Configuring Security

Release 4.3
NN47500-601
Issue 01.01
March 2016

© 2016, Avaya, Inc.
All Rights Reserved.

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: https://support.avaya.com/helpcenter/getGenericDetails?detailId=C20091120112456651010 under the link “Warranty & Product Lifecycle” 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.

“Hosted Service” means a hosted service subscription that You acquire from either Avaya or an authorized Avaya Channel Partner (as applicable) and which is described further in Hosted SAS or other service description documentation regarding the applicable hosted service. If You purchase a Hosted Service subscription, the foregoing limited warranty may not apply but You may be entitled to support services in connection with the Hosted Service as described further in your service description documents for the applicable Hosted Service. Contact Avaya or Avaya Channel Partner (as applicable) for more information.

Hosted Service

THE FOLLOWING APPLIES IF YOU PURCHASE A HOSTED SERVICE SUBSCRIPTION FROM AVAYA OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE), THE TERMS OF USE FOR HOSTED SERVICES ARE AVAILABLE ON THE AVAYA WEBSITE, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO UNDER THE LINK “Avaya Terms of Use for Hosted Services” OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, AND ARE APPLICABLE TO ANYONE WHO ACCESSES OR USES THE HOSTED SERVICE. BY ACCESSING OR USING THE HOSTED SERVICE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE DOING SO (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THE TERMS OF USE. IF YOU ARE ACCEPTING THE TERMS OF USE ON BEHALF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE TERMS OF USE. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT WISH TO ACCEPT THESE TERMS OF USE, YOU MUST NOT ACCESS OR USE THE HOSTED SERVICE OR AUTHORIZE ANYONE TO ACCESS OR USE THE HOSTED SERVICE. YOUR USE OF THE HOSTED SERVICE SHALL BE LIMITED BY THE NUMBER AND TYPE OF LICENSES PURCHASED UNDER YOUR CONTRACT FOR THE HOSTED SERVICE, PROVIDED, HOWEVER, THAT FOR CERTAIN HOSTED SERVICES IF APPLICABLE, YOU MAY HAVE THE OPPORTUNITY TO USE FLEX LICENSES, WHICH WILL BE INVOICED ACCORDING TO ACTUAL USAGE ABOVE THE CONTRACT LICENSE LEVEL. CONTACT AVAYA OR AVAYA’S CHANNEL PARTNER FOR MORE INFORMATION ABOUT THE LICENSES FOR THE APPLICABLE HOSTED SERVICE, THE AVAILABILITY OF ANY FLEX LICENSES (IF APPLICABLE), PRICING AND BILLING INFORMATION, AND OTHER IMPORTANT INFORMATION REGARDING THE HOSTED SERVICE.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO, UNDER THE LINK “AVAYA SOFTWARE LICENSE TERMS (Avaya Products)” 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 computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products, pre-installed on hardware products, and any upgrades, updates, patches, 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.

License 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 is the software contained within the list of Heritage Nortel Products located at https://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 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.

Virtualization

The following applies if the product is deployed on a virtual machine. Each product has its own ordering code and license types. Note that each Instance of a product must be separately licensed and ordered. For example, if the end user customer or Avaya Channel Partner would like to install two Instances of the same type of products, then two products of that type must be ordered.

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 products, Documentation or on Avaya's website at: https://support.avaya.com/Copyright or such successor site as designated by Avaya. The open source software license terms provided as Third Party Terms are consistent with the license rights granted in these Software License Terms, and may contain additional rights benefiting You, such as modification and distribution of the open source software. The Third Party Terms shall take precedence over these Software License Terms, solely with respect to the applicable Third Party Components to the extent that these Software License Terms impose greater restrictions on You than the applicable Third Party Terms.

The following applies if the H.264 (AVC) codec is distributed with the product. THIS PRODUCT IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Service Provider

THE FOLLOWING APPLIES TO AVAYA CHANNEL PARTNER'S HOSTING OF AVAYA PRODUCTS OR SERVICES. THE PRODUCT OR HOSTED SERVICE MAY USE THIRD PARTY COMPONENTS SUBJECT TO THIRD PARTY TERMS AND REQUIRE A SERVICE PROVIDER TO BE INDEPENDENTLY LICENSED DIRECTLY FROM THE THIRD PARTY SUPPLIER. AN AVAYA CHANNEL PARTNER'S HOSTING OF AVAYA PRODUCTS MUST BE AUTHORIZED IN WRITING BY AVAYA AND IF THOSE HOSTED PRODUCTS USE OR EMBED CERTAIN THIRD PARTY SOFTWARE, INCLUDING BUT NOT LIMITED TO MICROSOFT SOFTWARE OR CODECS, THE AVAYA CHANNEL PARTNER IS REQUIRED TO INDEPENDENTLY OBTAIN ANY APPLICABLE LICENSE AGREEMENTS, AT THE AVAYA CHANNEL PARTNER'S EXPENSE, DIRECTLY FROM THE APPLICABLE THIRD PARTY SUPPLIER.

WITH RESPECT TO CODECS, IF THE AVAYA CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE G.729 CODEC, H.264 CODEC, OR H.265 CODEC, THE AVAYA CHANNEL PARTNER ACKNOWLEDGES AND AGREES THE AVAYA CHANNEL PARTNER IS RESPONSIBLE FOR ANY AND ALL RELATED FEES AND/OR ROYALTIES. THE G.729 CODEC IS LICENSED BY SIPRO LAB TELECOM INC. SEE WWW.SIPRO.COM/CONTACT.HTML. THE H.264 (AVC) CODEC IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO: (I) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (II) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION FOR H.264 (AVC) AND H.265 (HEVC) CODECS MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Compliance with Laws

Customer acknowledges and agrees that it is responsible for complying with any applicable laws and regulations, including, but not limited to laws and regulations related to call recording, data privacy, intellectual property, trade secret, fraud, and music performance rights, in the country or territory where the Avaya product is used.

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

If You suspect that You are being victimized by Toll Fraud and You need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: https://support.avaya.com or such successor site as designated by Avaya.

Security Vulnerabilities

Information about Avaya's security support policies can be found in the Security Policies and Support section of https://support.avaya.com/security.

Suspected Avaya product security vulnerabilities are handled per the Avaya Product Security Support Flow (https://support.avaya.com/css/P8/documents/100161515).

Downloading Documentation

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

Contact Avaya Support

See the Avaya Support website: https://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: https://support.avaya.com (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

Trademarks

The trademarks, logos and service marks ("Marks") displayed in this site, the Documentation, Hosted Service(s), and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third parties. Users are not permitted to use such

Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the Documentation, Hosted Service(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners. Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Contents

Chapter 1: New in this document

Configuring Security is a new document for Release 4.3 so all the features are new in this release. See *Release Notes* for a full list of features.

Chapter 2: Security fundamentals

This section provides conceptual content to help you configure and customize the security services on the switch.

Security overview

Security is a critical attribute of networking devices such as the switch. Security features are split into two main areas:

- Control path—protects the access to the device from a management perspective.
- Data path—protects the network from malicious users by controlling access authorization to the network resources (such as servers and stations). This protection is primarily accomplished by using filters or access lists.

You can protect the control path using

- logon and passwords
- access policies, in which you specify the network and address that can use a service or daemon
- secure protocols, such as Secure Shell (SSH), Secure Copy (SCP), and the Simple Network Management Protocol version 3 (SNMPv3)
- the Message Digest 5 Algorithm (MD5), which protects routing updates, Open Shortest Path First (OSPF), and Border Gateway Protocol (BGP)

You can protect the data path using

- Media Access Control (MAC) address filtering
- Layer 3 filtering, such as Internet Protocol (IP) and User Datagram Protocol (UDP)/ Transmission Control Protocol (TCP) filtering
- routing policies, which prevent users from accessing restricted areas of the network

Security modes

The switch supports three security modes:

- Enhanced secure
- Hsecure
- SSH secure

Enable SSH secure mode to allow only SSH to be used and disable all other access-service protocols. Enabling this mode disables Telnet, rlogin, FTP, SNMP, TFTP, HTTP, and HTTPS by setting the boot flags for these protocols to off. You can override the configuration and enable required protocols individually for run-time use. The administrator will have to enable required protocols individually for run-time use again following a reboot even if you save the configuration. This is because the SSH secure mode enable takes precedence at the time of reboot and the other protocols will be disabled even though the configuration file has them set to enabled.

Note:

Disabling SSH secure mode will not automatically enable the operations, administration, and management (OA&M) protocols that were disabled. The boot flags for the required protocols will have to be individually set to enabled.

The following table lists the differences between enhanced secure mode and hsecure mode.

Table 1: Enhanced secure mode versus hsecure mode

Feature	Enhanced secure	Hsecure
Authentication	Role-based: • admin • privilege • operator • security • auditor	Access-level based: • rwa • rw • ro • l3 • l2 • l1
Password length	Minimum of 8 characters with the exception of the Admin account, which requires a minimum of 15 characters	10 characters, minimum
Password rules	1 or 2 upper case, lower case, numeric and special characters	Minimum of 2 upper case, 2 lower case, 2 numeric and 2 special characters
Password expiration	Per-user minimum change interval is enforced, which is programmed by the Administrator	Global expiration, configured by the Administrator

Table continues…

Feature	Enhanced secure	Hsecure
Password-unique	Previous passwords and common passwords between users are prevented	The same
Password renewal	Automatic password renewal is enforced	The same
Audit logs	Audit logs are encrypted, and authorized users are able to view, modify, and delete.	Standard operation
SNMPv3	Password rules apply to SNMPv3 Auth&Priv. SNMPv3 is required (V1/V2 disabled)	SNMPv1 and SNMPv2 can be enabled.
EDM	Site Admin to enable or disable	Disabled
Telnet and FTP	Site Admin to enable or disable	The same
DOS attack Prevention	Not available	Prevents DOS attacks by filtering IP addresses and IP address ranges.

For information on Enhanced secure mode and SSH, see *Administering*.

hsecure mode

The switch supports a flag called high secure (hsecure). hsecure introduces the following behaviors for passwords:

- 10-character enforcement
- aging time
- limitation of failed logon attempts
- protection mechanism to filter certain IP addresses.

After you enable the hsecure flag, the software enforces the 10-character rule for all passwords. This password must contain a minimum of two uppercase characters, two lowercase characters, two numbers, and two special characters.

After you enable hsecure, the system requires you to save the configuration file and reboot the system for hsecure to take effect. If the existing password does not meet the minimum requirements for hsecure, the system prompts you to change the password during the first login.

The default username is rwa and the default password is rwa. In hsecure, the system prompts you to change these during first login because they do not meet the minimum requirements for hsecure.

When you enable hsecure, the system disables Simple Network Management Protocol (SNMP) v1, SNMPv2 and SNMPv3. If you want to use SNMP, you must re-enable SNMP, using the command **`no boot config flag block-snmp`**.

Aging enforcement

After you enable the hsecure flag, you can configure a duration after which you must change your password. You configure the duration by using the aging parameter.

For SNMP and File Transfer Protocol (FTP), after a password expires, access is denied. Before you access the system, you must change a community string to a new string consisting of more than eight characters.

Important:

Consider the following after you enable the hsecure flag:

- You cannot enable the Web server for Enterprise Device Manager (EDM) access.
- You cannot enable the Secure Shell (SSH) password authentication.

For more information, see *Administering*.

Filtering mechanism

Incorrect IP source addresses as network or broadcast addresses are filtered at the virtual router interface. Source addresses 192.168.168.0 and 192.168.168.255 are discarded.

This change is valid for all IP subnets, not only for /24.

You can filter addresses only if you enable the hsecure mode.

CLI passwords

The switch ships with default passwords assigned for access to the command line interface (CLI) through a console or management session. If you have read/write/all access authority, and you are using SNMPv3, you can change passwords that are in an encrypted format. If you are using Enterprise Device Manager (EDM), you can also specify the number of available Telnet sessions and rlogin sessions.

Important:

The default passwords are documented and well known. Change the default passwords and community strings immediately after you first log on.

If you enable enhanced secure mode with the **`boot config flags enhancedsecure-mode`** command, you enable new access levels, along with stronger password complexity, length, and minimum change intervals. For more information on system access fundamentals and configuration, see *Administering*.

Port Lock feature

You can use the Port Lock feature to administratively lock a port or ports to prevent other users from changing port parameters or modifying port action. You cannot modify locked ports until the ports are first unlocked.

Access policies for services

You can control access to the switch by creating an access policy. An access policy specifies the hosts or networks that can access the device through various services, such as Telnet, SNMP, Trivial File Transfer Protocol (TFTP), File Transfer Protocol (FTP), Hypertext Transfer Protocol (HTTP), Remote Shell (RSH), and remote login (rlogin). You can enable or disable access services by setting flags from CLI.

You can define network stations that can explicitly access the switch or stations that cannot access it. For each service you can also specify the level of access, such as read-only or read-write-all.

Important:

A third-party security scan shows the switch service ports open and in the listen state. No connections are accepted on these ports unless you enable the particular daemon. The switch does not dynamically start and stop the daemons at runtime and needs to keep them running from system startup.

For more information about configuring access policies, see *Administering*.

Denial-of-service attack prevention

The switch supports a configurable flag, called high secure (hsecure). High secure mode introduces a protection mechanism to filter certain IP addresses, and two restrictions on passwords: 10-character enforcement and aging time.

If the device starts in hsecure mode with default factory settings, and no previously configured password, the system will prompt you to change the password. The new password must follow the rules mandated by high secure mode. After you enable hsecure and restart the system, if you have an invalid-length password you must change the password.

If you enable hsecure for the first time and the password file does not exist, then the device creates a normal default username (rwa) and password (rwa). In this case, the password does not meet the minimum requirements for hsecure and as a result the system prompts you to change the password.

The following information describes hsecure mode operations:

- When you enable the hsecure flag, after a certain duration you are asked to change your password. If not configured, the aging parameter defaults to 90 days.

- For SNMP and FTP, access is denied when a password expires. You must change the community strings to a new string made up of more than eight characters before accessing the system.
- You cannot enable the Web server at any time.
- You cannot enable the SSH password-authentication feature at any time.

Hsecure is disabled by default. When you enable hsecure, the desired behavior applies to all ports.

For more information, see the following tasks:

- Configuring directed broadcast on page 20
- Preventing certain types of DOS attacks on page 21

Configuration considerations

Use the information in this section to understand the limitations of some security functions such as BSAC RADIUS servers and Layer 2 protocols before you attempt to configure security.

Single profile enhancement for BSAC RADIUS servers

Before enabling Remote Access Dial-In User Services (RADIUS) accounting on the device, you must configure at least one RADIUS server.

The switch software supports Microsoft Radius Servers (NPS Windows 2008, Windows 2003 IAS Server), BaySecure Access Control (BSAC), Merit Network servers and Linux based servers. To use these servers, you must first obtain the software for the server. You must also make changes to one or more configuration files for these servers.

Single Profile is a feature that is specific to BSAC RADIUS servers. In a BSAC RADIUS server, when you create a client profile, you can specify all the returnable attributes. When you use the same profile for different products, you specify all the returnable attributes in the single profile.

Attribute format for a third-party RADIUS server

If you use a third-party RADIUS server and need to modify the dictionary files, you must add a vendor-specific attribute (attribute #26) and use 1584 as vendor code for all the devices and then send back access-priority vendor-assigned attribute number 192 with a decimal value of 1 to 6, depending upon whether you want read only to read-write-all.

RADIUS on management ports

When the switch includes a management port, the port supports the RADIUS protocol. When RADIUS packets are sent out of the management port, the SRC-IP address is properly entered in the RADIUS header.

For more information about the supported RADIUS servers, see the documentation of the RADIUS server.

SNMP cloned user considerations

If the user from which you are cloning has authentication, you can choose for the new user to either have the same authentication protocol as the user from which it was cloned, or no authentication. If you choose authentication for the new user, you must provide a password for that user. If you want a new user to have authentication, you must indicate that at the time you create the new user. You can assign a privacy protocol only to a user that has authentication.

If the user from which you are cloning has no authentication, then the new user has no authentication.

Security configuration using CLI

Configure security information used on the control and data paths to protect the network from uncontrolled access to network resources.

For more information about how to configure passwords and access policies, see *Administering*.

Enabling hsecure

The hsecure flag is disabled by default. When you enable it, the software enforces the 10 character rule for all passwords.

About this task

When you upgrade from a previous release, if the password does not have at least 10 characters, you receive a prompt to change your password to the mandatory 10-character length.

If you enable hsecure for the first time and the password file does not exist, then the device creates a normal default username (rwa) and password (rwa). In this case, the password does not meet the minimum requirements for hsecure and as a result the system prompts you to change the password.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Enable or disable hsecure mode:

   ```
   boot config flags hsecure
   ```

   The following warning messages appear:

   ```
   Warning: For security purposes, all unsecure services - TFTP, FTP, Rlogin, Telnet,
   SNMP are disabled. Individually enable the required services.
   Warning: Please save boot configuration and reboot the switch for this to take
   effect.
   ```

3. Save the configuration and restart the device for the change to take effect.

Example

```
Switch:1> enable
```

```
Switch:1# configure terminal
```

Enable hsecure mode:

```
Switch:1(config)#boot config flags hsecure
```

```
Warning: For security purposes, all unsecure services - TFTP, FTP,
Rlogin, Telnet, SNMP are disabled. Individually enable the required
services. Warning: Please save boot configuration and reboot the switch
for this to take effect.
```

Save the configuration:

```
Switch:1(config)#save config
```

Restart the switch:

```
Switch:1(config)#reset
```

```
Are you sure you want to reset the switch (y/n)?y
```

Changing an invalid-length password

Before you begin

Important:

When you enable hsecure, passwords must contain a minimum of 10 characters or numbers with a maximum of 20. The password must contain a minimum of: two uppercase characters, two lowercase characters, two numbers, and two special characters.

About this task

After you enable **hsecure** and restart the system, change your password if you have an invalid-length password.

Procedure

1. At the CLI prompt, log on to the system.
2. Enter the password.

   When you have an invalid-length password, the following message appears:

   ```
   Your password is valid but less than mandatory 10 characters.
   Please change the password to continue.
   ```
3. When prompted, enter the new password.
4. When prompted, reenter the new password.

Example

Log on to the switch:

```
Login:rwa
```

Enter the password:

```
Password:***
```

```
Your password is valid but less than mandatory 10 characters. Please
change the password to continue.
```

Enter the new password:

```
Enter the new password: **********
```

Re-enter the new password:

```
Re-enter the new password: **********
```

```
Password successfully changed.
```

Changing passwords

Configure new passwords for each access level, or change the logon or password for the different access levels of the switch. After you receive the switch, use default passwords to initially access CLI. If you use Simple Network Management Protocol version 3 (SNMPv3), you can change encrypted passwords.

Before you begin

- You must use an account with read-write-all privileges to change passwords. For security, the switch saves passwords to a hidden file.

About this task

If you enable the hsecure flag, after the aging time expires, the system prompts you to change your password. If you do not configure the aging time, the default is 90 days.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Change a password:

   ```
   cli password WORD<1-20> {layer1|layer2|layer3|read-only|read-write|
   read-write-all}
   ```

3. Enter the old password.
4. Enter the new password.
5. Enter the new password a second time.
6. Configure password options:

   ```
   password access-level WORD<2-8>
   ```

   ```
   password aging-time day <1-365>
   ```

   ```
   password default-lockout-time <60-65000>
   ```

   ```
   password lockout WORD<0-46> [time <60-65000>]
   ```

```
    password min-passwd-len <10-20>

    password password-history <3-32>
```

Example

```
Switch:1> enable

Switch:1# configure terminal
```

Change a password:

```
Switch:1(config)# password smith read-write-all
```

Enter the old password:

```
Switch:1(config)# *********
```

Enter the new password:

```
Switch:1(config)# *********
```

Enter the new password a second time:

```
Switch:1(config)# *********
```

Set password to an access level of read-write-all and the expiration period for the password to 60 days:

```
Switch:1(config)# access-level rwa aging-time 60
```

Variable definitions

Use the data in the following table to use the **`cli password`** command.

Variable	Value
layer1|layer2|layer3|read-only|read-write|read-write-all	Changes the password for the specific access level.
WORD<1–20>	Specifies the user logon name.

Use the data in the following table to use the **`password`** command.

Variable	Value
access level WORD<2–8>	Permits or blocks this access level. The available access level values are as follows: • l1 • l2 • l3 • ro • rw • rwa

Table continues…

Variable	Value
aging-time day *<1-365>*	Configures the expiration period for passwords in days, from 1–365. The default is 90 days.
default-lockout-time *<60-65000>*	Changes the default lockout time after three invalid attempts. Configures the lockout time, in seconds, and is in the 60–65000 range. The default is 60 seconds. To configure this option to the default value, use the default operator with the command.
lockout *WORD<0–46> time <60-65000>*	Configures the host lockout time. • *WORD<0–46>* is the host IP address in the format a.b.c.d. • *<60-65000>* is the lockout-out time, in seconds, in the 60–65000 range. The default is 60 seconds.
min-passwd-len *<10-20>*	Configures the minimum length for passwords in high-secure mode. The default is 10 characters. To configure this option to the default value, use the default operator with the command.
password-history *<3-32>*	Specifies the number of previous passwords the switch stores. You cannot reuse a password that is stored in the password history. The default is 3. To configure this option to the default value, use the default operator with the command.

Configuring directed broadcast

A directed broadcast is a frame sent to the subnet broadcast address on a remote IP subnet. When you disable (or suppress) directed broadcasts on an interface, all frames sent to the subnet broadcast address for a local router interface are dropped. Disabling directed broadcasts protects hosts from possible denial-of-service (DOS) attacks. By default, this feature is enabled on the device.

Procedure

1. Enter VLAN Interface Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

   ```
   interface vlan <1-4059>
   ```

2. Configure the switch to forward directed broadcasts for a VLAN:

   ```
   ip directed-broadcast enable
   ```

Example

```
Switch:1> enable
Switch:1# configure terminal
Switch:1(config)# interface vlan 2
Switch:1(config-if)# ip directed-broadcast enable
```

Variable definitions

Use the data in the following table to use the **`ip directed-broadcast`** command.

Variable	Value
enable	Enables the device to forward directed broadcast frames to the specified VLAN. The default setting for this feature is enabled.

Preventing certain types of DOS attacks

Protect the switch against IP packets with illegal IP addresses such as loopback addresses or a source IP address of ones, or Class D or Class E addresses from being routed. The switch supports high-secure configurable flag.

About this task

Important:

After you enable this flag, the desired behavior (not routing source packets with an IP address of 255.255.255.255) applies to all ports that belong to the same port.

Important:

The setting to enable hsecure only takes effect for packets going to the CP, not to datapath traffic.

Procedure

1. Enter GigabitEthernet Interface Configuration mode:

   ```
   enable
   configure terminal
   interface GigabitEthernet {slot/port[/sub-port][-slot/port[/sub-port]][,...]}
   ```

   Note:

   If your platform supports channelization for 40 Gbps ports and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

2. Enable high-secure mode:

```
high-secure [port {slot/port[/sub-port][-slot/port[/sub-port]]
[,...]}] enable
```

Example

```
Switch:1> enable

Switch:1# configure terminal

Switch:1(config)# interface GigabitEthernet 1/16

Switch:1(config-if)# high-secure enable
```

Variable definitions

Use the data in the following table to use the **`high-secure`** command.

Variable	Value
port {slot/port[/sub-port][-slot/port[/sub-port]][,...]}	Specifies the port on which you want to enable high-secure mode. Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If your platform supports channelization for 40 Gbps ports and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.
enable	Enables the high-secure feature that blocks packets with illegal IP addresses. This flag is disabled by default. Use the no operator to remove this configuration. To configure this option to the default value, use the default operator with the command.

Configuring port lock

Configure port lock to administratively lock a port or ports to prevent other users from changing port parameters or modifying port action. You cannot modify a locked port until you unlock the port.

Procedure

1. Enter Global Configuration mode:

   ```
   enable

   configure terminal
   ```

2. Enable port lock globally:

   ```
   portlock enable
   ```

3. Enter GigabitEthernet Interface Configuration mode:

   ```
   interface gigabitethernet {slot/port[/sub-port][-slot/port[/sub-
   port]][,...]}
   ```

4. Lock a port:

```
lock [port {slot/port[/sub-port][-slot/port[/sub-port]][,...]}]
enable
```

Example

```
Switch:1> enable
```

```
Switch:1# configure terminal
```

Log on to GigabitEthernet Interface Configuration mode:

```
Switch:1(config)# interface GigabitEthernet 1/1
```

Lock port 1/1:

```
Switch:1(config-if)# lock port 1/1 enable
```

Unlock port 1/1:

```
Switch:1(config-if)# no lock port 1/1 enable
```

Variable definitions

Use the data in the following table to use the **interface gigabitethernet** command.

Variable	Value
{slot/port[/sub-port][-slot/port[/sub-port]][,...]}	Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If your platform supports channelization for 40 Gbps ports and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

Use the data in the following table to use the **lock port** command.

Variable	Value
{slot/port[/sub-port][-slot/port[/sub-port]][,...]}	Specifies the port you want to lock. Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If your platform supports channelization for 40 Gbps ports and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port. The default is disabled.

Security configuration using Enterprise Device Manager

Configure security information used on the control and data paths to protect the network from uncontrolled access to network resources.

For more information about how to configure passwords and access policies, see *Administering*.

Enabling port lock

About this task

Use the port lock feature to administratively lock a port or ports to prevent other users from changing port parameters or modifying port action. You cannot modify locked ports until you first unlock the port.

Procedure

1. In the navigation tree, open the following folders: **Configuration** > **Security** > **Control Path**.
2. Click **General**.
3. Click the **Port Lock** tab.
4. To enable port lock, select the **Enable** check box.
5. Click **Apply**.

Port Lock field descriptions

Use the data in the following table to use the **Port Lock** tab.

Name	Description
Enable	Activates the port lock feature. Clear this check box to unlock ports. The default is disabled.
LockedPorts	Lists the locked ports. Click the ellipsis (...) button to select the ports you want to lock or unlock.

Locking a port

Before you begin

- You must enable port lock before you lock or unlock a port.

About this task

Use the port lock feature to administratively lock a port or ports to prevent other users from changing port parameters or modifying port action. You cannot modify locked ports until you first unlock the port.

Procedure

1. In the navigation tree, open the following folders: **Configuration** > **Security** > **Control Path**.
2. Click **General**.
3. Click the **Port Lock** tab.
4. In the **LockedPorts** box, click the ellipsis **(...)** button.
5. Click the desired port or ports.
6. Click **Ok**.
7. In the Port Lock tab, click **Apply**.

Port Lock field descriptions

Use the data in the following table to use the **Port Lock** tab.

Name	Description
Enable	Activates the port lock feature. Clear this check box to unlock ports. The default is disabled.
LockedPorts	Lists the locked ports. Click the ellipsis (...) button to select the ports you want to lock or unlock.

Changing passwords

About this task

Configure new passwords for each access level, or change the logon or password for the different access levels of the system to prevent unauthorized access. After you receive the switch, use default passwords to initially access CLI. If you use Simple Network Management Protocol version 3 (SNMPv3), you can change passwords in encrypted format.

Procedure

1. In the navigation pane, expand the following folders: **Configuration** > **Security** > **Control Path**.
2. Click **General**.
3. Click the **CLI** tab.
4. Specify the username and password for the appropriate access level.
5. Click **Apply**.

CLI field descriptions

Use the data in the following table to use the **CLI** tab.

Name	Description
RWAUserName	Specifies the user name for the read-write-all CLI account.
RWAPassword	Specifies the password for the read-write-all CLI account.
RWEnable	Activates the read-write access level.
RWUserName	Specifies the user name for the read-write CLI account.
RWPassword	Specifies the password for the read-write CLI account.
RWL3Enable	Activates the read-write Layer 3 access level.
RWL3UserName	Specifies the user name for the Layer 3 read-write CLI account.
RWL3Password	Specifies the password for the Layer 3 read-write CLI account.
RWL2Enable	Activates the read-write Layer 2 access level.
RWL2UserName	Specifies the user name for the Layer 2 read-write CLI account.
RWL2Password	Specifies the password for the Layer 2 read-write CLI account.
RWL1Enable	Activates the read-write Layer 1 access level.
RWL1UserName	Specifies the user name for the Layer 1 read-write CLI account.
RWL1Password	Specifies the password for the Layer 1 read-write CLI account.
ROEnable	Activates the read/only CLI account level.
ROUserName	Specifies the user name for the read-only CLI account.
ROPassword	Specifies the password for the read-only CLI account.
MaxTelnetSessions	Indicates the maximum number of concurrent Telnet sessions (0–8). The default is 8.
MaxRloginSessions	Indicates the maximum number of concurrent Rlogin sessions (0–8). The default is 8.
Timeout	Indicates the number of seconds of inactivity for a Telnet or Rlogin session before automatic timeout and disconnect (30–65535 seconds). The default is 900.
NumAccessViolations	Indicates the number of CLI access violations detected by the system. This field is a read-only field.

Configuring directed broadcast on a VLAN

Configure directed broadcast on a VLAN to enable or disable directed broadcast traffic forwarding for an IP interface.

Procedure

1. In the navigation pane, expand the following folders: **Configuration** > **VLAN**.
2. Click **VLANs**.
3. Select the **Basic** tab.
4. Select a VLAN.
5. Click **IP**.
6. Click the **Direct Broadcast** tab.
7. Select **DirectBroadcastEnable**.

   ❗ **Important:**

   Configure multiple VLANs or IPs in the same subnet but in different systems simultaneously.
8. Click **Apply**.

Direct Broadcast field descriptions

Use the data in the following table to use the **Direct Broadcast** tab.

Name	Description
DirectBroadcastEnable	Specifies that an Isolated Routing Port (IRP) can forward directed broadcast traffic. A directed broadcast is a frame sent to the subnet broadcast address on a remote IP subnet. By disabling or suppressing directed broadcast on an interface, all frames sent to the subnet broadcast address for a local router interface are dropped. Disabling this function protects a host from possible denial of service (DoS) attacks. With the feature enabled, the Control Processor (CP) does not receive a copy of the directed broadcast. As a result, the system does not respond to a subnet broadcast ping sent from a remote subnet. The default is disabled.

Chapter 3: Extensible Authentication Protocol over LAN

Extensible Authentication Protocol over LAN (EAPoL) is a port-based network access control protocol. EAPoL provides security by preventing users from accessing network resources before they are authenticated. The EAPoL authentication feature prevents users from accessing a network to assume a valid identity and access confidential material or launch denial-of-service attacks.

You can use EAPoL to set up network access control on internal LANs and to exchange authentication information between an end station or server that connects to a switch and an authentication server (such as a RADIUS server). This security feature extends the benefits of remote authentication to internal LAN clients. For example, if a new client PC fails the authentication process, EAPoL prevents the new client PC from accessing the network.

Important:

The current release supports only one EAP Supplicant for each port. If the device receives frames from different MAC addresses on the same port, that system disables the port.

EAPoL terminology

The following section lists some components and terms used with EAPoL-based security.

- Supplicant—a device, such as a PC, that applies for access to the network.
- Authenticator—software on a switch that authorizes or rejects a Supplicant attached to the other end of a LAN segment.
    - Port Access Entity (PAE)—software that controls each port on the device. The PAE, which resides on the switch, supports the Authenticator functionality.
    - Controlled Port—any port on the device with EAPoL enabled.
- Authentication Server—a RADIUS server that provides AAA services to the authenticator.

EAPoL configuration considerations

The following section lists EAPoL configuration considerations.

- You must configure at least one EAPoL RADIUS server and shared secret fields.
- You cannot configure EAPoL on ports that are currently configured for the following:
    - Shared segments
    - MultiLink Trunking
- Change the authentication status to auto for each port that you want to control. The *auto* setting automatically authenticates the port according to the results of the RADIUS server. The default authentication setting for each port is *authorized*.

- You can connect only a single client on each port that is configured for EAPoL. (If you attempt to add additional clients on the EAPoL authorized port, the port goes to force-unauthorized mode).
- When multiple clients are authenticated on the same port, the priority of the latest incoming client is applied on the port, and this priority is retained until all the clients log out on that port.

Configuration process

The Authenticator facilitates the authentication exchanges that occur between the Supplicant and the Authentication Server. The Authenticator PORT ACCESS ENTITY (PAE) encapsulates the EAPoL message into a RADIUS packet, and then sends the packet to the Authentication Server.

The Authenticator manages the access to controlled port. At system initialization, or when a Supplicant initially connects to one of the controlled ports on the device, the system blocks data traffic of the Supplicant until gets authenticated. After the Authentication Server notifies the Authenticator PAE about the success or failure of the authentication, the Authenticator decides whether to permit/deny the traffic of client on controlled port.

NonEAPoL frames transmit according to the following rules:

- If authentication succeeds, the client blocked from accessing is allowed to the controlled port, which means the system allows all the incoming and outgoing traffic from that client through the port.
- If authentication fails, client is blocked from accessing, which means both incoming and outgoing traffic is not allowed to client.

The following figure illustrates how the switch, configured with EAPoL, reacts to a new network connection.

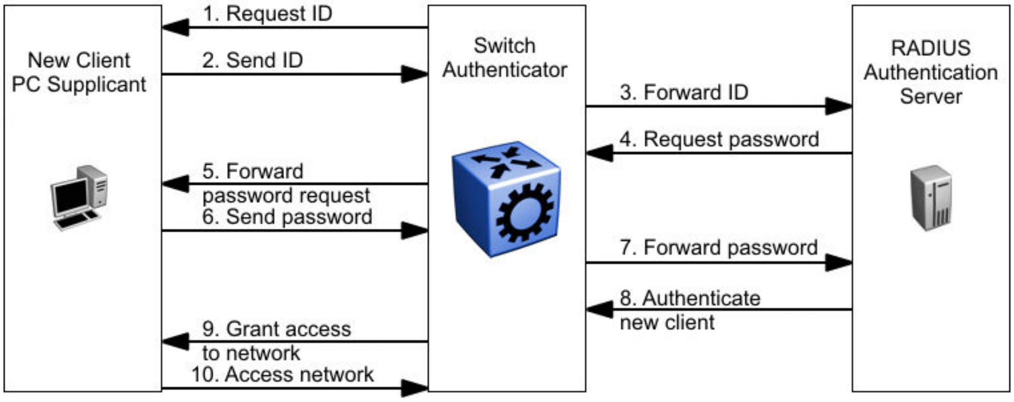


Figure 1: EAPoL configuration example

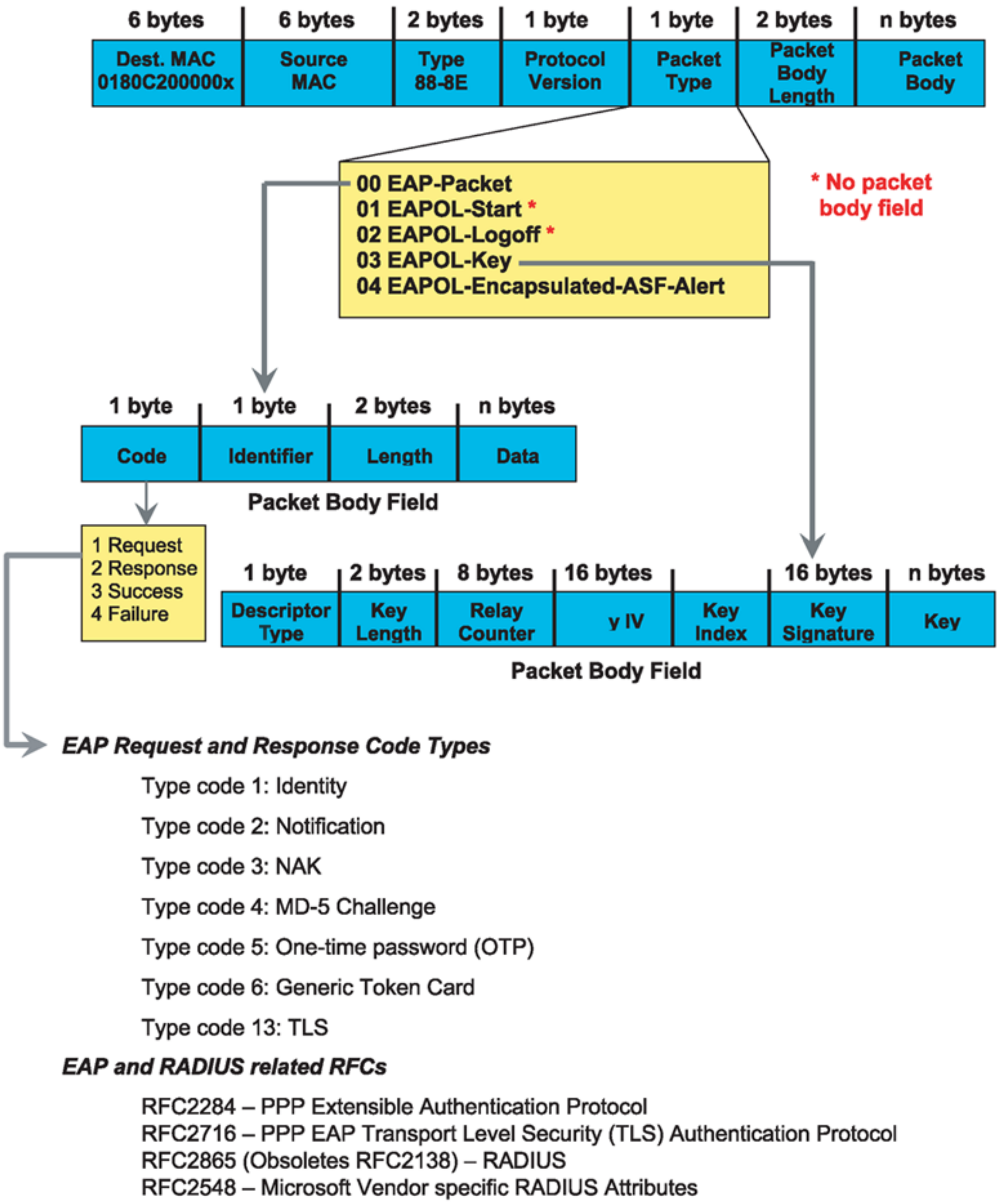
In Figure 1: EAPoL configuration example on page 29, the switch uses the following steps to authenticate a new client:

1. The switch detects a new connection on one of its EAPoL-enabled ports and requests a user ID from the new client PC.
2. The new client sends its user ID to the switch.
3. The switch uses RADIUS to forward the user ID to the RADIUS server.
4. The RADIUS server responds with a request for the password of the user.
5. The switch forwards the request from the RADIUS server to the new client.

