: 1c:bd:b9:e5:cb:42
I    00:00:56:59     88       Trap:  bsnEapAccessViolation
I    00:00:56:59     87       EAP Client blocked (Block Subsequent MAC
Authentication): EAP Use Rav Not enabled
[...]
```

EAP and Non-EAP separation

Use the EAP/ NEAP separation command to disable EAP clients without disabling NEAP clients.

Follow the steps in *Configuring Security on Avaya Ethernet Routing Switch 4000 Series* NN47205-505 to configure the command.

Display EAP protocol status

Display EAP protocol status on the interface:

```
4xxx(config)#show eapol multihost interface X
[...]
EAPOL Protocol:  Disabled
[…]
```

OR

```
4xxx(config)#show eapol multihost interface X
[...]
```

```
EAPOL Protocol:  Enable
[…]
```

802.3at LLDP based discovery

ERS 4000 Series PWR+ devices support the IEEE 802.3at-2009 standard for an Link Layer Discovery Protocol (LLDP) configuration with a Powered Device (PD). The LLDP support for PoE+ is added by extending the existing standard LLDP DOT3 Power via MDI TLV defined by the IEEE 802.1ab with the new fields and values defined in the IEEE 802.3at-2009 standard. Information for power negotiation between PD and Power Sourcing Equipment (PSE) is described in Power via MDI, which is the optional TLV.

The PoE PD communicates through the Data Link Layer (DLL) classification instead of Physical Layer (high power mode). Hence, the PoE+ capable devices can deliver power greater than 15.4 watts for each port.

You can configure the PoE PD detection type (802.3at or 802.3at_and_legacy) to support a DLL classification for communication. The Data Link Layer classification provides finer power resolution and the ability for PSE and PD to participate in dynamic power allocation. The allocated power to the PD can change one or more times during PD operation.

Before you begin

Follow the steps in *Configuring Systems on Avaya Ethernet Routing Switch 4000 Series* NN47205-500.

Procedure

1. Check the LLDPDUs are enabled for transmission and reception on the PoE+ enabled port:

   ```
   show lldp [port <portlist> | all][local-sys-data {dot1 | dot3 | detail |
   med }]
   ```

2. Check the LLDP DOT3 Power-via-MDI TLV is enabled for transmission in LLDPDUs on the PoE+ enabled port:

   ```
   show lldp [port <portlist> | all][local-sys-data {dot1 | dot3 | detail |
   med }][rx-stats] [tx-stats] [pdu-tlv-size] [tx-tlv {dot1 | dot3 | med |
   vendor-specific}]
   ```

3. Display the LLDP DOT3 Power-via-MDI TLV local port data:

   ```
   show lldp [port <portlist> | all][local-sys-data {dot1 | dot3 | detail |
   med }]
   ```

4. Display the LLDP DOT3 Power-via-MDI TLV neighbor data (for example, a PoE+ endpoint device, like an Avaya IP Phone). If a neighbor does not support this extended TLV, the supplementary information is not displayed.

   ```
   show lldp [port <portlist> | all] [neighbor {dot1 | dot3 | detail | med }
   ```

5. Display the PoE+ main status. Check that PD Detect type is 802.3at or 802.3at and Legacy:

   ```
   show poe-main-status
   ```

6. Check the PoE port status. It should deliver power. Note the PoE classification for the endpoint device detected on the port, and the power limit set for the port:

   ```
   show poe-port-status [<portlist>]
   ```

7. Display the port PoE power measurement:

   ```
   show poe-power-measurement
   ```

Example

```
(config)#sho lldp port 7 tx-tlv dot3
-------------------------------------------------------------------------------
                            LLDP port dot3 tlvs
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
Port    MacPhy        MdiPower      Link         MaxFrameSize
      ConfigStatus    Support      Aggregation
-------------------------------------------------------------------------------
7       false         true          false         false
-------------------------------------------------------------------------------
```

```
(config)#sho lldp port 7 tx-tlv dot3
-------------------------------------------------------------------------------
                            LLDP port dot3 tlvs
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
Port    MacPhy        MdiPower      Link         MaxFrameSize
      ConfigStatus    Support      Aggregation
-------------------------------------------------------------------------------
7       false         true          false         false
-------------------------------------------------------------------------------
```

```
(config)#sho lldp port 7 local-sys-data dot3
-------------------------------------------------------------------------------
                      LLDP local-sys-data chassis
-------------------------------------------------------------------------------
-------------------------------------------------------------------------------
        ChassisId: MAC address        84:83:71:0a:f8:00
        SysName:
        SysCap:    rB / B             (Supported/Enabled)
        SysDescr:
Ethernet Routing Switch 4826GTS-PWR+  HW:10       FW:5.6.2.1   SW:v5.7.0.114
-------------------------------------------------------------------------------
                      LLDP local-sys-data port
-------------------------------------------------------------------------------
Port:  7
 Dot3-MAC/PHY Auto-neg: supported/enabled       OperMAUtype:  1000BaseTFD
 PSE MDI power:         supported/enabled       Port class:   PSE
 PSE power pair:        signal/not controllable Power class:  0
   PSE: Type: Type 2 PSE    Source: Primary     Priority: Low
   PSE: PD  requested power:  23.0 Watts
   PSE: PSE allocated power:  23.0 Watts
 LinkAggr: not aggregatable/not aggregated      AggrPortID:   0
                                                MaxFrameSize: 9216
 PMD auto-neg:          10Base(T, TFD), 100Base(TX, TXFD), (FdxA)Pause,
                        1000Base(TFD)
-------------------------------------------------------------------------------
```

```
Sys capability: O-Other; R-Repeater; B-Bridge; W-WLAN accesspoint; r-Router;
T-Telephone; D-DOCSIS cable device; S-Station only.
```

```
(config)#sho lldp port 7 neighbor dot3
--------------------------------------------------------------------------------
                            LLDP neighbor
--------------------------------------------------------------------------------
Port: 7     Index: 4                  Time: 0 days, 00:53:04
        ChassisId: MAC address        00:10:18:82:0b:bd
        PortId:    MAC address        00:10:18:82:0b:bf
 PSE MDI power:         not supported/disabled  Port class:   PD
 PSE power pair:        spare/not controllable  Power class:  4
   PD: Type: Type 2 PD     Source: PSE         Priority: Low
   PD: PD  requested power:  23.0 Watts
   PD: PSE allocated power:  23.0 Watts
--------------------------------------------------------------------------------
Sys capability: O-Other; R-Repeater; B-Bridge; W-WLAN accesspoint; r-Router;
T-Telephone; D-DOCSIS cable device; S-Station only.
Total neighbors: 3
```

```
(config)# show poe-main-status
PoE Main Status - Stand-alone
--------------------------------------------------
Available DTE Power         : 855 Watts
DTE Power Status            : Normal
DTE Power Consumption       : 5 Watts
DTE Power Usage Threshold   : 80 %
PD Detect Type              : 802.3at and Legacy
Power Source Present        : AC Only
Primary Power Status        : Present and operational
Redundant Power Status      : Not Present
IP Phone Priority           : N/A
IP Phone Power Limit        : N/A
```

```
(config)#show poe-port-status 7
      Admin      Current                               Limit
Port  Status     Status             Classification   (Watts)  Priority
----  -------    -----------------   --------------   -------  --------
7     Enable     Delivering Power          4          32       Low
```

```
show poe-power-measurement 21
Port  Volt(V)  Current(mA)   Power(Watt)
----  -------  -----------   ---------------
21    53.7     108           5.800
```

Run scripts

According to Avaya best practices for converged solutions, you can use the scripts to configure the parameters for an Avaya stackable Ethernet Switch. The scripts can be executed in a default or verbose mode. In this release, run scripts are available in non-verbose and verbose mode for IP Office, and verbose mode for Link Layer Discovery Protocol (LLDP) and Auto Detect Auto Configuration (ADAC).

Follow the steps in *Configuring Systems on Avaya Ethernet Routing Switch 4000 Series* NN47205-500.

- Run the scripts on a default configuration, otherwise previous settings may conflict with the script settings and errors may occur.
- Do not run other commands while a script is in progress, especially when the script is run via SNMP (the EDM version), because this will slow down the execution and EDM may time out while waiting for a response.
- When using CLI, the scripts show confirmation messages for the settings that are made.
- If a setting cannot be made, the currently running script stops and an error message is shown.
- The script also logs messages and sends traps to indicate whether it has been successfully executed or an error was encountered. The final configuration can be verified with the ”show running” command.
- Error messages examples:

  -
    ```
    % Error setting VLAN attributes
    % Error setting Switch Management IP and network mask % Error configuring
    802.1AB
    % Error creating Voice VLAN
    % Error setting uplink ports
    % Error enabling IP Routing
    ```

Link-state tracking

Link-state tracking (LST) binds the link state of multiple interfaces. The Link-state tracking feature identifies the upstream and downstream interfaces. The associations between these two interfaces form link-state tracking group.

Follow the steps in *Configuring Systems on Avaya Ethernet Routing Switch 4000 Series* NN47205-500.

Guidelines

Follow these guidelines when using Link-state tracking:

- The maximum number of upstream members is 8.
- The maximum number of downstream members is 384.
- Valid interfaces are ports and trunks (MLT / LAG).
- An interface can belong only to a single link-state tracking group.
- A trunk-member port cannot be added to a link-state tracking group by itself.
- Only enabled MLTs can be tracking group members.
- A trunk which is a tracking group member cannot be disabled.
- Ports with link aggregation enabled cannot be added to a tracking group.
- The user is prevented from enabling link aggregation on a tracking group member port.

- Only LAGs with static trunk ids are valid tracking group members.
- A tracking group member LAG cannot be associated with another LACP key, nor can its key binding be removed.
- A LACP key bound with a tracking group member cannot be associated with another set of ports.
- Operational state for interfaces or tracking groups is not saved in binary / ASCII configuration, they are dynamically determined during switch operation.