6. The new client sends an encrypted password to the switch, within the EAPoL packet.
7. The switch forwards the EAPoL packet to the RADIUS server.
8. The RADIUS server authenticates the password.
9. The switch grants the new client access to the network.
10. The new client accesses the network.

If the RADIUS server cannot authenticate the new client, it denies the new client access to the network.

The following figure shows the Ethernet frames and the corresponding codes for EAPoL as specified by 802.1x.



EAP Request and Response Code Types

Type code 1: Identity

Type code 2: Notification

Type code 3: NAK

Type code 4: MD-5 Challenge

Type code 5: One-time password (OTP)

Type code 6: Generic Token Card

Type code 13: TLS

EAP and RADIUS related RFCs

RFC2284 – PPP Extensible Authentication Protocol
RFC2716 – PPP EAP Transport Level Security (TLS) Authentication Protocol
RFC2865 (Obsoletes RFC2138) – RADIUS
RFC2548 – Microsoft Vendor specific RADIUS Attributes

Figure 2: 802.1x Ethernet frame

The following figure shows the flow diagram for EAPoL on a switch.

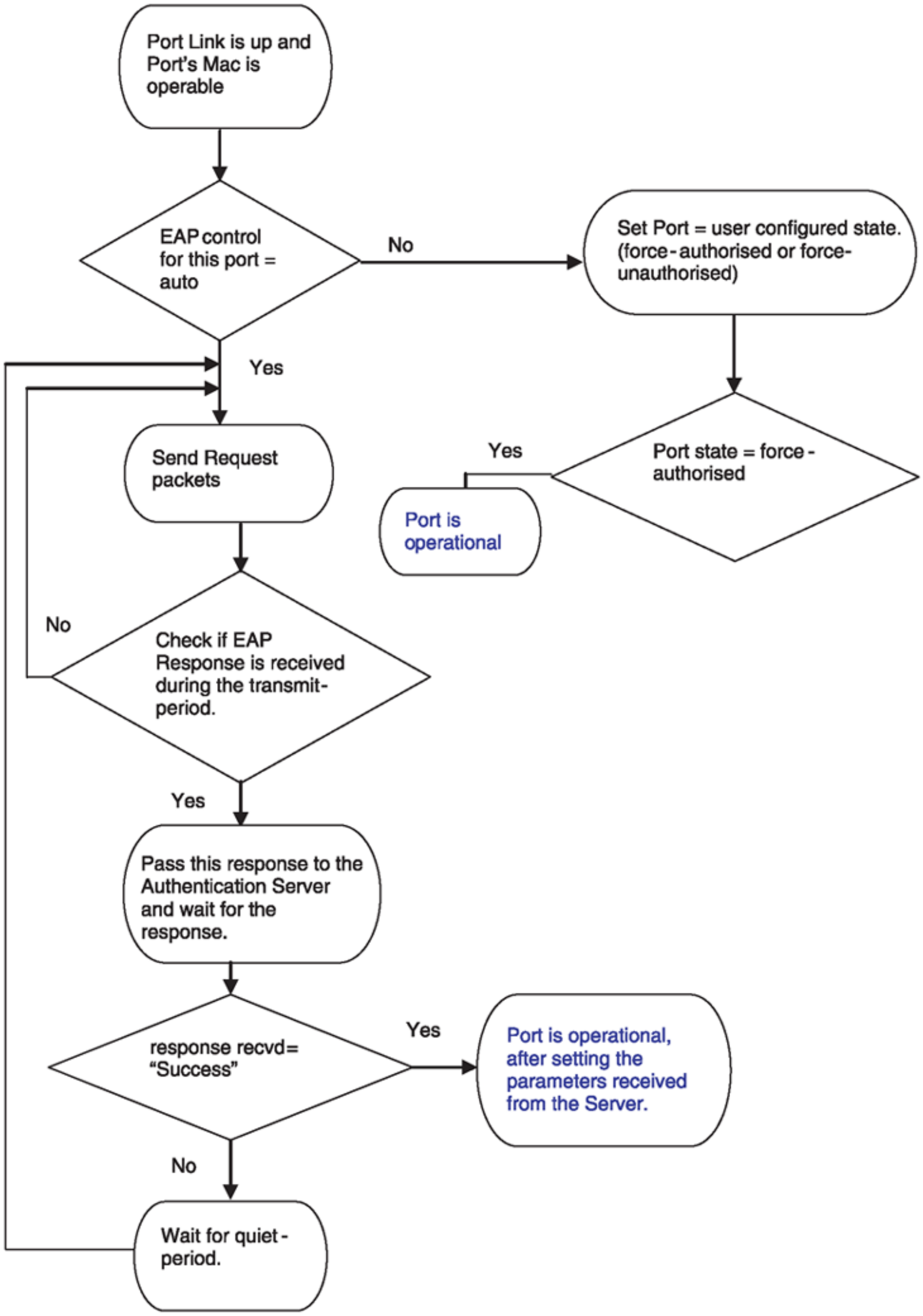

Port Link is up and Port's Mac is operable
EAP control for this port = auto
No
Set Port = user configured state. (force-authorised or force-unauthorised)
Yes
Port state = force-authorised
Yes
Port is operational
Send Request packets
No
Check if EAP Response is received during the transmit-period.
Yes
Pass this response to the Authentication Server and wait for the response.
response recvd= "Success"
Yes
Port is operational, after setting the parameters received from the Server.
No
Wait for quiet-period.

Figure 3: EAPoL flow diagram

System requirements

The following are the minimum system requirements for EAPoL:

- RADIUS server

- Client software that supports EAPoL

You must specify the RADIUS server that supports EAP as the primary RADIUS server for the switch. You must configure your switch for VLANs and EAPoL security.

If you configure EAPoL on a port, the following limitations apply:

- You cannot enable EAPoL on ports that belong to an MLT group.
- You cannot enable tagging on EAPoL enabled ports.
- You cannot add EAPoL-enabled ports to an MLT group.
- You can only configure one Supplicant for each EAPoL-enabled port.
- You cannot configure EAPoL on MLT/LACP interfaces.
- You cannot add EAPoL-enabled ports to an MLT/LACP group.
- You cannot enable VLACP on EAPoL enabled ports.
- You cannot make VLAN changes on EAPoL enabled ports other than RADIUS VLAN assignment.
- You cannot enable MACsec on EAPoL enabled ports.
- You cannot enable EAPoL on NNI interfaces.
- You cannot egress mirror an EAPoL PDU.
- Do not use EAPoL with a brouter port.
- Ping to and from services between nodes over the NNI will work even when it contains only EAPoL enabled ports with no authenticated clients on it.

EAPoL dynamic VLAN assignment

If you configure a RADIUS server to send a VLAN ID in the Access-Accept response, the EAPOL feature dynamically changes the VLAN configuration of the port by adding the port to the specified VLAN.

EAPoL dynamic VLAN assignment affects the following VLAN configuration values:

- Port membership
- Port priority

When you disable EAPoL on a port that was previously authorized, VLAN configuration values for that port are restored directly from the nonvolatile random access memory (NVRAM) of the device.

The following exception applies to dynamic VLAN assignments:

- The dynamic VLAN configuration values assigned by EAPoL are not stored in the switch NVRAM.

You can set up your Authentication Server (RADIUS server) for EAPoL dynamic VLAN assignments. You can use the Authentication Server to configure user-specific settings for VLAN memberships and port priority.

When you log on to a system that is configured for EAPoL authentication, the Authentication Server recognizes your user ID and notifies the device to assign preconfigured (user-specific) VLAN membership and port priorities to the device. The configuration settings are based on configuration parameters that were customized for your user ID and previously stored on the Authentication Server.

Note:

Static entries like IGMP, ARP, FDB configured on a port of an VLAN interface, will not be retained if the port is assigned a same VLAN by the RADIUS server and the client authenticated on the port gets disconnected or unauthenticated.

RADIUS return attributes supported for EAPoL

The switch uses the RADIUS tunnel attributes to place a port into a particular VLAN to support dynamic VLAN switching based on authentication.

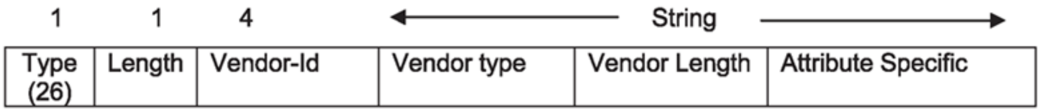
The RADIUS server indicates the desired VLAN by including the tunnel attribute within the Access-Accept message. RADIUS uses the following tunnel attributes:

- Tunnel-Type = VLAN (13)
- Tunnel-Medium-Type = 802
- Tunnel-Private-Group-ID = VLAN ID

The VLAN ID is 12 bits, uses a value from <*1-4059*>, and is encoded as a string.

In addition, you can set up the RADIUS server to send a vendor-specific attribute to configure port priority. You can assign the switch Supplicant port a QoS value from 0 to 6.

The following figure shows the RADIUS vendor-specific frame format.



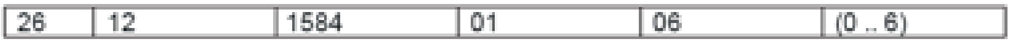
1	1	4	← String →		
Type (26)	Length	Vendor-Id	Vendor type	Vendor Length	Attribute Specific

Figure 4: RADIUS vendor-specific frame format

The following list provides the switch Port Priority frame format:

- vendor specific type = 26
- length = 12
- vendor-id = 1584
- string = vendor type = 1 + vendor length = 6 + attribute specific = priority

The following figure shows the port priority frame format.



26	12	1584	01	06	(0 .. 6)

Figure 5: Port priority frame format

RADIUS configuration prerequisites for EAPoL

Connect the RADIUS server to a force-authorized port. This ensures that the port is always available and not tied to whether or not the device is EAPoL-enabled. To set up the Authentication Server, set the following Return List attributes for all user configurations (for more information, see your Authentication Server documentation):

- VLAN membership attributes
  - Tunnel-Type: value 13, Tunnel-Type-VLAN

- Tunnel-Medium-Type: value 6, Tunnel-Medium-Type-802
- Tunnel-Private-Group-ID: ASCII value 1 to 4059 (this value identifies the specified VLAN)

- Port priority (vendor-specific) attributes
  - Vendor ID: value 1584
  - Attribute Number: value 1, Port Priority
  - Attribute Value: value 0 (zero) to 6 (this value indicates the port priority value assigned to the specified user)

Important:

You need to configure these attributes only if you require Dynamic VLAN membership or Dynamic Port priority.

RADIUS accounting for EAPoL

The switch provides the ability to account EAPoL sessions using the RADIUS accounting protocol. A user session is defined as the interval between the instance at which a user is successfully authenticated (port moves to authorized state) and the instance at which the port moves out of the authorized state.

The following table summarizes the accounting events and information logged.

Table 2: Summary of accounting events and information logged

Event	Radius attributes	Description
User is authenticated by EAPoL	Acct-Status-Type	Start
	Nas-IP-Address	IP address to represent the switch
	Nas-Port	Port number on which the user is EAPoL authorized
	Acct-Session-ID	Unique string representing the session
	User-Name	EAPoL user name
User logs off	Acct-Status-Type	Stop
	Nas-IP-Address	IP address to represent the switch
	Nas-Port	Port number on which the user is EAPoL unauthorized
	Acct-Session-ID	Unique string representing the session
	User-Name	EAPoL user name
	Acct-Input-Octets	Number of octets input to the port during the session
	Acct-Output-Octets	Number of octets output to the port during the session
	Acct-Terminate-Cause	Reason for terminating user session. For more information about the mapping of 802.1x session termination cause to

Table continues…

Event	Radius attributes	Description
		RADIUS accounting attribute, see Table 3: 802.1x session termination mapping on page 36.
	Acct-Session-Time	Session interval

The following table describes the mapping of the causes of 802.1x session terminations to the corresponding RADIUS accounting attributes.

Table 3: 802.1x session termination mapping

IEEE 802.1Xdot1xAuthSessionTerminateCause Value	RADIUSAcct-Terminate-Cause Value
supplicantLogoff(1)	User Request (1)
portFailure(2)	Lost Carrier (2)
supplicantRestart(3)	Supplicant Restart (19)
reauthFailed(4)	Reauthentication Failure (20)
authControlForceUnauth(5)	Admin Reset (6)
portReInit(6)	Port Reinitialized (21)
portAdminDisabled(7)	Port Administratively Disabled (22)
notTerminatedYet(999)	—

Non-EAP hosts on EAP-enabled ports

For an EAPOL-enabled port configured for non-EAPOL host support, devices with MAC addresses getting authenticated are allowed access to the port.

The switch allows the following types of non-EAPOL users:

- Non-EAPOL hosts whose MAC addresses are authenticated by RADIUS.

Support for non-EAPOL hosts on EAPOL-enabled ports is primarily intended to accommodate printers and other passive devices sharing a hub with EAPOL clients.

Support for non-EAPOL hosts on EAPOL-enabled ports includes the following features:

- Authenticated non-EAPOL clients are hosts that satisfy one of the following criteria:
  - Host MAC address is authenticated by RADIUS.
- Non-EAPOL hosts are allowed even if no authenticated EAPOL hosts exist on the port.
- When a new host is seen on the port, non-EAPOL authentication is performed as follows:
  - The switch generates a <username, password> pair, which it forwards to the network RADIUS server for authentication.

Non-EAPOL MAC RADIUS authentication

For RADIUS authentication of a non-EAPOL host MAC address, the switch generates a <username, password> pair as follows:

- The username is the non-EAPOL MAC address in string format.

- The password is a string that combines the switch IP address, MAC address, port number and user-configurable key string. If padding option is enabled, the system will specify a dot(.) for every missing parameter. IP address is represented by three decimal characters per octet.

Important:

Follow these Global Configuration examples to select a password format that combines one or more of these three elements:

- Padding enabled , password = 010010011253..05. (when the switch IP address and port are used).
- Padding enabled, password = 010010011253… (when only the switch IP address is used).
- No padding (default option). Password = 000011220001 (when only the user's MAC address is used).

The following example illustrates the <username, password> pair format with no padding enabled and using the IP address, MAC address, and key-string as the password.

```
switch IP address = 10.10.11.253
non-EAP host MAC address = 00 C0 C1 C2 C3 C4
port = 25
Key-String = abcdef
```

- username = 00C0C1C2C3C4
- password = 010010011253.00C0C1C2C3C4.25.abcdef

Use the command **`show eapol system`** to verify the formatting.

```
Switch:1(config)#show eapol system

================================================================================
                                  Eapol System
================================================================================
                      eap : enabled
          non-eap-pwd-fmt : ip-addr.mac-address.abcdef
      non-eap-pwd-fmt key : abcdef
  non-eap-pwd-fmt padding : disabled
```

Non-EAP client re-authentication

The Non-EAP (NEAP) client re-authentication feature supports the re-authentication of non-EAP clients at defined intervals.

When you enable NEAP client re-authentication, an authenticated NEAP client is only removed from the authenticated client list if you remove the client account from the RADIUS server, or if you clear the NEAP authenticated client from the switch.

If an authenticated NEAP client does not generate traffic on the network, the system removes the MAC address for that client from the MAC address table when MAC ages out. Although the client MAC address does not appear in the MAC Address table, the client can appear as an authenticated client.

If you enable NEAP client re-authentication and the RADIUS server that the switch connects to becomes unavailable, the system clears all authenticated NEAP and removes those clients from the switch NEAP client list.

You cannot authenticate one NEAP client on more than one switch port simultaneously. If you connect NEAP clients to a switch port through a hub, those clients are authenticated on that switch port. If you disconnect a NEAP client from the hub and connect it directly to another switch port, the client is authenticated on the new port and its authentication is removed from the port to which the hub is connected.

MAC move for authenticated Non-EAP clients

When you move a Non-EAP client that is authenticated on a specific port, to another port on which EAPoL or Non-EAP is enabled, MAC move of the client to the new port does not automatically happen. This is as designed.

As a workaround, do *one* of the following:

- Clear the non-EAP session on the port that the client is first authenticated on, before you move the client to another port.
- Create a VLAN on the switch with the same VLAN ID as that dynamically assigned by the RADIUS server during client authentication. Use the command **`vlan create <2-4059> type port-mstprstp <0-63>`**. Ensure that the new port is a member of this VLAN.

EAPoL configuration using CLI

EAPoL uses RADIUS protocol for EAPoL-authorized logons. RADIUS supports IPv4 and IPv6 addresses, with no difference in functionality or configuration.

Before configuring your device, you must configure at least one EAPoL RADIUS server and shared secret fields.

You cannot configure EAPoL on ports that are currently configured for:

- Shared segments
- MultiLink Turnking (MLT)

Change the status of each port that you want to be controlled to auto. The auto setting automatically authenticates the port according to the results of the RADIUS server. The default authentication setting for each port is authorized.

You can connect only a single client on each port configured for EAPoL. If you attempt to add additional clients on the EAPoL authorized port, then the system denies access to the new client and displays a warning message.

Globally enabling EAPoL on the device

Enable EAPoL globally on the switch before you enable it on a port or interface.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Globally configure EAPoL:

   ```
   eapol enable
   ```

Example

```
Switch:1> enable

Switch:1# configure terminal

Switch:1(config)# eapol enable
```

Configuring EAPoL on an interface

Configure EAPoL on an interface.

Before you begin

- EAPoL must be globally enabled.

About this task

When you configure a port with the EAP status of auto (Authorization depends on result of EAP authentication), only one supplicant is allowed on this port. Multiple EAP supplicants are not allowed on the same physical switch port.

Procedure

1. Enter GigabitEthernet Interface Configuration mode:

   ```
   enable

   configure terminal

   interface GigabitEthernet {slot/port[/sub-port][-slot/port[/sub-port]][,...]}
   ```

   Note:

   If your platform supports channelization for 40 Gbps ports and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

2. Enable EAPoL on an interface:

   ```
   eapol status {authorized|auto}
   ```

3. Disable EAPoL on on interface:

   ```
   no eapol status
   ```

Example

Enable EAPoL on an interface:

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#interface GigabitEthernet 1/2
Switch:1(config-if)# eapol status auto
```

Disable EAPoL on an interface:

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#interface GigabitEthernet 1/2
Switch:1(config-if)# no eapol status
```

Variable definitions

Use the data in the following table to use the **`eapol status`** command.

Variable	Value
authorized	Specifies that the port is always authorized. The default value is authorized.
auto	Specifies that port authorization depends on the results of the EAPoL authentication by the RADIUS server. The default value is authorized.

Configuring EAPoL on a port

Configure EAPoL on a specific port when you do not want to apply EAPoL to all of the switch ports.

Procedure

1. Enter GigabitEthernet Interface Configuration mode:

   ```
   enable
   
   configure terminal
   
   interface GigabitEthernet {slot/port[/sub-port][-slot/port[/sub-port]][,...]}
   ```

   Note:

   If your platform supports channelization for 40 Gbps ports and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

2. Configure the maximum EAP requests sent to the supplicant before timing out the session:

   ```
   eapol port {slot/port[/sub-port][-slot/port[/sub-port]][,...]} max-request <1-10>
   ```

3. Configure the time interval between authentication failure and the start of a new authentication:

   ```
   eapol port {slot/port[/sub-port][-slot/port[/sub-port]][,...]} quiet-interval <1-65535>
   ```

4. Enable reauthentication:

   ```
   eapol port {slot/port[/sub-port][-slot/port[/sub-port]][,...]} re-authentication enable
   ```

5. Configure the time interval between successive authentications:

```
eapol port {slot/port[/sub-port][-slot/port[/sub-port]][,...]} re-
authentication-period <1-65535>
```

6. Configure the EAP authentication status:

```
eapol port {slot/port[/sub-port][-slot/port[/sub-port]][,...]}
status {authorized|auto}
```

Example

Configure the maximum EAP requests sent to the supplicant before timing out the session:

Note:

Slot and port information can differ depending on hardware platform. See *Installing* for specific hardware information.

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#interface GigabitEthernet 1/2
Switch:1(config-if)#eapol max-request 10
Switch:1(config-if)#eapol port 1/2 quiet-interval 500
```

Variable definitions

Use the data in the following table to use the **eapol port** command.

Variable	Value
{slot/port[/sub-port][-slot/port[/sub-port]][,...]}	Specifies the port or list of ports used by EAPoL. Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If your platform supports channelization for 40 Gbps ports and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.
max-request <1-10>	Specifies the maximum EAP requests sent to the supplicant before timing out the session. The default is 2.
quiet-interval <1-65535>	Specifies the time interval in seconds between the authentication failure and start of a new authentication. The default is 60.
re-authentication enable	Enables reauthentication of an existing supplicant at a specified time interval.
re-authentication-period <1-65535>	Specifies the time interval in seconds between successive reauthentications. The default is 3600 (1 hour).
status {authorized|auto}	Specifies the desired EAP authentication status for this port.

Configuring an EAPoL-enabled RADIUS server

The switch uses RADIUS servers for authentication and accounting services. Use the no form to delete a RADIUS server.

Before you begin

- You must enable EAPoL globally.

About this task

The RADIUS server uses the secret key to validate users.

RADIUS supports IPv4 and IPv6 addresses, with no difference in functionality or configuration.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Add an EAPoL-enabled RADIUS server:

   ```
   radius server host WORD <0-46> used-by eapol acct-enable
   ```

   ```
   radius server host WORD <0-46> used-by eapol acct-port <1-65536>
   ```

   ```
   radius server host WORD <0-46> used-by eapol enable
   ```

   ```
   radius server host WORD <0-46> used-by eapol key WORD<0-20>
   ```

   ```
   radius server host WORD <0-46> used-by eapol port <1-65536>
   ```

   ```
   radius server host WORD <0-46> used-by eapol priority <1-10>
   ```

   ```
   radius server host WORD <0-46> used-by eapol retry <0-6>
   ```

   ```
   radius server host WORD <0-46> used-by eapol source-ip WORD <0-46>
   ```

   ```
   radius server host WORD <0-46> used-by eapol timeout <1-20>
   ```

   By default, the switch uses RADIUS UDP port 1812 for authentication, and port 1813 for accounting. You can change the port numbers or other RADIUS server options.

Example

```
Switch:1> enable
```

```
Switch:1# configure terminal
```

Add an EAPoL RADIUS server:

```
Switch:1(config)# radius server host fe80:0:0:0:21b:4fff:fe5e:73fd key
radiustest used-by eapol
```

Variable definitions

Use the data in the following table to configure an EAPoL-enabled RADIUS server with the **radius server host** command.

Variable	Value
host *WORD<0–46>*	Specifies the IP address of the selected server. RADIUS supports IPv4 and IPv6 addresses, with no difference in functionality or configuration.
WORD<0-20>	Specifies the secret key, which is a string of up to 20 characters.

Use the data in the following table to use optional arguments of the **`radius server host`** command.

Variable	Value
port *<1-65535>*	Specifies the port ID number.
priority *<1-10>*	Specifies the priority number. The lowest number is the highest priority.
retry *<0-6>*	Specifies the retry count of the account.
timeout *<1-10>*	Specifies the timeout of the server. The default is 30.
enable	Enables the functions used by the RADIUS server host.
acct-port *<1-65536>*	Specifies the port account.
acct-enable	Enables the account.
source-ip *WORD<0–46>*	Specifies the IP source. RADIUS supports IPv4 and IPv6 addresses, with no difference in functionality or configuration.

Configuring the switch for EAPoL and RADIUS

Perform the following procedure to configure the switch for EAPoL and RADIUS.

About this task

You must configure the switch, through which user-based-policy (UBP) users connect to communicate with the RADIUS server to exchange EAPoL authentication information, as well as user role information. You must specify the IP address of the RADIUS server, as well as the shared secret (a password that authenticates the device with the RADIUS server as an EAPoL access point). You must enable EAPoL globally on each device, and you must configure EAPoL authentication on each device port, through which EAPoL/UBP users connect.

RADIUS supports IPv4 and IPv6 addresses, with no difference in functionality or configuration.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Create a RADIUS server that is used by EAPoL:

   ```
   radius server host WORD <0–46> key WORD<0-20> used-by eapol
   ```

3. Log on to the Interface Configuration mode:

```
interface vlan <1-4059>
```

4. Enable the device to communicate through EAPoL:

   ```
   eapol enable
   ```

5. Exit from VLAN interface mode:

   ```
   exit
   ```

6. Enter Interface Configuration mode:

   ```
   interface GigabitEthernet {slot/port[/sub-port][-slot/port[/sub-port]][,...]}
   ```

7. Enable device ports for EAPoL authentication:

   ```
   eapol port {slot/port[/sub-port][-slot/port[/sub-port]][,...]} status auto
   ```

8. Enable periodic supplicant re-authenticating:

   ```
   eapol port {slot/port[/sub-port][-slot/port[/sub-port]][,...]} re-authentication enable
   ```

9. Save your changes:

   ```
   save config
   ```

Example

```
Switch:1> enable
```

```
Switch:1# configure terminal
```

Create a RADIUS server that is used by EAPoL:

```
Switch:1(config)# radius server host fe90:0:0:0:21b:4eee:fe5e:75fd key radiustest used-by eapol
```

```
Switch:1(config)# interface vlan 2
```

Enable the device to communicate through EAPoL:

```
Switch:1(config-if)# eapol enable
```

Save your changes:

```
Switch:1(config-if)# save config
```

Variable definitions

Use the data in the following table to use the **radius server host WORD<0-46> usedby eapol** command.

Variable	Value
host *WORD<0–46>*	Specifies the IP address of the selected server.

Table continues…

Variable	Value
	This address tells the device where to find the RADIUS server, from which it obtains EAPoL authentication and user role information. RADIUS supports IPv4 and IPv6 addresses, with no difference in functionality or configuration.
key *WORD<0-20>*	Specifies the shared secret key that you use for RADIUS authentication. The shared secret is held in common by the RADIUS server and all EAPoL-enabled devices in your network. It authenticates each device with the RADIUS server as an EAPoL access point. When you configure your RADIUS server, you must configure the same shared secret value as you specify here.

Changing the authentication status of a port

The switch authorizes ports by default, which means that the ports are always authorized and are not authenticated by the RADIUS server.

You can also make the ports controlled so that they are dependent on being authorized by the Radius Server when you globally enable EAPoL (auto).

Procedure

1. Enter GigabitEthernet Interface Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

   ```
   interface GigabitEthernet {slot/port[/sub-port][-slot/port[/sub-port]][,...]}
   ```

   Note:

   If your platform supports channelization for 40 Gbps ports and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

2. Configure the authorization status of a port:

   ```
   eapol status {authorized|auto}
   ```

Example

```
Switch:1> enable
```

```
Switch:1# configure terminal
```

```
Switch:1(config)# interface GigabitEthernet 3/1
```

Configure the authorization status of a port:

```
Switch:1(config-if)# eapol status auto
```

Variable definitions

Use the data in the following table to use the **`eapol status`** command.

Variable	Value
authorized	Specifies that the port is always authorized. The default value is authorized.
auto	Specifies that port authorization depends on the results of the EAPoL authentication by the RADIUS server. The default value is authorized.

Deleting an EAPoL-enabled RADIUS server

Delete an EAPoL-enabled RADIUS server if you want to remove the server.

About this task

RADIUS supports IPv4 and IPv6 addresses, with no difference in functionality or configuration.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Delete an EAPoL-enabled RADIUS server:

   ```
   no radius server host WORD<0–46> used-by eapol
   ```

Example

```
Switch:1> enable

Switch:1# configure terminal

Switch:1(config)# no radius server host fe79:0:0:0:21d:4fdf:fe5e:73fd
used-by eapol
```

Variable definitions

Use the data in the following table to use the **`radius server host WORD<0–46> usedby eapol`** command.

Variable	Value
host *WORD<0–46>*	Specifies the IP address of the selected server. This address tells the device where to find the RADIUS server, from which it obtains EAPoL authentication and user role information. RADIUS supports IPv4 and IPv6 addresses, with no difference in functionality or configuration.

Table continues…

Variable	Value
key *WORD<0-20>*	Specifies the shared secret key that you use for RADIUS authentication. The shared secret is held in common by the RADIUS server and all EAPoL-enabled devices in your network. It authenticates each device with the RADIUS server as an EAPoL access point. When you configure your RADIUS server, you must configure the same shared secret value as you specify here.

Displaying the current EAPOL-based security status

Use the following procedure to display the status of the EAPOL-based security.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. Display the current EAPoL-based security status:

   ```
   show eapol auth-stats interface [gigabitEthernet {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}]
   ```

   ```
   show eapol multihost non-eap-mac status [vlan <1-4059>] [{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}]
   ```

   ```
   show eapol port {interface [gigabitEthernet {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}] | {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}}
   ```

   ```
   show eapol session-stats interface [gigabitEthernet {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}]
   ```

   ```
   show eapol status interface [vlan <1-4059>] [gigabitEthernet {slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}]
   ```

   ```
   show eapol system
   ```

Example

```
Switch:#enable
Switch:1#show eapol system
================================================================================
                                  Eapol System
================================================================================
                      eap : enabled
          non-eap-pwd-fmt : ip-addr.mac-addr.port-number
      non-eap-pwd-fmt key :
  non-eap-pwd-fmt padding : disabled
--------------------------------------------------------------------------------
```

Variable definitions

Use the data in the following table to use the **show eapol** command.

Variable	Value
auth-stats [gigabitEthernet *{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}*]	Displays the authentication statistics interface. **Note:** auth-stats [gigabitEthernet *{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}* is useful only for EAP supplicants. The command output changes only when the EAP supplicant tries to access the network.
multihost non-eap-mac status [vlan <*1-4059*>] [*{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}*]	Displays EAPoL multihost configuration.
port {interface [gigabitEthernet *{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}*] | *{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}*}	Specifies the ports to display. If no port is entered, all ports are displayed.
session-stats interface [gigabitEthernet *{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}*]	Displays the authentication session statistics interface.
status interface [vlan <*1-4059*>] [gigabitEthernet *{slot/port[/sub-port] [-slot/port[/sub-port]] [,...]}*]	Displays the port EAP operation statistics.
system	Displays EAPoL settings.

Configuring the format of the RADIUS password attribute when authenticating non-EAP MAC addresses using RADIUS

Use the following procedure to configure the format of the RADIUS password when authenticating non-EAP MAC addresses using RADIUS.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Configure the RADUIS password format:

   ```
   eapol multihost non-eap-pwd-fmt {[ip-addr] [key WORD<1-32>] [mac-addr] [padding] [port-number]}
   ```

Variable definitions

Use the data in the following table to use the **`eapol multihost non-eap-pwd-fmt`** command.

Variable	Value
ip-addr	Management ip-address of the switch.
key WORD<1-32>	Key value used for non-eap password format.
mac-addr	Mac-Address of the client.
padding	Includes a dot in the RADIUS password for every missing parameter.
port-number	Index of the port on which MAC is received.

Note:

To derive the port number for an interface, use the command **`show interfaces gigabit [{slot/port[/sub-port][-slot/port[/sub-port]][,...]}]`** .

If you configure interface 1/6 on the product, to derive the port-number for this interface, use the command **`show interfaces gigabitEthernet 1/6`**. From this command, you can ascertain that port number used in the NEAP password is 197.

Slot and port information can differ depending on hardware platform. See *Installing* for specific hardware information.

```
Switch:1(config)# show interfaces gigabitEthernet 1/6

==========================================================================================
                                      Port Interface
==========================================================================================
PORT                            LINK  PORT          PHYSICAL          STATUS
NUM      INDEX DESCRIPTION      TRAP  LOCK     MTU  ADDRESS           ADMIN  OPERATE
------------------------------------------------------------------------------------------
1/6      197   1000BaseTX       true  false    1950 f8:15:47:e1:dd:05 up     up
```

Enabling RADIUS authentication of non-EAPoL hosts on EAPoL enabled ports

For RADIUS authentication of non-EAPOL hosts on EAPOL-enabled ports, you must enable EAPOL globally on the switch and then enable non-EAPOL hosts on the local interface.

Procedure

1. Enter GigabitEthernet Interface Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

   ```
   interface GigabitEthernet {slot/port[/sub-port][-slot/port[/sub-port]][,...]}
   ```

   Note:

   If your platform supports channelization for 40 Gbps ports and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

2. Enable RADIUS authentication of non-EAPoL hosts on the local interface:

   ```
   eapol multihost radius-non-eap-enable
   ```

EAPoL configuration using Enterprise Device Manager

EAPoL uses RADIUS protocol for EAPoL-authorized logons. RADIUS supports IPv4 and IPv6 addresses with no difference in functionality or configuration in all but the following case. When adding a RADIUS server in Enterprise Device Manager (EDM) or modifying a RADIUS configuration in EDM, you must specify if the address type is an IPv4 or an IPv6 address.

Before you begin

- Before configuring your device, you must configure at least one EAPoL RADIUS server and shared secret fields.
- You cannot configure EAPoL on ports that are currently configured for:
  - Shared segments
  - MultiLink Trunking (MLT)
- Change the status of each port that you want to be controlled to auto. For more information on changing the status, see Configuring EAPoL on a port on page 51. The auto setting automatically authenticates the port according to the results of the RADIUS server. The default authentication setting for each port is force-authorized.
- You can connect only a single client on each port configured for EAPoL. If you attempt to add additional clients on the EAPoL authorized port, the client traffic will be blocked from the switch till mac-ageing occurs for that client.

Globally configuring EAPoL on the server

About this task

Globally enable or disable EAPoL on the server. By default, EAPoL is disabled. This feature sets all controlled ports on the server as EAPoL-enabled.

Procedure

1. In the navigation tree, expand the following folders: **Configuration** > **Security** > **Data Path**.
2. Click **802.1x - EAPOL**.
3. Click the **Global** tab.
4. From the AccessControl options, select **enable**.
5. **(Optional)** Select the appropriate **NonEapRadiusPwdAttrFmt** check boxes to configure the format of the RADIUS password when authenticating non-EAP MAC addresses using RADIUS.
6. **(Optional)** Enter the key string in the **NonNonEapRadiusPwdAttkeystring** field.

7. Click **Apply**.

Global field descriptions

Use the data in the following table to use the **Global** tab.

Name	Description
EapolVersion	Displays the Eapol version on the switch.
AccessControl	Enables system authentication control. EAPol is enabled by default.
NonEapRadiusPwdAttrFmt	Specifies the password attribute format for non EAPol RADIUS authentication. • ipAdd: Specifies IP address. • macAddr: Specifies MAC address. • portNumber: Specifies port number • padding: Specifies padding.
NonEapRadiusPwdAttrKeyString	Specifies the attribute key string for non EAPol RADIUS password. The range is 0– 32 characters.

Configuring EAPoL on a port

About this task

Configure EAPoL or change the authentication status on one or more ports.

Ports are force-authorized by default. Force-authorized ports are always authorized and are not authenticated by the RADIUS server. You can change this setting so that the ports are always unauthorized.

Procedure

1. In the Device Physical View tab, select the port you need to configure.
2. In the navigation tree, expand the following folders: **Configuration** > **Edit** > **Port**.
3. Click **General**.
4. Click the **EAPOL** tab.
5. **(Optional)** Select the **PortInitialize** check box to initialize EAPoL authentication on this port.
6. **(Optional)** Select the **AllowNonEapHost** check box to allow hosts that do not participate in 802.1X authentication to get network access.
7. Select the **Status** option as **auto** or **forceAuthorized**.
8. Select the **ReAuthEnabled** field.
9. In the **QuietPeriod** field, type the time interval.
10. In the **ReauthPeriod** field, type the time between reauthentication.

11. In the **RetryMax** field, type the number of times.
12. Click **Apply**.

EAPoL field descriptions

Use the data in the following table to use the **EAPoL** tab.

Name	Description
PortInitialize	Initializes EAPoL authentication on this port. After the port initializes, this field reverts to its default, which is disabled.
PortCapabilities	Displays the capabilities of the Port Access Entity (PAE) associated with the port. This parameter indicates whether Authenticator functionality, supplicant functionality, both, or neither, is supported by the PAE of the port. The following capabilities are supported by the PAE of the port: • suppImplemented: A Port Access Controller Protocol (PACP) Extensible Authentication Protocol (EAP) supplicant functions are implemented. • authImplemented: A Port Access Controller Protocol (PACP) Extensible Authentication Protocol (EAP) authenticator functions are implemented. • mkaImplemented: The KaY MKA functions are implemented in this. • macsecImplemented: The MACsec functions in the Controlled Port are implemented in this PAE. • announcementsImplemented: The EAPOL announcement can be sent. • listenerImplemented: This PAE can receive EAPOL announcement. • virtualPortsImplemented: Virtual Port functions are implemented.
PortVirtualPortsEnable	Displays the status of the Virtual Ports function for the real port as True or False.
PortCurrentVirtualPorts	Displays the current number of virtual ports running in the port
PortAuthenticatorEnable	Displays the status of the Authenticator function in the Port Access Entity (PAE) as True or False.
PortSupplicantEnable	Displays the Supplicant function in the Port Access Entity (PAE) as True or False.
AllowNonEapHost	Enables the system to allow hosts that do not participate in 802.1X authentication to get network access. The default is disabled.

Table continues…

Name	Description
Status	Configures the authentication status for this port. The default is forceAuthorized. • auto: enables the EAPoL authentication process by sending the EAPoL request messages to the RADIUS server. • forceAuthorized: disables the EAPoL authentication and puts the port into force-full authorized mode.
Authenticator configuration	Displays the current Authenticator Port Access Entity (PAE) state. The states are: • authenticate • authenticated • Failed
ReAuthEnabled	Reauthenticates an existing supplicant at the time interval specified in ReAuthPeriod. The default is disabled.
QuietPeriod	Configures the time interval (in seconds) between authentication failure and the start of a new authentication. The allowed range is 1–65535; the default is 60.
ReAuthPeriod	Reauthenticates an existing supplicant at the time interval specified in ReAuthPeriod. Specifies the time interval in seconds between successive reauthentications. The allowed range is 1–2147483647; the default is 3600 (1 hour)
RetryMax	Specifies the maximum Extensible Authentication Protocol (EAP) requests sent to the supplicant before timing out the session. The default is 2.
RetryCount	Specifies the maximum number of retries attempted.

Showing the Port Access Entity Port table

About this task

Use the Port Access Entity (PAE) Port Table to display system-level information for each port the PAE supports. An entry appears in this table for each port of this system.

Procedure

1. In the navigation tree, expand the following folders: **Configuration** > **Security** > **Data Path**.
2. Click **802.1x - EAPOL**.
3. Click the **EAP Security** tab.

EAP Security field descriptions

Use the data in the following table to use the **EAP Security** tab.

Name	Description
PortNumber	Indicates the port number associated with this port.
PortInitialize	Indicates the initialization control for this port. Configure this attribute true to initialize the port. The attribute value reverts to false when initialization is complete.
PortCapabilties	Indicates the PAE functionality that this port supports and that can be managed through this MIB. • dot1xPaePortAuthCapable(0)—Authenticator functions are supported. • dot1xPaePortSuppCapable(1)—Supplicant functions are supported.
PortVirtualPortsEnable	Displays the status of the Virtual Ports function for the real port as True or False.
PortCurrentVirtualPorts	Displays the current number of virtual ports running in the port
PortAuthenticatorEnable	Displays the status of the Authenticator function in the Port Access Entity (PAE) as True or False.
PortSupplicantEnable	Displays the Supplicant function in the Port Access Entity (PAE) as True or False.
AllowNonEapHost	Displays the status if the system is enabled to allow hosts that do not participate in 802.1X authentication to get network access.
Status	Displays the authentication status for this port. The default is forceAuthorized.

Showing EAPoL Authentication

About this task

Use the Authenticator Configuration table to display configuration objects for the Authenticator PAE associated with each port.

Procedure

1. In the navigation pane, expand the following folders: **Configuration** > **Security** > **Data Path**.
2. Click **802.1x - EAPOL**.
3. Click the **Authentication** tab.

Authentication field descriptions

Use the data in the following table to use the **Authentication** tab.

Name	Description
PortNumber	Indicates the number associated with this port.
Authenticate	Indicates the status of the Port Access Entity (PAE) authenticator requesting authentication.
Authenticated	Indicates the current authentication status of the Port Access Entity (PAE) authenticator.
Failed	Indicates the authentication status for failed or terminated state .
ReAuthEnabled	Indicates the re-authentication status of an existing supplicant at the time interval specified in ReAuthPeriod.
QuietPeriod	Indicates the time interval (in seconds) between authentication failure and the start of a new authentication. The allowed range is 1–65535; the default is 60.
ReAuthPeriod	Indicates the time interval in seconds between successive re-authentications. The allowed range is 1–2147483647; the default is 3600 (1 hour)
RetryMax	Indicates the maximum Extensible Authentication Protocol (EAP) requests sent to the supplicant before timing out the session. The default is 2
RetryCount	Indicates the count of the number of authentication attempts.

Viewing Multihost status information

Use the following procedure to display multiple host status for a port.

Procedure

1. In the navigation pane, expand the following folders: **Configuration** --> **Security** --> **Data Path**.
2. Click **802.1x–EAPOL**.
3. Click the **MultiHost Status** tab.

MultiHost status field descriptions

The following table describes values on the **MultiHost Status** tab.

Name	Description
PortNumber	Indicates the port number associated with this port.
ClientMACAddr	Indicates the MAC address of the client.
PaeState	Indicates the current state of the authenticator PAE state machine.
VlanId	Indicates the VLAN assigned to the client.

Viewing EAPoL session statistics

Use the following procedure to display multiple host session information for a port.

Procedure

1. In the navigation pane, expand the following folders: **Configuration** --> **Security** --> **Data Path**.
2. Click **802.1x–EAPOL**.
3. Click the **MultiHost Session** tab.

MultiHost session field descriptions

The following table describes values on the **MultiHost Session** tab.

Name	Description
StatsPortNumber	Indicates the port number associated with this port.
StatsClientMACAddr	Indicates the MAC address of the client.
Id	Indicates the unique identifier for the session.
AuthenticMethod	Indicates the authentication method used to establish the session.
Time	Indicates the elapsed time of the session.
TerminateCause	Indicates the cause of the session termination.
UserName	Indicates the user name that represents the identity of the supplicant PAE.

Viewing non-EAPoL MAC information

Use this procedure to view non-EAPoL client MAC information on a port.

Procedure

1. In the navigation pane, expand the following folders: **Configuration** --> **Security** --> **Data Path**.
2. Click **802.1x–EAPOL**.
3. Click the **NEAP Radius** tab.

NEAP Radius field descriptions

The following table describes values on the **NEAP Radius** tab.

Name	Description
MacPort	Indicates the port number associated with this port.
MacAddr	Indicates the MAC address of the client.
MacStatus	Indicates the authentication status of the non EAP host that is authenticated using the RADIUS server.
VlanId	Indicates the VLAN assigned to the client.

Chapter 4: IPsec

The following sections describe Internet Protocol Security (IPsec) and its configuration.

Internet Protocol Security (IPsec)

This section provides information on Internet Protocol Security (IPsec).

IPsec

Internet Protocol Security (IPsec) ensures the authenticity, integrity, and confidentiality of data at the network layer of the Open System Interconnection (OSI) stack.

The IPsec feature is a set of security protocols and cryptographic algorithms that protect communication in a network. Use IPsec in scenarios where you need to encrypt packets between two hosts, or two routers, or a router and a host.

IPsec adds support for OSPF virtual link for the security protection of the communication between the end points. You can also use IPsec with OSPFv3 on a brouter port or VLAN interface, for example, if you want to encrypt OSPFv3 control traffic on a broadcast network. You can also use IPsec with ICMPv6.

The following figure displays the movement of traffic using IPsec.

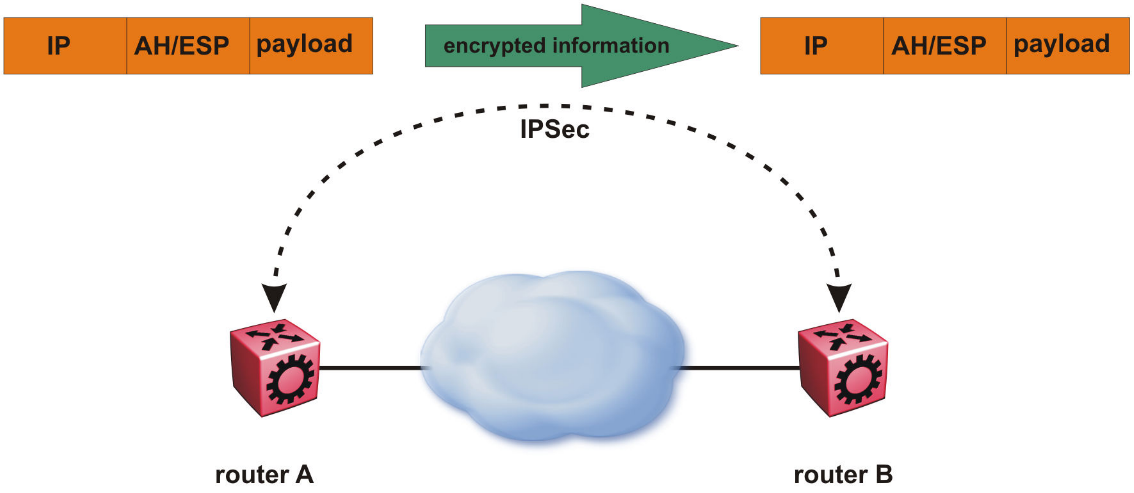


Figure 6: Internet Protocol Security (IPsec)

The IPsec feature uses security ciphers and encryption algorithms like AES, DES, and 3DES to ensure confidentiality of data, and keyed MAC for authenticity of data. The encryption algorithms require shared keys to secure the communication. In this release, the device only supports manual keying and configuration for IPsec. The IPsec feature only supports IPv6 interfaces in this release.

To configure IPsec, you create an IPsec policy, and then link the IPsec policy to an interface. You also link each IPsec policy to an IPsec security association. The IPsec policies define the amount of security applied to specific traffic on a specific interface. The IPsec feature supports the following security protocols:

- Encapsulating security payload (ESP)
- Authentication header (AH)

The device restricts IPsec encryption to control traffic through the CPU. This release restricts IPsec to transport mode only. The IPsec feature processes either the ingress, the egress, or both the egress and ingress control packets to and from the CPU.

The device checks every ingress or egress packet for the IPsec base protocol, either AH or ESP. The base protocol interacts with the security policy database (SPD) and security association database (SADB) to check the level of security to apply to the packet. The device consults the SPD for both ingress and egress traffic. For egress traffic, the device consults the SPD to determine if IPsec needs to apply security considerations. For ingress traffic, the device consults the SPD to determine whether the traffic received with IPsec encapsulation complies with the policies defined in the system.

For more information on IPsec, see *Configuring IPv6 Routing* and *Monitoring Performance*.

Authentication header

The authentication header (AH) authenticates IP traffic and ensures you connect with who you want to connect. The authentication header can detect if data is altered in transit and protect against replay attacks. The authentication header does not encrypt traffic.

The authentication header provides a small header that precedes the payload with the use of the security parameters index (SPI) and sequence number. The authentication header provides:

- IP datagram sender authentication by HMAC or MAC
- IP datagram integrity assurance by HMAC or MAC
- Replay detection and protection by sequence number

The IPsec feature inserts the AH header after the IP header in transport mode. Transport mode with AH authenticates only the payload of the IP packet. The device only supports transport mode in this release.

The device does not support tunnel mode in this release. Tunnel mode authenticates the entire IP packet, including the IP header and data, to provide a secure hop between two hosts, two routers, or a router and a host.

You can apply AH alone, or in combination with the Encapsulating Security Payload (ESP).

The following figures show an original IP packet and an IP packet with an AH header.

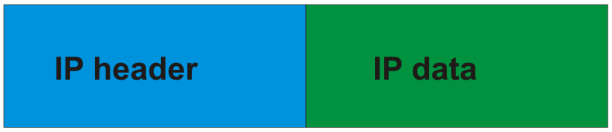


Figure 7: Original IP packet

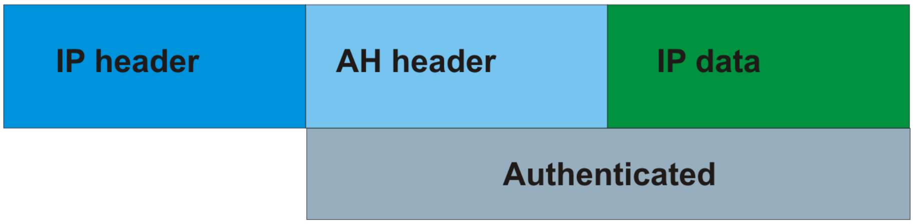


Figure 8: AH in transport mode

Encapsulating security payload

The encapsulating security payload (ESP) encrypts traffic with use of encryption algorithms, such as 3DES, AES-CBC, and AES-CTR. The security association specifies the algorithm and key used in ESP.

The encapsulating security payload can protect origin authenticity, integrity, and confidentiality of packets. ESP supports encryption-only and authentication-only configurations. The IPsec feature inserts the ESP header after the IP header and before the next layer protocol header in transport mode. Transport mode with ESP encrypts or authenticates only the payload of the IP packet. The device only supports transport mode in this release.

The device does not support tunnel mode in this release. Tunnel mode encrypts or authenticates the entire IP packet, including the IP header and data, to provide a secure hop between two hosts, two routers, or a router and a host.

The following figures display the original IP packet and an IP packet with ESP.

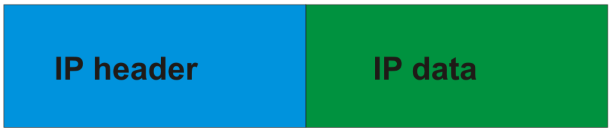


Figure 9: Original IP packet

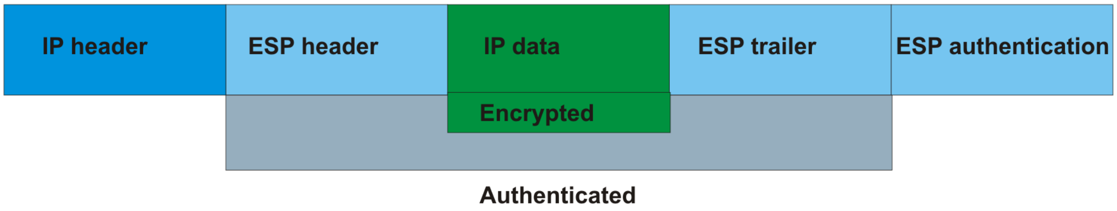


Figure 10: ESP in transport mode

IPsec modes

The IPsec feature security protocols use two different modes to protect the entire IP payload or the upper layer protocols:

- Transport mode
- Tunnel mode

The device only supports transport mode for this release. The device uses transport mode to protect the upper layer protocols. In transport mode, IPsec adds an IPsec header between the IP header and upper layer protocol header.

This release does not support tunnel mode. Under tunnel mode IPsec protects the whole IP packet. In tunnel mode, IPsec inserts the IPsec header between another IP datagram IP header and inner IP header.

Security association

A security association (SA) is a group of algorithms and parameters used to encrypt and authenticate the flow of IP traffic in a particular direction. An SA contains the information IPsec needs to process an IP packet. IPsec identifies SAs by:

- Security Parameter Index (SPI)
- Protocol value (either AH or ESP)
- Destination address to which the SA applies

Creation of a security association

Typically SAs exist in pairs; one in each direction, either inbound or outbound.

You can create SAs manually or dynamically. After you create an SA manually, the SA has no defined lifetime and the SA exists until you manually delete the SA.

After the device creates the SA dynamically, the SA can have a lifetime value that IPsec peers negotiate through use of a key management protocol. If the device uses the key excessively unauthorized access can occur. You must define the IPsec lifetime and other configurable parameters manually.

Security associations reside in the Security Association Database (SADB), which maintains a list of active SAs. The IPsec feature uses outbound SAs to secure the outgoing traffic and inbound SAs to process the incoming traffic. The device checks every ingress or egress packet for the IPsec base protocol, either AH or ESP. The base protocol interacts with the security policy database (SPD) and security association database (SADB) to check the level of security to apply to that packet.

The IPsec feature restricts SAs to the source and destination address of the connected router.

Security policy

Use IPsec to create IPsec security policies that define the levels of security for different types of traffic. You can use IPsec security policies to create rules to filter traffic with IPsec. IPsec policies determine what IP traffic to secure. An IPsec security policy typically consists of:

- An IP filter
- Security algorithms for authentication and key exchange
- An action

Creation of a security policy

You can configure IPsec on IPv6 interfaces. First, create and configure an IPsec policy, and then add and enable the policy on an interface.

After you enable IPsec, the device encrypts all control traffic on the interface based on the policy. You have to specify individual policies to target a particular interface address or multiple addresses. By default, this implementation does not work on a subnet.

The Security Policy Database (SPD) maintains the IPsec security policies. The device checks every ingress or egress packet for the IPsec base protocol, either AH or ESP. The base protocol interacts with the security policy database (SPD) and security association database (SADB) to check the level of security to apply to that packet.

The IPsec feature only adds policies if the source address in the policy specified matches an interface IP address.

The IPsec feature restricts the policy match source address to the interface address of the router and destination IPv6 address.

IPsec limitations

This section describes the limitations associated with IPsec.

- The device only supports IPsec for IPv6 traffic, and an interface must support IPv6 to apply IPsec. No support exists for IPv4 traffic in this release.
- The device only supports IPsec transport mode in this release. IPsec does not support tunnel mode in this release.

- The IPsec feature implementation is available only in software. Hardware implementation is not available. Only control packets to and from the CPU are subject to IPsec. IPsec implements IPsec policies in the software on the control path.
- The IPsec feature does not support automatic keying in this release. No support exists for the Internet Key Exchange (IKE) protocol.
- The device does not support address ranges facility for an IPsec policy.
- No fast-path support exists for IPsec.

IPsec configuration using CLI

The following section provides procedures to configure Internet Protocol Security (IPsec).

Creating an IPsec policy

Use the following procedure to configure an IPsec policy for an IPv6 interface. An IPsec policy defines the level of security for different types of traffic.

The device only supports IPsec for IPv6 traffic, and an interface must support IPv6 to apply IPsec.

Procedure

1. Enter Global Configuration mode:

   `enable`

   `configure terminal`

2. Create an IPsec policy:

   `ipv6 ipsec policy` *`WORD<1–32>`*

3. **(Optional)** Delete an IPsec policy:

   `no ipv6 ipsec policy` *`WORD<1–32>`*

Example

Create an IPsec policy named `newpolicy`:

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)# ipv6 ipsec policy newpolicy
```

Variable definitions

Use the data in the following table to use the **`ipv6 ipsec policy`** command.

Variable	Value
WORD<1–32>	Specifies the IPsec policy name.

Enabling an IPsec policy

Use the following procedure to enable an IPsec policy. An IPsec policy defines the level of security for different types of traffic.

The device only supports IPsec for IPv6 traffic, and an interface must support IPv6 to apply IPsec.

Before you begin

- Create an IPsec policy.

About this task

The IPsec feature adds policies only if the admin status of the policy and the IPsec status on the interface are enabled.

If you disable the IPsec policy on an IPv6 interface, IPsec removes the policy-related information from the security policy database (SPD) and the security association database (SADB), but the information remains on the system. After you re-enable, the information reapplies on the IPv6 interface.

Procedure

1. Enter Global Configuration mode:

   `enable`

   `configure terminal`

2. Enable an IPsec policy:

   `ipv6 ipsec policy` *`WORD<1–32>`* `admin enable`

3. **(Optional)** Disable an IPsec policy:

   `no ipv6 ipsec policy` *`WORD<1–32>`* `admin enable`

Example

Enable an IPsec policy named `newpolicy`:

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#ipv6 ipsec policy newpolicy admin enable
```

Variable definitions

Use the data in the following table to use the **`ipv6 ipsec policy`** command.

Variable	Value
admin enable	Enables the policy.
WORD<1–32>	Specifies the IPsec policy name.

Creating an IPsec security association

Use the following procedure to create an IPsec security association. A security association (SA) is a group of algorithms and parameters used to encrypt and authenticate the flow of IP traffic in a particular direction. An SA contains the information IPsec needs to process an IP packet.

The device only supports IPsec for IPv6 traffic, and an interface must support IPv6 to apply IPsec.

About this task

You cannot delete or modify a security association if the security association links to a policy. To modify a parameter in the security association or to delete the security association, you must first unlink the security association from a policy.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Create an IPsec security association:

   `ipv6 ipsec security-association` *`WORD<1–32>`*

3. **(Optional)** Delete an IPsec security association:

   `no ipv6 ipsec security-association` *`WORD<1–32>`*

Example

Create an IPsec security association named `newsa`:

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#ipv6 ipsec security-association newsa
```

Variable definitions

Use the data in the following table to use the **`ipv6 ipsec security-association`** command.

Variable	Value
WORD<1–32>	Specifies the security association identifier.

Configuring an IPsec security association

Use the following procedure to configure an IPsec security association (SA). An SA is a group of algorithms and parameters used to encrypt and authenticate the flow of IP traffic in a particular direction. An SA contains the information IPsec needs to process an IP packet.

The device only supports IPsec for IPv6 traffic, and an interface must support IPv6 to apply IPsec.

Before you begin

- Create an IPsec security association to configure.

About this task

You cannot delete or modify a security association if the security association links to a policy. To modify a parameter in the security association, or to delete the security association, you must first unlink the security association from a policy. You can only unlink a security association from a policy if the policy does not link to an interface. If a policy links to an interface, you must first unlink the policy from the interface, and then unlink the policy from the security association.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Configure the IPsec security association key-mode:

   ```
   ipv6 ipsec security-association WORD<1-32> key-mode <automatic|
   manual>
   ```

   This release only supports manual mode.

3. Configure the IPsec security association mode:

   ```
   ipv6 ipsec security-association WORD<1-32> mode <transport|tunnel>
   ```

   This release only supports transport mode.

4. Configure the IPsec security association encapsulation protocol:

   ```
   ipv6 ipsec security-association WORD<1-32> encap-proto <AH|ESP>
   ```

5. Configure the IPsec security association security parameters index:

   ```
   ipv6 ipsec security-association WORD<1-32> spi <1-4294967295>
   ```

   For IPsec to function, each peer must have the same SPI value configured on both peers for a particular policy.

6. Configure the IPsec security association encryption algorithm:

   ```
   ipv6 ipsec security-association WORD<1-32> Encrpt-algo <3DES|AES-
   CBC|AES-CTR|NULL> [EncrptKey WORD<1-256>][KeyLength <1-256>]
   ```

   The encryption algorithm parameters are only accessible if you configure the encapsulation protocol to ESP.

7. Configure the IPsec security association authentication algorithm:

   ```
   ipv6 ipsec security-association WORD<1-32> auth-algo <AES-XCBC-MAC|
   MD5|NULL|SHA1> [auth-key WORD<1-256>][KeyLength <1-256>]
   ```

8. Configure the IPsec security association lifetime value:

```
ipv6 ipsec security-association WORD<1–32> lifetime
<Bytes<1-4294967295>|seconds<1-4294967295>
```

9. **(Optional)** Delete the IPsec security association:

```
no ipv6 ipsec security-association WORD<1–32>
```

Example

Configure an IPsec security association named new_sa to have a key-mode of `ASCII`, an SA mode of `transport`, and an encapsulation protocol of `ESP`. Configure the encryption algorithm to `3DES`, with an encryption key of `111111111111111111111111`, and a keylength of `24`. Configure the authorization algorithm to `SHA1`, the authorization key to `11111111111111111111`, and key length to `20`. Configure the SPI to `1` and the lifetime in seconds to `1000`.

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#ipv6 ipsec security-association newsa key-mode manual
Switch:1(config)#ipv6 ipsec security-association newsa mode transport
Switch:1(config)#ipv6 ipsec security-association newsa encap-proto ESP
Switch:1(config)#ipv6 ipsec security-association newsa Encrpt-algo 3DES Encrpt-key
111111111111111111111111 KeyLength 24
Switch:1(config)#ipv6 ipsec security-association newsa auth-algo SHA1 auth-key
11111111111111111111 KeyLength 20
Switch:1(config)#ipv6 ipsec security-association newsa spi 1
Switch:1(config)#ipv6 ipsec security-association newsa lifetime seconds 1000
```

Variable definitions

Use the data in the following table to use the **`ipv6 ipsec security-association`** command.

Variable	Value
WORD<1–32>	Specifies the security association.
auth-algo *<AES-XCBC-MAC|MD5|NULL|SHA1>* [auth-key *WORD<1–256>*] [KeyLength *<1–256>*]	Specifies the authorization algorithm, which includes one of the following values: • AES-XCBC-MAC • MD5 • NULL • SHA1 The default authentication algorithm name is MD5. The parameter auth-key specifies the authentication key. The KeyLength parameter specifies a string value of 1 to 256 characters in length. The default KeyLength is 128. The KeyLength values are as follows: 3DES is 48, AES-CBC is 32, 48, or 64, AES-CTR is 32.
encap-proto *<AH|ESP>*	Specifies the encapsulation protocol: • AH—Specifies authentication header. • ESP—Specifies encapsulation security payload.

Table continues…

Variable	Value
	If you configure the encapsulation protocol as AH, you cannot configure the encryption algorithms and other encryption related attributes. You can only access the encryption algorithm parameters if you configure the encapsulation protocol to ESP. The default value is ESP.
Encrpt-algo <*3DES*|*AES-CBC*|*AES-CTR*|*NULL*> [EncrptKey *WORD<1–256>*] [KeyLength *<1–256>*]	Specifies the encryption algorithm value as one of the following: • 3DES-CBC • AES-CBC • AES-CTR • NULL—Only use the NULL parameter to debug. Do not use this parameter in any other circumstance. The default encryption algorithm is AES-CBC. You can only access the encryption algorithm parameters if you configure the encapsulation protocol to ESP. The EncrptKey specifies the encryption key. The KeyLength specifies the key length value in a string from 1 to 256 characters. The default KeyLength is 128. The KeyLength values are as follows: 3DES is 48, AES-CBC is 32, 48, or 64, AES-CTR is 32.
key-mode <*automatic* | *manual*>	Specifies the key-mode as one of the following: • automatic • manual The default is manual. This release only supports manual.
lifetime <Bytes*<1-4294967295>* | seconds*<1-4294967295>*	Specifies the lifetime value in seconds or kilobytes. The default lifetime value in seconds is 0, which is infinite. The default value in bytes is 0, which is infinite.
mode <*transport* | *tunnel*>	Specifies the mode value as one of the following: • transport—Transport mode encapsulates the IP payload and provides a secure connection between two end points. This release only supports transport mode.

Table continues…

Variable	Value
	• tunnel—Tunnel mode encapsulates the entire IP packet and provides a secure tunnel. This release does not support tunnel mode. The default is transport mode.
spi<*1-4294967295*>	Specifies the security parameters index (SPI) value, which is a unique value. SPI is a tag IPsec adds to the IP header. The tag enables the system that receives the IP packet to determine under which security association to process the received packet. For IPsec to function, each peer must have the same SPI value configured on both peers for a particular policy. The default value is 0.

Configuring an IPsec policy

Use the following procedure to configure an IPsec policy. An IPsec policy defines the level of security for different types of traffic.

The device only supports IPsec for IPv6 traffic, and an interface must support IPv6 to apply IPsec.

Before you begin

- Create an IPsec policy.

About this task

You cannot delete or modify a policy if the policy links to a security association, or if the policy links to a port or VLAN interface. If you need to modify a policy you must first unlink the policy from the security association, and the port or VLAN interface.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Configure the remote address:

   ```
   ipv6 ipsec policy WORD<1-32> raddr WORD<1-39>
   ```

3. **(Optional)** Configure the local address:

   ```
   ipv6 ipsec policy WORD<1-32> laddr WORD<1-39>
   ```

   The `laddr` parameter is an optional parameter that you can configure to have multiple local addresses for each remote address.

4. Configure the protocol:

```
ipv6 ipsec policy WORD<1–32>[protocol <icmpv6|ospfv3|tcp|udp>]
[sport<1–65535|any>][dport<1–65535|any>]
```

5. Configure the policy action:

```
ipv6 ipsec policy WORD<1–32> [action <drop|permit>]
```

Example

Configure the remote address to `2001:db8:0:0:0:0:0:1` and local address to `2001:db8:0:0:0:0:0:15`. configure the protocol to TCP sport `4` dport `5`. Configure the policy to `permit`.

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#ipv6 ipsec policy newpolicy raddr 2001:db8:0:0:0:0:0:1
Switch:1(config)#ipv6 ipsec policy newpolicy laddr 2001:db8:0:0:0:0:0:15
Switch:1(config)#ipv6 ipsec policy newpolicy protocol tcp sport 4 dport 5
Switch:1(config)#ipv6 ipsec policy newpolicy action permit
```

Variable definitions

Use the data in the following table to use the **`ipv6 ipsec policy`** command.

Variable	Value
action <*drop*|*permit*>	Specifies the action the policy takes. The default is permit.
laddr *WORD<1–39>*	Specifies the local address. The laddr parameter is optional. The laddr parameter is an optional parameter that you can configure to have multiple local addresses for each remote address. The default is 0::0.
protocol <*icmpv6*|*ospfv3*|*tcp*|*udp*>] [sport<*1–65535*>|*any*>][dport<*1–65535*>|*any*>]	Specifies the protocol, as one of the following: • ICMPv6 • OSPFv3 • TCP • UDP sport — Specifies the source port for TCP and UDP. You can specify any to configure any port as the source port. dport — Specifies the destination port for TCP and UDP. You can specify any to configure any port as the destination port. The default protocol is TCP any.
raddr *WORD<1–39>*	Specifies the remote address. The default is 0::0.
WORD<1–32>	Specifies the policy name.

Linking the IPsec security association to an IPsec policy

Use the following procedure to link the security association to an IPsec policy.

The device only supports IPsec for IPv6 traffic, and an interface must support IPv6 to apply IPsec.

Before you begin

- The IPsec security association and IPsec policy must exist.

About this task

You cannot delete or modify a security association if the security association links to a policy. To modify a parameter in the security association, or to delete the security association, you must first unlink the security association from the policy. You can only unlink a security association from a policy if the policy does not link to an interface. If a policy links to an interface, you must first unlink the policy from the interface, and then unlink the policy from the security association.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Link the IPsec security association to the IPsec policy:

   ```
   ipv6 ipsec policy WORD<1–32> security-association WORD<1–32>
   ```

3. **(Optional)** Unlink the IPsec security association to the IPsec policy:

   ```
   no ipv6 ipsec policy WORD<1–32> security-association WORD<1–32>
   ```

Example

Link the IPsec security association named `new_sa` to the IPsec policy named `newpolicy`:

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#ipv6 ipsec policy newpolicy security-association newsa
```

Variable definitions

Use the data in the following table to use the **`ipv6 ipsec policy`** command.

Variable	Value
WORD<1–32>	Specifies the policy ID.
security-association *WORD<1–32>*	Specifies the security association ID.

Enabling IPsec on an interface

Use the following procedure to enable IPsec on an interface.

The device only supports IPsec for IPv6 traffic, and an interface must support IPv6 to apply IPsec.

Procedure

1. Enter Interface Configuration mode:

   `enable`

   `configure terminal`

   `interface GigabitEthernet {slot/port[/sub-port][-slot/port[/sub-port]][,...]}` or `interface vlan` *`<1-4059>`*

   Note:

   If your platform supports channelization for 40 Gbps ports and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

2. Enable IPsec on an interface:

   `ipv6 ipsec enable`

   `default ipv6 ipsec enable`

3. **(Optional)** Disable IPsec on an interface:

   `no ipv6 ipsec enable`

Example

Enable the IPsec on VLAN 100:

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#interface vlan 100
Switch:1(config-if)#ipv6 ipsec enable
```

Variable definition

Use the data in the table to use the **`ipv6 ipsec`** command.

Variable	Value
enable	Enables IPsec on the IPv6 interface.

Linking an IPsec policy to an interface

Use the following procedure to link an IPsec policy to an interface, and configure a policy direction. By default, the direction is both.

The device only supports IPsec for IPv6 traffic, and an interface must support IPv6 to apply IPsec.

Before you begin

- You must enable IPsec on the interface first, and then you link the IPsec policy to the interface.

About this task

You cannot delete or modify an IPsec policy if the policy links to a port or VLAN interface. If you need to modify the policy, first unlink the policy from the port or VLAN interface.

Procedure

1. Enter Interface Configuration mode:

   `enable`

   `configure terminal`

   `interface GigabitEthernet {slot/port[/sub-port][-slot/port[/sub-port]][,...]}` or `interface vlan <1-4059>`

   Note:

   If your platform supports channelization for 40 Gbps ports and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

2. Link the IPsec policy to an interface:

   `ipv6 ipsec policy WORD<1-32> dir <both|in|out>`

3. **(Optional)** Unlink the IPsec policy to an interface:

   `no ipv6 ipsec policy WORD<1-32> dir <both|in|out>`

Example

Link the IPsec policy newpolicy to the interface VLAN 100:

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#interface vlan 100
Switch:1(config-if)#ipv6 ipsec policy newpolicy dir both
```

Variable definitions

Use the data in the following table to use the **`ipv6 ipsec policy`** command.

Variable	Value
WORD<1–32>	Specifies the policy ID.
dir <*both*|*in*|*out*>	Specifies the direction you want to protect with IPsec: • both—Specifies both ingress and egress traffic. • in—Specifies ingress traffic. • out—Specifies egress traffic. The default is both.

Enabling IPsec on a management interface

Use the following procedure to enable IPsec on a management interface.

The device only supports IPsec for IPv6 traffic, and an interface must support IPv6 to apply IPsec.

By default, IPsec is disabled on the management interface.

About this task

This procedure only applies to hardware with a dedicated, physical management interface.

Procedure

1. Enter mgmtEthernet Interface Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

   ```
   interface mgmtEthernet mgmt
   ```

2. Enable IPsec on an interface:

   ```
   ipv6 ipsec enable
   ```

Example

Enable IPsec on the management interface:

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#interface mgmtEthernet mgmt
Switch:1(config-if)#ipv6 ipsec enable
```

Linking an IPsec policy to a management interface

Use the following procedure to link an IPsec policy to a management interface, and configure a policy direction. By default, the direction is both.

The device only supports IPsec for IPv6 traffic, and an interface must support IPv6 to apply IPsec.