Retrieving LST group information

LST group information is accessible through CLI:

```
4526GTS(config)#show link state detail
Link State Group:     1
Status:               Enabled
VLACP Upstream State: Active on Ports : 2,4
                                Trunks : 1
Operational Status:   Up
Upstream Ports:       1(Up)    2(Down)    3(Down)    4(Down)
Upstream Trunks:      1(Down)
Downstream Ports:     11(Up)   12(Down)   13(Down)   14(Up)
Downstream Trunks:    2(Down)
```

Chapter 11: Troubleshooting IPv6

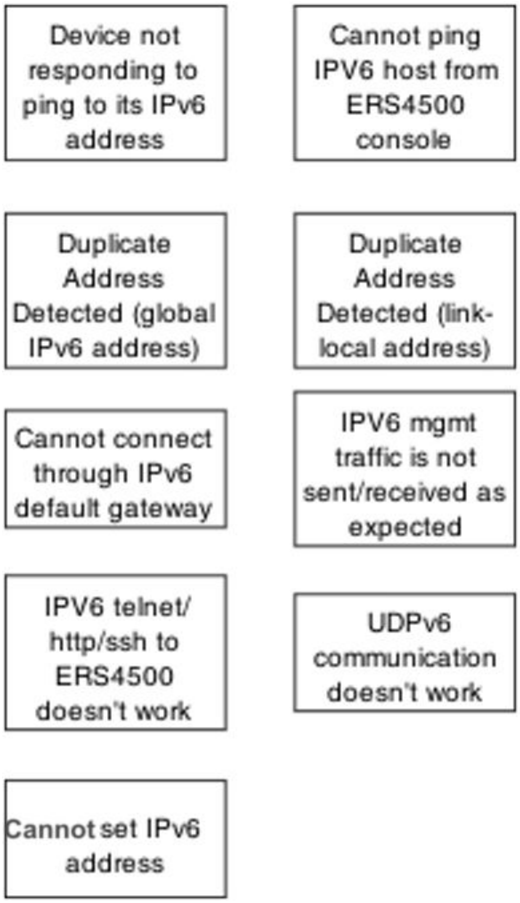
This chapter contains details about how to troubleshoot common IPv6 problems you may encounter.

Troubleshooting IPv6 work flow

About this task

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

Procedure



Device not responding to ping to its IPv6 address
Cannot ping IPV6 host from ERS4500 console
Duplicate Address Detected (global IPv6 address)
Duplicate Address Detected (link-local address)
Cannot connect through IPv6 default gateway
IPV6 mgmt traffic is not sent/received as expected
IPV6 telnet/ http/ssh to ERS4500 doesn't work
UDPv6 communication doesn't work
Cannot set IPv6 address

Device not responding to ping to its IPv6 address

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

Device not responding to ping to its IPv6 address task flow

About this task

Use these task flows to restore the connectivity through IPv6.

Procedure

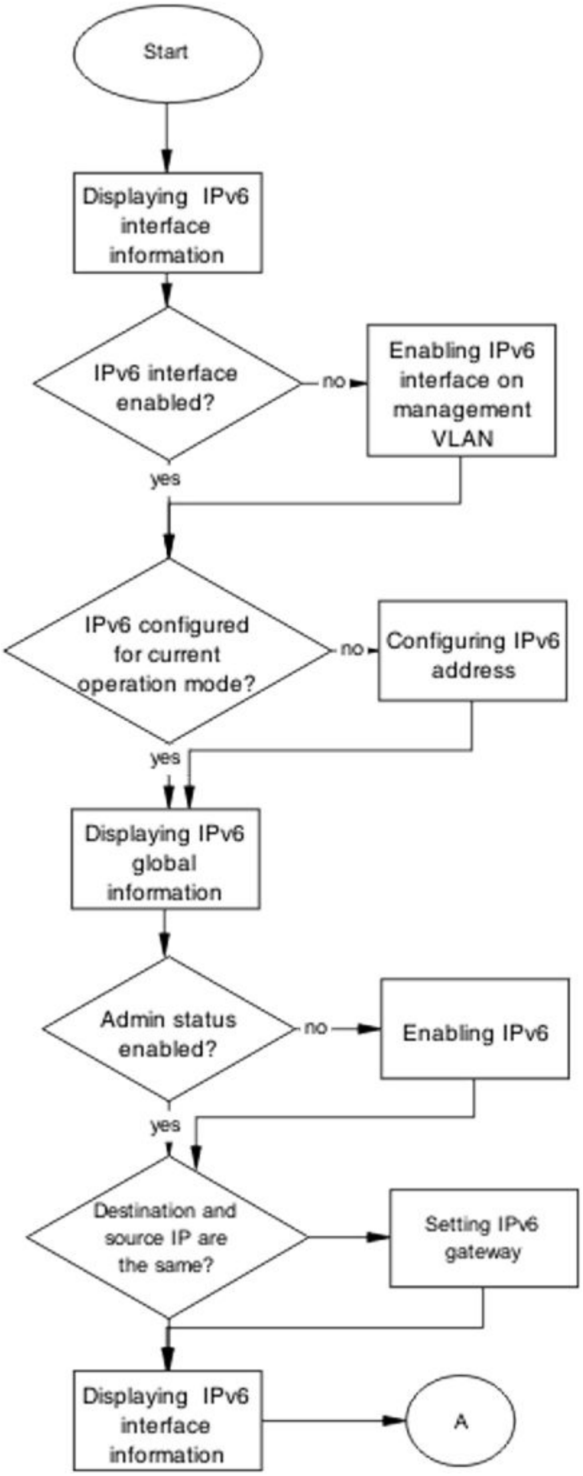

Start
Displaying IPv6 interface information
IPv6 interface enabled?
no
Enabling IPv6 interface on management VLAN
yes
IPv6 configured for current operation mode?
no
Configuring IPv6 address
yes
Displaying IPv6 global information
Admin status enabled?
no
Enabling IPv6
yes
Destination and source IP are the same?
Setting IPv6 gateway
Displaying IPv6 interface information
A

Figure 66: Task flow: Device not responding to ping to its IPv6 address part 1

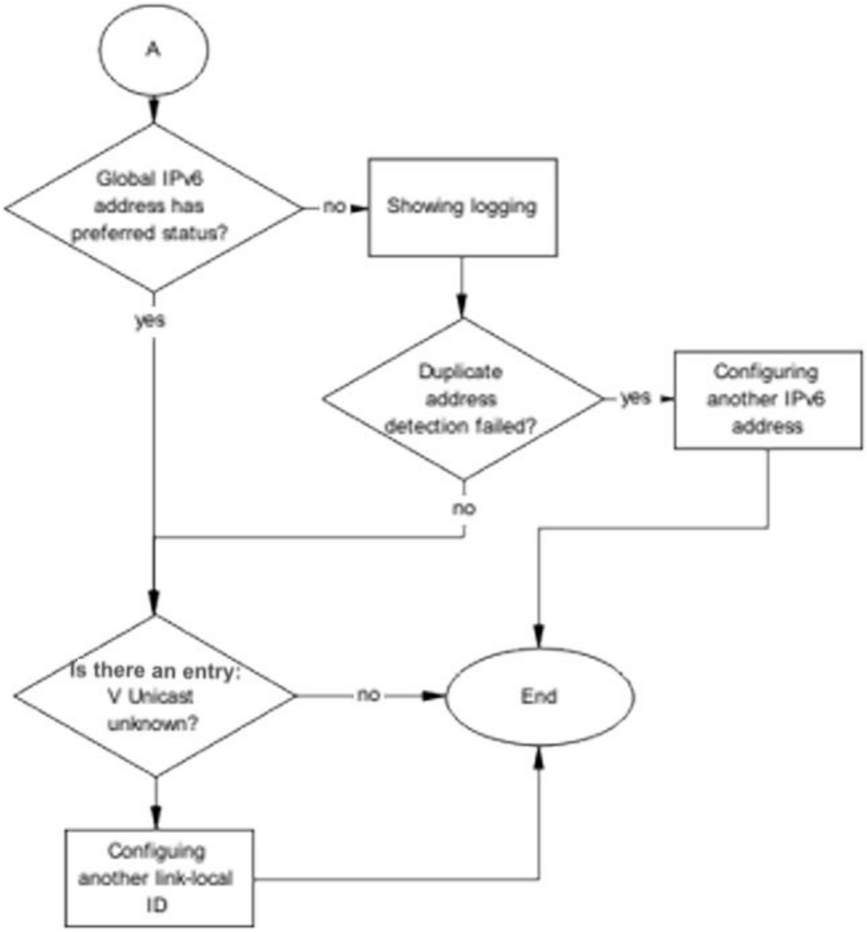

A
Global IPv6 address has preferred status?
no
Showing logging
yes
Duplicate address detection failed?
yes
Configuring another IPv6 address
no
Is there an entry: V Unicast unknown?
no
End
Configuring another link-local ID

Figure 67: Task flow: Device not responding to ping to its IPv6 address part 2

Displaying IPv6 interface information

About this task

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

Procedure

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

Enabling IPv6 interface on management VLAN

About this task

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

Procedure

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

Configuring IPv6 address

About this task

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

Procedure

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

Displaying IPv6 global information

About this task

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

Procedure

1. Use the **`show ipv6 global`** command to display the IPv6 global information.

2. Ensure that admin status is enabled.

Enabling IPv6

About this task

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

Procedure

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

Setting IPv6 gateway

About this task

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

Procedure

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

Displaying IPv6 interface information

About this task

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

Procedure

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

Showing logging

About this task

Use the procedure in this section to display logging information.

Procedure

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

Configuring another IPv6 address

About this task

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

Procedure

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

Configuring another link-local ID

About this task

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

Procedure

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

Cannot ping IPV6 host from device console

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

Cannot ping IPV6 host from device console task flow

About this task

Use this task flow to restore the connectivity through IPv6.

Procedure

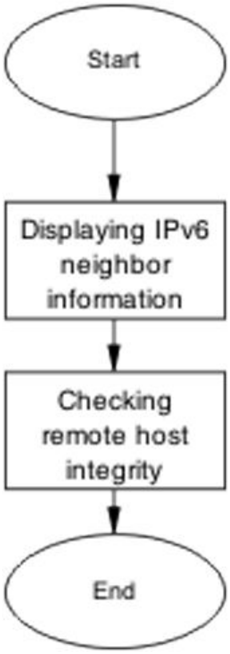

Start
Displaying IPv6 neighbor information
Checking remote host integrity
End

Figure 68: Task flow: Cannot ping IPV6 host from device console

Displaying IPv6 neighbor information

About this task

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

Procedure

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

Checking remote host integrity

About this task

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

Procedure

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

Duplicate address detected (global IPv6 address)

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

Duplicate address detected (global IPv6 address)

About this task

Use this task flow to restore the connectivity through IPv6.

Procedure

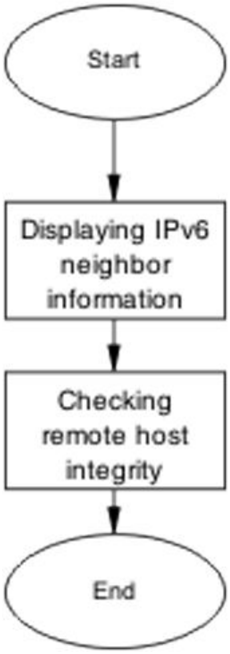

Start
Displaying IPv6 neighbor information
Checking remote host integrity
End

Figure 69: Task flow: Duplicate Address Detected (global IPv6 address)

Displaying IPv6 neighbor information

About this task

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

Procedure

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

Checking remote host integrity

About this task

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

Procedure

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

Duplicate address detected (link-local address)

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

Duplicate address detected (link-local address)

About this task

Use this task flow to restore the connectivity through IPv6.

Procedure

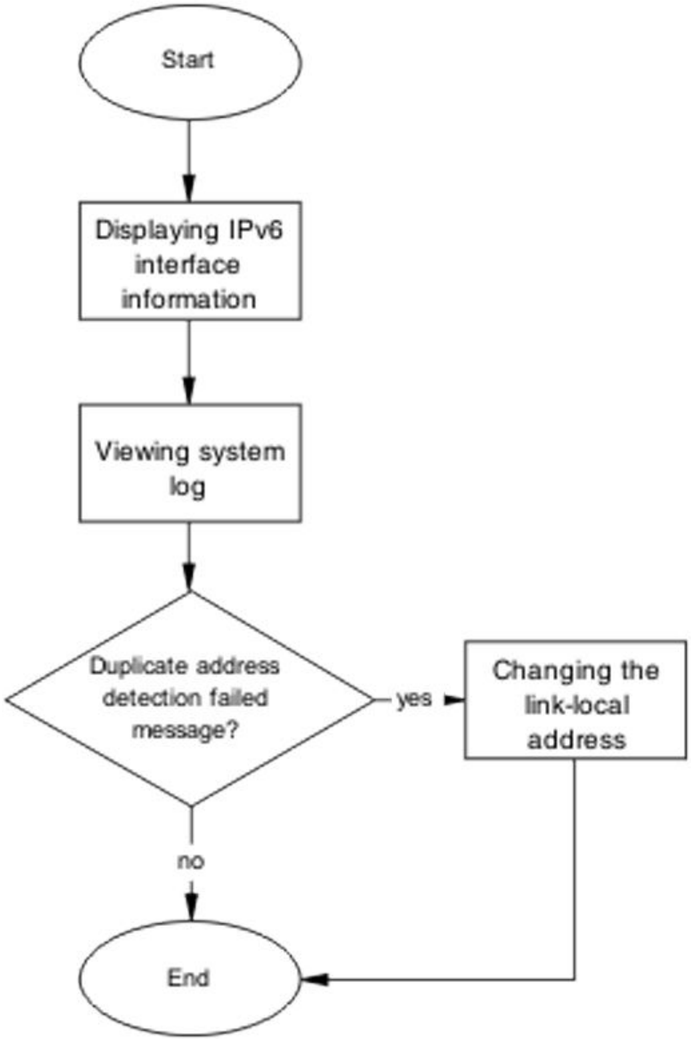

Start
Displaying IPv6 interface information
Viewing system log
Duplicate address detection failed message?
yes
Changing the link-local address
no
End

Figure 70: Task flow: Duplicate Address Detected (link-local address)

Displaying IPv6 interface information

About this task

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

Procedure

1. Use the **`show ipv6 interface <IPv6 address>`** command to display the details of the IPv6 neighbor.

2. Identify if the state is UNKNOWN.

Viewing the system log

About this task

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

Procedure

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

Changing the link-local address

About this task

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

Procedure

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

Cannot connect through IPv6 default gateway

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

Cannot connect through IPv6 default gateway

About this task

Use this task flow to restore the connectivity through IPv6.

Procedure

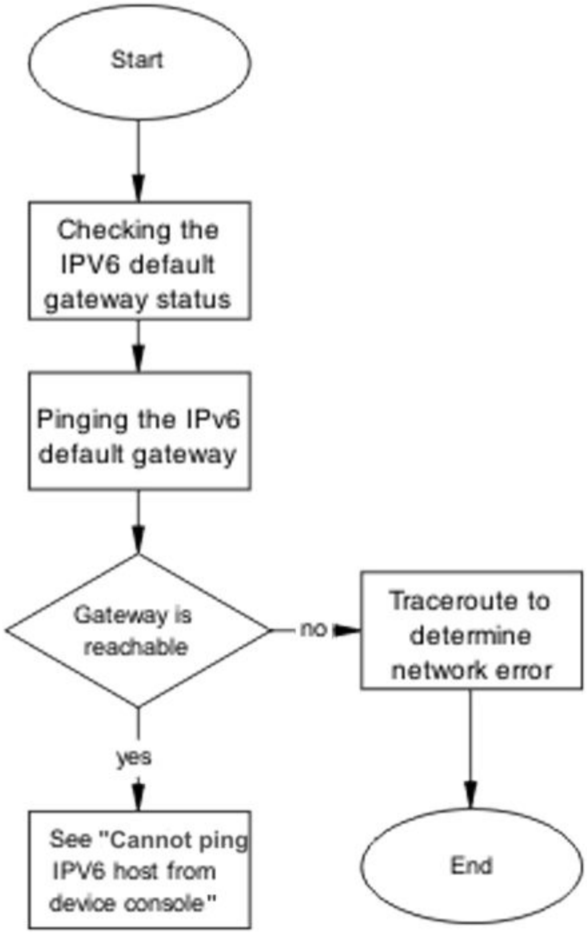

Start
Checking the IPV6 default gateway status
Pinging the IPv6 default gateway
Gateway is reachable
no
Traceroute to determine network error
yes
See "Cannot ping IPV6 host from device console"
End

Figure 71: Task flow: Cannot connect through IPv6 default gateway

Checking the IPV6 default gateway status

About this task

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

Procedure

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

Pinging the IPv6 default gateway

About this task

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

Procedure

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

Using traceroute to determine network error

About this task

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

Procedure

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

IPv6 management traffic is not sent/received as expected

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

IPv6 management traffic is not sent/received as expected

About this task

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

Procedure

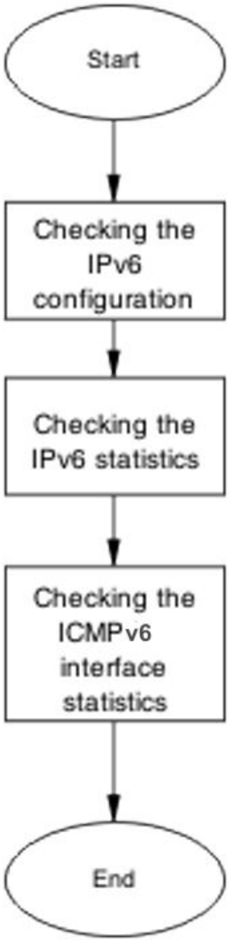

Start
Checking the IPv6 configuration
Checking the IPv6 statistics
Checking the ICMPv6 interface statistics
End

Figure 72: Task flow: IPv6 management traffic is not sent/received as expected

Checking the IPv6 configuration

About this task

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

Procedure

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

Checking the IPv6 statistics

About this task

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

Procedure

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

Checking the ICMPv6 statistics

About this task

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

Procedure

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

IPV6 telnet/http/ssh to device does not work

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

IPV6 telnet/http/ssh to device does not work

About this task

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

Procedure

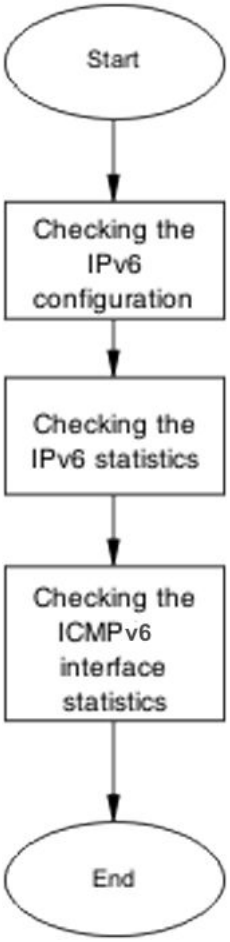

Start
Checking the IPv6 configuration
Checking the IPv6 statistics
Checking the ICMPv6 interface statistics
End

Figure 73: Task flow: IPV6 telnet/http/ssh to device does not work

Checking the IPv6 configuration

About this task

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

Procedure

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

Checking TCP statistics

About this task

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

Procedure

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

UDPv6 communication does not work

This task flow assists you to correct UDPv6 connectivity issues.

UDPv6 communication does not work

About this task

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

Procedure

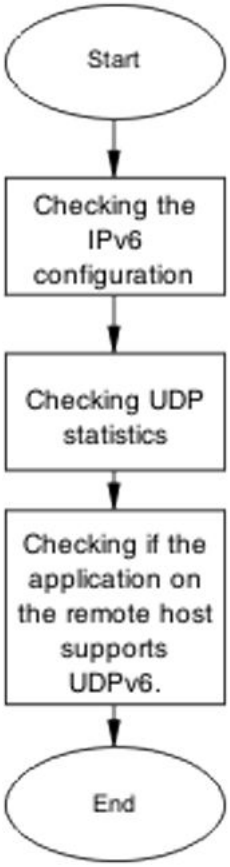

Start
Checking the IPv6 configuration
Checking UDP statistics
Checking if the application on the remote host supports UDPv6.
End

Figure 74: Task flow: UDPv6 communication does not work

Checking the IPv6 configuration

About this task

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

Procedure

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

Checking UDP statistics

About this task

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

Procedure

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

Checking if the application on the remote host supports UDPv6.