About this task

This procedure only applies to hardware with a dedicated, physical management interface.

Before you begin

- You must enable IPsec on the interface first, and then you link the IPsec policy to the interface.

Procedure

1. Enter mgmtEthernet Interface Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

```
interface mgmtEthernet mgmt
```

2. Link the IPsec policy to an interface:

   ```
   ipv6 ipsec policy WORD<1-32> dir <both|in|out>
   ```

3. **(Optional)** Unlink the IPsec policy to an interface:

   ```
   no ipv6 ipsec policy WORD<1-32> dir <both|in|out>
   ```

Example

Link the IPsec policy newpolicy to the management interface:

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#interface mgmtEthernet mgmt
Switch:1(config-if)#ipv6 ipsec policy newpolicy dir both
```

Variable definitions

Use the data in the following table to use the **`ipv6 ipsec policy`** command.

Variable	Value
WORD<1–32>	Specifies the policy ID.
dir <*both*|*in*|*out*>	Specifies the direction you want to protect with IPsec: • both—Specifies both ingress and egress traffic. • in—Specifies ingress traffic. • out—Specifies egress traffic. The default is both.

Displaying IPsec information on an interface

Use the following procedure to display IPsec information on an interface.

Procedure

1. Log on to the switch to enter User EXEC mode.
2. Display the IPsec status on an Ethernet interface:

   ```
   show ipv6 ipsec interface gigabitethernet {slot/port[/sub-port][-
   slot/port[/sub-port]][,...]}
   ```

   The command only works on an interface where you enable IPv6. If you do not enable IPv6 on the interface, the command displays an error.

3. Display the IPsec status on a VLAN interface:

   ```
   show ipv6 ipsec interface vlan <1-4059>
   ```

The command only works on an interface where you enable IPv6. If you do not enable IPv6 on the interface, the command displays an error.

4. Display the IPsec status on a management interface:

   ```
   show ipv6 ipsec interface mgmtethernet mgmt
   ```

   Note:

   This step applies to hardware that includes a physical management interface.

Example

Display IPsec status on interfaces.

```
Switch:1>enable
Switch:1#show ipv6 ipsec interface vlan 10

=========================================================================
                          VLAN Interface Policy Table
=========================================================================
Vlan Interface         Policy Name           IPsec State
--------------------------------------------------------------------------------
10                             ospfany                         Enable
--------------------------------------------------------------------------------

Switch:1#show ipv6 ipsec interface port 2/3
=========================================================================
                          PORT Interface Policy Table
=========================================================================
Interface        Policy Name         IPsec State
--------------------------------------------------------------------------------
2/3                   ospf1                 Enable
--------------------------------------------------------------------------------
```

Variable definitions

Use the data in the following table to use the **`show ipv6 ipsec interface`** command:

Variable	Value
gigabitethernet {slot/port[/sub-port][-slot/port[/sub-port]][,...]}	Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If your platform supports channelization for 40 Gbps ports and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.
mgmtethernet mgmt	Identifies the interface as the management interface.
vlan *<1-4059>*	Specifies the VLAN ID in the range of 1 to 4059. VLAN IDs 1 to 4059 are configurable. The system reserves VLAN IDs 4060 to 4094 for internal use. VLAN ID 1 is the default VLAN and you cannot create or delete VLAN ID 1.

Job aid

The following table describes the fields in the output for the **`show ipv6 ipsec interface vlan`** command.

Parameter	Description
Vlan Interface	Specifies the VLAN interface.
Policy Name	Specifies the IPsec policy that associates with the specific VLAN or VLANs.
IPsec State	Specifies whether the IPsec policy is enabled on the VLAN interface.

The following table describes the fields in the output for the **`show ipv6 ipsec interface gigabitethernet`** command.

Parameter	Description
Interface	Specifies the interface.
Policy Name	Specifies the IPsec policy that associates with the specific port or ports.
IPsec State	Specifies whether the IPsec policy is enabled on the interface.

The following table describes the fields in the output for the **`show ipv6 ipsec interface mgmtethernet mgmt`** command.

Parameter	Description
Vlan Interface	Specifies the VLAN interface.
Policy Name	Specifies the IPsec policy that associates with the management port.
IPsec State	Specifies whether the IPsec policy is enabled on the interface.
Direction	Specifies the policy direction.

Displaying configured IPsec policies

Use the following procedure to display IPsec policies.

Procedure

1. Log on to the switch to enter User EXEC mode.
2. Display all of the IPsec policies on the switch:

   ```
   show ipv6 ipsec policy all
   ```

3. Display a specific IPsec policy based on the policy name on the interface:

   ```
   show ipv6 ipsec policy interface WORD<1-32>
   ```

4. Display the IPsec policy based on the policy name:

   `show ipv6 ipsec policy name` *`WORD<1–32>`*

Example

Display IPsec policy information:

```
Switch:1>enable
Switch:1#show ipv6 ipsec policy all
=========================================================================
                               IPSEC Policy Table
=========================================================================
PolicyName          : ospf1
LocalAddress: 0::0
RemoteAddress: 0::0
Protocol: ospfv3
src-port: 0
dest-port: 0
Action: Permit
Admin: Enable

Switch:1#show ipv6 ipsec policy interface ospf1

=========================================================================
                          IPsec Policy Interface Table
=========================================================================
--------------------------------------------------------------------------------
POLICY NAME       InterfaceIndex            Policy State
--------------------------------------------------------------------------------
ospf1              2/3                           Enable

Switch:1#show ipv6 ipsec policy name ospf1
=========================================================================
                               IPSEC Policy Table
=========================================================================
PolicyName          : ospf1
LocalAddress: 0::0
RemoteAddress: 0::0
Protocol: ospfv3
src-port: 0
dest-port: 0
Action: Permit
Admin: Enable
```

Variable definitions

Use the data in the following table to use the **`show ipv6 ipsec policy`** command.

Variable	Value
all	Displays all of the IPsec policies on the switch.
interface *WORD<1–32>*	Displays a specific IPsec policy based on the policy name on the interface.
name *WORD<1–32>*	Displays the IPsec policy based on the name of the policy.

Job aid

The following table describes the fields in the output for the **`show ipv6 ipsec policy all`** and **`show ipv6 ipsec policy name`** commands.

Parameter	Description
PolicyName	Specifies the IPsec policy name.
LocalAddress	Specifies the local address. The default is 0::0.
RemoteAddress	Specifies the remote address. The default is 0::0.
Protocol	Specifies the protocol.
src-port	Specifies the source port.
dest-port	Specifies the destination port.
Action	Specifies the action as either: permit or drop.
Admin	Specifies whether the policy is enabled.

The following table describes the fields in the output for the **`show ipv6 ipsec policy interface`** command.

Parameter	Description
POLICY NAME	Specifies the IPsec policy name.
InterfaceIndex	Specifies the interface.
Policy State	Specifies whether the policy is enabled.

Displaying IPsec security association information

Use the following procedure to display IPsec security association information.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. Display all IPsec security associations:

   ```
   show ipv6 ipsec sa all
   ```

3. Display a specific IPsec security association:

   ```
   show ipv6 ipsec sa name WORD<1-32>
   ```

4. Display all security associations linked to a specific policy:

   ```
   show ipv6 ipsec sa-policy
   ```

Example

Display information on IPsec security association policies:

```
Switch:1>enable
Switch:1#show ipv6 ipsec sa all
=========================================================================
                        IPSEC Security Association Table
=========================================================================
sa-name: ospf1
key-Mode: manual
Encap protocol: ESP
SPI Value: 9
Encrypt Algorithm: 3dec-cbc
Encrypt-key: 52fb29f723b0800870dc83e3
Encrypt-key-Len: 24
Auth Algorithm: hmac-md5
Auth-key: 123456789abcdef0
Auth-key-Len: 16
Mode: transport
Lifetime-Sec: 1000
Lifetime-Byte: 20000

Switch:1#show ipv6 ipsec sa name ospf1

=========================================================================
                        IPSEC Security Association Table
=========================================================================
sa-name: ospf1
key-Mode: manual
Encap protocol: ESP
SPI Value: 9
Encrypt Algorithm: 3dec-cbc
Encrypt-key: 52fb29f723b0800870dc83e3
Encrypt-key-Len: 24
Auth Algorithm: hmac-md5
Auth-key: 123456789abcdef0
Auth-key-Len: 16
Mode: transport
Lifetime-Sec: 1000
Lifetime-Byte: 20000

Switch:1#show ipv6 ipsec sa-policy

=========================================================================
                                SA POLICY TABLE
=========================================================================
 Policy Name       Security Association
-------------------------------------------------------------------------
 ospf1             ospf1
-------------------------------------------------------------------------
```

Variable definitions

Use the data in the following table to use the **`show ipv6 ipsec sa`** command.

Variable	Value
all	Displays all security associations.
name *WORD<1–32>*	Displays a specific security association based on name.

Use the data in the following table to use the **`show ipv6 ipsec`** command.

Variable	Value
sa-policy	Displays all security associations linked to a specific policy.

Job aid

The following table describes the fields in the output for the **`show ipv6 ipsec sa all`** and **`show ipv6 ipsec saname`** commands.

Parameter	Description
sa-name	Specifies all of the IPsec security association names.
key-Mode	Specifies the key mode as manual or automatic. The default is automatic.
Encap protocol	Specifies the encapsulation protocol.
SPI Value	Specifies the SPI value, which is a tag added to the IP header. For IPsec to function, each peer must have the same SPI value configured on both peers for a particular policy.
Encrypt Algorithm	Specifies the encrypt algorithm as one of the following: • 3DES-CBC • AES-CBC • AES-CTR • NULL—Only used to debug.
Encrypt-key	Specifies the encrypt-key parameter for the authentication key in either: • hex– Specifies hexadecimal. • ascii–Specifies ASCII, the American Standard Code for Information Interchange character encoding scheme.
Encrypt-key-Len	Specifies the key length value in a string from 1 to 256 characters. The default KeyLength is 128.
Mode	Specifies the mode value as one of the following: • tunnel—Tunnel mode encapsulates the entire IP packet and provides a secure tunnel. This release does not support tunnel mode. • transport—Transport mode encapsulates the IP payload and provides a secure connection between two endpoints. This release only supports transport mode.

Table continues…

Parameter	Description
	The default is transport mode.
Lifetime-Sec	Specifies the lifetime value in seconds. The default is 0, which is infinite.
Lifetime-Byte	Specifies the lifetime value in bytes. The default is 0, which is infinite.

The following table describes the fields in the output for the **`show ipv6 ipsec sa-policy`** command.

Parameter	Description
Policy Name	Specifies the IPsec policy name.
Security Association	Specifies the security association name.

IPsec configuration using EDM

The following section provides procedures to configure Internet Protocol security (IPsec).

Creating an IPsec policy

Use the following procedure to configure an IPsec policy for an IPv6 interface. An IPsec policy defines the level of security for different types of traffic.

The device only supports IPsec for IPv6 traffic, and an interface must support IPv6 to apply IPsec.

About this task

You cannot delete or modify a policy if the policy links to a security association, or if the policy links to a port or VLAN interface. If you need to modify a policy you must first unlink the policy from the security association, and the port or VLAN interface.

Procedure

1. In the navigation pane, expand the following folders: **Configuration** > **IPv6**.
2. Click **IPSec**.
3. Click the **Policy** tab.
4. Click **Insert**.
5. In the **Name** field, type a policy name.
6. Complete the remaining optional configuration to customize the policy.
7. Click **Insert**.

Policy field descriptions

Use the data in the following table to use the **Policy** tab.

Name	Description
Name	Specifies the IPsec policy name.
DstAddress	Specifies the remote address. The default is 0::0.
SrcAddress	Specifies the local address. The local address is optional that you can configure to have multiple local addresses for each remote (destination) address. The default is 0::0.
SrcPort	Specifies the source port for TCP and UDP. Leave this field empty to configure any port as the source port. The default is value is 1.
DstPort	Specifies the destination port for TCP and UDP. Leave this field empty to configure any port as the destination port. The default value is 1.
AdminFlag	Enables or disables the policy. The default is disabled.
L4Protocol	Specifies the protocol, as one of the following: • TCP • UDP • ICMPv6 • OSPFv3 The default is TCP.
Action	Specifies the action the policy takes. The default is to permit the packet.

Creating an IPsec security association

Use the following procedure to create an IPsec security association. A security association (SA) is a group of algorithms and parameters used to encrypt and authenticate the flow of IP traffic in a particular direction. An SA contains the information IPsec needs to process an IP packet.

The device only supports IPsec for IPv6 traffic, and an interface must support IPv6 to apply IPsec.

About this task

You cannot delete or modify a security association if the security association links to a policy. To modify a parameter in the security association or to delete the security association, you must first unlink the security association from a policy.

You can only unlink a security association from a policy if the policy does not link to an interface. If a policy links to an interface, you must first unlink the policy from the interface, and then unlink the policy from the security association.

Procedure

1. In the navigation pane, expand the following folders: **Configuration** > **IPv6**.
2. Click **IPSec**.
3. Click the **Security Association** tab.
4. Click **Insert**.
5. In the **Name** field, type a name to identify the SA.
6. In the **SPI** field, type the security parameters index.

   ✱ **Note:**

   For IPsec to function, each peer must have the same SPI value configured for a particular policy.
7. Complete the remaining optional configuration.
8. Click **Insert**.

Security Association field descriptions

Use the data in the following table to use the **Security Association** tab.

Name	Description
Name	Specifies the name of the security association.
Spi	Specifies the security parameters index (SPI) value, which is a unique value. SPI is a tag IPsec adds to the IP header. The tag enables the system that receives the IP packet to determine under which security association to process the received packet. For IPsec to function, each peer must have the same SPI value configured for a particular policy. The default value is 0.
HashAlgorithm	Specifies the authorization algorithm, which includes one of the following values: • AES-XCBC-MAC • MD5 • NULL • SHA1 The default authentication algorithm name is MD5.
EncryptAlgorithm	specifies the encryption algorithm value as one of the following: • 3DES-CBC • AES-CBC

Table continues…

Name	Description
	• AES-CTR • NULL—Only use the NULL parameter to debug. Do not use this parameter in any other circumstance. The default encryption algorithm is AES-CBC. You can only access the encryption algorithm parameters if you configure the encapsulation protocol to ESP.
AuthMethod	Specifies the encapsulation protocol: • ah—Specifies authentication header. • es—Specifies encapsulation security payload. If you configure the encapsulation protocol as ah, you cannot configure the encryption algorithms and other encryption related attributes. You can only access the encryption algorithm parameters if you configure the encapsulation protocol to es. The default value is es.
Mode	Specifies the mode value as one of the following: • transport—Transport mode encapsulates the IP payload and provides a secure connection between two end points. This release only supports transport mode. • tunnel—Tunnel mode encapsulates the entire IP packet and provides a secure tunnel. This release does not support tunnel mode. The default is transport mode.
KeyMode	Specifies the key-mode as one of the following: • manual • auto The default is manual.
EncryptKeyName	Specifies the encryption key.
EncryptKeyLength	Specifies the numbers of bits used in the encryption key. The key length values are as follows: • 3DES-CBC is 48 • AES-CBC is 32, 48, 64 • AES-CTR is 32
HashKeyName	Specifies the authentication key.

Table continues…

Name	Description
HashKeyLength	Specifies the numbers of bits used in the hash key. The key length values are as follows: • AES-XCBC-MAC is 32 • MD5 is 32 • SHA1 is 40
LifetimeSeconds	Specifies the lifetime value in seconds. The lifetime determines the traffic that can pass between IPsec peers using a security association before that security association expires. The default lifetime value in seconds is 0, which is infinite.
LifetimeKbytes	Specifies the lifetime value in kilobytes. The lifetime determines the traffic that can pass between IPsec peers using a security association before that security association expires. The default value in kilobytes is 0, which is infinite.

Linking the IPsec security association to an IPsec policy

Use the following procedure to link the security association to an IPsec policy.

The device only supports IPsec for IPv6 traffic, and an interface must support IPv6 to apply IPsec.

About this task

You cannot delete or modify a security association if the security association links to a policy. To modify a parameter in the security association, or to delete the security association, you must first unlink the security association from the policy. You can only unlink a security association from a policy if the policy does not link to an interface. If a policy links to an interface, you must first unlink the policy from the interface, and then unlink the policy from the security association.

Before you begin

- The IPsec security association and IPsec policy must exist.

Procedure

1. In the navigation pane, expand the following folders: **Configuration** > **IPv6**.
2. Click **IPSec**.
3. Click the **Policy SA Link** tab.
4. Click **Insert**.
5. In the **PolicyName** field, type the IPsec policy name.
6. In the **SAName** field, type the security association name.
7. Click **Insert**.

Policy SA Link field descriptions

Use the data in the following table to use the **Policy SA Link** tab.

Name	Description
PolicyName	Specifies the name of the IPsec policy.
SAName	Specifies the name of the security association.

Enabling IPsec on an interface

Use the following procedure to enable IPsec on an interface.

The device only supports IPsec for IPv6 traffic, and an interface must support IPv6 to apply IPsec

Procedure

1. Enable IPsec on a VLAN:
    a. In the navigation pane, expand the following folders: **Configuration** > **VLAN**.
    b. Click **VLANs**.
    c. Click the **Advanced** tab.
    d. In the row for the VLAN, double-click the **IpsecEnable** field, and then select **enable**.
    e. Click **Apply**.
2. Enable IPsec on a port:
    a. In the Device Physical View, select a port.
    b. In the navigation pane, expand the following folders: **Configuration** > **Edit** > **Port**.
    c. Click **General**.
    d. Click the **Interface** tab.
    e. For the **IpsecEnable** field, select **enable**.
    f. Click **Apply**.
3. Enable IPsec on a management port:

    Note:

    This step only applies to hardware with a dedicated, physical management interface.

    a. In the Device Physical View, select the management port.
    b. In the navigation pane, expand the following folders: **Configuration** > **Edit**.
    c. Click **Mgmt Port**.
    d. Click the **General** tab.
    e. For the **IpsecEnable** field, select **enable**.
    f. Click **Apply**.

Linking an IPsec policy to an interface

Use the following procedure to link an IPsec policy to an interface, and configure a policy direction. By default, the direction is both.

The device only supports IPsec for IPv6 traffic, and an interface must support IPv6 to apply IPsec.

About this task

You cannot delete or modify an IPsec policy if the policy links to a port or VLAN interface. If you need to modify the policy, first unlink the policy from the port or VLAN interface.

Before you begin

- You must enable IPsec on the interface first, and then you link the IPsec policy to the interface.

Procedure

1. In the navigation pane, expand the following folders: **Configuration** > **IPv6**.
2. Click **IPSec**.
3. Click the **Interface Policy** tab.
4. Click **Insert**.
5. In the **Name** field, type the name of the IPsec policy.
6. In the **IfIndex** field, click either **Port** , **Vlan**, or **Mgmt Port**, and then select an interface.

   Note:

   The Mgmt Port button only appears for hardware with a dedicated, physical management interface. If you click this button, EDM automatically populates the IfIndex value.
7. Click **Okay**.
8. Complete the remaining optional configuration.
9. Click **Insert**.

Interface Policy field descriptions

Use the data in the following table to use the Interface Policy tab.

Name	Description
Name	Specifies the IPsec policy name.
IfIndex	Links a policy to either a port, VLAN, or management interface.
IfEnabled	Shows if the IPsec is enabled on the interface and if the administrative state of the policy is enabled.

Table continues…

Name	Description
IfDirection	Specifies the direction you want to protect with IPsec: • inbound—Specifies ingress traffic. • outbound—Specifies egress traffic. • bothDirections—Specifies both ingress and egress traffic. The default is bothDirections.

IPsec configuration examples

The following section provides examples to configure Internet Protocol Security (IPsec).

IPsec configuration example

Review the following information to understand IPsec configuration.

Use the following steps to configure IPsec.

1. Create and configure an IPsec policy under IPv6.
2. Enable the policy.
3. Create an IPsec security association to correspond with the IPsec policy.
4. Configure the key mode format.
5. Configure the security association.
6. Link the IPsec security association to the IPsec policy.
7. Enable the IPsec policy on the interface.
8. Link the IPsec policy with the interface.
9. Enable the IPsec on the interface that links to the IPsec policy.

For an example configuration and for more information on IPsec OSPFv3 and OSPFv3 virtual link, see *Configuring IPv6 Routing*.

Create a policy named `newpolicy` with a security association named `new_sa` on VLAN 100.

The following displays the IPv6 IPsec policy configuration:

```
ipv6 ipsec policy newpolicy raddr 2001:db8:0:0:0:0:0:1
ipv6 ipsec policy newpolicy laddr 2001:db8:0:0:0:0:0:15
ipv6 ipsec policy newpolicy protocol tcp sport 4 dport 5
ipv6 ipsec policy newpolicy action permit
```

The following example displays the IPv6 IPsec security association:

```
ipv6 ipsec security-association new_sa
ipv6 ipsec security-association new_sa key-mode manual
```

```
ipv6 ipsec security-association new_sa mode transport
ipv6 ipsec security-association new_sa encap-proto ESP
ipv6 ipsec security-association new_sa Encrpt-algo 3DES-CBC encrypt-key
111111111111111111111111 KeyLength 24
ipv6 ipsec security-association new_sa auth-algo SHA1 auth-key 11111111111111111111
KeyLength 20
ipv6 ipsec security-association new_sa spi 1
ipv6 ipsec security-association new_sa lifetime seconds 1000
```

IPsec with ICMPv6 configuration example

The following displays configuration of IPsec with ICMPv6.

Note:

Slot and port information can differ depending on hardware platform. See *Installing* for specific hardware information.

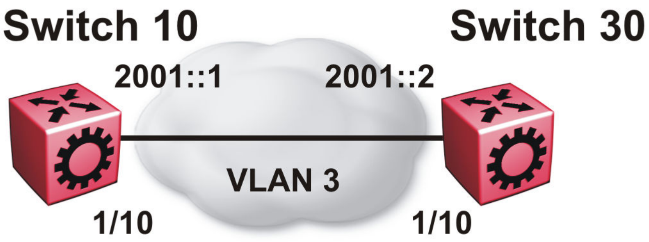


Figure 11: IPsec configuration with ICMPv6

Switch 10 security association configuration

The following example displays the configuration of the security association on Switch 10.

```
ipv6 ipsec security-association icmp
ipv6 ipsec security-association icmp encap-proto ESP
ipv6 ipsec security-association icmp mode transport
ipv6 ipsec security-association icmp spi 1
ipv6 ipsec security-association icmp auth-algo SHA1 auth-key
1234567890123456789012345678901234567890 keyLength 40
ipv6 ipsec security-association icmp Encrpt-algo AES-CBC EncrptKey
12345678901234567890123456789012 keyLength 32
ipv6 ipsec security-association icmp key-mode manual
ipv6 ipsec security-association icmp lifetime seconds 1
ipv6 ipsec security-association icmp lifetime bytes 1
```

Switch 10 policy configuration

The following example displays the configuration of the security policy on Switch 10.

```
ipv6 ipsec policy ICMP_Policy
ipv6 ipsec policy ICMP_Policy admin  enable
ipv6 ipsec policy ICMP_Policy raddr 2001::2
ipv6 ipsec policy ICMP_Policy laddr 2001::1
ipv6 ipsec policy ICMP_Policy protocol icmpv6
```

```
ipv6 ipsec policy ICMP_Policy action permit
ipv6 ipsec policy ICMP_Policy security-association icmp
```

Switch 10 interface configuration

The following example displays the configuration of IPsec on slot/port 1/10.

```
interface gigabitEthernet 1/10
no shut
ipv6 interface vlan 3
ipv6 interface address 2000::1
ipv6 interface enable
ipv6 ipsec policy ICMP_Policy dir both
ipv6 ipsec enable
```

Switch 10 VLAN configuration

The following example displays the creation and configuration of VLAN 3 with IPsec.

```
interface gigabitEthernet 1/10
no shut
exit
vlan create 3 type port-mstprstp 3
vlan members add 3 1/10 portmember
interface vlan 3
ipv6 interface enable
ipv6 interface address 2000::1
ipv6 ipsec policy ICMP_Policy dir both
ipv6 ipsec enable
```

Switch 30 security association configuration

The following example displays the configuration of the security association on Switch 30.

```
ipv6 ipsec security-association icmp
ipv6 ipsec security-association icmp encap-proto ESP
ipv6 ipsec security-association icmp mode transport
ipv6 ipsec security-association icmp spi 1
ipv6 ipsec security-association icmp auth-algo SHA1 auth-key
1234567890123456789012345678901234567890 keyLength 40
ipv6 ipsec security-association icmp Encrpt-algo AES-CBC EncrptKey
12345678901234567890123456789012 keyLength 32
ipv6 ipsec security-association icmp key-mode manual
ipv6 ipsec security-association icmp lifetime seconds 1
ipv6 ipsec security-association icmp lifetime bytes 1
```

Switch 30 policy configuration

The following example displays the configuration of the security policy on Switch 30.

```
ipv6 ipsec policy ICMP_Policy
ipv6 ipsec policy ICMP_Policy admin enable
ipv6 ipsec policy ICMP_Policy raddr 2001::1
ipv6 ipsec policy ICMP_Policy laddr 2001::2
ipv6 ipsec policy ICMP_Policy action permit
ipv6 ipsec policy ICMP_Policy protocol icmpv6
ipv6 ipsec policy ICMP_Policy security-association icmp
```

Switch 30 interface configuration

The following example displays the configuration of IPsec on slot/port 1/10.

```
interface gigabitEthernet 1/10
no shut
ipv6 interface enable
ipv6 interface vlan 3
```

```
ipv6 interface address 2001::2
ipv6 ipsec policy ICMP_Policy dir both
ipv6 ipsec enable
```

Switch 30 VLAN configuration

The following example displays the creation and configuration of VLAN 3 with IPsec.

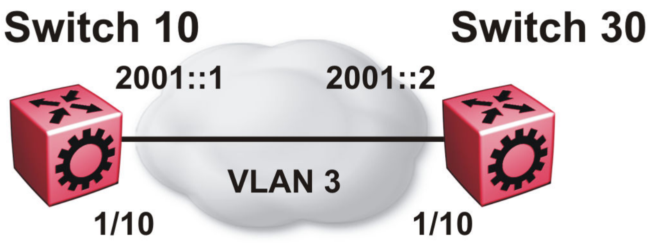
```
interface gigabitEthernet 1/10
no shut
exit
vlan create 3 type port-mstprstp 0
vlan members add 3 1/20
interface vlan 3
ipv6 interface enable
ipv6 interface address 2001::2
ipv6 ipsec policy ICMP_Policy dir both
ipv6 ipsec enable
```

OSPFv3 IPsec configuration example

The following example displays a network using IPsec used with OSPFv3.

Note:

Slot and port information can differ depending on hardware platform. See *Installing* for specific hardware information.



Switch 10 security associations

The following example displays the configuration of security associations for OSPFv3 for Switch 10.

```
ipv6 ipsec security-association ospf1
ipv6 ipsec security-association ospf1 encap-proto ESP
ipv6 ipsec security-association ospf1 mode transport
ipv6 ipsec security-association ospf1 spi 1
ipv6 ipsec security-association ospf1 auth-algo MD5 auth-key
12345678901234567890123456789012 keyLength 32
ipv6 ipsec security-association ospf1 Encrpt-algo AES-CTR EncrptKey
12345678901234567890123456789012 keyLength 32
ipv6 ipsec security-association ospf1 key-mode manual
ipv6 ipsec security-association ospf1 lifetime seconds 1
ipv6 ipsec security-association ospf1 lifetime bytes 1
```

```
ipv6 ipsec security-association ospf2
ipv6 ipsec security-association ospf2 encap-proto ESP
ipv6 ipsec security-association ospf2 mode transport
ipv6 ipsec security-association ospf2 spi 2
ipv6 ipsec security-association ospf2 auth-algo MD5 auth-key
12345678901234567890123456789012 keyLength 32
ipv6 ipsec security-association ospf2 Encrpt-algo AES-CTR EncrptKey
12345678901234567890123456789012 keyLength 32
ipv6 ipsec security-association ospf2 key-mode manual
ipv6 ipsec security-association ospf2 lifetime seconds 1
ipv6 ipsec security-association ospf2 lifetime bytes 1

ipv6 ipsec security-association ospf3
ipv6 ipsec security-association ospf3 encap-proto ESP
ipv6 ipsec security-association ospf3 mode transport
ipv6 ipsec security-association ospf3 spi 3
ipv6 ipsec security-association ospf3 auth-algo MD5 auth-key
12345678901234567890123456789012 keyLength 32
ipv6 ipsec security-association ospf3 Encrpt-algo AES-CTR EncrptKey
12345678901234567890123456789012 keyLength 32
ipv6 ipsec security-association ospf3 key-mode manual
ipv6 ipsec security-association ospf3 lifetime seconds 1
ipv6 ipsec security-association ospf3 lifetime bytes 1

ipv6 ipsec security-association ospf4
ipv6 ipsec security-association ospf4 encap-proto ESP
ipv6 ipsec security-association ospf4 mode transport
ipv6 ipsec security-association ospf4 spi 4
ipv6 ipsec security-association ospf4 auth-algo MD5 auth-key
12345678901234567890123456789012 keyLength 32
ipv6 ipsec security-association ospf4 Encrpt-algo AES-CTR EncrptKey
12345678901234567890123456789012 keyLength 32
ipv6 ipsec security-association ospf4 key-mode manual
ipv6 ipsec security-association ospf4 lifetime seconds 1
ipv6 ipsec security-association ospf4 lifetime bytes 1

ipv6 ipsec security-association ospf5
ipv6 ipsec security-association ospf5 encap-proto ESP
ipv6 ipsec security-association ospf5 mode transport
ipv6 ipsec security-association ospf5 spi 5
ipv6 ipsec security-association ospf5 auth-algo MD5 auth-key
12345678901234567890123456789012 keyLength 32
ipv6 ipsec security-association ospf5 Encrpt-algo AES-CTR EncrptKey
12345678901234567890123456789012 keyLength 32
ipv6 ipsec security-association ospf5 key-mode manual
ipv6 ipsec security-association ospf5 lifetime seconds 1
ipv6 ipsec security-association ospf5 lifetime bytes 1

ipv6 ipsec security-association ospf6
ipv6 ipsec security-association ospf6 encap-proto ESP
ipv6 ipsec security-association ospf6 mode transport
ipv6 ipsec security-association ospf6 spi 6
ipv6 ipsec security-association ospf6 auth-algo MD5 auth-key
12345678901234567890123456789012 keyLength 32
ipv6 ipsec security-association ospf6 Encrpt-algo AES-CTR EncrptKey
12345678901234567890123456789012 keyLength 32
ipv6 ipsec security-association ospf6 key-mode manual
ipv6 ipsec security-association ospf6 lifetime seconds 1
ipv6 ipsec security-association ospf6 lifetime bytes 1
```

Switch 10 policy configuration

The following example displays the configuration of policies on Switch 10. The link local address is fe80:0:0:0:b2ad:aaff:fe43:100 and the remote link local address is fe80:0:0:0:b2ad:aaff:fe43:4d00.

The following displays the policy with the laddr configured to the link local address and raddr configured to the remote link local address, with the direction configured as outbound.

```
ipv6 ipsec policy ospf1
ipv6 ipsec policy ospf1 admin enable
ipv6 ipsec policy ospf1 raddr fe80:0:0:0:b2ad:aaff:fe43:4d00
ipv6 ipsec policy ospf1 laddr fe80:0:0:0:b2ad:aaff:fe43:100
ipv6 ipsec policy ospf1 protocol ospfv3
ipv6 ipsec policy ospf1 action permit
```

The following example displays the configuration of policies on Switch 10. The link local address is fe80:0:0:0:b2ad:aaff:fe43:100 and the remote link local address is fe80:0:0:0:b2ad:aaff:fe43:4d00. The following displays the policy with the laddr configured to the link local address and raddr configured to the remote link local address, with the direction configured as inbound.

For a policy direction of inbound, laddr and raddr are reversed before storing to the stack. Because of this, even though the policy requires you to configure the laddr as the remote link local address, you need to configure laddr as the link local address in the configuration.

```
ipv6 ipsec policy ospf2
ipv6 ipsec policy ospf2 admin enable
ipv6 ipsec policy ospf2 raddr fe80:0:0:0:b2ad:aaff:fe43:4d00
ipv6 ipsec policy ospf2 laddr fe80:0:0:0:b2ad:aaff:fe43:100
ipv6 ipsec policy ospf2 protocol ospfv3
ipv6 ipsec policy ospf2 action permit
```

Laddr is configured to the link local and raddr is configured to ff02::05 with the direction configured as outbound.

```
ipv6 ipsec policy ospf3
ipv6 ipsec policy ospf3 admin enable
ipv6 ipsec policy ospf3 raddr ff02::05
ipv6 ipsec policy ospf3 laddr fe80:0:0:0:b2ad:aaff:fe43:100
ipv6 ipsec policy ospf3 protocol ospfv3
ipv6 ipsec policy ospf3 action permit
```

Laddr is configured to the remote link local and raddr is configured to ff02::05 with the direction configured as inbound.

```
ipv6 ipsec policy ospf4
ipv6 ipsec policy ospf4 admin enable
ipv6 ipsec policy ospf4 raddr fe80:0:0:0:b2ad:aaff:fe43:4d00
ipv6 ipsec policy ospf4 laddr ff02::05
ipv6 ipsec policy ospf4 protocol ospfv3
ipv6 ipsec policy ospf4 action permit
```

Laddr is configured to the link local and raddr is configured to ff02::06 with the direction as outbound.

```
ipv6 ipsec policy ospf5
ipv6 ipsec policy ospf5 admin enable
ipv6 ipsec policy ospf5 raddr ff02::06
ipv6 ipsec policy ospf5 fe80:0:0:0:b2ad:aaff:fe43:100
ipv6 ipsec policy ospf5 protocol ospfv3
ipv6 ipsec policy ospf5 action permit
```

Laddr is configured to the remote link local and raddr is configured to ff02::06 with the direction configured as inbound.

```
ipv6 ipsec policy ospf6
ipv6 ipsec policy ospf6 admin enable
ipv6 ipsec policy ospf6 raddr fe80:0:0:0:b2ad:aaff:fe43:4d00
ipv6 ipsec policy ospf6 laddr ff02::06
```

```
ipv6 ipsec policy ospf6 protocol ospfv3
ipv6 ipsec policy ospf6 action permit
```

Switch 10 link table configuration

The following example displays the linking of the policy with the security association on Switch 10.

```
ipv6 ipsec policy ospf1 security-association ospf1
ipv6 ipsec policy ospf2 security-association ospf2
ipv6 ipsec policy ospf3 security-association ospf3
ipv6 ipsec policy ospf4 security-association ospf4
ipv6 ipsec policy ospf5 security-association ospf5
ipv6 ipsec policy ospf6 security-association ospf6
```

Switch 10 OSPFv3 configuration

The following example displays the OSPFv3 configuration on Switch 10.

```
router ospf ipv6-enable
router ospf
ipv6 router-id 1.1.1.1
ipv6 area 0.0.0.1
```

Switch 10 interface configuration

The following example displays the interface configuration on slot/port 1/10.

```
interface gigabitEthernet 1/10
no shut
ipv6 interface vlan 3
ipv6 interface address 2000::1/64
ipv6 interface enable
ipv6 ospf area 0.0.0.1
ipv6 ospf enable
ipv6 ipsec policy ospf1 dir out
ipv6 ipsec policy ospf2 dir in
ipv6 ipsec policy ospf3 dir out
ipv6 ipsec policy ospf4 dir in
ipv6 ipsec policy ospf5 dir out
ipv6 ipsec policy ospf6 dir in
ipv6 ipsec enable
```

Switch 10 VLAN configuration

The following example displays the creation of VLAN 3 and the configuration of IPsec on VLAN 3.

```
interface gigabitEthernet 1/10
no shut
exit
vlan create 3 type port-mstprstp 3
vlan members add 3 1/10 portmember
interface vlan 3
ipv6 interface enable
ipv6 interface address 2000::1/64
ipv6 ospf area 0.0.0.1
ipv6 ospf enable
ipv6 ipsec policy ospf1 dir out
ipv6 ipsec policy ospf2 dir in
ipv6 ipsec policy ospf3 dir out
ipv6 ipsec policy ospf4 dir in
ipv6 ipsec policy ospf5 dir out
ipv6 ipsec policy ospf6 dir in
ipv6 ipsec enable
```

Switch 30 security associations

The following example displays the configuration of security associations for OSPFv3 for Switch 30.