About this task

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

Cannot set IPv6 address

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

Cannot set IPv6 address

About this task

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

Procedure

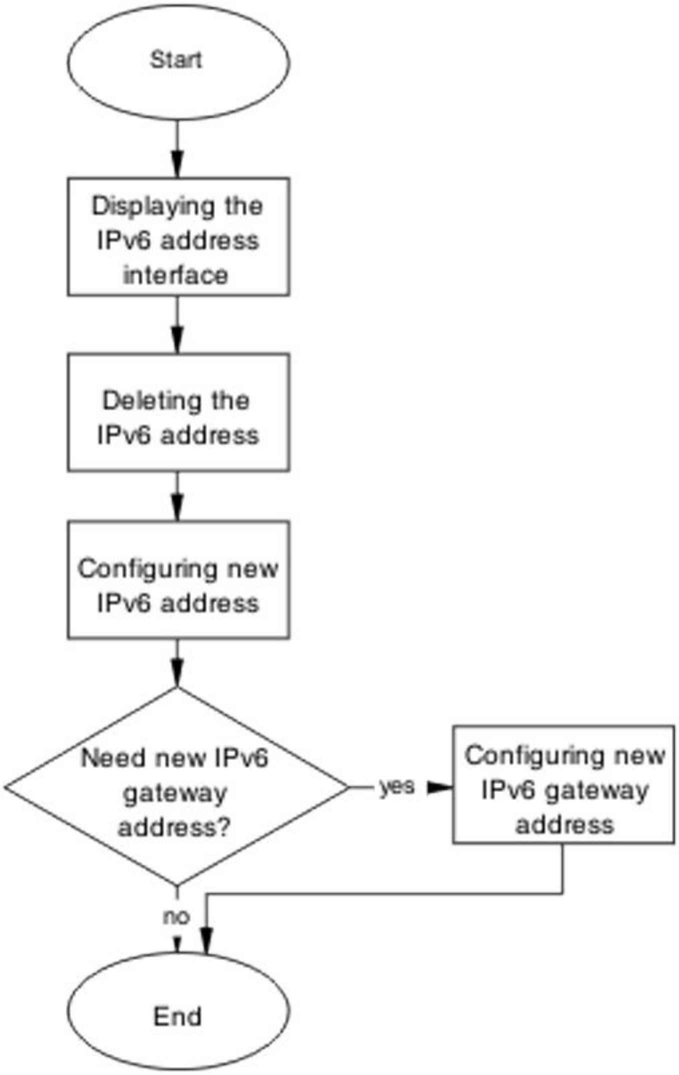

Start
Displaying the IPv6 address interface
Deleting the IPv6 address
Configuring new IPv6 address
Need new IPv6 gateway address?
yes
Configuring new IPv6 gateway address
no
End

Figure 75: Task flow: Cannot set IPv6 address

Displaying the IPv6 address interface

About this task

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

Procedure

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

Deleting the IPv6 address

About this task

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

Procedure

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

Configuring new IPv6 address

About this task

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

Procedure

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

Configuring new IPv6 gateway address

About this task

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

Procedure

1. Use the `ipv6 default-gateway <IPv6 address>` command to configure the gateway IPv6 address.

2. Observe the command output.

Chapter 12: Troubleshooting XFP/SFP

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

Troubleshooting XFP/SFP workflow

About this task

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

Procedure

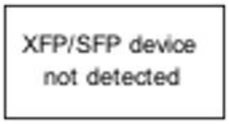


Figure 76: Work flow: Troubleshooting XFP/SFP

Result

Navigation

- Troubleshooting XFP/SFP on page 191

XFP/SFP device not detected

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

XFP/SFP device not detected task flow

About this task

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

Procedure

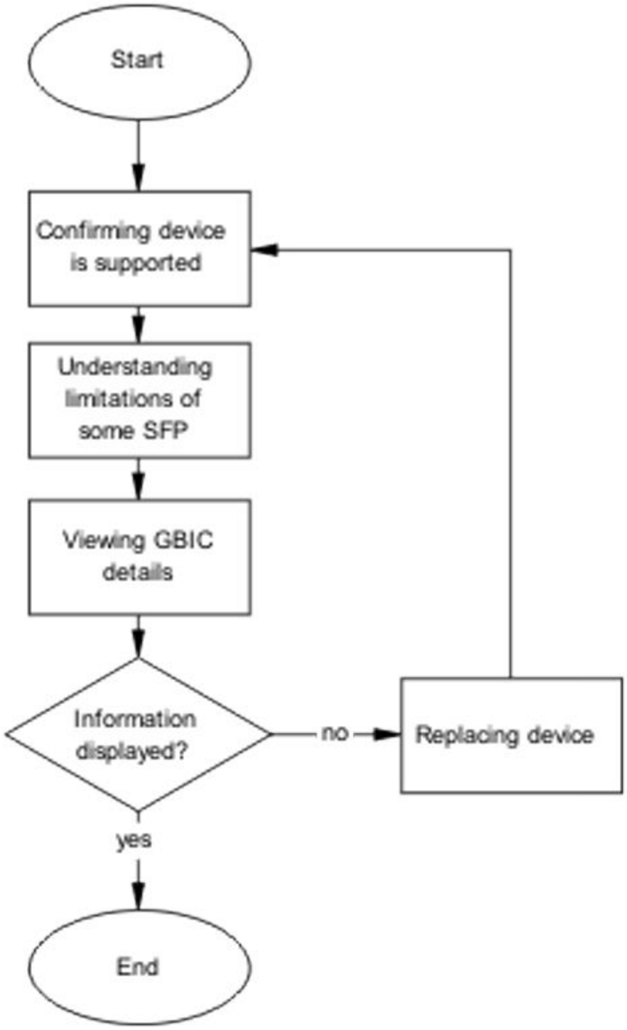


Figure 77: Task flow: XFP/SFP device not detected

Confirming device is supported

About this task

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

- *Release Notes for Avaya Ethernet Routing Switch 4000 Series*, NN47205-400
- *Installing Transceivers and Optical Components on Avaya Ethernet Routing Switch 4000 Series*, NN47205-301

Understanding limitations of some SFPs

About this task

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

Procedure

1. Use the **`show stack-info`** command to display device information.
2. Use the **`show interfaces gbic-info`** command to display device information.
3. Confirm that SFP AA1419075-E6 1-port T1 SFP and AA1419074-E6 1-port 100Base-FX SFP is only connected to a 4526T, 4526T-PWR, 4526T-PWR+, 4526FX, 4524GT, 4550T, 4550T-PWR, 4550T-PWR+, 4524GT-PWR, 4826GTS, 4826GTS-PWR+, 4850GTS or 4850GTS-PWR+.

   ✱ **Note:**

   You cannot use a T1 SFP or a 100Base-FX SFP on ERS 48xx SFP+ ports.

Viewing GBIC details

About this task

Use this procedure to display the GBIC device details.

Procedure

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

Replacing device

About this task

Use this procedure to replace a device.

Procedure

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

Chapter 13: Troubleshooting IGMP

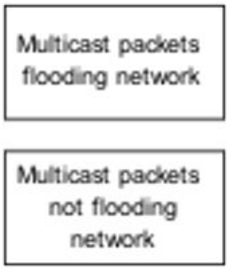
This sections assists you to resolve multicast flooding issues.

Troubleshooting IGMP workflow

About this task

The following workflow assists you to resolve multicast flooding.

Procedure


Multicast packets flooding network
Multicast packets not flooding network

Result

Navigation

- Multicast packets flooding network on page 195
- Multicast packets not flooding network on page 201

Multicast packets flooding network

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

Multicast packets flooding network task flow

About this task

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

Procedure

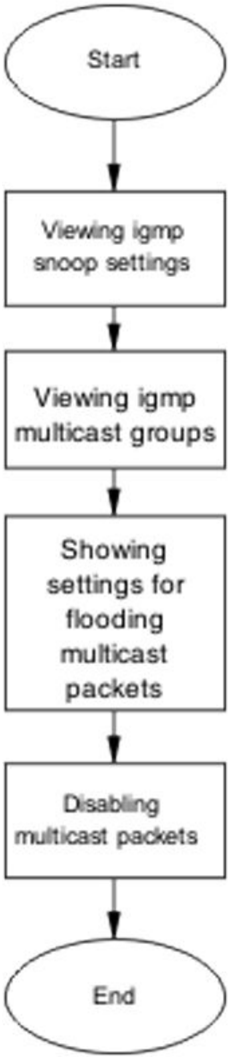

Start
Viewing igmp snoop settings
Viewing igmp multicast groups
Showing settings for flooding multicast packets
Disabling multicast packets
End

Figure 78: Task flow: Multicast packets flooding network

Result

Navigation

- Viewing IGMP snoop settings on page 197
- Viewing IGMP multicast groups on page 199
- Showing settings for flooding multicast packets on page 200
- Disabling multicast packets on page 201

Viewing IGMP snoop settings

About this task

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

Procedure

1. Enter Interface Configuration mode:

   enable

   configure terminal

   interface vlan <vid>
2. Use the **`show ip igmp interface`** command to display IGMP interface information.
3. Use the **`show ip igmp snooping`** command to display information about the IGMP snooping configuration.
4. Observe the displayed information.

Variable Definitions

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

Job aid

The following table describes the output of the command **`show ip igmp interface`**.

Field	Description
VLAN	Indicates the VLAN on which IGMP is configured.
Query Intvl	Specifies the frequency (in seconds) at which host query packets are transmitted on the interface.
Vers	Specifies the version of IGMP configured on this interface.
Oper Vers	Specifies the version of IGMP running on this interface.
Querier	Specifies the IP address of the IGMP querier on the IP subnet to which this interface is attached.
Query MaxRspT	Indicates the maximum query response time (in tenths of a second) advertised in IGMPv2 queries on this interface.
Wrong Query	Indicates the number of queries received whose IGMP version does not match the Interface version. You must configure all routers on a LAN to run the same version of IGMP. Thus, if queries are received with the wrong version, a configuration error occurs.
Joins	Indicates the number of times a group membership was added on this interface.
Robust	Specifies the robust value configured for expected packet loss on the interface.
LastMbr Query	Indicates the maximum response time (in tenths of a second) inserted into group-specific queries sent in response to leave group messages, and is also the amount of time between group specific query messages. Use this value to modify the leave latency of the network. A reduced value results in reduced time to detect the loss of the last member of a group. This does not apply if the interface is configured for IGMPv1.
Send Query	Indicates whether the ip igmp send-query feature is enabled or disabled. Values are YES or NO. Default is disabled.

The following table describes the output of the command **`show ip igmp snooping`**.

Field	Description
Vlan	Indicates the VLAN ID.
Snoop Enable	Indicates whether snoop is enabled (true) or disabled (false).
Proxy Snoop Enable	Indicates whether IGMP proxy is enabled (true) or disabled (false).
Static Mrouter Ports	Indicates the static mrouter ports in this VLAN that provide connectivity to an IP multicast router.
Active Mrouter Ports	Displays all dynamic (querier port) and static mrouter ports that are active on the interface.
Mrouter Expiration Time	Specifies the time remaining before the multicast router is aged out on this interface. If the switch does not receive queries before this time expires, it flushes out all group memberships known to the VLAN. The Query Max Response Interval (obtained from the queries received) is used as the timer resolution.

Viewing IGMP multicast groups

About this task

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

Procedure

1. Use the **`show ip igmp group`** command to display the information.
2. Observe the displayed information.

Job aid

The following table describes the output of the command.

Field	Description
Group Address	Indicates the multicast group address
VLAN	Indicates the VLAN interface on which the group exists.

Field	Description
Member Address	Indicates the IP address of the IGMP receiver (host or IGMP reporter). The IP address is 0.0.0.0 if the type is static.
Expiration	Indicates the time left before the group report expires. This variable is updated upon receiving a group report.
Type	Specifies the type of membership: static or dynamic
In Port	Identifies the member port for the group. This is the port on which group traffic is forwarded and in those case where the type is dynamic, it is the port on which the IGMP join was received.

Showing settings for flooding multicast packets

About this task

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

Procedure

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

Job aid

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

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

Field	Description
	disabled, the unknown multicast traffic is forwarded on all ports. Default is disabled.

Job aid

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

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

Disabling multicast packets

About this task

Use this procedure to disable the multicast flooding.

Procedure

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

Multicast packets not flooding network

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

Multicast packets not flooding network task flow

About this task

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

Procedure

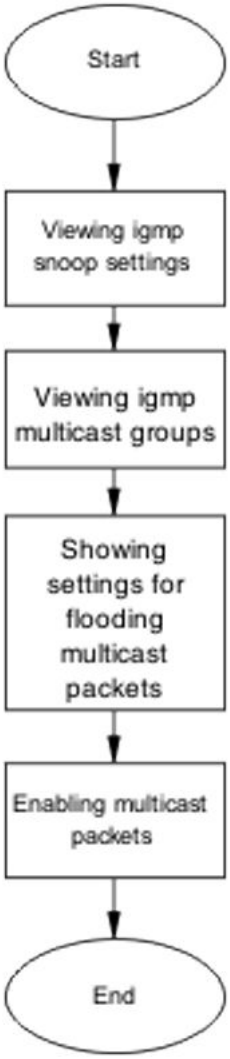

Start
Viewing igmp snoop settings
Viewing igmp multicast groups
Showing settings for flooding multicast packets
Enabling multicast packets
End

Figure 79: Task flow: Multicast packets not flooding network

Result

Navigation

- Viewing IGMP snoop settings on page 203
- Viewing IGMP multicast groups on page 205
- Showing settings for flooding multicast packets on page 206
- Enabling multicast packets on page 207

Viewing IGMP snoop settings

About this task

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

Procedure

1. Enter Interface Configuration mode:

   enable

   configure terminal

   interface vlan <vid>
2. Use the **`show ip igmp interface`** command to display IGMP interface information.
3. Use the **`show ip igmp snooping`** command to display information about the IGMP snooping configuration.
4. Observe the displayed information.

Variable Definitions

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

Job aid

The following table describes the output of the command **`show ip igmp interface`**.

Field	Description
VLAN	Indicates the VLAN on which IGMP is configured.
Query Intvl	Specifies the frequency (in seconds) at which host query packets are transmitted on the interface.
Vers	Specifies the version of IGMP configured on this interface.

Field	Description
Oper Vers	Specifies the version of IGMP running on this interface.
Querier	Specifies the IP address of the IGMP querier on the IP subnet to which this interface is attached.
Query MaxRspT	Indicates the maximum query response time (in tenths of a second) advertised in IGMPv2 queries on this interface.
Wrong Query	Indicates the number of queries received whose IGMP version does not match the Interface version. You must configure all routers on a LAN to run the same version of IGMP. Thus, if queries are received with the wrong version, a configuration error occurs.
Joins	Indicates the number of times a group membership was added on this interface.
Robust	Specifies the robust value configured for expected packet loss on the interface.
LastMbr Query	Indicates the maximum response time (in tenths of a second) inserted into group-specific queries sent in response to leave group messages, and is also the amount of time between group specific query messages. Use this value to modify the leave latency of the network. A reduced value results in reduced time to detect the loss of the last member of a group. This does not apply if the interface is configured for IGMPv1.
Send Query	Indicates whether the ip igmp send-query feature is enabled or disabled. Values are YES or NO. Default is disabled.

The following table describes the output of the command **`show ip igmp snooping`**.

Field	Description
Vlan	Indicates the VLAN ID.
Snoop Enable	Indicates whether snoop is enabled (true) or disabled (false).
Proxy Snoop Enable	Indicates whether IGMP proxy is enabled (true) or disabled (false).

Field	Description
Static Mrouter Ports	Indicates the static mrouter ports in this VLAN that provide connectivity to an IP multicast router.
Active Mrouter Ports	Displays all dynamic (querier port) and static mrouter ports that are active on the interface.
Mrouter Expiration Time	Specifies the time remaining before the multicast router is aged out on this interface. If the switch does not receive queries before this time expires, it flushes out all group memberships known to the VLAN. The Query Max Response Interval (obtained from the queries received) is used as the timer resolution.

Viewing IGMP multicast groups

About this task

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

Procedure

1. Use the **`show ip igmp group`** command to display the information.
2. Observe the displayed information.

Job aid

The following table describes the output of the command.

Field	Description
Group Address	Indicates the multicast group address
VLAN	Indicates the VLAN interface on which the group exists.
Member Address	Indicates the IP address of the IGMP receiver (host or IGMP reporter). The IP address is 0.0.0.0 if the type is static.
Expiration	Indicates the time left before the group report expires. This variable is updated upon receiving a group report.

Field	Description
Type	Specifies the type of membership: static or dynamic
In Port	Identifies the member port for the group. This is the port on which group traffic is forwarded and in those case where the type is dynamic, it is the port on which the IGMP join was received.

Showing settings for flooding multicast packets

About this task

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

Procedure

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

Job aid

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

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

Job aid

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

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

Enabling multicast packets

About this task

Use this procedure to enable the multicast flooding.

Procedure

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

Chapter 14: Troubleshooting RSTP SNMP traps

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

Troubleshooting RSTP SNMP traps workflow

About this task

The following workflow assists you to resolve RSTP trap issues.