```
ipv6 ipsec security-association ospf1 auth-algo MD5 auth-key
12345678901234567890123456789012 keyLength 32
ipv6 ipsec security-association ospf1 Encrpt-algo AES-CTR EncrptKey
12345678901234567890123456789012 keyLength 32
ipv6 ipsec security-association ospf1 key-mode manual
ipv6 ipsec security-association ospf1 lifetime seconds 1
ipv6 ipsec security-association ospf1 lifetime bytes 1

ipv6 ipsec security-association ospf2
ipv6 ipsec security-association ospf2 encap-proto ESP
ipv6 ipsec security-association ospf2 mode transport
ipv6 ipsec security-association ospf2 spi 2
ipv6 ipsec security-association ospf2 auth-algo MD5 auth-key
12345678901234567890123456789012 keyLength 32
ipv6 ipsec security-association ospf2 Encrpt-algo AES-CTR EncrptKey
12345678901234567890123456789012 keyLength 32
ipv6 ipsec security-association ospf2 key-mode manual
ipv6 ipsec security-association ospf2 lifetime seconds 1
ipv6 ipsec security-association ospf2 lifetime bytes 1

ipv6 ipsec security-association ospf3
ipv6 ipsec security-association ospf3 encap-proto ESP
ipv6 ipsec security-association ospf3 mode transport
ipv6 ipsec security-association ospf3 spi 3
ipv6 ipsec security-association ospf3 auth-algo MD5 auth-key
12345678901234567890123456789012 keyLength 32
ipv6 ipsec security-association ospf3 Encrpt-algo AES-CTR EncrptKey
12345678901234567890123456789012 keyLength 32
ipv6 ipsec security-association ospf3 key-mode manual
ipv6 ipsec security-association ospf3 lifetime seconds 1
ipv6 ipsec security-association ospf3 lifetime bytes 1

ipv6 ipsec security-association ospf4
ipv6 ipsec security-association ospf4 encap-proto ESP
ipv6 ipsec security-association ospf4 mode transport
ipv6 ipsec security-association ospf4 spi 4
ipv6 ipsec security-association ospf4 auth-algo MD5 auth-key
12345678901234567890123456789012 keyLength 32
ipv6 ipsec security-association ospf4 Encrpt-algo AES-CTR EncrptKey
12345678901234567890123456789012 keyLength 32
ipv6 ipsec security-association ospf4 key-mode manual
ipv6 ipsec security-association ospf4 lifetime seconds 1
ipv6 ipsec security-association ospf4 lifetime bytes 1

ipv6 ipsec security-association ospf5
ipv6 ipsec security-association ospf5 encap-proto ESP
ipv6 ipsec security-association ospf5 mode transport
ipv6 ipsec security-association ospf5 spi 5
ipv6 ipsec security-association ospf5 key-mode manual
ipv6 ipsec security-association ospf5 lifetime seconds 1
ipv6 ipsec security-association ospf5 lifetime bytes 1

ipv6 ipsec security-association ospf6
ipv6 ipsec security-association ospf6 encap-proto ESP
ipv6 ipsec security-association ospf6 mode transport
ipv6 ipsec security-association ospf6 spi 6
ipv6 ipsec security-association ospf6 auth-algo MD5 auth-key
12345678901234567890123456789012 keyLength 32
ipv6 ipsec security-association ospf6 Encrpt-algo AES-CTR EncrptKey
12345678901234567890123456789012 keyLength 32
ipv6 ipsec security-association ospf6 key-mode manual
```

```
ipv6 ipsec security-association ospf6 lifetime seconds 1
ipv6 ipsec security-association ospf6 lifetime bytes 1
```

Switch 30 policy configuration

In the example, the local addrress is fe80:0:0:0:b2ad:aaff:fe43:4d00, and the remote addrress is fe80:0:0:0:b2ad:aaff:fe43:100. The policy has the laddr confiugred to the link local address and the raddr is configured to the remote link local address with the direction configured to outbound.

```
ipv6 ipsec policy ospf1
ipv6 ipsec policy ospf1 admin enable
ipv6 ipsec policy ospf1 raddr fe80:0:0:0:b2ad:aaff:fe43:100
ipv6 ipsec policy ospf1 laddr fe80:0:0:0:b2ad:aaff:fe43:4d00
ipv6 ipsec policy ospf1 protocol ospv3
ipv6 ipsec policy ospf1 action permit
```

Laddr is configured to the remote link local address and raddr is configured to the local link local address with the direction configured to inbound.

```
ipv6 ipsec policy ospf2
ipv6 ipsec policy ospf2 admin enable
ipv6 ipsec policy ospf2 raddr fe80:0:0:0:b2ad:aaff:fe43:100
ipv6 ipsec policy ospf2 laddr fe80:0:0:0:b2ad:aaff:fe43:4d00
ipv6 ipsec policy ospf2 protocol ospfv3
ipv6 ipsec policy ospf2 action permit
```

Laddr is configured to the link local address and raddr is configured to ff02::05 with the direction configured to outbound.

```
ipv6 ipsec policy ospf3
ipv6 ipsec policy ospf3 admin enable
ipv6 ipsec policy ospf3 raddr ff02::05
ipv6 ipsec policy ospf3 laddr fe80:0:0:0:b2ad:aaff:fe43:4d00
ipv6 ipsec policy ospf3 protocol ospfv3
ipv6 ipsec policy ospf3 action permit
```

Laddr is configured to the remote link local address and the raddr is configured to ff02::05 with the direction configured to inbound.

```
ipv6 ipsec policy ospf4
ipv6 ipsec policy ospf4 admin enable
ipv6 ipsec policy ospf4 raddr fe80:0:0:0:b2ad:aaff:fe43:100
ipv6 ipsec policy ospf4 laddr ff02::05
ipv6 ipsec policy ospf4 protocol ospfv3
ipv6 ipsec policy ospf4 action permit
```

Laddr is configured to the link local address and raddr is configured to ff02::06 with the direction configured to outbound.

```
ipv6 ipsec policy ospf5
ipv6 ipsec policy ospf5 admin enable
ipv6 ipsec policy ospf5 raddr ff02::06
ipv6 ipsec policy ospf5 laddr fe80:0:0:0:b2ad:aaff:fe43:4d00
ipv6 ipsec policy ospf5 protocol ospfv3
ipv6 ipsec policy ospf5 action permit
```

Laddr is configured to the remote link local address and raddr is configured to ff02::06 with the direction configured to inbound.

```
ipv6 ipsec policy  ospf6
ipv6 ipsec policy  ospf6 admin enable
ipv6 ipsec policy ospf6 raddr fe80:0:0:0:b2ad:aaff:fe43:100
ipv6 ipsec policy ospf6 laddr ff02::06
ipv6 ipsec policy ospf6 protocol ospfv3
ipv6 ipsec policy ospf6 action permit
```

Switch 30 link table configuration

The following example displays the linking of the policy with the security association on Switch 30.

```
ipv6 ipsec  policy ospf1 security-association ospf1
ipv6 ipsec  policy ospf2 security-association ospf2
ipv6 ipsec  policy ospf3 security-association ospf4
ipv6 ipsec  policy ospf4 security-association ospf3
ipv6 ipsec  policy ospf5 security-association ospf5
ipv6 ipsec  policy ospf6 security-association ospf6
```

Switch 30 OSPFv3 configuration

The following example displays the OSPFv3 configuration on Switch 30.

```
router ospf ipv6-enable
router ospf
ipv6 router-id 2.2.2.2
ipv6 area 0.0.0.1
```

Switch 30 interface configuration

The following example displays the interface configuration on slot/port 1/10.

```
interface gigabitEthernet  1/10
no shut
ipv6 interface vlan 3
ipv6 interface address 2001::2/64
ipv6 interface enable
ipv6 ospf area 0.0.0.1
ipv6 ospf enable
ipv6 ipsec policy ospf1 dir out
ipv6 ipsec policy ospf2 dir in
ipv6 ipsec policy ospf3 dir out
ipv6 ipsec policy ospf4 dir in
ipv6 ipsec policy ospf5 dir out
ipv6 ipsec policy ospf6 dir in
ipv6 ipsec enable
```

Switch 30 VLAN configuration

The following example displays the creation of VLAN 3 and the configuration of IPsec on VLAN 3.

```
interface gigabitEthernet 1/10
no shut
exit
minvlan create 3 type port-mstprstp 0
vlan members add 3 1/10 portmember
interface vlan 3
ipv6 interface enable
ipv6 interface address 2001::2/64
ipv6 ospf area 0.0.0.1
ipv6 ospf enable
ipv6 ipsec policy ospf1 dir out
ipv6 ipsec policy ospf2 dir in
ipv6 ipsec policy ospf3 dir out
ipv6 ipsec policy ospf4 dir in
ipv6 ipsec policy ospf5 dir out
ipv6 ipsec policy ospf6 dir in
ipv6 ipsec enable
```

OSPFv3 virtual link IPsec configuration example

The following example displays a network using IPsec with OSPFv3 virtual link.

Note:

Slot and port information can differ depending on hardware platform. See *Installing* for specific hardware information.

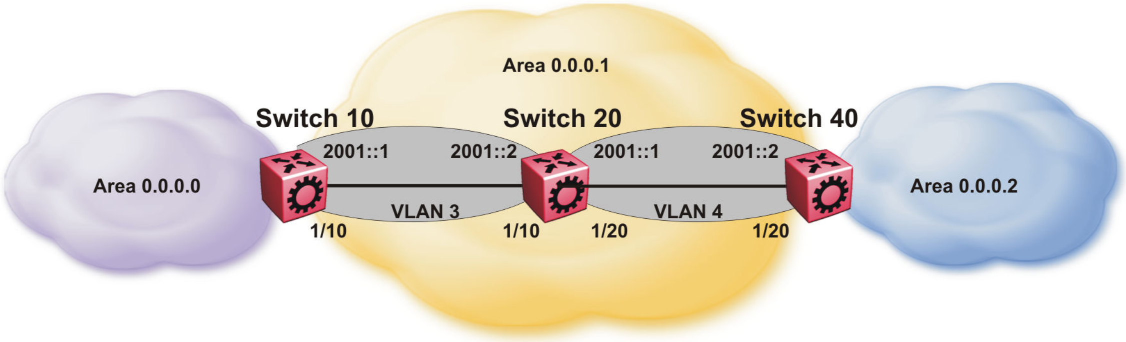


Figure 12: OSPFv3 virtual link with IPsec configuration

The following example displays the configuration of IPsec with OSPFv3 virtual link. For OSPFv3 conceptual and procedural information, see *Configuring IPv6 Routing*.

Switch 10 security association configuration

The following example displays the configuration of security associations for OSPFv3 for Switch 10.

```
ipv6 ipsec security-association ospf1
ipv6 ipsec security-association ospf1 encap-proto ESP
ipv6 ipsec security-association ospf1 mode transport
ipv6 ipsec security-association ospf1 spi 1
ipv6 ipsec security-association ospf1 auth-algo MD5 auth-key
12345678901234567890123456789012 keyLength 32
ipv6 ipsec security-association ospf1 Encrpt-algo AES-CTR EncrptKey
12345678901234567890123456789012 keyLength 32
ipv6 ipsec security-association ospf1 key-mode manual
ipv6 ipsec security-association ospf1 lifetime seconds 1
ipv6 ipsec security-association ospf1 lifetime bytes 1
```

Switch 10 OSPFv3 configuration

The following example displays the OSPFv3 configuration on Switch 10.

```
router ospf ipv6-enable
ipv6 forwarding
router ospf
ipv6 router-id 1.1.1.1
ipv6 area 0.0.0.1
ipv6 as-boundary-router
ipv6 area 0.0.0.0
```

Switch 10 virtual link and policy configuration

The following example displays the configuration of a OSPFv3 virtual link.

```
ipv6 area virtual-link 0.0.0.1 3.3.3.3
ipv6 area virtual-link 0.0.0.1 3.3.3.3 ipsec
ipv6 area virtual-link 0.0.0.1 3.3.3.3 ipsec security-association  ospf1
ipv6 area virtual-link 0.0.0.1 3.3.3.3 ipsec action permit
ipv6 area virtual-link 0.0.0.1 3.3.3.3 ipsec direction both
ipv6 area virtual-link 0.0.0.1 3.3.3.3 ipsec  enable
```

Switch 10 interface configuration

The following example displays the interface configuration on slot/port 1/10.

```
interface gigabitEthernet 1/10
no shut
ipv6 interface vlan 3
ipv6 interface address 2000::1/64
ipv6 interface enable
ipv6 ospf area 0.0.0.1
ipv6 ospf enable
```

Switch 10 VLAN configuration

The following example displays the creation of VLAN 3 and the configuration of IPsec on VLAN 3.

```
interface gigabitEthernet 1/10
no shut
exit
vlan create 3 type port-mstprstp 3
vlan members add 3 1/10 port-member
interface vlan 3
ipv6 interface enable
ipv6 interface address 2000::1/64
ipv6 ospf area 0.0.0.1
ipv6 ospf enable
```

Switch 20 OSPFv3 configuration

The following example displays the OSPFv3 configuration on Switch 20.

```
router ospf ipv6-enable
ipv6 forwarding
router ospf
ipv6 router-id 2.2.2.2
ipv6 area 0.0.0.1
```

Switch 20 interface configuration

The following example displays the interface configuration on slot/port 1/10 and 1/20.

```
interface gigabitEthernet 1/10
no shut
ipv6 interface vlan 3
ipv6 interface address 2000::2/64
ipv6 interface enable
ipv6 ospf area 0.0.0.1
ipv6 ospf enable

interface gigabitEthernet 1/20
no shut
ipv6 interface vlan 4
ipv6 interface address 2001::1/64
ipv6 interface enable
```

```
ipv6 ospf area 0.0.0.1
ipv6 ospf enable
```

Switch 20 VLAN configuration

The following example displays the creation of VLAN 3 and the configuration of IPsec on VLAN 3 and VLAN 4.

```
interface gigabitEthernet 1/10
no shut
exit
vlan create 3 type port-mstprstp 0
vlan members add 3 1/10 portmember
interface vlan 3
ipv6 interface enable
ipv6 interface address 2000::2/64
ipv6 ospf area 0.0.0.1
ipv6 ospf enable

interface gigabitEthernet 1/20
no shut
exit
vlan create 4 type port-mstprstp 0
vlan members add 4 1/20 portmember
interface vlan 4
ipv6 interface enable
ipv6 interface address 2001::1/64
ipv6 ospf area 0.0.0.1
ipv6 ospf enable
```

Switch 40 security association configuration

The following example displays the configuration of security associations for OSPFv3 for Switch 40.

```
ipv6 ipsec security-association ospf1
ipv6 ipsec security-association ospf1 encap-proto ESP
ipv6 ipsec security-association ospf1 mode transport
ipv6 ipsec security-association ospf1 spi 1
ipv6 ipsec security-association ospf1 auth-algo MD5 auth-key
12345678901234567890123456789012 keyLength 32
ipv6 ipsec security-association ospf1 Encrpt-algo AES-CTR EncrptKey
12345678901234567890123456789012 keyLength 32
ipv6 ipsec security-association ospf1 key-mode manual
ipv6 ipsec security-association ospf1 lifetime seconds 1
ipv6 ipsec security-association ospf1 lifetime bytes 1
```

Switch 40 OSPFv3 configuration

The following example displays the OSPFv3 configuration on Switch 40.

```
router ospf ipv6-enable
ipv6 forwarding
router ospf
ipv6 router-id 3.3.3.3
ipv6 area 0.0.0.1
ipv6 area 0.0.0.2
ipv6 as-boundary-router
```

Switch 40 OSPFv3 virtual link and policy configuration

The following example displays the configuration of a OSPFv3 virtual link.

```
ipv6 area virtual-link 0.0.0.1 1.1.1.1
ipv6 area virtual-link 0.0.0.1 1.1.1.1 ipsec
ipv6 area virtual-link 0.0.0.1 1.1.1.1 ipsec security-association  ospf1
ipv6 area virtual-link 0.0.0.1 1.1.1.1 ipsec action permit
```

```
ipv6 area virtual-link 0.0.0.1 1.1.1.1 ipsec direction both
ipv6 area virtual-link 0.0.0.1 1.1.1.1 ipsec enable
```

Switch 40 interface configuration

The following example displays the interface configuration on slot/port 1/20.

```
interface gigabitEthernet 1/20
no shut
ipv6 interface vlan 4
ipv6 interface address 2001::2/64
ipv6 interface enable
ipv6 ospf area 0.0.0.1
ipv6 ospf enable
```

Switch 40 VLAN interface configuration

The following example displays the creation of VLAN 4 and the configuration of IPsec on VLAN 4.

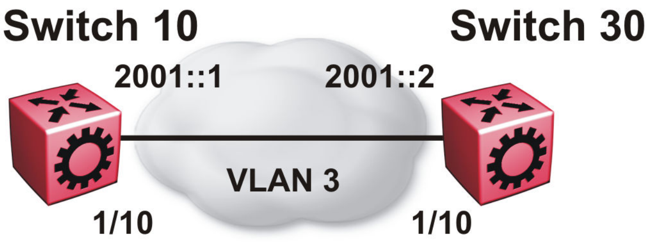
```
interface gigabitEthernet 1/20
no shut
exit
vlan create 4 type port-mstprstp 0
vlan members add 4 1/20
interface vlan 4
ipv6 interface enable
ipv6 interface address 2001::2/64
ipv6 ospf area 0.0.0.1
ipv6 ospf enable
```

IPsec configuration of TCP

The following example displays the configuration of IPsec for TCP.

Note:

Slot and port information can differ depending on hardware platform. See *Installing* for specific hardware information.



Switch 10 IPsec security association configuration

The following example displays the configuration of the IPsec security association for TCP for Switch 10.

```
ipv6 ipsec security-association tcp1
ipv6 ipsec security-association tcp1 encap-proto ESP
ipv6 ipsec security-association tcp1 mode transport
ipv6 ipsec security-association tcp1 spi 100
ipv6 ipsec security-association tcp1 auth-algo MD5 auth-key
12345678901234567890123456789012 keyLength 32
ipv6 ipsec security-association tcp1 Encrpt-algo AES-CTR EncrptKey
12345678901234567890123456789012 keyLength 32
ipv6 ipsec security-association tcp1 key-mode manual
ipv6 ipsec security-association tcp1 lifetime seconds 1
ipv6 ipsec security-association tcp1 lifetime bytes 1
```

Switch 10 IPsec policy configuration

The following example displays the configuration of the IPsec policy for TCP for Switch 10.

```
ipv6 ipsec policy tcp1
ipv6 ipsec policy tcp1 admin enable
ipv6 ipsec policy tcp1 raddr 2000::2
ipv6 ipsec policy tcp1 raddr 2000::2 laddr 2000::1
ipv6 ipsec policy tcp1 raddr 2000::2 protocol tcp sport 23 dport 23
ipv6 ipsec policy tcp1 raddr 2000::2 action permit
```

Switch 10 linking the IPsec policy with the IPsec security association

The following example displays the linking of the IPsec policy with the IPsec security association

```
ipv6 ipsec policy tcp1 security-association tcp1
```

Switch 10 interface configuration

The following examples displays the configuration of IPsec for slot/port 1/10.

```
interface gigabitEthernet 1/10
no shut
ipv6 interface vlan 3
ipv6 interface address 2000::1/64
ipv6 interface enable
ipv6 ipsec policy tcp1 dir both
ipv6 ipsec enable
```

Switch 10 VLAN configuration

The following example displays the creation and configuration of VLAN 3.

```
interface gigabitEthernet 1/10
no shut
exit
vlan create 3 type port-mstprstp 3
vlan members add 3 1/10 portmember
interface vlan 3
ipv6 interface enable
ipv6 interface address 2000::1/64
ipv6 ipsec policy tcp1 dir both
ipv6 ipsec enable
```

Switch 30 IPsec security association configuration

The following example displays the configuration of the IPsec security association for TCP for Switch 10.

```
ipv6 ipsec security-association tcp1
ipv6 ipsec security-association tcp1 encap-proto ESP
ipv6 ipsec security-association tcp1 mode transport
ipv6 ipsec security-association tcp1 spi 100
ipv6 ipsec security-association tcp1 auth-algo MD5 auth-key
12345678901234567890123456789012 keyLength 32
ipv6 ipsec security-association tcp1 Encrpt-algo AES-CTR EncrptKey
12345678901234567890123456789012 keyLength 32
ipv6 ipsec security-association tcp1 key-mode manual
ipv6 ipsec security-association tcp1 lifetime seconds 1
ipv6 ipsec security-association tcp1 lifetime bytes 1
```

Switch 30 IPsec policy configuration

The following example displays the configuration of the IPsec policy for TCP for Switch 10.

```
ipv6 ipsec policy tcp1
ipv6 ipsec policy tcp1 admin enable
ipv6 ipsec policy tcp1 raddr 2000::1
ipv6 ipsec policy tcp1 raddr 2000::1 laddr 2000::2
ipv6 ipsec policy tcp1 raddr 2000::1 protocol tcp sport 23 dport 23
ipv6 ipsec policy tcp1 raddr 2000::1 action permit
```

Switch 30 linking the IPsec policy with the IPsec security association

The following example displays the linking of the IPsec policy with the IPsec security association

```
ipv6 ipsec policy tcp1 security-association tcp1
```

Switch 30 interface configuration

The following examples displays the configuration of IPsec for slot/port 1/10.

```
interface gigabitEthernet 1/10
no shut
ipv6 interface vlan 3
ipv6 interface address 2000::2/64
ipv6 interface enable
ipv6 ipsec policy tcp1 dir both
ipv6 ipsec enable
```

Switch 30 VLAN configuration

The following example displays the creation and configuration of VLAN 3.

```
interface gigabitEthernet 1/10
no shut
exit
vlan create 3 type port-mstprstp 3
vlan members add 3 1/10 portmember
interface vlan 3
ipv6 interface enable
ipv6 interface address 2000::2/64
ipv6 ipsec policy tcp1 dir both
ipv6 ipsec enable
```

Chapter 5: MACsec

The following sections describe Media Access Control Security (MACsec) and its configuration.

Note:

This feature is not supported on all hardware platforms. If you do not see commands for this feature in the command list or EDM, the feature is not supported on your hardware. For more information about feature support, see *Release Notes*.

MACsec fundamentals

MAC Security (MACsec) is based on the IEEE 802.1ae standard that allows authorized systems in a network to transmit data confidentially and to protect against data transmitted or modified by unauthorized devices.

You can use MACsec for core and enterprise edge switches to secure site-to-site connectivity between data centers, provide data security on links that run over public ground, or outside the physically secure boundaries of a site. You can use MACsec on access switches to secure host to switch connectivity, and host to switch connectivity in an environment where both trusted and untrusted hosts co-exist.

In addition to host level authentication, MACsec capable LANs provide data origin authentication, data confidentiality, and data integrity between authenticated hosts or systems. MACsec protects data from external hacking while the data passes through the public network to reach a receiver host.

MACsec enabled hosts encrypt and decrypt every frame exchanged between them using a MACsec key. The source MACsec host encrypts data frames and destination MACsec host decrypts the frames, ensuring delivery of the frame in its original condition to the recipient host. This ensures secure data communication.

You can configure MACsec encryption over any type of point-to-point Ethernet or emulated Ethernet connection, which includes:

- Dark fiber
- Conventional wavelength-division multiplexing/dense wavelength-division multiplexing (CWDM/DWDM) service
- Multiprotocol label switching (MPLS) point-to-point (ELINE)
- Provider Backbone Bridge Traffic Engineering (PBB-TE)

You can configure MACsec on a physical port or on a trunk group level, which includes: Split MultiLink Trunking (SMLT), distributed MultiLink Trunking (DMLT), or Link aggregate group (LAG).

You configure a pre-shared key on either end of the MACsec link. The pre-shared key is an interface parameter, not a switch-wide parameter.

Note:

MACsec encrypts all packets. If you configure MACsec on one or more MultiLink Trunking (MLT) port members on one side, you must configure MACsec on the same port members on the other side. If you do not do this, the port can physically be up, but any overlying protocols can be down. You do not have to provision MACsec on all MLT port members, but if you configure MACsec on an MLT port member on one side, you must also provision MACsec on the corresponding MLT port on the other side.

One way to detect a mismatch of MACsec configuration is to use Virtual Link Aggregation Protocol (VLACP) on the links.

MACsec provides security at the data link layer or the physical layer. It provides enhancements at the MAC service sub layer for its operation and services to the upper layer.

MACsec is an interface level feature and is disabled by default.

MACsec keys

MACsec provides industry-standard security through secure point-to-point Ethernet links. The point-to-point links are secured after matching security keys.

Security keys are of two types:

- connectivity association key (CAK), which is a configured *pre-shared key*. If you enable MACsec using the static connectivity association key (CAK) security mode.

  Important:

  The switch currently supports the configuration of a pre-shared key to enable MACsec using the static connectivity association key (CAK) security mode.

  The CAK must be identical across both ends of MACsec links.

- secure association key (SAK), which is a configured *static secure association key*. If you use the static secure association key (SAK) security mode. SAKs are short-lived keys derived from the CAK or pre-configured for a particular secure channel (SC). MACsec uses a timer to refresh these keys so that the key, as well the session, is secure.

MACsec uses derived keys to encrypt or decrypt data at each end of the MACsec links.

Integrity Check Verification (ICV)

MACsec ensures data integrity using Integrity Check Verification (ICV). MACsec introduces an 8 or 16 byte SecTag after the Ethernet header, and an 8 or 16 byte calculated ICV after the Encrypted Payload. MACsec computes the ICV for the entire frame, starting from the Ethernet header, SecTag until the Checksum. The receiving side recalculates the ICV after data decryption and verifies if the received ICV and computed ICV match. If the ICVs do not match, it indicates that data is modified, and MACsec drops the frame.

MACsec security modes

The static Connectivity Association Key (CAK) security mode is the only supported MACsec security mode on the platform, and is also the most common mode to enable MACsec.

When you use the static connectivity association key (CAK) security mode to enable MACsec, you configure a community association on both ends of the link. A pre-shared key establishes the MACsec relationship between the switches on each end of the Ethernet link. The two pre-shared security association keys (SAKs) include a connectivity association key name (CKN) and its own connectivity association key (CAK). The MACsec CKN and CAK are configured in a connectivity association and the CAK must match on both ends of the link to initially enable MACsec.

To ensure link security, the system periodically refreshes keys based on traffic volume and link speed.

To enable MACsec at the port level, you must first associate the port to the connectivity association. You complete the configuration within the connectivity association, but outside of the secure channel.

When you use the static CAK security mode, the system automatically creates two secure channels, one for inbound traffic and another for outbound traffic. You cannot configure any parameters in the automatically-created secure channels.

The CAK security mode ensures security by frequently refreshing to a new random security key, and by only sharing the security key between the two devices on the MACsec-secured point-to-point link.

MACsec provides options to encrypt user payload, or send in a clear confidential offset, to start the encryption from selectable bytes of 0, 30, and 50 after the SecTag header.

You can choose to configure the following optional features:

- Data encryption — If you disable encryption, MACsec forwards traffic in clear text. You can view that data that is not encrypted in the Ethernet frame that travels across the link. Even if you disable encryption the MACsec header applies to the frame and integrity checks make sure that traffic has not been tampered with.
- Confidentiality offset — If encryption is enabled, and an offset is not configured, all traffic in the connectivity is encrypted. The confidentiality offset provides a way to start encryption after a few bytes following the Ethernet header. The confidentiality offset facilitates traffic flow inspection and classification on intermediate devices by not encrypting the Network Layer header for IPv4 or IPv6. For instance, if you configure the offset to 30, the IPv4 header and the TCP/UDP header are not encrypted. If you configure the offset to 50, the IPv6 header and the TCP/UDP header is not encrypted.

Connectivity associations (CA) and secure channels (SC)

You configure MACsec in connectivity associations. You can enable MACsec after you attach a connectivity association to an interface. To use the static CAK security mode to enable MACsec, you must create, and configure connectivity associations on both ends of the link.

A connectivity association (CA) is a logical representation of a MACsec domain within a network. Each connectivity association is associated with a connectivity association key (CAK). MACsec links are associated with a CA to establish end-to-end MACsec communication. Every MACsec enabled interface is a member of one connectivity association. Switch ports are members of a connectivity association, and can only be a member of one connectivity association.

A secure channel (SC) is a unidirectional channel that connects two endpoints of MACsec. A secure channel is a long-term relationship that persists through the sequence of secure associations.

A secure association (SA) is a short-lived relationship within an SC. MACsec identifies each security association by AN, and supported Secure association key (SAK), which is derived from the CAK. The secure association key is used on both ends of MACsec links to encrypt and decrypt the frames. SAKs are frequently refreshed for security reasons. Periodically changing SAs allows the use of fresh keys without terminating the SC relationship.

You configure connectivity associations. Secure channels and secure associations are internally created in the hardware.

MACsec components

MACsec has three major components:

- **Security entity (SecY)**

  SecY is the entity that operates the MACsec protocol within the system. You configure a secure community association (CA) to meet the requirements of MACsec for connectivity between stations that attach to an individual LAN. Unidirectional secure channels (SC) support each CA. Each SC supports secure transmission of frames through the use of symmetric key cryptography from one of the systems to all the others in the CA.

  Each SecY transmits frames conveying secure MACsec service requests on a single SC, and receives frames conveying secure service indications on separate SCs, one for each of the other SecYs that participate in the secure CA.

  A connectivity association (CA) is a logical representation of a MACsec domain within a network. Each connectivity association is associated with a connectivity association key (CAK). MACsec links are associated with a CA to establish end-to-end MACsec communication. Every MACsec enabled interface is a member of one connectivity association. Switch ports are members of a connectivity association, and can only be a member of one connectivity association.

A secure channel (SC) is a unidirectional channel that connects two endpoints of MACsec. A secure channel is a long-term relationship that persists through the sequence of secure associations. An SC is a unidirectional point to multipoint communication, and can persist through Secure Association Key (SAK) changes. A sequence of Secure Associations (SAs) support each SC and allow for the periodic use of fresh keys without terminating the relationship. A single secret key or a set of keys support each SA, where the cryptographic operations used to protect one frame require more than one key. An SCI identifies each SC. An SCI is comprised of a unique 48-bit universally administered MAC address, identifying the system to which the transmitting SecY belongs, concatenated with a 16-bit port number, identifying the SecY within that system.

The SCI concatenated with a two-bit AN identifies each SA. The Secure Association Identifier (SAI) created allows the receiving SecY to identify the SA, and the SAK used to decrypt and authenticate the received frame. The AN, and hence the SAI, are only unique for the SAs that can be used or recorded by participating SecYs at any instant.

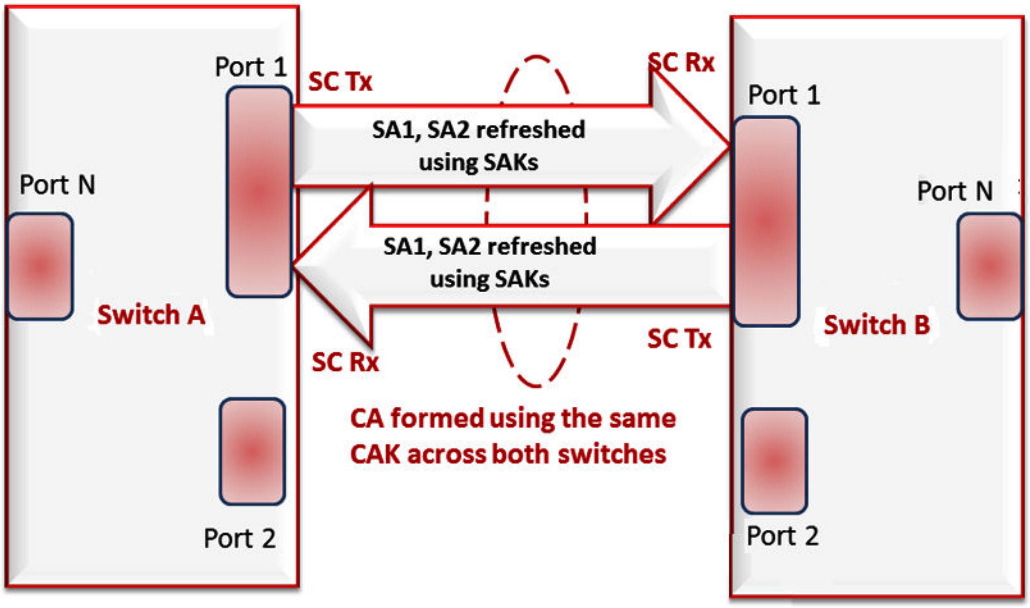

Port 1
SC Tx
SC Rx
Port 1
SA1, SA2 refreshed using SAKs
Port N
Port N
SA1, SA2 refreshed using SAKs
Switch A
Switch B
SC Tx
SC Rx
CA formed using the same CAK across both switches
Port 2
Port 2

Figure 13: MACsec relationship

- **Key agreement entity (KaY)**

  The KaY in MACsec is responsible for CAK and SAK computations, distributions and maintenance of those keys. CAK is a global key which is persistent until the CA exists. When you configure the CAK, ensure that it is identical across MACsec links. SAK are short-lived keys derived from the CAK, or pre-configured for a particular SC. MACsec uses a timer to refresh these keys so that the key, as well the session, is secure.

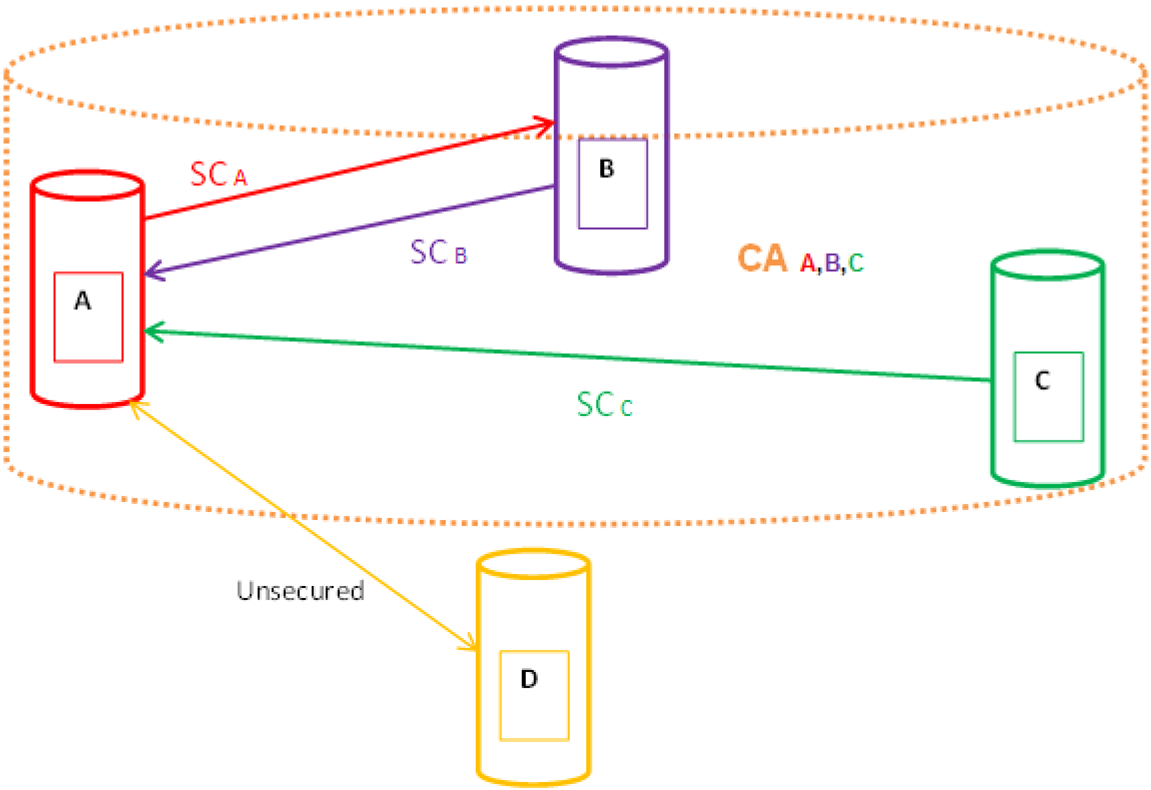
  A separate 802.1x-2010 standard is available to automate the above key exchanges and maintenance. The keys are pre-configured.

- **Integrity check verification (ICV) or Cryptographic entity**

  The Cryptographic entity provides integrity check protection and validation for frames transmitted or received through the SecY layer. The ICV is calculated for the frame SA/DA, SecTag, User Payload, and CRC. The calculated ICV is appended at the end-of-frame, recalculated at the receiver side of MACsec link and validated to see if they are equal. This is called Integrity Check Verification (ICV). The frames that pass the integrity check are further processed, while the system drops the frames that fail the integrity check.

MACsec configuration provides options to encrypt user payload or send in the clear. The option to start the encryption from N bytes after the Ethernet header also exists.

In the following figure, CA connects switches A, B, and C by their respective SC and SAK. Station D cannot participate in the secure communication between A, B, or C as station D does not know the SAK.



MACsec operation

As shown in the following figure, a host that connects to Switch A sends an Ethernet frame to a host that connects to Switch B. Switch A encrypts the frame, excluding the Ethernet header and optionally the 802.1Q header. Switch A also appends MACsec information like SecTag and ICV to the encrypted payload and transmits the frame using normal frame transmission. This process ensures data confidentiality.

On receiving the frame, Switch B decrypts the frame. Switch B recalculates the ICV using a MACsec key and the SecTag present in the frame. If the ICV present in the received frame matches the recalculated ICV, the switch processes the frame. If the two ICVs do not match, the switch discards the frame. This process ensures data origin authenticity and data integrity. The encryption and decryption algorithms follow the AES-GCM-128 standard.

The MACsec key between switches A and B are statically pre-configured.

Note:

MACsec will be operational between two switches across Point-to-Point Connectivity only when the switches are either directly connected or across a network cloud that provides P2P connectivity between the two switches.

For example, in the following figure you can enable MACsec between two switches across a network cloud where P2P connectivity between the switches is provided via services such as P2P, MPLS, Layer 2 VPN (ELINE), or connectivity across Dark Fiber. However, it is important to note that MACsec will not be operational between two switches across a network cloud if the intermediate routers/switches need to inspect the VLAN tag or IP header for service classification. This is because MACsec encrypts the entire data frame including the VLAN header and as such the intermediate switches/routers will not have visibility into the same to perform service classification.

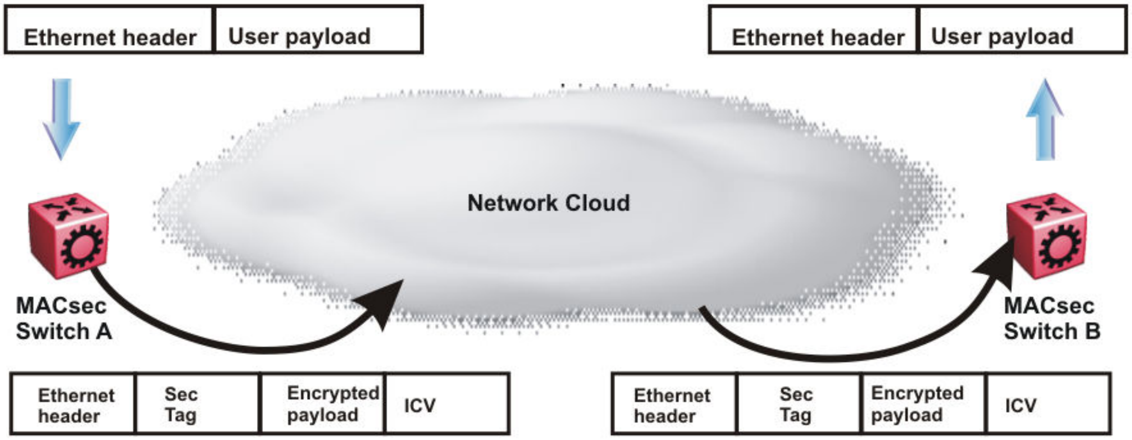


Figure 14: MACsec operation

MACsec performance

To monitor MACsec performance, view the performance statistics. For information on the supported statistics, see *Monitoring Performance*.

MACsec configuration using CLI

Configuring a connectivity association

Use the following procedure to configure a connectivity association (CA) in static CAK security mode using CLI.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Configure a connectivity association (CA):

   ```
   macsec connectivity-association WORD<5-15> connectivity-association-key WORD<10-32>
   ```

3. Enter GigabitEthernet Interface Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

   ```
   interface GigabitEthernet {slot/port[/sub-port][-slot/port[/sub-port]][,...]}
   ```

   Note:

   If your platform supports channelization for 40 Gbps ports and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

4. Associate a port with CA:

   ```
   macsec connectivity-association WORD<5-15>
   ```

5. Enable MACsec on the port:

   ```
   macsec enable
   ```

Example

Configure a connectivity association and enable MACsec on a port:

Note:

Slot and port information can differ depending on hardware platform. See *Installing* for specific hardware information.

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#macsec connectivity-association caname1 connectivity-association-key
1029384756abcdef
```

```
Switch:1(config)#interface gigabitethernet 1/2
Switch:1(config-if)#macsec connectivity-association caname1
```