Procedure

Figure 80: Work flow: Troubleshooting RSTP SNMP traps

No RSTP SNMP traps are received

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

No RSTP SNMP traps are received task flow

About this task

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

Procedure

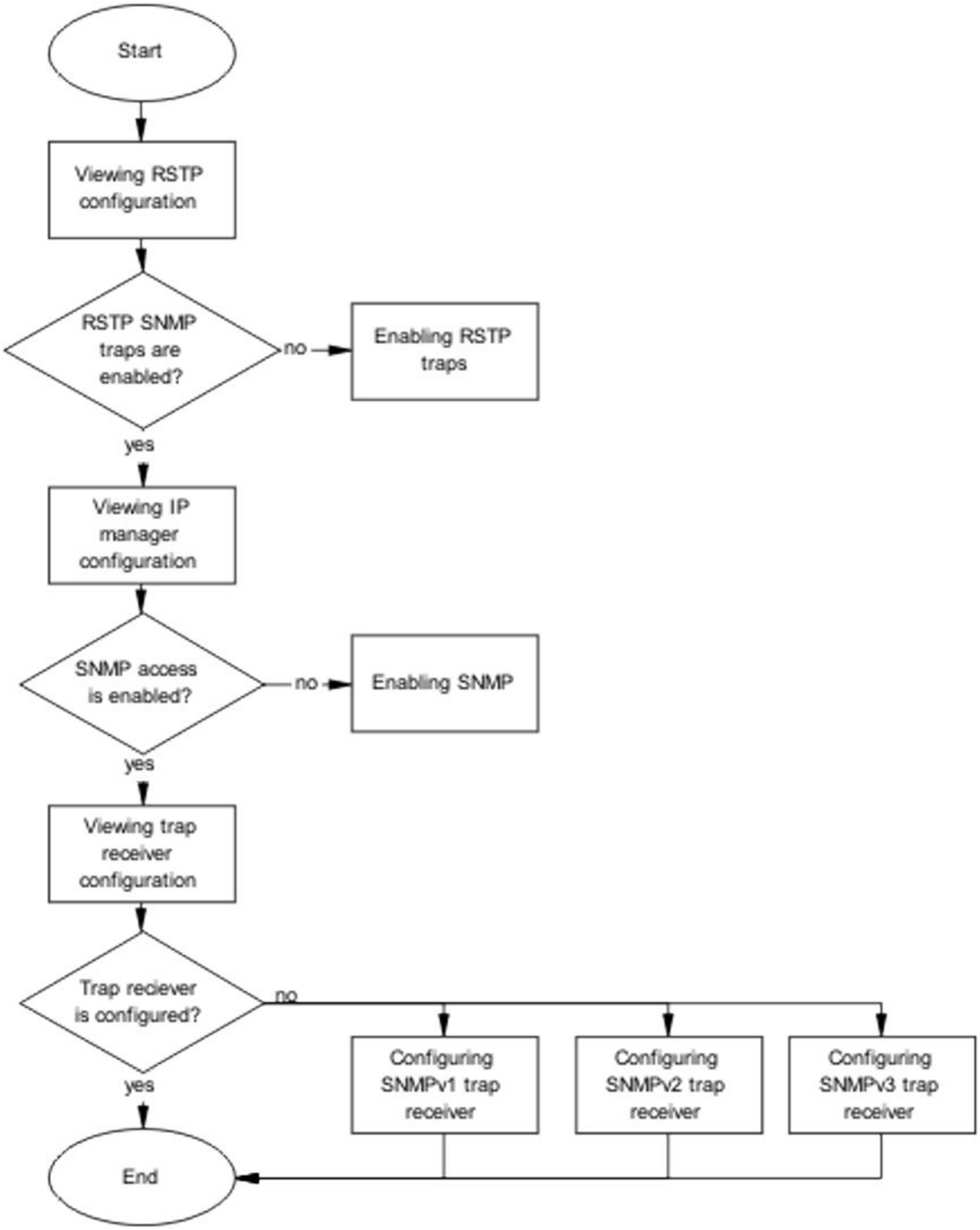

Start
Viewing RSTP configuration
RSTP SNMP traps are enabled?
no
Enabling RSTP traps
yes
Viewing IP manager configuration
SNMP access is enabled?
no
Enabling SNMP
yes
Viewing trap receiver configuration
Trap reciever is configured?
no
Configuring SNMPv1 trap receiver
Configuring SNMPv2 trap receiver
Configuring SNMPv3 trap receiver
yes
End

Figure 81: Task flow: No RSTP SNMP traps are received

Viewing RSTP configuration

About this task

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

Procedure

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

Job aid

The following is an example of output from the command.

```
Priority (hex):                               8000
Stp Version:                                  Rstp Mode
Bridge Max Age Time:                          20 seconds
Bridge Hello Time:                            2 seconds
Bridge Forward Delay Time:                    15 seconds
Tx Hold Count:                                3
Path Cost Default Type:                       32-bit
STP Traps:                                    Disabled
```

Enabling RSTP traps

About this task

Use the procedure in this section to enable RSTP traps.

Procedure

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

Viewing IP manager configuration

About this task

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

Procedure

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

Job aid

The following is an example of output from the command.

```
TELNET Access:                                Enabled

SNMP Access:                                  Disabled

WEB Access:                                   Enabled

SSH Access:                                   Enabled
```

Enabling SNMP

About this task

Use the procedure in this section to enable SNMP.

Procedure

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

2. Observe the command output.

Viewing trap receiver configuration

About this task

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

Procedure

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

Configuring SNMPv1 trap receiver

About this task

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

Procedure

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

Variable Definitions

Variable	Definition
IP address	IPv4 address of the server host

Configuring SNMPv2 trap receiver

About this task

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

Procedure

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

Variable Definitions

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

Configuring SNMPv3 trap receiver

About this task

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

Procedure

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

Variable Definitions

Variable	Definition
IP address	IPv4 address of the server host
user	The user that has been defined for sending SNMPv3 traps

Chapter 15: Troubleshooting SPBM

You can configure Shortest Path Bridging MAC (SPBM) only on the ERS 4800 series and the stack operation mode must be pure.

Displaying IS-IS configuration

About this task

Display the IS-IS configuration.

Procedure

1. Display global IS-IS information:

   `show isis`

2. Verify the ISIS interfaces administration and operations status are `UP`:

   `show isis interface`

3. Display IS-IS adjacencies:

   `show isis adjacencies`

4. Display IS-IS configuration components:

   `show isis system-id`

   `show isis int-auth`

   `show isis int-ckt-level`

Example

```
ERS-1# show isis

===========================================
              ISIS General Info
===========================================
            AdminState : enabled
            RouterType : Level 1
             System ID : 00aa.bbcc.0001
  Max LSP Gen Interval : 900
  Min LSP Gen Interval : 30
                Metric : wide

              Overload : true
         Csnp Interval : 10
         PSNP Interval : 2
     Rxmt LSP Interval : 5
             spf-delay : 100
```

```
           Router Name : ERS-1
     Num of Interfaces : 1
 Num of Area Addresses : 1
```

```
ERS-1# show isis interface
================================================================================
                                ISIS Interfaces
================================================================================
IFIDX      TYPE    LEVEL     OP-STATE  ADM-STATE  ADJ    UP-ADJ  SPBM-L1-METRIC
--------------------------------------------------------------------------------
Port1/20   pt-pt   Level 1   UP        UP         1      1       10
```

```
ERS-1# show isis adjacencies
================================================================================
 ISIS Adjacencies
================================================================================
INTERFACE L STATE        UPTIME PRI HOLDTIME SYSID             HOST-NAME
--------------------------------------------------------------------------------
Port1/20  1 UP         01:49:31 127       18 00dd.eeff.0008    ERS-8
```

```
ERS-1# show isis system-id
================================================================================
                                 ISIS System-Id
================================================================================
SYSTEM-ID
--------------------------------------------------------------------------------
00aa.bbcc.0001

ERS-1# show isis int-auth
================================================================================
                              ISIS Interface Auth
================================================================================
IFIDX        AUTH-TYPE       AUTH-KEYID      AUTH-KEY
--------------------------------------------------------------------------------

Port1/20     none            0

ERS-1# show isis int-ckt-level
================================================================================
                         ISIS Circuit Level Parameters
================================================================================
IFIDX           LEVEL                DIS                  CKTID
--------------------------------------------------------------------------------

Port1/20        Level 1                                   1
```

Displaying SPBM configuration

About this task

Use the following procedure to display the SPBM IS-IS configuration.

Procedure

1. Display SPBM configuration:

   `show isis spbm`

2. Display SPBM Unicast FIB information:

   `show isis spbm unicast-fib`

3. Display SPBM unicast tree information:

   `show isis spbm unicast-tree`

4. Display SPBM multicast FIB information:

   `show isis spbm multicast-fib`

5. Display SPBM nick-name:

   `show isis spbm nick-name`

Example

```
ERS-1# show isis spbm
====================================================
                   ISIS SPBM Info
====================================================
SPBM           B-VID      PRIMARY    NICK         LSDB
INSTANCE                  VLAN       NAME         TRAP
-----------------------------------------------------------
1              40,41      40             0.10.01      disable
```

```
ERS-1# show isis spbm-fib

================================================================================
                          SPBM UNICAST FIB ENTRY INFO
================================================================================
DESTINATION        BVLAN  SYSID            HOST-NAME         OUTGOING     COST
ADDRESS                                                      INTERFACE
--------------------------------------------------------------------------------
00:aa:bb:cc:00:02  40     00aa.bbcc.0002   ERS-2             1/20         20
00:dd:ee:ff:00:08  40     00dd.eeff.0008   ERS-8             1/20         10
00:aa:bb:cc:00:02  41     00aa.bbcc.0002   ERS-2             1/20         20
00:dd:ee:ff:00:08  41     00dd.eeff.0008   ERS-8             1/20         10
```

```
ERS-1# show isis spbm multicast-fib
================================================================================
                         SPBM MULTICAST FIB ENTRY INFO
================================================================================
MCAST DA           ISID   BVLAN  SYSID               HOST-NAME         OUTGOING
                                                                       INTERFACES
--------------------------------------------------------------------------------
03:10:01:00:03:e8  1000   40    00aa.bbcc.0001      ERS-1           3/5,1/20
03:10:02:00:03:e8  1000   40     00aa.bbcc.0002       VSP-2            3/5
03:10:01:00:03:e8  1000   41    00aa.bbcc.0001      ERS-1           3/5,1/20
03:10:02:00:03:e8  1000   41     00aa.bbcc.0002       VSP-2            3/5
03:10:01:00:03:e9  1001   40    00aa.bbcc.0001      ERS-1           3/6,1/20
03:10:02:00:03:e9  1001   40     00aa.bbcc.0002       VSP-2            3/6
03:10:01:00:03:e9  1001   41    00aa.bbcc.0001      ERS-1           3/6,1/20
03:10:02:00:03:e9  1001   41     00aa.bbcc.0002       VSP-2           3/6
```

```
ERS-1# show isis spbm nick-name

=====================================================
                              ISIS SPBM NICK-NAME
=====================================================
LSP ID                         LIFETIME  NICK-NAME HOST-NAME
------------------------------------------------------------------------
00aa.bbcc.0001.00-00           334       0.10.01   ERS-1
```

```
00aa.bbcc.0002.00-00           576       0.10.02   ERS-2
00dd.eeff.0008.00-00           828       0.10.08   ERS-8
```

Displaying VLAN to ISID associations

About this task

Display VLAN to ISID associations.

Tip:

Other useful commands include:

```
show vlan
```

```
show vlan interface info
```

```
show vlan interface vids
```

Procedure

Display VLAN to ISID associations:

```
show vlan i-sid
```

Example

```
ERS-1# show vlan i-sid
===============================================
                                   Vlan I-SID
===============================================
VLAN_ID    I-SID
--------------------------------------------------------------------------------
1
23         1000
111        1001

ERS-2# show vlan i-sid
===============================================
                                   Vlan I-SID
===============================================
VLAN_ID    I-SID
--------------------------------------------------------------------------------
1
23         1000
111        1001
```

Verifying Forwarding Database information

About this task

Verify the forwarding database (FDB) information.

Procedure

Display the FDB information:

`show mac-address vid <1-`

`show vlan remote-mac-table <1-`

Example

```
ERS-1# show mac-address vid 23
   MAC Address    Vid       Source            MAC Address    Vid       Source
----------------- ---- ---------------     ----------------- ---- ---------------
00-91-00-23-00-03   23 Unit:3 Port: 5      00-81-00-23-00-01   23 I-SID-1000
00-81-00-23-00-02   23 I-SID-1000
```

```
ERS-1# show vlan  remote-mac-table 23
===================================================================================
=
                            Vlan Remote Mac Table
===================================================================================
=
VLAN STATUS  MAC-ADDRESS        DEST-MAC          BVLAN DEST-SYSNAME      PORTS
-----------------------------------------------------------------------------------
-
23   learned 00:81:00:23:00:01  00:aa:bb:cc:00:02  40    ERS-2             1/20
23   learned 00:81:00:23:00:02  00:aa:bb:cc:00:02  40    ERS-2             1/20
```

Verifying ISIS interfaces and receive protocol control packets

About this task

Verify ISIS interfaces and receive protocol control packets.

Procedure

Display ISIS interfaces and receive protocol control packets:

```
show isis int-l1-cntl-pkts
```

Example

```
ERS-1# show isis int-l1-cntl-pkts
===============================================================================
                        ISIS L1 Control Packet Counters
===============================================================================
IFIDX         DIRECTION     HELLO        LSP          CSNP         PSNP
===============================================================================
Unit/Port: 1/15 Transmitted   236383       2005         2            4939

Unit/Port: 1/15 Received      239601       4613         126          2338

Unit/Port: 1/23 Transmitted   0            0            0            0

Unit/Port: 1/23 Received      0            0            0            0
```

Verifying UNI configuration

About this task

Verify UNI configuration.

Procedure

Display UNI information:

```
show i-sid
```

```
show vlan interface info <port>
```

Example

```
ERS-1# show i-sid
I-SID     Vid  UNI-type    Ports
--------- ---- ----------- ------------
11        11   C-VLAN      1/5, 2/7
1001      1001 C-VLAN      NONE
```

```
ERS-1# show vlan interface info 1/5
      Filter     Filter
     Untagged Unregistered
Port  Frames     Frames      PVID PRI    Tagging    Name
---- -------- ------------ ---- --- ------------- --------------
1/5  No       Yes          11   0   TagAll        Unit 1, Port 5
```

Verifying SPBM Unicast FIB entries

About this task

Verify SPBM Unicast FIB entries for nodes in the SPBM cloud.

Procedure

Display the SPBM FIB entry information:

```
show isis spbm unicast-fib
```

Example

```
ERS-1# show isis spbm unicast-fib
===============================================================================
                           SPBM UNICAST FIB ENTRY INFO
===============================================================================
DESTINATION        BVLAN  SYSID           HOST-NAME       OUTGOING   COST
ADDRESS                                                   INTERFACE
===============================================================================
00:1a:8f:10:53:df  100    001a.8f10.53df  MERS2-8606      Port: 1/15 30
00:1a:8f:10:53:e0  100    001a.8f10.53df  MERS2-8606      Port: 1/15 30
00:1a:8f:10:53:df  101    001a.8f10.53df  MERS2-8606      Port: 1/15 30
00:1a:8f:10:53:e0  101    001a.8f10.53df  MERS2-8606      Port: 1/15 30
00:1a:8f:10:53:e0  100    001a.8f10.b3df  MERS4-8606      Port: 1/15 10
00:1a:8f:10:b3:df  100    001a.8f10.b3df  MERS4-8606      Port: 1/15 10
00:1a:8f:10:53:e0  101    001a.8f10.b3df  MERS4-8606      Port: 1/15 10
00:1a:8f:10:b3:df  101    001a.8f10.b3df  MERS4-8606      Port: 1/15 10
fc:a8:41:f3:11:11  100    fca8.41f3.1111  stack-gicu      Port: 1/15 20
fc:a8:41:f3:11:11  101    fca8.41f3.1111  stack-gicu      Port: 1/15 20
fc:a8:41:f3:9f:df  100    fca8.41f3.9fdf  apancu          Port: 1/15 20
fc:a8:41:f3:9f:df  101    fca8.41f3.9fdf  apancu          Port: 1/15 20
fc:a8:41:f5:04:00  100    fca8.41f5.0400  VSP7000                    0
fc:a8:41:f5:04:00  101    fca8.41f5.0400  VSP7000                    0
```

Verifying SPBM network topology

About this task

Verify SPBM network topology.

Procedure

Verify the SPBM network topology:

```
show isis spbm unicast-tree <1-
```

Example

```
ERS-1# show isis spbm unicast-tree 100
Node:fca8.41fd.0400.00 (marius11) -> Node:001a.8f10.53df.00 (MERS2-8606) ->
    Node:fca8.41f3.1111.00 (stack-gicu) ->
    Node:001a.8f10.b3df.00 (MERS4-8606) -> ROOT

Node:fca8.41f3.9fdf.00 (apancu) -> Node:001a.8f10.b3df.00 (MERS4-8606) -> ROOT

Node:fca8.41f3.1111.00 (stack-gicu) -> Node:001a.8f10.b3df.00 (MERS4-8606) ->
    ROOT

Node:001a.8f10.b3df.00 (MERS4-8606) -> ROOT

Node:001a.8f10.53df.00 (MERS2-8606) -> Node:fca8.41f3.1111.00 (stack-gicu) ->
    Node:001a.8f10.b3df.00 (MERS4-8606) -> ROOT
```

Verify SPBM Multicast FIB entries

About this task

Verify SPBM Multicast FIB entries (carry b-cast and m-cast traffic).

Procedure

Verify SPBM Multicast FIB entries:

```
show isis spbm unicast-fib
```

Example

```
ERS-1# show isis spbm unicast-fib
===============================================================================
                           SPBM UNICAST FIB ENTRY INFO
===============================================================================
DESTINATION        BVLAN  SYSID           HOST-NAME       OUTGOING   COST
ADDRESS                                                   INTERFACE
===============================================================================
00:1a:8f:10:53:df  1000   001a.8f10.53df  MERS2-8606      Port: 1/15 10
00:1a:8f:10:53:e0  1000   001a.8f10.53df  MERS2-8606      Port: 1/15 10
00:1a:8f:10:53:df  1001   001a.8f10.53df  MERS2-8606      Port: 1/15 10
00:1a:8f:10:53:e0  1001   001a.8f10.53df  MERS2-8606      Port: 1/15 10
fc:a8:41:f5:07:df  1000   fca8.41f5.07df  puiub-stack                0
fc:a8:41:f5:07:df  1001   fca8.41f5.07df  puiub-stack                0
-------------------------------------------------------------------------------
  Total number of SPBM UNICAST FIB entries 6
-------------------------------------------------------------------------------
```

Verifying LSDB information

About this task

Verify LSDB information.

Procedure

Verify LSDB information:

```
show isis lsdb
```

Example

```
ERS-1# show isis lsdb
===============================================================================
                                 ISIS LSDB
===============================================================================
LSP ID                    LEVEL     LIFETIME  SEQNUM     CHKSUM     HOST-NAME

===============================================================================
001a.8f10.53df.00-00      1         1134      0x2095     0x9288     MERS2-8606

001a.8f10.b3df.00-00      1         1140      0x1923     0x130b     MERS4-8606

fca8.41f3.1111.00-00      1         630       0x248      0x4a67     stack-gicu

fca8.41f3.9fdf.00-00      1         364       0x264      0x5526     apancu

fca8.41f5.0400.00-00      1         777       0x6        0xc0e0     puiub-stack

fca8.41fd.0400.00-00      1         624       0x4e5      0x3a78     marius11

===============================================================================
Level-1 : 6 out of 6 Total Num of LSP Entries
Level-2 : 0 out of 6 Total Num of LSP Entries
===============================================================================

puiub-stack(config)#show isis lsdb detail
===============================================================================
                               ISIS LSDB (DETAIL)
===============================================================================



Level-1 LspID: 001a.8f10.53df.00-00     SeqNum: 0x00000469      Lifetime:  8341
        Chksum: 0x9288  PDU Length: 419
        Host_name: MERS2-8606
        Attributes:     IS-Type 1

TLV:1   Area Addresses: 1
        Area Address:01

TLV:22  Extended IS reachability:
        Adjacencies: 2
                 fca8.41fd.0400.00(marius11)      Metric:10
                                port id: 155 num_port 1
                                Metric: 10
                 fca8.41f3.1111.00(stack-gicu)    Metric:10
```

```
                                port id: 138 num_port 1
                                Metric: 10
```

Using CFM

About this task

Use CFM to diagnose the network.

Procedure

Use CFM to diagnose the network:

```
cfm spbm enable

show cfm

l2ping

l2traceroute

l2tracetree
```

Chapter 16: Troubleshooting SLA Monitor Agent

Use SLA Mon™ Agent to detect, identify, and isolate issues which impact end-to-end network performance.

Architecture

R5.7 supports the ability to perform QoS and DSCP tests via CLI between any two Networking devices with SLA Mon™ Agents without need for an SLA Mon™ server. In addition, R5.7 supports secure agent-server communication through certificate-based authentication and encrypted agent-server communication secure communications, and is intended to interoperate with the Avaya Diagnostic Server R2.0 when it releases. Avaya Diagnostic Server will provide network-wide QoS and DSCP monitoring, along with graphical display, alarms and alerts, trend analysis, and logging.

Supporting NTR and RTP

Note:

Server control over agent may impact NTR and RTP results.

NTR

The target device does not need to support SLAMon. If standard Traceroute works, NTR traces are available. Server control over agent may impact the NTR results.

When programming in ACLI, agents registered with a server should refuse server tests while manual NTR tests are being performed.

RTP

The target device must support SLAMon and SLAMon must be enabled.

When programming in ACLI, “Server bypass” is required if agent not registered. Agents that are registered with a server should refuse server tests while manual RTP tests are being performed.

Chapter 17: Troubleshooting DHCP/BootP relay

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

Troubleshooting DHCP/BootP relay work flow

About this task

The following workflow helps you to identify some common issues.