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#macsec connectivity-association caname1 connectivity-association-key
1029384756abcdef
Switch:1(config)#interface gigabitethernet 4/17
Switch:1(config-if)#macsec connectivity-association caname1
```

Variable definitions

Use the data in the following table to use the **`macsec`** command.

Variable	Value
connectivity-association *WORD<5–15>*	Specifies a connectivity-association name. It is a 5 to 15 character alphanumeric string.
connectivity-association-key *WORD<10–32>*	Specifies the value of the connectivity-association key (CAK). A 32 character hexadecimal string is recommended.

Use the data in the following table to use the **`interface gigabitethernet`** command.

Variable	Value
{slot/port[/sub-port][-slot/port[/sub-port]][,...]}	Specifies the port that you want to associate with the connectivity association (CA). Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If your platform supports channelization for 40 Gbps ports and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

Updating the connectivity association key (CAK)

Use the following procedure to update the connectivity association key (CAK).

Procedure

1. Enter GigabitEthernet Interface Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

   ```
   interface GigabitEthernet {slot/port[/sub-port][-slot/port[/sub-port]][,...]}
   ```

Note:

If your platform supports channelization for 40 Gbps ports and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

2. Disable MACsec on the port:

   ```
   no macsec enable
   ```

3. Update the connectivity association key (CAK):

   ```
   macsec connectivity-association WORD<5–15> connectivity-association
   key WORD<10–32>
   ```

4. Enable MACsec on the port:

   ```
   macsec enable
   ```

Example

Update the connectivity association key (CAK):

Note:

Slot and port information can differ depending on hardware platform. See *Installing* for specific hardware information.

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#interface gigabit 1/2
Switch:1(config-if)#no macsec enable
Switch:1(config-if)#macsec connectivity-association caname1 connectivity-association-key
1029384756abcdef
Switch:1(config-if)#macsec enable
```

Variable definitions

Use the data in the following table to use the **`macsec`** command.

Variable	Value
connectivity-association *WORD<5–15>*	Specifies a connectivity-association name. It is a 5 to 15 character alphanumeric string.
connectivity-association-key *WORD<10–32>*	Specifies the value of the connectivity-association key (CAK). A 32 character hexadecimal string is recommended.

Use the data in the following table to use the **`interface gigabitethernet`** command.

Variable	Value
{slot/port[/sub-port][-slot/port[/sub-port]][,...]}	Specifies the port that you want to associate with the connectivity association (CA). Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If your platform supports channelization for 40 Gbps ports

Variable	Value
	and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

Configuring MACsec encryption on a port

Use the following procedure to enable or disable encryption on a MACsec capable port. The default is disabled.

About this task

If you disable encryption, MACsec forwards traffic in clear text. You can view that data that is not encrypted in the Ethernet frame that travels across the link. Even if you disable encryption the MACsec header applies to the frame and integrity checks make sure that traffic has not been tampered with.

Procedure

1. Enter GigabitEthernet Interface Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

   ```
   interface GigabitEthernet {slot/port[/sub-port][-slot/port[/sub-port]][,...]}
   ```

   Note:

   If your platform supports channelization for 40 Gbps ports and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

2. Enable MACsec encryption on the port:

   ```
   macsec encryption enable
   ```

3. Disable MACsec encryption on the port:

   ```
   no macsec encryption enable
   ```

Example

Configure MACsec encryption on a port:

Note:

Slot and port information can differ depending on hardware platform. See *Installing* for specific hardware information.

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#interface gigabit 1/2
Switch:1(config-if)#macsec encryption enable
```

Configuring the confidentiality offset on a port

Use the following procedure to configure the confidentiality offset on a port. The default is disabled.

About this task

The confidentiality offset provides a way to start encryption after a few bytes following the Ethernet header. The confidentiality offset facilitates traffic flow inspection and classification on intermediate devices by not encrypting the Network Layer header for IPv4 or IPv6. For instance, if you configure the offset to 30, the IPv4 header and the TCP/UDP header are not encrypted. If you configure the offset to 50, the IPv6 header and the TCP/UDP header is not encrypted.

Procedure

1. Enter GigabitEthernet Interface Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

   ```
   interface GigabitEthernet {slot/port[/sub-port][-slot/port[/sub-port]][,...]}
   ```

   Note:

   If your platform supports channelization for 40 Gbps ports and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

2. Configure confidentiality offset on the port:

   ```
   macsec confidentiality-offset <30-50>
   ```

3. Disable the confidentiality offset on the port:

   ```
   no macsec confidentiality-offset
   ```

Example

Configuring the confidentiality offset on the port:

Note:

Slot and port information can differ depending on hardware platform. See *Installing* for specific hardware information.

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#interface gigabit 1/2
Switch:1(config-if)#macsec confidentiality-offset 30
```

Variable definitions

Use the data in the following table to use the **`macsec confidentiality-offset`** command.

Variable	Value
<30–50>	Specifies the bytes after the Ethernet header from which data encryption begins. Valid values are 30 and 50.

Use the data in the following table to use the **`interface gigabitethernet`** command.

Variable	Value
{slot/port[/sub-port][-slot/port[/sub-port]][,...]}	Specifies the port that you want to associate with the connectivity association (CA). Identifies the slot and port in one of the following formats: a single slot and port (slot/port), a range of slots and ports (slot/port-slot/port), or a series of slots and ports (slot/port,slot/port,slot/port). If your platform supports channelization for 40 Gbps ports and the port is channelized, you must also specify the sub-port in the format slot/port/sub-port.

Viewing the MACsec connectivity association details

Perform this procedure to view the MACsec connectivity association (CA) details.

Procedure

1. Enter Privileged EXEC mode:

   `enable`

2. View the MACsec connectivity association (CA) details:

   `show macsec connectivity-association` *`WORD<5-15>`*

   Note:

   This command displays the MACsec connectivity association (CA) details, including the MD5 hashed value of the CA key.

Example

View the MACsec connectivity association details:

Note:

Slot and port information can differ depending on hardware platform. For more information about specific hardware, see *Installing*.

```
Switch:1>enable
Switch:1#show macsec connectivity-association ca333

========================================================================
                     MACSEC Connectivity Associations Info
========================================================================
  Connectivity                  Connectivity                    Port
```

```
Association Name             Association Key Hash           Members
------------------------------------------------------------------------
 ca333                1304a8fcc51296e7229683ff6882424a       1/40
```

Viewing MACsec status

Perform this procedure to view MACsec status.

About this task

This command displays the status for the following:

- MACsec status
- MACsec encryption status
- The associated Connectivity Association (CA) name

Note:

If you do not specify a port number, the information on all MACsec capable interfaces is displayed.

Procedure

1. Enter Privileged EXEC mode:

   ```
   enable
   ```

2. View the MACsec status:

   ```
   show macsec status {slot/port[/sub-port][-slot/port[/sub-port]]
   [,...]}
   ```

Example

View the MACsec status:

Note:

Slot and port information can differ depending on hardware platform. For more information about specific hardware, see *Installing*.

The current release does not support replay protect.

```
Switch:1>enable
Switch:1#show macsec status

===========================================================================
                               MACSEC Port Status
===========================================================================
        MACSEC   Encryption  Replay       Replay        Encryption     CA
PortId  Status      Status   Protect   Protect W'dow     Offset       Name
---------------------------------------------------------------------------
1/39    enabled    enabled    disabled       --      ipv4Offset(30) ca333
1/40    disabled   disabled   disabled       --        none         Nil
```

```
Switch:1#show macsec status 1/40

===========================================================================
                               MACSEC Port Status
```

```
============================================================================
        MACSEC   Encryption  Replay       Replay        Encryption     CA
PortId  Status     Status    Protect   Protect W'dow     Offset        Name
----------------------------------------------------------------------------
1/40    enabled    enabled    disabled       --      ipv4Offset(30)  ca333
```

MACsec configuration using EDM

Configuring connectivity associations

Use the following procedure to configure connectivity associations (CA) using EDM.

Procedure

1. In the navigation tree, expand the following folders: **Configuration** > **Edit**.
2. Click **Chassis**.
3. In the Chassis window, click the **MAC Security** tab.
4. Click **Insert**.
   a. In the **AssociationName** field, type the connectivity-association name.
   b. In the **AssociationKey** field, type the value of the connectivity-association key.

      Note:

      The connectivity-association key appears as an MD5-hashed text in the MAC security table.

   c. Click **Insert** to save the configuration.
5. Click **Apply**.

Configuring CA field descriptions

Use the data in the following table to use the **MAC Security** tab.

Name	Description
AssociationName	Specifies a name for each connectivity association configured on the device.
AssociationKey	Specifies a pre-shared, connectivity association key associated with each connectivity association configured on the device.
AssociationPortMembers	Specifies the set of ports for which this connectivity association is associated.

Associating a port with a connectivity association

Use the following procedure to associate a port with a connectivity association (CA) using EDM.

Procedure

1. In the Device Physical View, click on the port that you want to associate with the connectivity association.
2. In the navigation tree, expand the following folders: **Configuration** > **Edit** > **Port**.
3. Click **General**.
4. In the Port General window, click the **MAC Security** tab.
5. In the **CAName** field, type the connectivity-association name.
6. In the **OffsetValue** field, select the value of confidentiality offset to be achieved.
7. Select the **EncryptionEnable** checkbox to enable encryption for the frames transmitted on the port.
8. Select the **Macsec Enable** checkbox to enable MACsec on the port.
9. Click **Apply** to save the configuration.

Associating a port with CA field descriptions

Use the data in the following table to configure the **MAC security** tab.

Name	Description
CAName	Specifies the name of the connectivity association attached to the port or interface.
OffsetValue	Offsets MACsec encryption in an IPv4 TCP/UDP header or IPv6 TCP/UDP header. The confidentiality offset provides a way to start encryption after a few bytes following the Ethernet header. The confidentiality offset facilitates traffic flow inspection and classification on intermediate devices by not encrypting the Network Layer header for IPv4 or IPv6. For instance, if you configure the offset to 30, the IPv4 header and the TCP/UDP header are not encrypted. If you configure the offset to 50, the IPv6 header and the TCP/UDP header is not encrypted.
EncryptionEnable	Specifies the encryption status per port. Use this field to enable or disable encryption for each MACsec capable port.
Macsec Enable	Enables or disables MACsec on the port.

Chapter 6: RADIUS

Remote Access Dial-In User Services (RADIUS) is a distributed client/server system that assists in securing networks against unauthorized access, allowing a number of communication servers and clients to authenticate user identity through a central database. The database within the RADIUS server stores information about clients, users, passwords, and access privileges including the use of shared secret.

RADIUS is a fully open and standard protocol, defined by two Requests for Comments (RFC) (Authentication: RFC 2865, Accounting: RFC 2866). With the switch, you use RADIUS authentication to get secure access to the system (console/Telnet/SSH/EDM), and RADIUS accounting to track the management sessions (CLI only).

RADIUS support for IPv6

RADIUS supports both IPv4 and IPv6 with no differences in functionality or configuration in all but the following case. When you add or update a RADIUS server in Enterprise Device Manager (EDM) you must specify if the address type is an IPv4 or an IPv6 address.

How RADIUS works

A RADIUS application has two components:

- RADIUS server

  A computer equipped with server software (for example, a UNIX workstation) that is located at a central office or campus. The server has authentication and access information in a form that is compatible with the client. Typically, the database in the RADIUS server stores client information, user information, password, and access privileges, including the use of a shared secret. A network can have one server for both authentication and accounting, or one server for each service.

- RADIUS client

  A device, router, or a remote access server, equipped with client software, that typically resides on the same local area network (LAN) segment as the server. The client is the network access point between the remote users and the server.

The two RADIUS processes are

- RADIUS authentication—Identifies remote users before you give them access to a central network site.
- RADIUS accounting—Performs data collection on the server during a remote user's dial-in session with the client.

Configuration of the RADIUS server and client

For more information about how to configure a RADIUS server, see the documentation that came with the server software.

To use these servers, you must first obtain the software for the server you will use. Also, you must make changes to one or more configuration files for these servers.

RADIUS authentication

You can use RADIUS authentication to use a remote server to authenticate logons. The RADIUS server also provides access authority. RADIUS assists network security and authorization by managing a database of users. The device uses this database to verify user names and passwords as well as information about the type of access priority available to the user.

When the RADIUS client sends an authentication request requesting additional information such as a SecurID number, it sends it as a challenge-response. Along with the challenge-response, it sends a reply-message attribute. The reply-message is a text string, such as `Please enter the next number on your SecurID card:`. The RFC defined maximum length of each reply-message attribute is 253 characters. If you have multiple instances of reply-message attributes that together form a large message that displays to the user, the maximum length is 2000 characters.

You can use additional user names to access the device, in addition to the six existing user names of ro, L1, L2, L3, rw, and rwa. The RADIUS server authenticates the user name and assigns one of the existing access priorities to that name. Unauthenticated user names are denied access to the device. You must add user names ro, L1, L2, L3, rw, and rwa to the RADIUS server if you enable authentication. Users not added to the server are denied access.

The following list shows the user configurable options of the RADIUS feature:

- Up to 10 RADIUS servers in each device for fault tolerance (each server is assigned a priority and is contacted in that order).
- A secret key for each server to authenticate the RADIUS client
- The server UDP port
- Maximum retries allowed
- Time-out period for each attempt

Note:

If you enable enhanced secure mode with the **`boot config flags enhancedsecure-mode`** command, you enable new access levels, along with stronger password complexity, length, and minimum change intervals. With enhanced secure mode enabled, the switch supports the following access levels for RADIUS authentication:

- Administrator
- Privilege
- Operator
- Auditor
- Security

The switch associates each username with a certain role and appropriate authorization rights to view and configure commands. For more information on system access fundamentals and configuration, see *Administering*.

Use of RADIUS to modify user access to CLI commands

The switch provides CLI command access based on the configured access level of a user. However, you can use RADIUS to override CLI command access provided by the switch.

To override user access to CLI commands, you must configure the command-access-attribute on the switch and on the RADIUS server. (The switch uses decimal value 194 as the default for this parameter.) On the RADIUS server, you can then define the commands that the user can or cannot access.

Important:

When you enable RADIUS on the switch and configure a RADIUS server to be used by CLI or EDM, the server authenticates the connection, whether it is FTP, HTTPS, SSH, or Telnet. However, in the event that the RADIUS server is unresponsive or is unreachable, the switch falls back to the local authentication, so that you can access the switch using your local login credentials.

Regardless of the RADIUS server configuration, you must configure the user's access on the switch based on the six platform access levels.

RADIUS accounting

RADIUS accounting logs all of the activity of each remote user in a session on the centralized RADIUS accounting server.

Session-IDs for each RADIUS account generate as 12-character strings. The first four characters in the string form a random number in hexadecimal format. The last eight characters in the string indicate the number of user sessions started since the last restart, in hexadecimal format.

The Network Address Server (NAS) IP address for a session is the address of the device interface to which the remote session is connected over the network. For a console session, modem session, and sessions running on debug ports, this value is set to 0.0.0.0, as is the case with RADIUS authentication.

The following table summarizes the events and associated accounting information logged at the RADIUS accounting server.

Table 4: Accounting events and logged information

Event	Accounting information logged at server
Accounting is turned on at router	• Accounting on request: NAS IP address
Accounting is turned off at router	• Accounting off request: NAS IP address
User logs on	• Accounting start request: NAS IP address • Session ID • User name
More than 40 CLI commands are executed	• Accounting interim request: NAS IP address

Table continues…

Event	Accounting information logged at server
	• Session ID • CLI commands • User name
User logs off	• Accounting stop request: NAS IP address • Session ID • Session duration • User name • Number of input octets for session • Number of octets output for session • Number of packets input for session • Number of packets output for session • CLI commands

When the device communicates with the RADIUS accounting server, the following actions occur:

1. If the server sends an invalid response, the response is silently discarded and the server does not make an attempt to resend the request.
2. User-specified number of attempts are made if the server does not respond within the user-configured timeout interval. If a server does not respond to any of the retries, requests are sent to the next priority server (if configured). You can configure up to 10 RADIUS servers for redundancy.

RADIUS configuration using CLI

You can configure Remote Access Dial-In User Services (RADIUS) to secure networks against unauthorized access, and allow communication servers and clients to authenticate users identity through a central database.

The database within the RADIUS server stores client information, user information, password, and access privileges, including the use of shared secret.

RADIUS supports IPv4 and IPv6 addresses.

RADIUS is a fully open and standard protocol, defined by RFCs (Authentication: RFC 2865, accounting RFC 2866). With the switch, you use RADIUS authentication to secure access to the device (console/Telnet/SSH), and RADIUS accounting to track the management sessions for Command Line Interface (CLI) only.

RADIUS authentication allows the remote server to authenticate logons. RADIUS accounting logs all of the activity of each remote user in a session on the centralized RADIUS accounting server.

Configuring RADIUS attributes

Configure RADIUS to authenticate user identity through a central database.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Configure RADIUS access priority:

   ```
   radius access-priority-attribute <192-240>
   ```

3. Configure RADIUS accounting:

   ```
   radius accounting {attribute-value <192-240>|enable|include-cli-commands}
   ```

4. Configure the RADIUS authentication info attribute value:

   ```
   radius auth-info-attr-value <0-255>
   ```

5. Clear RADIUS statistics:

   ```
   radius clear-stat
   ```

6. Configure the value of the CLI commands:

   ```
   radius cli-commands-attribute <192-240>
   ```

7. Configure the value of the command access attribute:

   ```
   radius command-access-attribute <192-240>
   ```

8. Configure the maximum number of servers allowed:

   ```
   radius maxserver <1-10>
   ```

9. Configure the multicast address attribute:

   ```
   radius mcast-addr-attr-value <0-255>
   ```

Example

```
Switch:1> enable
```

```
Switch:1# configure terminal
```

Configure RADIUS access priority:

```
Switch:1(config)# radius access-priority-attribute 192
```

Configure RADIUS accounting to include CLI commands:

```
Switch:1(config)# radius accounting include-cli-commands
```

Variable definitions

Use the data in the following table to use the **radius** command.

Variable	Value
access-priority-attribute <192-240>	Specifies the value of the access priority attribute in the range of 192 to 240. The default is 192.
accounting {attribute-value <192-240>|enable|include-cli-commands}	Configures the accounting attribute value, enable accounting, or configure if accounting includes CLI commands. The default is false. Use the no option to disable the accounting attribute value: **no radius accounting enable**.
auth-info-attr-value <0-255>	Specifies the value of the authentication information attribute in the range of 0 to 255.The default is 91.
clear-stat	Clears RADIUS statistics.
cli-cmd-count <1–40>	Specifies how many CLI commands, from 1 to 40, before the system sends a RADIUS accounting interim request. The default value is 40.
cli-commands-attribute <192-240>	Specifies the value of CLI commands attribute in the range of 192 to 240. The default is 195.
cli-profile	Enable RADIUS CLI profiling. CLI profiling grants or denies access to users being authenticated by way of the RADIUS server. You can add a set of CLI commands to the configuration on the RADIUS server, and you can specify the command-access more for these commands. The default is false.
command-access-attribute <192-240>	Specifies the value of the command access attribute in the range of 192 to 240. The default is 194.
enable	Enable RADIUS authentication globally on the switch.
maxserver <1-10>	Specific to RADIUS authentication, configures the maximum number of servers allowed for the device. The range is between 1 and 10. The default is 10.
mcast-addr-attr-value <0-255>	Specifies the value of the multicast address attribute in the range of 0 to 255. The default is 90.
server host *WORD<0–46>* key *WORD<0–32>* [used-by {cli|snmp|web} [acct-enable] [acct-port *<1–65536>*] [enable] [port *<1–65536>*] [priority *<1–10>*] [retry *<0–6>*] [source-ip *WORD<0–46>*] [timeout *<1–60>*]	• host *WORD<0–46>* Creates a host server. WORD<0–46> signifies an IP address. • key *WORD<0–32>* Specifies a secret key in the range of 0–32 characters. • used-by *{cli|snmp|web}* Specifies how the server functions. Configures the server for authentication for - cli - snmp - web

Table continues…

Variable	Value
	• acct-enable Enables RADIUS accounting on this server. The system enables RADIUS accounting by default. • acct-port <*1–65536*> Specifies a UDP port of the RADIUS accounting server (1 to 65536). The default value is 1816. The UDP port value set for the client must match the UDP value set for the RADIUS server. • enable Enables the server. The default is true. • port <*1–65536*> Specifies a UDP port of the RADIUS server. The default value is 1812. • priority <*1–10*> Specifies the priority value for this server. The default is 10. • retry <*0–6*> Specifies the maximum number of authentication retires. The default is 3. • source-ip *WORD<0–46*> Specifies a configured IP address as the source address when transmitting RADIUS packets. WORD<0–46> signifies an IP address. • timeout <*1–60*> Specifies the number of seconds before the authentication request times out. The default is 3.
sourceip-flag	Enable the source IP so the switch uses a configured source IP address. If the outgoing interface fails, a different source IP address is used — requiring you to make configuration changes to define the new RADIUS client on the RADIUS server. To simplify RADIUS server configuration, you can configure the switch to use a Circuitless IP (CLIP) address as the source IP and NAS IP address when transmitting RADIUS packets. A CLIP is not associated with a physical interface and is always in an active and operational state. You can configure the switch with multiple CLIP interfaces. By default, the switch uses the IP address of the outgoing interface as the source IP, and the NAS IP address for RADIUS packets that it transmits.

Configuring RADIUS profile

Use RADIUS CLI profiling to grant or deny CLI command access to users being authenticated by way of the RADIUS server. You can add a set of CLI commands to the configuration file on the radius server, and you can specify the command-access mode for these commands. The default is false.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Enable RADIUS CLI profiling:

   ```
   radius cli-profile
   ```

Example

```
Switch:1> enable

Switch:1# configure terminal

Switch:1(config)# radius cli-profile
```

Enabling RADIUS authentication

About this task

Enable or disable RADIUS authentication globally on the device to allow further configuration to take place. Use the no option to disable RADIUS authentication globally. The default is false or disabled.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Enable RADIUS authentication globally on the switch:

   ```
   radius enable
   ```

Enabling the source IP flag for the RADIUS server

Before you begin

- To configure the CLIP as the source IP address, you must enable the global RADIUS sourceip-flag. You can then configure the source-ip address parameter while defining the RADIUS server on the switch. The source IP address must be a CLIP address, and that you can configure a different CLIP address for each RADIUS server.

Important:

Use the source IP option only for the RADIUS servers connected to the in-band network.

About this task

By default, the switch uses the IP address of the outgoing interface as the source IP, and the NAS IP address for RADIUS packets that it transmits. Enable the source IP so the switch uses a configured source IP address instead. Therefore, if the outgoing interface on the switch fails, a different source IP address is used—requiring that you make configuration changes to define the new RADIUS Client on the RADIUS server.

RADIUS supports IPv4 and IPv6 addresses, with no difference in functionality or configuration in CLI.

To simplify RADIUS Server configuration, you can configure the switch to use a Circuitless IP Address (CLIP) as the source IP and NAS IP address when transmitting RADIUS packets. A CLIP is not associated with a physical interface and is always in an active and operational state. You can configure the switch with multiple CLIP interfaces.

The default for **`radius sourceip-flag`** is false.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Enable the RADIUS packet source IP flag:

   ```
   radius sourceip-flag
   ```

Enabling RADIUS accounting

Before you begin

- You must configure a RADIUS server before you can enable RADIUS accounting.

About this task

Enable Remote Access Dial-in User Services (RADIUS) accounting to log all of the activity of each remote user in a session on the centralized RADIUS accounting server.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Enable RADIUS accounting globally:

```
radius accounting enable
```

3. Include or exclude CLI commands in RADIUS accounting updates:

   ```
   radius accounting include-cli-commands
   ```

4. Specify the integer value of the CLI commands attribute:

   ```
   radius accounting attribute-value <192–240>
   ```

Example

```
Switch:1> enable
Switch:1# configure terminal
Switch:1(config)# radius accounting enable
Switch:1(config)# radius accounting include-cli-commands
```

Variable definitions

Use the data in the following table to use the `radius accounting` command.

Table 5: Variable definitions

Variable	Value
enable	Enable RADIUS globally.
include-cli-commands	Include or exclude CLI commands in RADIUS accounting updates.
attribute-value <*192–240*>	Specify the integer value of the CLI commands attribute.

Enabling RADIUS-SNMP accounting

Before you begin

- You must configure a RADIUS server before you can enable RADIUS-SNMP accounting.

About this task

Enable Remote Access Dial-in User Services (RADIUS) Simple Network Managing Protocol (SNMP) accounting globally. Use SNMP to remotely collect management data. An SNMP agent is a software process that monitors the UDP port 161 for SNMP messages. Each SNMP message sent to the agent contains a list of management objects.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   configure terminal
   ```

2. Enable RADIUS Simple Network Management Protocol (SNMP) accounting globally:

   ```
   radius-snmp acct-enable
   ```

3. Set a timer to send a stop accounting message for RADIUS Simple Network Management Protocol (SNMP):

   ```
   radius-snmp abort-session-timer <30-65535>
   ```

4. Set the timer for re-authentication of the SNMP session:

   ```
   radius-snmp re-auth-timer <30-65535>
   ```

5. Specify the user name for SNMP access:

   ```
   radius-snmp user WORD <0-20>
   ```

Example

```
Switch:1> enable

Switch:1# configure terminal

Switch:1(config)# radius-snmp acct-enable

Switch:1(config)# radius-snmp abort-session-timer 30
```

Variable definitions

Use the data in the following table to use the `radius-snmp` command.

Table 6: Variable definitions

Variable	Value
acct-enable	Enables RADIUS accounting globally. You cannot enable RADIUS accounting before you configure a valid server. The system disables RADIUS accounting by default. The default is false. Use the no option to disable RADIUS accounting globally: **`no radius-snmp acct-enable`**
abort-session-timer <*30–65535*>	Set the timer, in seconds, to send a stop accounting message. The default is 180.
re-auth-timer <*30–65535*>	Sets timer for re-authentication of the SNMP session. The timer value ranges from 30 to 65535 seconds. The default is 180.
user *WORD <0–20>*	Specifies the user name for SNMP access. WORD <0–20> specifies the user name in a range of 0 to 20 characters. The default is snmp_user.

Configuring RADIUS accounting interim request

About this task

Configure RADIUS accounting interim requests to create a log whenever a user executes more than the number of CLI commands you specify.

If the packet size equals or exceeds 1.8 KB, an interim request packet is sent even if the configured limit is not reached. Therefore, the trigger to send out the interim request is either the configured value or a packet size greater than, or equal to 1.8 KB, whichever happens first.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Configure RADIUS accounting interim requests:

   ```
   radius cli-cmd-count <1-40>
   ```

3. Include or exclude CLI commands in RADIUS accounting:

   ```
   radius accounting include-cli-commands
   ```

   Important:

   You must configure the **radius accounting include-cli-commands** command for accounting interim requests to function.

Example

```
Switch:1> enable
Switch:1# configure terminal
Switch:1(config)# radius cli-cmd-count 30
Switch:1(config)# radius accounting include-cli-commands
```

Variable definitions

Use the data in the following table to use the **radius cli-cmd-count** command.

Variable	Value
<1-40>	Specifies how many CLI commands, from 1 to 40, before the system sends a RADIUS accounting interim request. The default value is 40.

Configuring RADIUS authentication and RADIUS accounting attributes

About this task

Configure RADIUS authentication and RADIUS accounting attributes to determine the size of the packets received.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Configure the RADIUS authentication attribute value:

```
radius command-access-attribute <192-240>
```

3. Configure the RADIUS accounting attribute value:

```
radius accounting attribute-value <192-240>
```

Example

```
Switch:1> enable
Switch:1# configure terminal
Switch:1(config)# radius command-access-attribute 192
Switch:1(config)# radius accounting attribute-value 192
```

Variable definitions

Use the data in the following table to use the **radius** command.

Variable	Value
access-priority-attribute <192-240>	Specifies the value of the access priority attribute in the range of 192 to 240. The default is 192.
accounting {attribute-value <192-240>|enable|include-cli-commands}	Configures the accounting attribute value, enable accounting, or configure if accounting includes CLI commands. The default is false. Use the no option to disable the accounting attribute value: **no radius accounting enable**.
auth-info-attr-value <0-255>	Specifies the value of the authentication information attribute in the range of 0 to 255.The default is 91.
clear-stat	Clears RADIUS statistics.
cli-cmd-count <1–40>	Specifies how many CLI commands, from 1 to 40, before the system sends a RADIUS accounting interim request. The default value is 40.
cli-commands-attribute <192-240>	Specifies the value of CLI commands attribute in the range of 192 to 240. The default is 195.
cli-profile	Enable RADIUS CLI profiling. CLI profiling grants or denies access to users being authenticated by way of the RADIUS server. You can add a set of CLI commands to the configuration on the RADIUS server, and you can specify the command-access more for these commands. The default is false.
command-access-attribute <192-240>	Specifies the value of the command access attribute in the range of 192 to 240. The default is 194.
enable	Enable RADIUS authentication globally on the switch.
maxserver <1-10>	Specific to RADIUS authentication, configures the maximum number of servers allowed for the device. The range is between 1 and 10. The default is 10.
mcast-addr-attr-value <0-255>	Specifies the value of the multicast address attribute in the range of 0 to 255. The default is 90.

Table continues…

Variable	Value
server host *WORD<0–46>* key *WORD<0–32>* [used-by {cli|snmp|web} [acct-enable] [acct-port *<1–65536>*] [enable] [port *<1–65536>*] [priority *<1–10>*] [retry *<0–6>*] [source-ip *WORD<0–46>*] [timeout *<1–60>*]	• host *WORD<0–46>* Creates a host server. WORD<0–46> signifies an IP address. • key *WORD<0–32>* Specifies a secret key in the range of 0–32 characters. • used-by *{cli|snmp|web}* Specifies how the server functions. Configures the server for authentication for - cli - snmp - web • acct-enable Enables RADIUS accounting on this server. The system enables RADIUS accounting by default. • acct-port *<1–65536>* Specifies a UDP port of the RADIUS accounting server (1 to 65536). The default value is 1816. The UDP port value set for the client must match the UDP value set for the RADIUS server. • enable Enables the server. The default is true. • port *<1–65536>* Specifies a UDP port of the RADIUS server. The default value is 1812. • priority *<1–10>* Specifies the priority value for this server. The default is 10. • retry *<0–6>* Specifies the maximum number of authentication retires. The default is 3. • source-ip *WORD<0–46>* Specifies a configured IP address as the source address when transmitting RADIUS packets. WORD<0–46> signifies an IP address. • timeout *<1–60>* Specifies the number of seconds before the authentication request times out. The default is 3.

Table continues…

Variable	Value
sourceip-flag	Enable the source IP so the switch uses a configured source IP address. If the outgoing interface fails, a different source IP address is used — requiring you to make configuration changes to define the new RADIUS client on the RADIUS server. To simplify RADIUS server configuration, you can configure the switch to use a Circuitless IP (CLIP) address as the source IP and NAS IP address when transmitting RADIUS packets. A CLIP is not associated with a physical interface and is always in an active and operational state. You can configure the switch with multiple CLIP interfaces. By default, the switch uses the IP address of the outgoing interface as the source IP, and the NAS IP address for RADIUS packets that it transmits.

Adding a RADIUS server

About this task

Add a RADIUS server to allow RADIUS service on the switch.

RADIUS supports IPv4 and IPv6 addresses, with no difference in functionality or configuration using CLI.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Add a RADIUS server:

   ```
   radius server host WORD <0-46> key WORD<0-32> [used-by {cli | eapol
   | snmp | web}] [acct-enable][acct-port <1-65536>] [enable] [port
   <1-65536>][priority <1-10>][retry <0-6>] [source-ip WORD <0-46>]
   [timeout <1-20>]
   ```

Example