Procedure

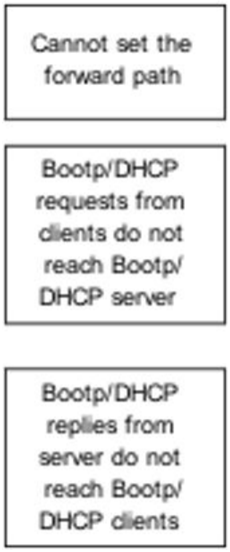

Cannot set the forward path
Bootp/DHCP requests from clients do not reach Bootp/ DHCP server
Bootp/DHCP replies from server do not reach Bootp/ DHCP clients

Figure 82: Work flow: Troubleshooting DHCP/BootP relay

Navigation

Cannot set the forward path

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

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

Cannot set the forward path task flow

About this task

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

Procedure

Start
Viewing VLAN IP information
End

Figure 83: Task flow: Cannot set the forward path

Navigation

- Viewing VLAN IP information on page 229

Viewing VLAN IP information

About this task

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

Procedure

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

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

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

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

About this task

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

Procedure

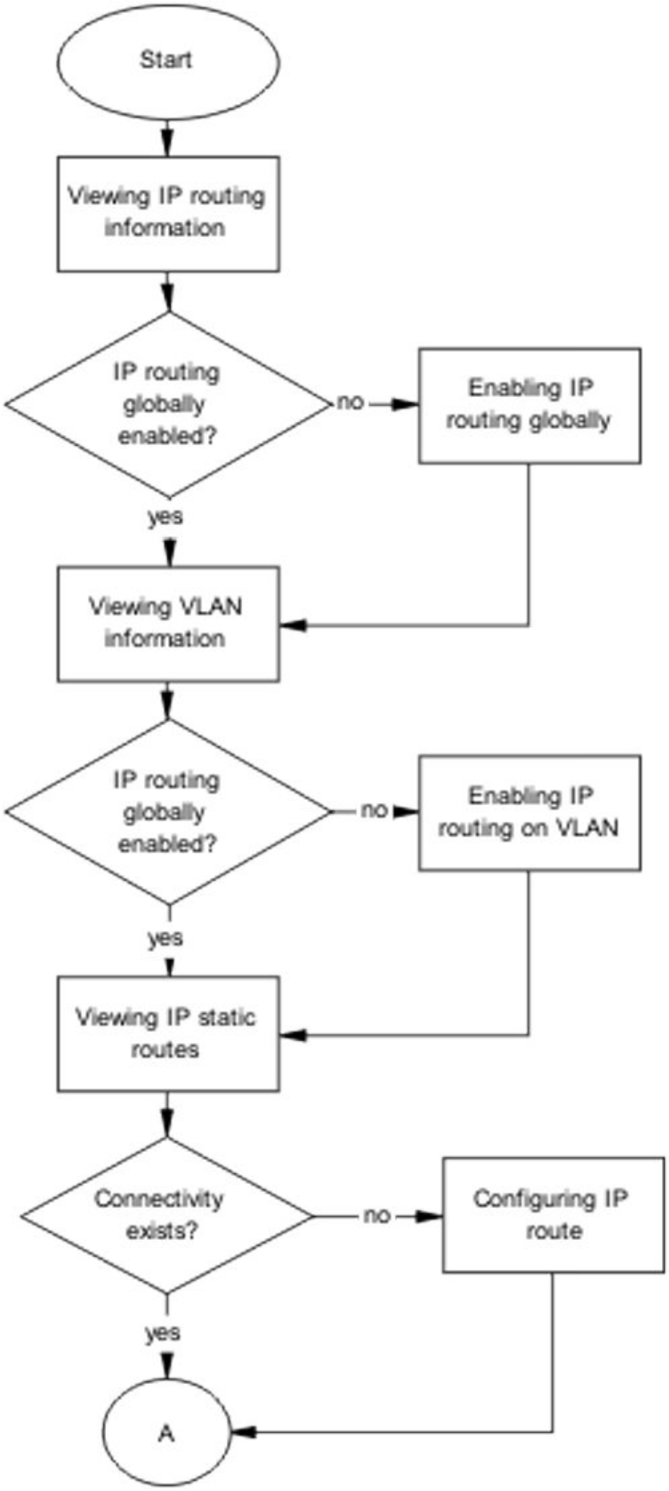

Start
Viewing IP routing information
IP routing globally enabled?
no
Enabling IP routing globally
yes
Viewing VLAN information
IP routing globally enabled?
no
Enabling IP routing on VLAN
yes
Viewing IP static routes
Connectivity exists?
no
Configuring IP route
yes
A

Figure 84: Task flow: Bootp/DHCP requests from clients do not reach Bootp/DHCP server part 1

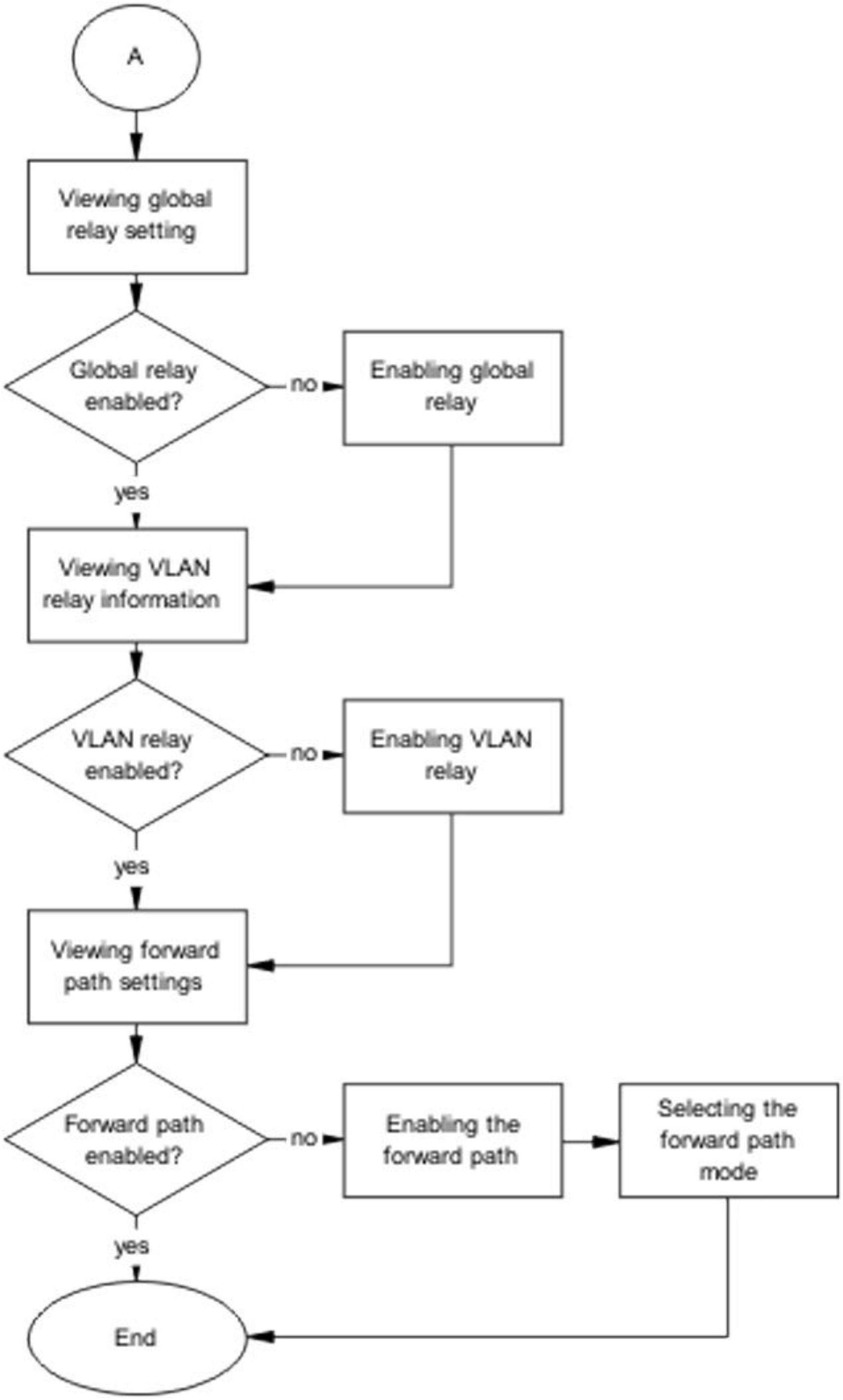

A
Viewing global relay setting
Global relay enabled?
no
Enabling global relay
yes
Viewing VLAN relay information
VLAN relay enabled?
no
Enabling VLAN relay
yes
Viewing forward path settings
Forward path enabled?
no
Enabling the forward path
Selecting the forward path mode
yes
End

Figure 85: Task flow: Bootp/DHCP requests from clients do not reach Bootp/DHCP server part 2

Viewing IP routing information

About this task

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

Procedure

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

Enabling IP routing globally

About this task

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

Procedure

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

Viewing VLAN information

About this task

Use the procedure in this section to view VLAN information.

Procedure

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

Enabling IP routing on VLAN

About this task

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

Procedure

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

Variable Definitions

Variable	Definition
VLANID	Unique ID of the VLAN

Viewing IP static routes

About this task

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

Procedure

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

Configuring IP route

About this task

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

Procedure

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

Viewing global relay setting

About this task

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

Procedure

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

Enabling global relay

About this task

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

Procedure

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

Viewing VLAN relay information

About this task

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

Procedure

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

2. Observe the command output.

Enabling VLAN relay

About this task

Use the procedure in this section to enable VLAN relay.

Procedure

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

Variable Definitions

Variable	Definition
VLANID	Unique ID of the VLAN

Viewing forward path settings

About this task

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

Procedure

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

Enabling the forward path

About this task

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

Procedure

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

Variable Definitions

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

Selecting the forward path mode

About this task

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

Procedure

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

Variable Definitions

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

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

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

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

About this task

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

Procedure

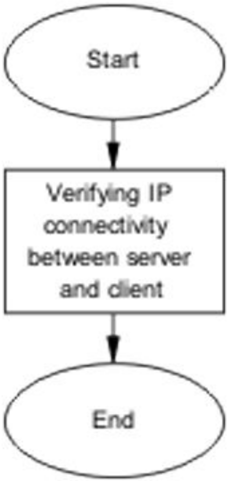


Figure 86: Task flow: Bootp/DHCP replies from server do not reach Bootp/DHCP clients

Navigation

- Verifying IP connectivity between server and client on page 238

Verifying IP connectivity between server and client

Before you begin

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

About this task

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

Procedure

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