```
Switch:1> enable
```

```
Switch:1# configure terminal
```

Add a RADIUS server:

```
Switch:1(config)# radius server host
4717:0000:0000:0000:0000:0000:7933:0001 key testkey1 used-by snmp port 12
retry 5 timeout 10 enable
```

Variable definitions

Use the data in the following table to use the `radius server` command.

Variable	Value
host WORD *<0–46>*	Creates a host server. WORD <0–46> signifies an IPv4 address in the format A.B.C.D or an IPv6 address in the format x:x:x:x:x:x:x:x. RADIUS supports IPv4 and IPv6 addresses, with no difference in functionality or configuration using CLI.
key *WORD<0-32>*	Specifies a secret key in the range of 0–32 characters.
used-by {cli | eapol | snmp | web}	Specifies how the server functions • cli—configure the server for CLI authentication. • eapol—configure the server for EAPoL authentication. • snmp—configure the server for SNMP authentication. • web—configure the server for http(s) authentication
acct-enable	Enables RADIUS accounting on this server. The system enables RADIUS accounting by default.
acct-port *<1-65536>*	Specifies a UDP port of the RADIUS accounting server (1 to 65536). The default value is 1816. ! **Important:** The UDP port value set for the client must match the UDP value set for the RADIUS server.
enable	Enables this server. The default is true.
port *<1-65536>*	Specifies a UDP port of the RADIUS server. The default value is 1812.
priority *<1-10>*	Specifies the priority value for this server. The default is 10.
retry *<0-6>*	Specifies the maximum number of authentication retries. The default is 3.
source-ip WORD *<0–46>*	Specifies a configured IP address as the source address when transmitting RADIUS packets. WORD <0–46> signifies an IPv4 address in the format A.B.C.D or an IPv6 address in the format x:x:x:x:x:x:x:x. RADIUS supports IPv4 and IPv6 addresses, with no difference in functionality or configuration using CLI.
timeout *<1-20>*	Specifies the number of seconds before the authentication request times out. The default is 3.

Modifying RADIUS server settings

About this task

Change a specified RADIUS server value without having to delete the server and recreate it again.

RADIUS supports IPv4 and IPv6 addresses, with no difference in functionality or configuration using CLI.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Modify a RADIUS server:

   ```
   radius server host WORD <0-46> {key WORD<0-32> | used-by {cli |
   eapol | snmp | web}} [port 1-65536] [priority <1-10>] [retry <0-6>]
   [timeout <1-20>] [enable] [acct-port <1-65536>] [acct-enable]
   [source-ip WORD <0-46>]
   ```

Example

```
Switch:1> enable
```

```
Switch:1# configure terminal
```

Modify a RADIUS server:

```
Switch:1(config)# radius server host
4717:0000:0000:0000:0000:0000:7933:0001 used-by snmp port 12 retry 5
timeout 10 enable
```

Variable definitions

Use the data in the following table to use the **radius server host** command.

Variable	Value
used-by {cli | eapol| snmp | web}	Specifies how the server functions • cli—configure the server for CLI authentication. • eapol—configure the server for EAPoL authentication. • snmp—configure the server for SNMP authentication. • web—configure the server for Web authentication.
host *WORD <0–46>*	Configures a host server. WORD <0–46> signifies an IPv4 address in the format A.B.C.D or an IPv6 address in the format x:x:x:x:x:x:x:x. RADIUS supports IPv4 and IPv6 addresses, with no difference in functionality or configuration using CLI.

Table continues…

Variable	Value
acct-enable	Enables RADIUS accounting on this server. The system enables RADIUS accounting by default.
acct-port *<1-65536>*	Configures the UDP port of the RADIUS accounting server (1 to 65536). The default value is 1813. **Important:** The UDP port value set for the client must match the UDP value set for the RADIUS server.
enable	Enables the RADIUS server. The default is true.
key *WORD <0–32>*	Configures the secret key of the authentication client.
port *<1-65536>*	Configures the UDP port of the RADIUS authentication server (1 to 65536). The default value is 1812.
priority *<1–10>*	Configures the priority value for this server (1 to 10). The default is 10.
retry *<0–6>*	Configures the number of authentication retries the server will accept (0 to 6). The default is 3.
source-ip *WORD <0–46>*	Specifies a configured IP address as the source address when transmitting RADIUS packets. To use this option, you must have the global RADIUS sourceip-flag set to true. RADIUS supports IPv4 and IPv6 addresses, with no difference in functionality or configuration using CLI.
timeout *<1–20>*	Configures the number of seconds before the authentication request times out. The default is 3.

Showing RADIUS information

Display the global status of RADIUS information to ensure you configured the RADIUS feature according to the needs of the network.

Procedure

1. Log on to the switch to enter User EXEC mode.
2. Display the global status of RADIUS information:

   ```
   show radius
   ```

Example

```
Switch:1>show radius
             acct-attribute-value : 193
                      acct-enable : false
        acct-include-cli-commands : false
        access-priority-attribute : 192
             auth-info-attr-value : 91
         command-access-attribute : 194
           cli-commands-attribute : 195
                    cli-cmd-count : 40
               cli-profile-enable : false
```

```
                           enable : false
                 igap-passwd-attr : standard
           igap-timeout-log-fsize : 512
                        maxserver : 10
            mcast-addr-attr-value : 90
                    sourceip-flag : false
```

Displaying RADIUS server information

If your system is configured with a RADIUS server you can display the RADIUS server information.

Procedure

1. Log on to the switch to enter User EXEC mode.
2. To display the RADIUS server information enter the following command:

   `show radius-server`

   Note:

   If no RADIUS server is configured, the system displays the following message:

   `no RADIUS server configured`

Example

```
Switch:1>show radius-server

===================================================================================
                              Radius Server Entries
===================================================================================
                                                             ACCT
Name               USED                       TIME EN-  ACCT EN-   SOURE
                   BY  SECRET PORT PRIO RETRY OUT ABLED PORT ABLED IP
1.1.1.1            cli ****** 1812 10   1     3   true  1813 true  0.0.0.0
1000:0:0:0:0:0:0:1 cli ****** 1812 10   1     3   true  1813 true  0:0:0:0:0:0:0:0
10.10.10.10        cli ****** 1812 10   1     3   true  1813 true  0.0.0.0
4000:0:0:0:0:0:0:1 cli ****** 1812 10   1     3   true  1813 true  0:0:0:0:0:0:0:0
```

Showing RADIUS SNMP configurations

Display current RADIUS SNMP configurations.

Procedure

1. Log on to the switch to enter User EXEC mode.
2. Display the current RADIUS server SNMP configurations:

   `show radius snmp`

Example

```
Switch:1>show radius snmp
              abort-session-timer : 180
                      acct-enable : false
                             user : snmp_user
```

```
                          enable : false
                   re-auth-timer : 180
```

RADIUS configuration using Enterprise Device Manager

You can configure Remote Access Dial-In User Services (RADIUS) to assist in securing networks against unauthorized access, and allow communication servers and clients to authenticate the identity of users through a central database.

The database within the RADIUS server stores client information, user information, password, and access privileges, including the use of shared secret.

RADIUS supports IPv4 and IPv6 addresses with no difference in functionality or configuration in all but the following case. When adding a RADIUS server in Enterprise Device Manager (EDM) or modifying a RADIUS configuration in EDM, you must specify if the address type is an IPv4 or an IPv6 address.

RADIUS is a fully open and standard protocol, defined by RFCs (Authentication: RFC 2865, accounting RFC 2866). With the switch, you use RADIUS authentication to secure access to the device (console/Telnet/SSH), and RADIUS accounting to track the management sessions for Command Line Interface (CLI) only.

RADIUS authentication allows the remote server to authenticate logons. RADIUS accounting logs all of the activity of each remote user in a session on the centralized RADIUS accounting server.

Enabling RADIUS authentication

About this task

Enable RADIUS authentication globally to allow all features and functions of RADIUS to operate with the RADIUS server.

Procedure

1. In the navigation tree, open the following folders: **Configuration** > **Security** > **Control Path**.
2. Click **RADIUS**.
3. In the **RADIUS Global** tab, select the **Enable** check box.
4. In the **MaxNumberServer** field, type a value for the maximum number of servers.
5. In the **AccessPriorityAttrValue** field, type an access policy value (by default, this value is 192).
6. Configure the rest of the parameters in the RADIUS global tab.
7. Click **Apply**.

RADIUS Global field descriptions

Use the data in the following table to use the **RADIUS Global** tab.

Name	Description
Enable	Enables the RADIUS authentication feature globally.
MaxNumberServer	Specifies the maximum number of servers to be used, between 1 and 10, inclusive.
AccessPriorityAttrValue	Specific to RADIUS authentication. Specifies the vendor-specific attribute value of the access-priority attribute to match the type value set in the dictionary file on the RADIUS server. The valid values are 192 through 240. The default is 192.
AcctEnable	Enables RADIUS accounting.
AcctAttriValue	Specific to RADIUS accounting. Specifies the vendor-specific attribute value of the CLI-command attribute to match the type value set in the dictionary file on the RADIUS server. This value must be different from the access-priority attribute value configured for authentication. The valid values are 192 through 240. The default value is 193.
AcctIncludeCli	Specifies whether you want CLI commands included in RADIUS accounting requests.
ClearStat	Clears RADIUS statistics from the device.
McastAttributeValue	Specifies the value of the Mcast attribute. The valid values are 0 through 255. The default value is 90.
AuthInfoAttrValue	Specifies the value of the authentication information attribute. The valid values are 0 through 255. The default value is 91.
CommandAccessAttrValue	Specifies the value of the command access attribute. The valid values are 192 through 240. The default value is 194.
CliCommandAttrValue	Specifies the value of the CLI command attribute. The valid values are 192 through 240. The default value is 195.
AuthInvalidServerAddress	Displays the number of access responses from unknown or invalid RADIUS servers.
SourceIpFlag	Includes a configured IP address as the source address in RADIUS packets. The default is false. RADIUS supports IPv4 and IPv6 addresses with no difference in functionality or configuration.
CliCmdCount	Gives the value for the CLI command count. Specify an integer from 1 to 40. The default is 40.
CliProfEnable	Enables RADIUS CLI profiling.

Enabling RADIUS accounting

Before you begin

- You must set up a RADIUS server and add it to the configuration file of the device before you can enable RADIUS accounting on the device. Otherwise, the system displays an error message.

About this task

Enable RADIUS accounting to log all of the activity of each remote user in a session on the centralized RADIUS accounting server.

Procedure

1. In the navigation tree, open the following folders: **Configuration** > **Security** > **Control Path**.
2. Click **RADIUS**.
3. In the **RADIUS Global** tab, select the **AcctEnable** check box.
4. In the **AcctAttrValue** field, type an access policy value (by default, this value is 193).
5. Click **Apply**.

RADIUS Global field descriptions

Use the data in the following table to use the **RADIUS Global** tab.

Name	Description
Enable	Enables the RADIUS authentication feature globally.
MaxNumberServer	Specifies the maximum number of servers to be used, between 1 and 10, inclusive.
AccessPriorityAttrValue	Specific to RADIUS authentication. Specifies the vendor-specific attribute value of the access-priority attribute to match the type value set in the dictionary file on the RADIUS server. The valid values are 192 through 240. The default is 192.
AcctEnable	Enables RADIUS accounting.
AcctAttriValue	Specific to RADIUS accounting. Specifies the vendor-specific attribute value of the CLI-command attribute to match the type value set in the dictionary file on the RADIUS server. This value must be different from the access-priority attribute value configured for authentication. The valid values are 192 through 240. The default value is 193.
AcctIncludeCli	Specifies whether you want CLI commands included in RADIUS accounting requests.
ClearStat	Clears RADIUS statistics from the device.
McastAttributeValue	Specifies the value of the Mcast attribute. The valid values are 0 through 255. The default value is 90.

Table continues…

Name	Description
AuthInfoAttrValue	Specifies the value of the authentication information attribute. The valid values are 0 through 255. The default value is 91.
CommandAccessAttrValue	Specifies the value of the command access attribute. The valid values are 192 through 240. The default value is 194.
CliCommandAttrValue	Specifies the value of the CLI command attribute. The valid values are 192 through 240. The default value is 195.
AuthInvalidServerAddress	Displays the number of access responses from unknown or invalid RADIUS servers.
SourceIpFlag	Includes a configured IP address as the source address in RADIUS packets. The default is false. RADIUS supports IPv4 and IPv6 addresses with no difference in functionality or configuration.
CliCmdCount	Gives the value for the CLI command count. Specify an integer from 1 to 40. The default is 40.
CliProfEnable	Enables RADIUS CLI profiling.

Disabling RADIUS accounting

Before you begin

- You cannot globally disable RADIUS accounting unless a server entry exists.

About this task

Disabling RADIUS accounting removes the accounting function from the RADIUS server.

Procedure

1. In the navigation tree, open the following folders: **Configuration** > **Security** > **Control Path**.
2. Click **RADIUS**.
3. In the **RADIUS Global** tab, disable RADIUS accounting by clearing the **AcctEnable** check box.
4. Click **Apply**.

Enabling RADIUS accounting interim request

About this task

Enable the RADIUS accounting interim request feature to create a log whenever more than the specified number of CLI commands are executed.

Procedure

1. In the navigation tree, open the following folders: **Configuration** > **Security** > **Control Path**.
2. Click **RADIUS**.

3. In the **RADIUS Global** tab, type the number of CLI commands in the **CliCmdCount** field.
4. Click **Apply**.

RADIUS Global field descriptions

Use the data in the following table to use the **RADIUS Global** tab.

Name	Description
Enable	Enables the RADIUS authentication feature globally.
MaxNumberServer	Specifies the maximum number of servers to be used, between 1 and 10, inclusive.
AccessPriorityAttrValue	Specific to RADIUS authentication. Specifies the vendor-specific attribute value of the access-priority attribute to match the type value set in the dictionary file on the RADIUS server. The valid values are 192 through 240. The default is 192.
AcctEnable	Enables RADIUS accounting.
AcctAttriValue	Specific to RADIUS accounting. Specifies the vendor-specific attribute value of the CLI-command attribute to match the type value set in the dictionary file on the RADIUS server. This value must be different from the access-priority attribute value configured for authentication. The valid values are 192 through 240. The default value is 193.
AcctIncludeCli	Specifies whether you want CLI commands included in RADIUS accounting requests.
ClearStat	Clears RADIUS statistics from the device.
McastAttributeValue	Specifies the value of the Mcast attribute. The valid values are 0 through 255. The default value is 90.
AuthInfoAttrValue	Specifies the value of the authentication information attribute. The valid values are 0 through 255. The default value is 91.
CommandAccessAttrValue	Specifies the value of the command access attribute. The valid values are 192 through 240. The default value is 194.
CliCommandAttrValue	Specifies the value of the CLI command attribute. The valid values are 192 through 240. The default value is 195.
AuthInvalidServerAddress	Displays the number of access responses from unknown or invalid RADIUS servers.
SourceIpFlag	Includes a configured IP address as the source address in RADIUS packets. The default is false. RADIUS supports IPv4 and IPv6 addresses with no difference in functionality or configuration.
CliCmdCount	Gives the value for the CLI command count. Specify an integer from 1 to 40. The default is 40.
CliProfEnable	Enables RADIUS CLI profiling.

Configuring the source IP option for the RADIUS server

Before you begin

- To configure the CLIP as the source IP address, you must configure the global RADIUS **sourceip-flag** parameter as true. You can configure the **source-ip** address parameter while you define the RADIUS Server on the switch. The source IP address must be a CLIP address, and you can configure a different CLIP address for each RADIUS server. For more information about configuring the source IP address, see Adding a RADIUS server on page 147.

Important:

Use the source IP option only for the RADIUS servers connected to the in-band network.

About this task

By default, the switch uses the IP address of the outgoing interface as the source IP and NAS IP address for RADIUS packets that it transmits. When you configure the RADIUS server, this IP address is used when defining the RADIUS Clients that communicate with it. Therefore, if the outgoing interface on the switch fails, a different source IP address is used—requiring that you make configuration changes to define the new RADIUS client on the RADIUS server.

To simplify RADIUS Server configuration, you can configure the switch to use a Circuitless IP Address (CLIP) as the source IP and NAS IP address when transmitting RADIUS packets. A CLIP is not associated with a physical interface and is always in an active and operational state. You can configure the switch with multiple CLIP interfaces.

RADIUS supports IPv4 and IPv6 addresses with no difference in functionality or configuration in all but the following case. When adding a RADIUS server in Enterprise Device Manager (EDM) or modifying a RADIUS configuration in EDM, you must specify if the address type is an IPv4 or an IPv6 address.

Procedure

1. In the navigation tree, open the following folders: **Configuration** > **Security** > **Control Path**.
2. Click **RADIUS**.
3. In the **RADIUS Global** tab, select the **SourceIpFlag** check box.
4. Click **Apply**.

RADIUS Global field descriptions

Use the data in the following table to use the **RADIUS Global** tab.

Name	Description
Enable	Enables the RADIUS authentication feature globally.
MaxNumberServer	Specifies the maximum number of servers to be used, between 1 and 10, inclusive.
AccessPriorityAttrValue	Specific to RADIUS authentication. Specifies the vendor-specific attribute value of the access-priority attribute to match the type

Table continues…

Name	Description
	value set in the dictionary file on the RADIUS server. The valid values are 192 through 240. The default is 192.
AcctEnable	Enables RADIUS accounting.
AcctAttriValue	Specific to RADIUS accounting. Specifies the vendor-specific attribute value of the CLI-command attribute to match the type value set in the dictionary file on the RADIUS server. This value must be different from the access-priority attribute value configured for authentication. The valid values are 192 through 240. The default value is 193.
AcctIncludeCli	Specifies whether you want CLI commands included in RADIUS accounting requests.
ClearStat	Clears RADIUS statistics from the device.
McastAttributeValue	Specifies the value of the Mcast attribute. The valid values are 0 through 255. The default value is 90.
AuthInfoAttrValue	Specifies the value of the authentication information attribute. The valid values are 0 through 255. The default value is 91.
CommandAccessAttrValue	Specifies the value of the command access attribute. The valid values are 192 through 240. The default value is 194.
CliCommandAttrValue	Specifies the value of the CLI command attribute. The valid values are 192 through 240. The default value is 195.
AuthInvalidServerAddress	Displays the number of access responses from unknown or invalid RADIUS servers.
SourceIpFlag	Includes a configured IP address as the source address in RADIUS packets. The default is false. RADIUS supports IPv4 and IPv6 addresses with no difference in functionality or configuration.
CliCmdCount	Gives the value for the CLI command count. Specify an integer from 1 to 40. The default is 40.
CliProfEnable	Enables RADIUS CLI profiling.

Adding a RADIUS server

About this task

Add a RADIUS server to allow RADIUS service on the switch.

Remote Dial-In User Services (RADIUS) supports both IPv4 and IPv6 addresses, with no differences in functionality or configuration in all but the following case. When adding a RADIUS server or updating a RADIUS server in Enterprise Device Manager (EDM) you must specify if the address type is an IPv4 or an IPv6 address.

Procedure

1. In the navigation tree, open the following folders: **Configuration** > **Security** > **Control Path**.
2. Click **RADIUS**.

3. Click the **RADIUS Servers** tab.
4. Click **Insert**.
5. In the **AddressType** box, select IPv4 or IPv6.
6. In the **Address** box, type the IP address of the RADIUS server that you want to add.
7. In the **UsedBy** box, select an option for the user logon.
8. In the **SecretKey** box, type a secret key.
9. In the **SourceIpAddr** box, type the IP address to use as the source address in RADIUS packets.
10. Click **Insert**.

RADIUS Servers field descriptions

Use the data in the following table to use the **RADIUS Servers** tab.

Name	Description
AddressType	Specifies either an IPv4 or an IPv6 address. RADIUS supports IPv4 and IPv6 addresses.
Address	Specifies the IP address of the RADIUS server. RADIUS supports IPv4 and IPv6 addresses.
UsedBy	Specifies the user logon. • cli: for cli logon • snmp: for snmp logon • eap: for EAPoL authentication • web: for HTTP(s) access authentication The default is cli.
Priority	Specifies the priority of each server, or the order of servers to send authentication. The default is 10.
TimeOut	Specifies the time interval in seconds before the client retransmits the packet. The default is 3.
Enable	Enables or disables authentication on the server. The default is true.
MaxRetries	Specifies the maximum number of retransmissions allowed. The default is 1.
UdpPort	Specifies the UDP port that the client uses to send requests to the server. The default value is 1812. The UDP port value set for the client must match the UDP value set for the RADIUS server.
SecretKey	Specifies the RADIUS server secret key, which is the password used by the client to be validated by the server.
AcctEnable	Enables or disable RADIUS accounting. The default is true.

Table continues…

Name	Description
AcctUdpPort	Specifies the UDP port of the RADIUS accounting server. The default value is 1813. The UDP port value set for the client must match the UDP value set for the RADIUS server.
SourceIpAddr	Specifies the IP address to use as the source address in RADIUS packets. To use this option, you must set the global RADIUS SourceIpFlag to true. RADIUS supports IPv4 and IPv6 addresses.

Reauthenticating the RADIUS SNMP server session

About this task

Specify the number of challenges that you want the RADIUS SNMP server to send to authenticate a given session.

Procedure

1. In the navigation tree, open the following folders: **Configuration** > **Security** > **Control Path**.
2. Click **RADIUS**.
3. Click the **RADIUS SNMP** tab.

   The RADIUS SNMP tab appears.
4. Select the **Enable** check box.
5. In the **ReauthenticateTimer** field, enter a value to specify the interval between RADIUS SNMP server reauthentications.

   The timer for reauthentication of the RADIUS SNMP server session is enabled.

   Important:

   To abort the RADIUS SNMP server session, enter a value for the AbortSessionTimer, and then click Enable.
6. Select the **AcctEnable** check box if desired.
7. Click **Apply**.

RADIUS SNMP field descriptions

Use the data in the following table to use the **RADIUS SNMP** tab.

Name	Description
Enable	Enables or disables timer authentication on the server. The default is true.
AbortSessionTImer	Specifies the allowable time, in seconds, before aborting the RADIUS SNMP server session (30 to 65535). The default is 180.

Table continues…

Name	Description
ReAuthenticateTimer	Specifies the time, in seconds, between reauthentications of the RADIUS SNMP server (30 to 65535). The default is 180.
AcctEnable	Enables or disables the RADIUS SNMP session timer.
UserName	Specifies the user name for the RADIUS SNMP accounting.

Configuring RADIUS SNMP

About this task

Configure RADIUS SNMP parameters for authentication and session times.

Procedure

1. In the navigation tree, open the following folders: **Configuration** > **Security** > **Control Path**.
2. Click **RADIUS.**
3. Select the **RADIUS SNMP** tab.
4. Select the **Enable** check box to enable RADIUS SNMP.
5. In the **AbortSessionTimer** field, enter the period after which the session expires in seconds.
6. In the **ReAuthenticateTimer** field, enter the period of time the system waits before reauthenticating in seconds.
7. Select the **AcctEnable** check box to enable RADIUS accounting for SNMP.
8. In the **UserName** field, type the RADIUS SNMP user name.
9. Click **Apply**.

RADIUS SNMP field descriptions

Use the data in the following table to use the **RADIUS SNMP** tab.

Name	Description
Enable	Enables or disables timer authentication on the server. The default is true.
AbortSessionTImer	Specifies the allowable time, in seconds, before aborting the RADIUS SNMP server session (30 to 65535). The default is 180.
ReAuthenticateTimer	Specifies the time, in seconds, between reauthentications of the RADIUS SNMP server (30 to 65535). The default is 180.
AcctEnable	Enables or disables the RADIUS SNMP session timer.
UserName	Specifies the user name for the RADIUS SNMP accounting.

Modifying a RADIUS configuration

About this task

Modify an existing RADIUS configuration or single function such as retransmissions and RADIUS accounting.

RADIUS supports IPv4 and IPv6 addresses with no difference in functionality or configuration in all except the following case. When modifying a RADIUS configuration in Enterprise Device Manager (EDM), you must specify if the address type is an IPv4 or an IPv6 address.

Procedure

1. In the navigation tree, open the following folders: **Configuration** > **Security** > **Control Path**.
2. Click **RADIUS**.
3. Click the **RADIUS Servers** tab.
4. In the row and field to modify, type the information or use the lists to make a selection. Access the lists by double-clicking in a field.
5. When you are done with modifying the RADIUS configuration, click **Apply**.

RADIUS Servers field descriptions

Use the data in the following table to use the **RADIUS Servers** tab.

Name	Description
AddressType	Specifies either an IPv4 or an IPv6 address. RADIUS supports IPv4 and IPv6 addresses.
Address	Specifies the IP address of the RADIUS server. RADIUS supports IPv4 and IPv6 addresses.
UsedBy	Specifies the user logon. • cli: for cli logon • snmp: for snmp logon • eap: for EAPoL authentication • web: for HTTP(s) access authentication The default is cli.
Priority	Specifies the priority of each server, or the order of servers to send authentication. The default is 10.
TimeOut	Specifies the time interval in seconds before the client retransmits the packet. The default is 3.
Enable	Enables or disables authentication on the server. The default is true.
MaxRetries	Specifies the maximum number of retransmissions allowed. The default is 1.

Table continues…

Name	Description
UdpPort	Specifies the UDP port that the client uses to send requests to the server. The default value is 1812. The UDP port value set for the client must match the UDP value set for the RADIUS server.
SecretKey	Specifies the RADIUS server secret key, which is the password used by the client to be validated by the server.
AcctEnable	Enables or disable RADIUS accounting. The default is true.
AcctUdpPort	Specifies the UDP port of the RADIUS accounting server. The default value is 1813. The UDP port value set for the client must match the UDP value set for the RADIUS server.
SourceIpAddr	Specifies the IP address to use as the source address in RADIUS packets. To use this option, you must set the global RADIUS SourceIpFlag to true. RADIUS supports IPv4 and IPv6 addresses.

Deleting a RADIUS configuration

About this task

Delete an existing RADIUS configuration.

Procedure

1. In the navigation tree, open the following folders: **Configuration** > **Security** > **Control Path**.
2. Click **RADIUS**.
3. Click the **RADIUS Servers** tab.
4. Identify the configuration to delete by clicking anywhere in the row.
5. Click **Delete**.

Chapter 7: Simple Network Management Protocol (SNMP)

You can use the Simple Network Management Protocol (SNMP) to remotely collect management data and configure devices.

An SNMP agent is a software process that monitors the UDP port 161 for SNMP messages. Each SNMP message sent to the agent contains a list of management objects to retrieve or modify.

SNMPv3

The SNMP version 3 (v3) is the third version of the Internet Standard Management Framework and is derived from and builds upon both the original Internet Standard Management Framework SNMP version 1 (v1) and the second Internet Standard Management Framework SNMP version 2 (v2).

The SNMPv3 is not a stand-alone replacement for SNMPv1 or SNMPv2. The SNMPv3 defines security capabilities you must use in conjunction with SNMPv2 (preferred) or SNMPv1. The following figure shows how SNMPv3 specifies a user-based security model (USM) that uses a payload of either an SNMPv1 or an SNMPv2 Protocol Data Unit (PDU).

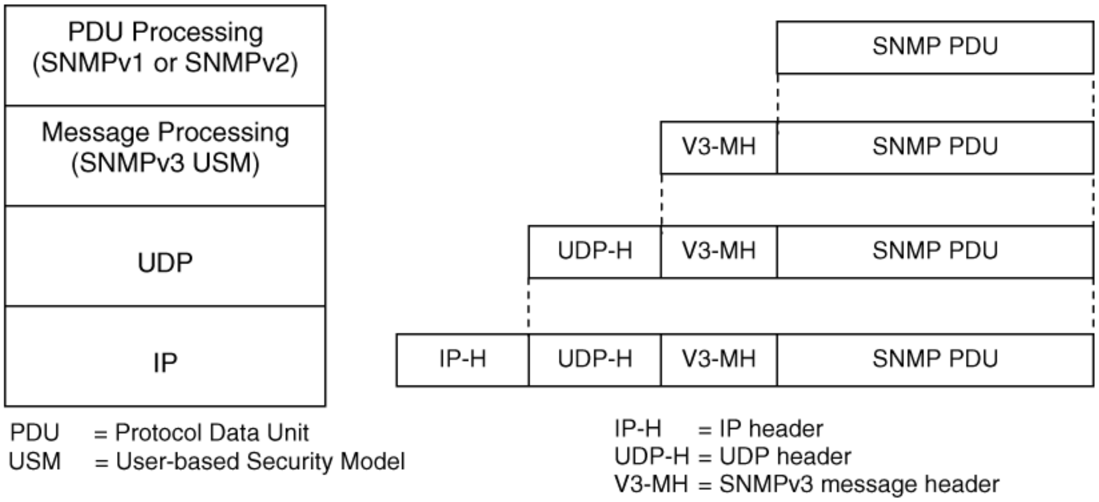

PDU Processing (SNMPv1 or SNMPv2)
Message Processing (SNMPv3 USM)
UDP
IP
SNMP PDU
V3-MH
UDP-H
IP-H
PDU = Protocol Data Unit
USM = User-based Security Model
IP-H = IP header
UDP-H = UDP header
V3-MH = SNMPv3 message header

Figure 15: SNMPv3 USM

SNMPv3 is an SNMP framework that supplements SNMPv2 by supporting the following:

- New SNMP message formats
- Security for messages
- Access control
- Remote configuration of SNMP parameters

The recipient of a message can use authentication within the USM to verify the message sender and to detect if the message is altered. According to RFC2574, if you use authentication, the USM checks the entire message for integrity.

An SNMP entity is an implementation of this architecture. Each SNMP entity consists of an SNMP engine and one or more associated applications.

SNMP engine

An SNMP engine provides services for sending and receiving messages, authenticating and encrypting messages, and controlling access to managed objects. A one-to-one association exists between an SNMP engine and the SNMP entity, which contains the SNMP engine.

EngineID

Within an administrative domain, an EngineID is the unique identifier of an SNMP engine. Because there is a one-to-one association between SNMP engines and SNMP entities, the ID also uniquely and unambiguously identifies the SNMP entity within that administrative domain. The system generates an EngineID during the startup process. The SNMP engine contains a:

- Dispatcher on page 154.
- Message processing subsystem on page 154.
- Security subsystem on page 154.
- Access control subsystem on page 155.

Dispatcher

The dispatcher is part of an SNMP engine. You can use the dispatcher for concurrent support of multiple versions of SNMP messages in the SNMP engine through the following ways:

- To send and receive SNMP messages to and from the network.
- To determine the SNMP message version and interact with the corresponding message processing model.
- To provide an abstract interface to SNMP applications for delivery of a PDU to an application.
- To provide an abstract interface for SNMP applications to send a PDU to a remote SNMP entity.

Message processing subsystem

The message processing subsystem prepares messages for sending and extracts data from received messages. The subsystem can contain multiple message processing models.

Security subsystem

The security subsystem provides the following features:

- Authentication

- Privacy
- Security

Authentication

You can use authentication within the SNMPv3 to verify the message sender and whether the message is altered. If you use authentication, the integrity of the message is verified. The supported SNMPv3 authentication protocols are HMAC-MD5 and HMAC-SHA-96. By default, the switch uses HMAC-SHA1-96 with 160-bit key length.

Privacy

SNMPv3 is an encryption protocol for privacy. Only the data portion of a message is encrypted; the header and the security parameters are not. The privacy protocol that SNMPv3 supports is CBC-DES Symmetric Encryption Protocol and Advanced Encryption Standard (AES).

Security

The SNMPv3 security protects against:

- Modification of information—protects against altering information in transit.
- Masquerade—protects against an unauthorized entity assuming the identity of an authorized entity.
- Message stream modification—protects against delaying or replaying messages.
- Disclosure—protects against eavesdropping.

The SNMPv3 security also offers:

- Discovery procedure—finds the EngineID of an SNMP entity for a given transport address or transport endpoint address.
- Time synchronization procedure—facilitates authenticated communication between entities

The SNMPv3 does not protect against the following:

- Denial-of-service—prevention of exchanges between manager and agent.
- Traffic analysis—general pattern of traffic between managers and agents.

Access control subsystem

SNMPv3 provides a group option for access policies.

The access policy feature in the switch determines the access level for the users connecting to the device with different services like File Transfer Protocol (FTP), Trivial FTP (TFTP), Telnet, and rlogin. The system access policy feature is based on the user access levels and network address. This feature covers services, such as TFTP, HTTP, SSH, rlogin, and SNMP. However, with the SNMPv3 engine, the community names do not map to an access level. The View-based Access Control Model (VACM) determines the access privileges.

Use the configuration feature to specify groups for the SNMP access policy. You can use the access policy services to cover SNMP. Because the access restriction is based on groups defined through the VACM, the synchronization is made using the SNMPv3 VACM configuration. The administrator uses this feature to create SNMP users (USM community) and associate them to groups. You can configure the access policy for each group and network.

The following are feature specifications for the group options:

- After you enable SNMP service, this policy covers all users associated with the groups configured under the access policy. The access privileges are based on access allow or deny. If you select allow, the VACM configuration determines the management information base (MIB)-views for access.

• The SNMP service is disabled by default for all access policies.

• The access level configured under **`access-policy policy <id>`** does not affect SNMP service. The VACM configuration determines the SNMP access rights.

User-based security model

In a USM system, the security model uses a defined set of user identities for any authorized user on a particular SNMP engine. A user with authority on one SNMP engine must also have authorization on all SNMP engines with which the original SNMP engine communicates.

The USM provides the following levels of communication:

- NoAuthNoPriv—communication without authentication and privacy.
- AuthNoPriv—communication with authentication and without privacy.
- AuthPriv—communication with authentication and privacy.

The following figure shows the relationship between USM and VACM.

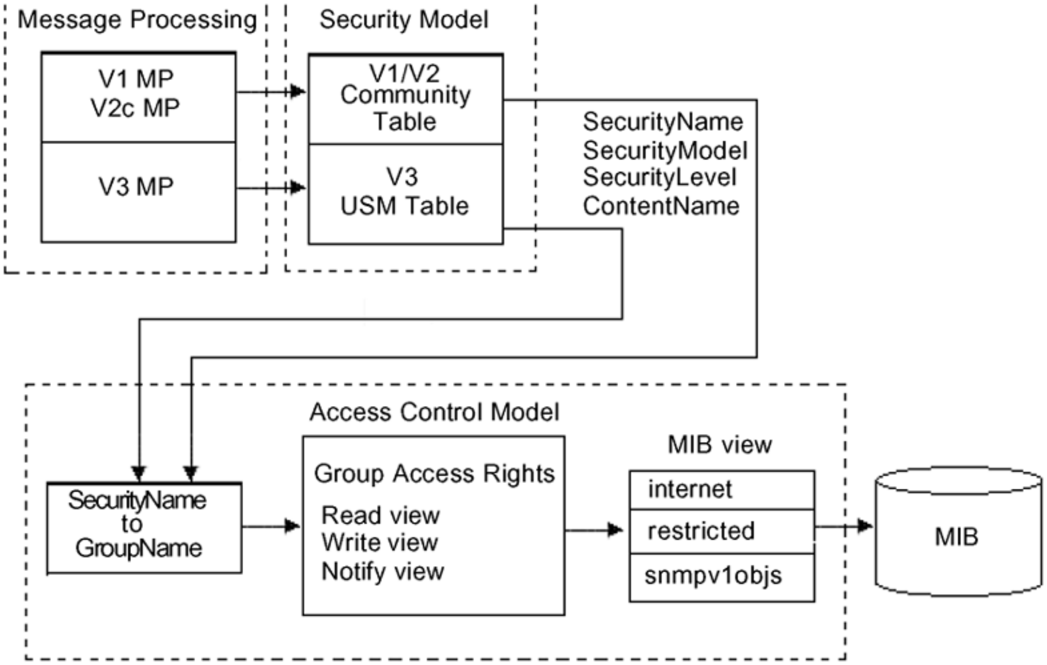


Figure 16: USM association with VACM

View-based Access Control

View-based Access Control Model (VACM) provides group access, group security levels, and context based on a predefined subset of MIB objects. These MIB objects define a set of managed objects and instances.

VACM is the standard access control mechanism for SNMPv3, and it provides:

- Authorization service to control access to MIB objects at the PDU level.

- Alternative access control subsystems.

The access is based on principal, security level, MIB context, object instance, and type of access requested (read or write). You can use the VACM MIB to define the policy and control remote management.

SNMPv3 encryption

A user-based security port for SNMPv3 is defined as a security subsystem within an SNMP engine. Currently the switch USM uses HMAC-MD5-96 and HMAC-SHA-96 as the authentication protocols, and CBC-DES as the privacy protocol. Use USM to use other protocols instead of, or concurrently with, these protocols. CFB128-AES-128, an AES-based Symmetric Encryption Protocol, is an alternative privacy protocol for the USM.

The AES standard is the current encryption standard, Federal Information Processing Standard 140-2 (FIPS 140-2), intended to be used by the U.S. Government organizations to protect sensitive information. The AES standard is also becoming a global standard for commercial software and hardware that uses encryption or other security features.

The AES-based symmetric encryption protocol

This symmetric encryption protocol provides support for data confidentiality. The system encrypts the designated portion of the SNMP message and includes it as part of the transmitted message.

The USM specifies that the scoped PDU is the portion of the message that requires encryption. An SNMP engine that can legitimately originate messages on behalf of the appropriate user shares a secret value, in combination with a timeliness value and a 64-bit integer, used to create the (localized) encryption/decryption key and the initialization vector.

The AES encryption key and Initialization Vector

The AES encryption key uses the first 128 bits of the localized key. The 128-bit Initialization Vector (IV) is the combination of the authoritative SNMP engine 32-bit snmpEngineBoot, the SNMP engine 32-bit snmpEngineTime, and a local 64-bit integer. The system initializes the 64-bit integer to a pseudo-random value at startup time.

Data encryption

The switch handles data encryption in the following manner:

1. The system treats data as a sequence of octets.
2. The system divides the plaintext into 128-bit blocks.

   The first input block is the IV, and the forward cipher operation is applied to the IV to produce the first output block.
3. The system produces the first cipher text block by executing an exclusive-OR function on the first plaintext block with the first output block.
4. The system uses the cipher text block as the input block for the subsequent forward cipher operation.
5. The system repeats the forward cipher operation with the successive input blocks until it produces a cipher text segment from every plaintext segment.
6. The system produces the last cipher text block by executing an exclusive-OR function on the last plaintext segment of r bits (r is less than or equal to 128) with the segment of the r most significant bits of the last output block.

Data decryption

The switch handles data decryption in the following manner:

1. In CFB decryption, the IV is the first input block, the system uses the first cipher text for the second input block, the second cipher text for the third input block, and this continues until the system runs out of blocks to decrypt.
2. The system applies the forward cipher function to each input block to produce the output blocks.
3. The system passes the output blocks through an exclusive-OR function with the corresponding cipher text blocks to recover the plaintext blocks.
4. The system sends the last cipher text block (whose size r is less than or equal to 128) through an exclusive-OR function with the segment of the r most significant bits of the last output block to recover the last plaintext block of r bits.

Trap notifications

You configure traps by creating SNMPv3 trap notifications, creating a target address to which you want to send the notifications, and specifying target parameters. For more information about how to configure trap notifications, see *Troubleshooting*.

SNMP community strings

For security reasons for SNMPv1 and SNMPv2, the SNMP agent validates each request from an SNMP manager before responding to the request by verifying that the manager belongs to a valid SNMP community. An SNMP community is a logical relationship between an SNMP agent and one or more SNMP managers (the manager software implements the protocols used to exchange data with SNMP agents). You define communities locally at the agent level.

The agent establishes one community for each combination of authentication and access control characteristics that you choose. You assign each community a unique name (community string), and all members of a community have the same access privileges, either read-only or read-write:

- Read-only: members can view configuration and performance information.
- Read-write: members can view configuration and performance information, and change the configuration.

By defining a community, an agent limits access to its MIB to a selected set of management stations. By using more than one community, the agent can provide different levels of MIB access to different management stations.

SNMP community strings are used when a user logs on to the device over SNMP, for example, using an SNMP-based management software. You set the SNMP community strings using CLI . If you have read/write/all access authority, you can modify the SNMP community strings for access to the device through Enterprise Device Manager (EDM).

Community strings exist for SNMPv1 and SNMPv2. If you want to use SNMPv3 only, you must disable SNMPv1 and SNMPv2 access by deleting the default community string entries and create the SNMPv3 user and group.SNMPv3 on page 153.

Note:

If you enable enhanced secure mode, the switch does not support the default SNMPv1 and default SNMPv2 community strings, and default SNMPv3 user name. The individual in the administrator access level role can configure a non-default value for the community strings, and the switch can continue to support SNMPv1 and SNMPv2. The individual in the administrator access level role can also configure a non-default value for the SNMPv3 user name and the switch can continue to support SNMPv3.

If you disable enhanced secure mode, the SNMPv1 and SNMPv2 support for community strings remains the same, and the default SNMPv3 user name remains the same. Enhanced secure mode is disabled by default.

For more information on enhanced secure mode, see *Administering*.

The following table lists the default community strings for SNMPv1 and SNMPv2.

VRF	Default community string	Access
GlobalRouter VRF	public	Read access
	private	Write access
ManagementRouter VRF	public:512	Read access
	private:512	Write access

Community strings are encrypted using the AES encryption algorithm. Community strings do not appear on the device and are not stored in the configuration file.

Caution:

Security risk

For security reasons, set the community strings to values other than the factory defaults.

The switch handles community string encryption in the following manner:

- When the device starts up, community strings are restored from the hidden file.
- When the SNMP community strings are modified, the modifications are updated to the hidden file.

Hsecure with SNMP

If you enable hsecure, the system disables SNMPv1, SNMPv2 and SNMPv3. If you want to use SNMP, you must use the command **`no boot config flag block-snmp`** to re-enable SNMP.

SNMPv3 support for VRF

Use Virtual Router Forwarding (VRF) to offer networking capabilities and traffic isolation to customers that operate over the same node (switch). Each virtual router emulates the behavior of a dedicated hardware router and is treated by the network as a separate physical router. You can use VRF Lite to perform the functions of many routers using a single router running VRF Lite. This substantially reduces the cost associated with providing routing and traffic isolation for multiple clients.

SNMP configuration using CLI

Configure the SNMP engine to provide services to send and receive messages, authenticate and encrypt messages, and control access to managed objects. A one-to-one association exists between an SNMP engine and the SNMP entity.

- To perform the procedures in this section, you must log on to the Global Configuration mode in CLI. For more information about how to use CLI, see *Using CLI and EDM*.

This task flow shows you the sequence of procedures you perform to configure basic elements of SNMP when using CLI.

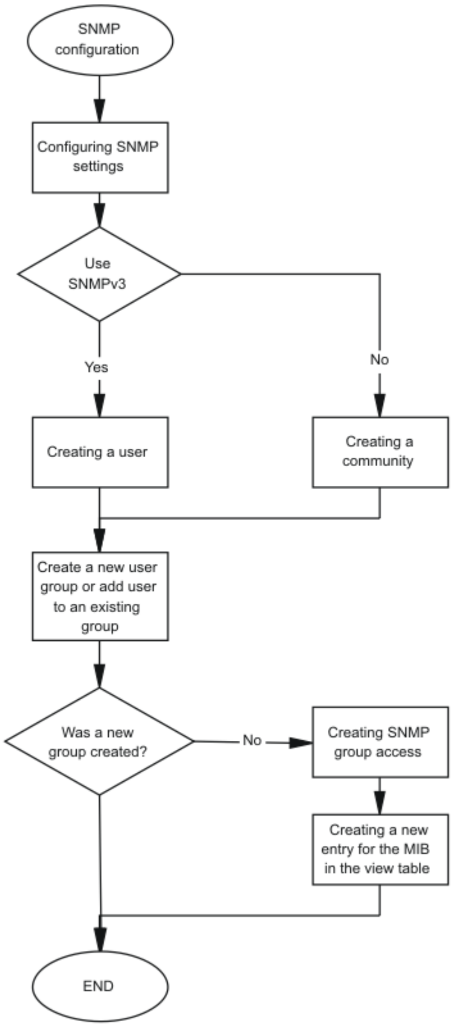

SNMP configuration
Configuring SNMP settings
Use SNMPv3
Yes
No
Creating a user
Creating a community
Create a new user group or add user to an existing group
Was a new group created?
No
Creating SNMP group access
Creating a new entry for the MIB in the view table
END

Figure 17: SNMP configuration procedures

Configuring SNMP settings

Configure Simple Network Management Protocol (SNMP) to define or modify the SNMP settings, and specify how secure you want SNMP communications.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   
   configure terminal
   ```

2. Enable the generation of authentication traps:

   ```
   snmp-server authentication-trap enable
   ```

3. Configure the contact information for the system:

   ```
   snmp-server contact WORD<0-255>
   ```

4. Configure the SNMP and IP sender flag to the same value:

   ```
   snmp-server force-iphdr-sender enable
   ```

5. Send the configured source address (sender IP) as the sender network in the notification message:

   ```
   snmp-server force-trap-sender enable
   ```

6. Create an SNMPv1 server host:

   ```
   snmp-server host WORD<1-256> [port <1-65535>] v1 WORD<1-32> [filter
   WORD<1-32>]
   ```

7. Create an SNMPv2 server host:

   ```
   snmp-server host WORD<1-256> [port <1-65535>] v2c WORD<1-32> [inform
   [timeout <1-2147483647>][retries <0-255>][mms <0-2147483647>]]
   [filter WORD<1-32>]
   ```

8. Create an SNMPv3 server host:

   ```
   snmp-server host WORD<1-256> [port <1-65535>] v3 {noAuthNoPriv|
   authNoPriv|authPriv WORD<1-32> [inform [timeout <1-2147483647>]
   [retries <0-255>]] [filter WORD<1-32>]
   ```

9. Configure the system location:

   ```
   snmp-server location WORD<0-255>
   ```

10. Configure the system name:

    ```
    snmp-server name WORD<0-255>
    ```

11. Create a new entry in the notify filter table:

    ```
    snmp-server notify-filter WORD<1-32> WORD<1-32>
    ```

12. Configure the SNMP trap receiver and source IP addresses:

    ```
    snmp-server sender-ip {A.B.C.D} {A.B.C.D}
    ```

Example

Enable the generation of SNMP traps. Configure the contact information for the system. Configure the SNMP and IP sender flag to the same value. Configure hosts to receive SNMP notifications:

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#snmp-server authentication-trap enable
Switch:1(config)#snmp-server contact xxxx@company.com
Switch:1(config)#snmp-server force-iphdr-sender enable
Switch:1(config)#snmp-server host 45.16.149.128 port 1 v1 SNMPv1 filter SNMPfilterv1
```

Variable definitions

Use the data in the following table to use the **snmp-server** command.

Variable	Value
bootstrap {min-secure|semi-secure|very-secure}	Creates an initial set of configuration data for SNMPv3. This configuration data follows the conventions described in the SNMPv3 standard (see RFC3515, Appendix A). This command creates a set of initial users, groups, and views. • min-secure—a minimum security configuration that gives read access and notify access to all processes (MIB view restricted) with noAuth-noPriv and read, write, and notify access to all processes (MIB view internet) using Auth-Priv. In this configuration, restricted MIB view matches internet MIB view. • semi-secure—a security configuration that gives read access and notify access to all processes (MIB view restricted) with noAuth-noPriv and read, write, and notify access to all processes (MIB view Internet) using Auth-Priv. In this configuration, restricted MIB view contains a smaller subset of views than Internet MIB view. For more information, see RFC 3515 Appendix A for details. • very-secure—a maximum security configuration that allows no access to the users. With this command all existing SNMP configurations in the SNMPv3 MIB tables are removed and replaced with entries as described in the RFC.
contact WORD<0-255>	Changes the sysContact information for the switch. WORD<0-255> is an ASCII string from 0–255 characters (for example a phone extension or e-mail address).
host WORD<1-256> [port <1-65535>] {v1 WORD<1-32>|v2c WORD<1-32> [inform [timeout <1-2147483647>][retries <0-255>] [mms <0-2147483647>]]|v3 {noAuthPriv|authNoPriv|authPriv} WORD<1-32> [inform [timeout <1-2147483647>][retries <0-255>]]} [filter WORD<1-32>]	Configures hosts to receive SNMP notifications. • host WORD<1-256> specifies the IPv4 or IPv6 host address • port <1-65535> specifies the port number • v1 WORD<1-32> specifies the SNMP v1 security name • v2c WORD<1-32> specifies the SNMPv2 security name • inform specifies the notify type • timeout <1-2147483647> specifies the timeout value • retries <0-255> specifies the number of retries • mms <1-2147483647> specifies the maximum message size • v3 specifies SNMPv3 • noAuthPriv|authNoPriv|authPriv specifies the security level • *WORD<1-32>* specifies the user name

Table continues…

Variable	Value
	• filter specifies a filter profile name
location WORD<0-255>	Configures the sysLocation information for the system. <WORD 0-255> is an ASCII string from 0–255 characters.
name WORD<0-255>	Configures the sysName information for the system. <WORD 0-255> is an ASCII string from 0–255 characters.
notify-filter WORD<1-32> WORD<1-32>	Creates a new entry in the notify filter table. The first WORD<1-32> specifies the filter profile name, and the second WORD<1-32> specifies the subtree OID.
sender-ip {A.B.C.D} {A.B.C.D}	The first {A.B.C.D} configures the SNMP trap receiver and source IP addresses. Specify the IP address of the destination SNMP server receives the SNMP trap notification in the first IP address. The second {A.B.C.D} specifies the source IP address of the SNMP trap notification packet that is transmitted in the second IP address. If you set this to 0.0.0.0, the system uses the IP address of the local interface that is closest (from an IP routing table perspective) to the destination SNMP server.

Creating a user

Create a new user in the USM table to authorize a user on a particular SNMP engine

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Create a user on a remote system:

   ```
   snmp-server user engine-id WORD<16—97> WORD<1-32>[{md5|sha}
   WORD<1-32>] [{aes|des} WORD<1-32>]
   ```

3. Create a user on the local system:

   ```
   snmp-server user WORD<1-32> [notify-view WORD<0-32>][read-view
   WORD<0-32>] [write-view WORD<0-32>] [{md5|sha} WORD<1-32>] [{aes|
   des} WORD<1-32>]
   ```

4. Add the user to a group:

   ```
   snmp-server user WORD<1-32> group WORD<1-32> [{md5|sha} WORD<1-32>]
   [{aes|des} WORD<1-32>]
   ```

Example

Create a user named test1 on a remote system with MD5:

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#snmp-server user test1 md5 auth-password aes test write-view test1
```

Variable definitions

Use the data in the following table to use the `snmp-server user` command.

Table 7: Variable definitions

Variable	Value
{aes|des} WORD<1-32>	Specifies a privacy protocol. If no value is entered, no authentication capability exists. The choices are aes or des. *WORD<1-32>* assigns a privacy password. If no value is entered, no privacy capability exists. The range is 1 to 32 characters. ❗ **Important:** You must set authentication before you can set the privacy option.
engine-id *WORD<16-97>*	Assigns an SNMPv3 engine ID. Use the no operator to remove this configuration.
group WORD<1-32>	Specifies the group access name.
{md5|sha} WORD<1-32>	Specifies an authentication protocol. If no value is entered, no authentication capability exists. The protocol choices are: MD5 and SHA. *WORD<1-32>* specifies an authentication password. If no value is entered, no authentication capability exists. The range is 1–32 characters.
notify-view WORD<0-32>	Specifies the view name in the range of 0 to 32 characters. The first instance is a noAuth view. The second instance is an auth view and the last instance is an authPriv view.
read-view WORD<0-32>	Specifies the view name in the range of 0 to 32 characters. The first instance is a noAuth view. The second instance is an auth view and the last instance is an authPriv view.
write-view WORD<0-32>	Specifies the view name in the range of 0 to 32 characters. The first instance is a noAuth view. The second instance is an auth view and the last instance is an authPriv view.
user WORD<1-32>	Creates the new entry with this security name. The name is used as an index to the table. The range is 1–32 characters. Use the no operator to remove this configuration.

Creating a new user group

Create a new user group to logically group users who require the same level of access. Create new access for a group in the View-based Access Control Model (VACM) table to provide access to managed objects.

Note:

Several default groups (public and private) exist that you can use. To see the list of default groups and their associated security names (secnames), enter **show snmp-server group**. If you use one of these groups, there is no need to create a new group.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Create a new user group:

   ```
   snmp-server group WORD <1-32> WORD<0-32> {auth-no-priv|auth-priv|no-auth-no-priv} [notify-view WORD<0-32>] [read-view WORD<0-32>]
   [write-view WORD<0-32>]
   ```

Example

This example uses the following variable names:

- The new group name is *lan6grp*.
- The context of the group is *""*, which represents the Global Router (VRF 0).
- The security level is *no-auth-no-priv*.
- The access view name is *v1v2only* for all three views: **notify-view**, **read-view**, and **write-view**.

```
Switch:1> enable
```

```
Switch:1# configure terminal
```

Create a new user group:

```
Switch:1(config)# snmp-server group lan6grp "" no-auth-no-priv notify-view
v1v2only read-view v1v2only write-view v1v2only
```

Variable definitions

Use the data in the following table use the **snmp-server group** command.

Variable	Value
auth-no-priv	Assigns the minimum level of security required to gain the access rights allowed by this conceptual row. If the auth-no-priv parameter is included, it creates one entry for SNMPv3 access.
auth-priv	Assigns the minimum level of security required to gain the access rights allowed by this conceptual row. If the auth-priv parameter is included, it creates one entry for SNMPv3 access.
group WORD<1-32> WORD<0-32>	WORD<1–32> specifies the group name for data access. Use the no operator to remove this configuration. WORD<0–32> specifies the context name. If you use a particular group name value but with different context names, you create multiple entries for different contexts for the same group. You can omit the context name and use the default. If the context name value ends in the wildcard character (*), the resulting entries match a context name that begins with that context. For example, a context name value of foo* matches contexts starting with foo, such as foo6 and foofofum. Use the no operator to remove this configuration.
no-auth-no-priv	Assigns the minimum level of security required to gain the access rights allowed by this conceptual row. If the no-auth-no-priv parameter is included, it creates 3 entries, one for SNMPv1 access, one for SNMPv2c access, and one for SNMPv3 access.
notify-view WORD<0-32>	Specifies the view name.
read-view WORD<0-32>	Specifies the view name.
write-view WORD<0-32>	Specifies the view name.

Creating a new entry for the MIB in the view table

Create a new entry in the MIB view table. The default Layer 2 MIB view cannot modify SNMP settings. However, a new MIB view created with Layer 2 permission can modify SNMP settings.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Create a new entry:

   ```
   snmp-server view WORD<1-32> WORD<1-32>
   ```

Example

```
Switch:1> enable
```

```
Switch:1# configure terminal
```

Create MIB views:

```
Switch:1(config) snmp-server view 2 1.3.8.7.1.4
```

Variable definitions

Use the data in the following table to use the `snmp-server view` command.

Table 8: Variable definitions

Variable	Value
The first *WORD<1-32>*	Specifies the prefix that defines the set of MIB objects accessible by this SNMP entity. The range is 1–32 characters.
The second *WORD<1-32>*	Specifies a new entry with this group name. The range is 1–32 characters.

Creating a community

Create a community to use in forming a relationship between an SNMP agent and one or more SNMP managers. You require SNMP community strings to access the system using an SNMP-based management software.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   
   configure terminal
   ```

2. Create a community:

   ```
   snmp-server community WORD<1-32> [group WORD<1-32>] [index
   WORD<1-32>] [secname WORD<1-32>]
   ```

   Important:

   - The **`group`** parameter is only required if you created a new user group using the procedure in Creating a new user group on page 166. If you use any of the default groups, the **`secname`** automatically links the community to its associated group so there is no need specify the group in this command.
   - If you do create a new group, use the **`snmp-server community`** command to create an SNMP community with a new security name and link it to the new group you created. There is no separate command to create a security name (secname). You use the **`snmp-server community`** command. The security name is the key to link the community name to a group.
   - You cannot use the `@` character or the string `::` when you create community strings.

Example

In the following example, the community name is *anewcommunity*, the index is *third*, and the secname is *readview*. There is no group specified because this is a default public/read only group.

```
Switch:1> enable

Switch:1# configure terminal

Switch:1(config)# snmp-server community anewcommunity index third secname
readview
```

Variable definitions

Use the data in the following table to use the `snmp-server community` command.

Table 9: Variable definitions

Variable	Value
community WORD<1-32>	Specifies a community string. The range is 1–32 characters.
group WORD<1-32>	Specifies the group name. The range is 1–32 characters.
index WORD<1-32>	Specifies the unique index value of a row in this table. The range is 1–32 characters.
secname WORD<1-32>	Maps the community string to the security name in the VACM Group Member Table. The range is 1-32 characters.

Adding a user to a group

Add a user to a group to logically group users who require the same level of access.

Procedure

1. Enter Global Configuration mode:

   ```
   enable

   configure terminal
   ```

2. Create a new user group:

   ```
   snmp-server user WORD<1-32> group WORD<1-32> [{md5 WORD<1-32>|sha
   WORD<1-32>) [{aes WORD<1-32>|des WORD<1-32>}]]
   ```

Example

```
Switch:1> enable

Switch:1# configure terminal
```

Add a user to a group to logically group users who require the same level of access:

```
Switch:1(config)# snmp-server user test1 group Grouptest1 md5 winter aes
summer
```

Variable definitions

Use the data in the following table to use the `snmp-server user` command.

Table 10: Variable definitions

Variable	Value
{aes|des} WORD<1-32>	Specifies a privacy protocol. If no value is entered, no authentication capability exists. The choices are aes or des. *WORD<1-32>* assigns a privacy password. If no value is entered, no privacy capability exists. The range is 1 to 32 characters. **Important:** You must set authentication before you can set the privacy option.
engine-id *WORD<16-97>*	Assigns an SNMPv3 engine ID. Use the no operator to remove this configuration.
group WORD<1-32>	Specifies the group access name.
{md5|sha} WORD<1-32>	Specifies an authentication protocol. If no value is entered, no authentication capability exists. The protocol choices are: MD5 and SHA. *WORD<1-32>* specifies an authentication password. If no value is entered, no authentication capability exists. The range is 1–32 characters.
notify-view WORD<0-32>	Specifies the view name in the range of 0 to 32 characters. The first instance is a noAuth view. The second instance is an auth view and the last instance is an authPriv view.
read-view WORD<0-32>	Specifies the view name in the range of 0 to 32 characters. The first instance is a noAuth view. The second instance is an auth view and the last instance is an authPriv view.
write-view WORD<0-32>	Specifies the view name in the range of 0 to 32 characters. The first instance is a noAuth view. The second instance is an auth view and the last instance is an authPriv view.
user WORD<1-32>	Creates the new entry with this security name. The name is used as an index to the table. The range is 1–32 characters. Use the no operator to remove this configuration.

Blocking SNMP

Disable SNMP by using the SNMP block flag. By default, SNMP access is enabled.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

```
configure terminal
```

2. Disable SNMP:

```
boot config flags block-snmp
```

Example

```
Switch:1> enable
```

```
Switch:1# configure terminal
```

Disable SNMP:

```
Switch:1(config)# boot config flags block-snmp
```

Variable definitions

Use the data in the following table to use the `boot config flags` command.

Table 11: Variable definitions

Variable	Value
block-snmp	Configures the block SNMP flag as active. Use the no operator to remove this configuration. The default is off. To set this option to the default value, use the default operator with the command.

Displaying SNMP system information

Display SNMP system information to view trap and authentication profiles.

Procedure

1. Log on to the switch to enter User EXEC mode.
2. Display SNMP system information:

```
show snmp-server
```

Example

```
Switch:1>show snmp-server


                 trap-sender :
           force-trap-sender : FALSE
          force-iphdr-sender : FALSE
                     contact : none
                    location : none
                        name : Switch1
          AuthenticationTrap : false
            LoginSuccessTrap : false
```

SNMP configuration using Enterprise Device Manager

Configure SNMP to provide services to send and receive messages, authenticate and encrypt messages, and control access to managed objects with Enterprise Device Manager (EDM).

The following task flow shows you the sequence of procedures you perform to configure basic elements of SNMP using EDM.

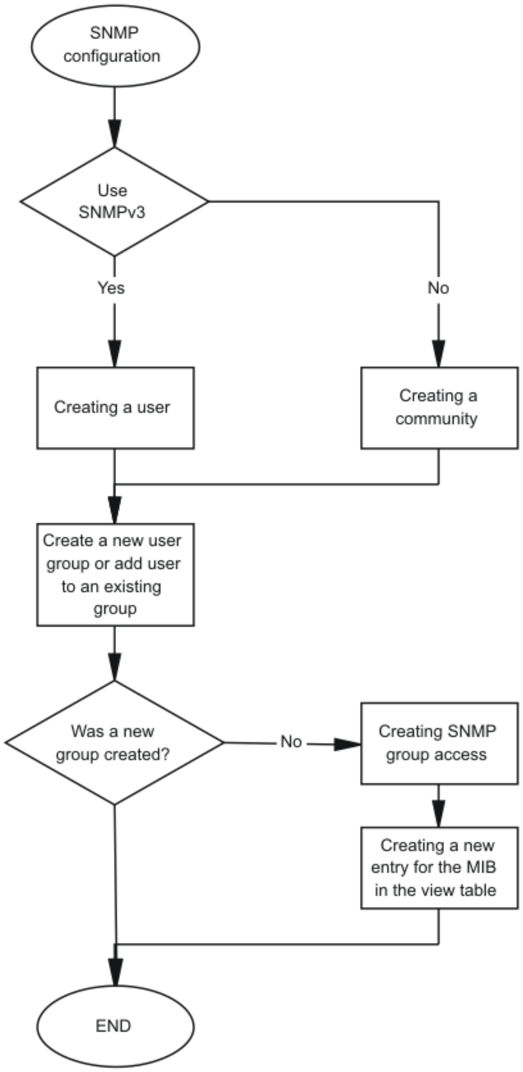

SNMP configuration
Use SNMPv3
Yes
No
Creating a user
Creating a community
Create a new user group or add user to an existing group
Was a new group created?
No
Creating SNMP group access
Creating a new entry for the MIB in the view table
END

Figure 18: SNMP configuration using Enterprise Device Manager procedures

Creating a user

About this task

Create a new user in the USM table to authorize a user on a particular SNMP engine.

Note:

In EDM, to create new SNMPv3 users you must use the **CloneFromUser** option. However, you cannot clone the default user, named initial. As a result, you must first use CLI to configure at least one user, and then you can use EDM to create subsequent users with the **CloneFromUser** option.

Procedure

1. In the navigation pane, expand the following folders: **Configuration** > **Edit** > **SnmpV3**.
2. Click **USM Table**.
3. Click **Insert**.
4. In the **EngineID** box, use the default Engine ID provided or type an administratively-unique identifier to an SNMP engine.
5. In the **User Name** box, type a name.
6. From the **CloneFromUser** list, select a security name from which the new entry copies authentication data and private data, if required.
7. From the **Auth Protocol** list, select an authentication protocol.
8. In the **Cloned User's Auth Password** box, type the authentication password of the cloned user.
9. In the **New User's Auth Password** box, type an authentication password for the new user.
10. From the **Priv Protocol** list, select a privacy protocol.
11. In the **Cloned User's Priv Password** box, type the privacy password of the cloned user.
12. In the **New User's Priv Password** box, type a privacy password for the new user.
13. Click **Insert**.

    Caution:

    Security risk

    To ensure security, change the GroupAccess table default view after you set up a new user in the USM table. This prevents unauthorized people from accessing the system using the default user logon. Also, change the Community table defaults, because the community name is used as a community string in SNMPv1/v2 PDU.

USM Table field descriptions

Use the data in the following table to use the **USM Table** tab and the **Insert USM Table** dialog box. Some fields appear only on the Insert USM Table dialog box.

Name	Description
EngineID	Specifies an administratively-unique identifier to an SNMP engine.
UserName	Creates the new entry with this security name. The name is used as an index to the table. The range is 1–32 characters.
SecurityName	Identifies the name on whose behalf SNMP messages are generated.
Clone From User	Specifies the security name from which the new entry must copy privacy and authentication parameters. The range is 1–32 characters. This option appears only in the **Insert USM Table** dialog box.
Auth Protocol (Optional)	Assigns an authentication protocol (or no authentication) from a list. If you select an authentication protocol, you must enter an old AuthPass and a new AuthPass.
Cloned User's Auth Password	Specifies the current authentication password of the cloned user. This option appears only in the **Insert USM Table** dialog box.
New User's Auth Password	Specifies the authentication password of the new user. This option appears only in the **Insert USM Table** dialog box.
Priv Protocol (Optional)	Assigns a privacy protocol (or no privacy) from a list. If you select a privacy protocol, you must enter an old PrivPass and a new PrivPass.
Cloned User's Priv Password	Specifies the current privacy password of the cloned user. This option appears only in the **Insert USM Table** dialog box.
New User's Priv Password	Specifies the privacy password of the new user. This option appears only in the **Insert USM Table** dialog box.

Creating a new group membership

About this task

Create a new group membership to logically group users who require the same level of access.

Note:

Several default groups (public and private) exist that you can use. To see the list of default groups and their associated security names (secnames), enter `show snmp-server group`. If you use one of these groups, there is no need to create a new group.

Procedure

1. In the navigation tree, open the following folders: **Configuration** > **Edit** > **SnmpV3**.
2. Click **VACM Table**.
3. Click the **Group Membership** tab.
4. Click **Insert**.
5. From the **SecurityModel** options, select a security model.
6. In the **SecurityName** box, type a security name.

7. In the **GroupName** box, type a group name.
8. Click **Insert**.

Group Membership field descriptions

Use the data in the following table to use the **Group Membership** tab.

Name	Description
SecurityModel	Specifies the security model to use with this group membership.
SecurityName	Specifies the security name assigned to this entry in the View-based Access Control Model (VACM) table. The range is 1–32 characters.
GroupName	Specifies the name assigned to this group in the VACM table. The range is 1–32 characters.

Creating access for a group

About this task

Create access for a group in the View-based Access Control Model (VACM) table to provide access to managed objects.

Procedure

1. In the navigation tree, open the following folders: **Configuration** > **Edit** > **SnmpV3**.
2. Click **VACM Table**.
3. Click the **Group Access Right** tab.
4. Click **Insert**.
5. In the **GroupName** box, type a VACM group name.
6. In the **ContextPrefix** box, select a VRF instance. This is an optional step.
7. From the **SecurityModel** options, select a model.
8. From the **SecurityLevel** options, select a security level.
9. In the **ContextMatch** option, select a value to match the context name. This value is **exact** by default.
10. In the **ReadViewName** box, type the name of the MIB view that forms the basis of authorization when reading objects. This is an optional step.
11. In the **WriteViewName** box, type the name of the MIB view that forms the basis of authorization when writing objects. This is an optional step.
12. In the **NotifyViewName** box, type MIB view that forms the basis of authorization for notifications. This is an optional step.
13. Click **Insert**.

Group Access Right field descriptions

Use the data in the following table to use the **Group Access Right** tab.

Name	Description
GroupName	Specifies the name of the new group in the VACM table. The range is 1–32 characters.
ContextPrefix	Specifies if the contextName must match the value of the instance of this object exactly or partially. The range is an SnmpAdminString, 1–32 characters.
SecurityModel	Specifies the authentication checking to communicate to the switch. The security models are: • SNMPv1 • SNMPv2 • USM
SecurityLevel	Specifies the minimum level of security required to gain the access rights allowed. The security levels are: • noAuthNoPriv • authNoPriv • authpriv
ContextMatch	Specifies if the prefix and the context name must match. If the value is exact, all rows where the contextName exactly matches vacmAccessContextPrefix are selected. If you do not select exact, all rows where the contextName with starting octets that exactly match vacmAccessContextPrefix are selected.
ReadViewName	Identifies the MIB view of the SNMP context to which this conceptual row authorizes read access. The default is the empty string.
WriteViewName	Identifies the MIB view of the SNMP context to which this conceptual row authorizes write access. The default is the empty string.
NotifyViewName	Identifies the MIB view of the SNMP context to which this conceptual row authorizes access for notifications. The default is the empty string.

Creating access policies for SNMP groups

About this task

Create an access policy to determine the access level for the users who connect to the switch with different services like File Transfer Protocol (FTP), Trivial FTP (TFTP), Telnet, and rlogin.

You only need to create access policies for SNMP groups if you have the access policy feature enabled. For more information about access policies, see *Administering*.

Procedure

1. In the navigation pane, expand the following folders: **Configuration** > **Security** > **Control Path**.
2. Click **Access Policies**.
3. Click the **Access Policies-SNMP Groups** tab.
4. Click **Insert**.
5. Enter an **ID**.
6. In the **Name** box, type a name.
7. From the **Model** options, select a security model.
8. Click **Insert**.

Access Policies — SNMP Groups field descriptions

Use the data in the following table to use the **Access Polices-SNMP Groups** tab.

Name	Description
Id	Specifies the ID of the group policy.
Name	Specifies the name assigned to the group policy. The range is 1–32 characters.
Model	Specifies the security model {SNMPv1|SNMPv2c|USM}.

Assigning MIB view access for an object

About this task

Create a new entry in the MIB View table.

You cannot modify SNMP settings with the default Layer 2 MIB view. However, you can modify SNMP settings with a new MIB view created with Layer 2 permissions.

Procedure

1. In the navigation tree, open the following folders: **Configuration** > **Edit** > **SnmpV3**.
2. Click **VACM Table**.
3. In the VACM Table tab, click the **MIB View** tab.
4. Click **Insert**.
5. In the **ViewName** box, type a view name.
6. In the **Subtree** box, type a subtree.
7. In the **Mask** box, type a mask.
8. From the **Type** options, select whether access to the MIB object is granted.
9. Click **Insert**.

MIB View field descriptions

Use the data in the following table to use the **MIB View** tab.

Name	Description
ViewName	Creates a new entry with this group name. The range is 1–32 characters.
Subtree	Specifies a valid object identifier that defines the set of MIB objects accessible by this SNMP entity, for example, 1.3.6.1.1.5.
Mask (optional)	Specifies a bit mask with vacmViewTreeFamilySubtree to determine whether an OID falls under a view subtree.
Type	Determines whether access to a MIB object is granted (included) or denied (excluded). The default is included.

Creating a community

About this task

Create a community to use in forming a relationship between an SNMP agent and one or more SNMP managers. You require SNMP community strings for access to the switch using an SNMP-based management software.

Procedure

1. In the navigation pane, expand the following folders: **Configuration** > **Edit** > **SnmpV3**.
2. Click **Community Table**.
3. Click **Insert**.
4. In the **Index** box, type an index.
5. In the **Name** box, type a name that is a community string.
6. In the **SecurityName** box, type a security name.
7. In the **ContextName** box, type the context name.
8. Click **Insert**.

Community Table field descriptions

Use the data in the following table to use the **Community Table** tab.

Name	Description
Index	Specifies the unique index value of a row in this table. The range is 1–32 characters.
Name	Specifies the community string for which a row in this table represents a configuration.

Table continues…

Name	Description
SecurityName	Specifies the security name in the VACM group member table to which the community string is mapped. The range is 1–32 characters.
ContextEngineID	Indicates the location of the context in which management information is accessed when using the community string specified in **Name**.
ContextName	Specifies the context in which management information is accessed when you use the specified community string.

Viewing all contexts for an SNMP entity

About this task

View contexts to see the contents of the context table in the View-based Access Control Model (VACM). This table provides information to SNMP command generator applications so that they can properly configure the VACM access table to control access to all contexts at the SNMP entity.

Procedure

1. In the navigation tree, open the following folders: **Configuration** > **Edit** > **SnmpV3**.
2. Click **VACM Table**.
3. In the **VACM Table** tab, click the **Contexts** tab.

Contexts field descriptions

Use the data in the following table to use the **Contexts** tab.

Variable	Value
ContextName	Shows the name identifying a particular context at a particular SNMP entity. The empty contextName (zero length) represents the default context.

Chapter 8: TACACS+

This chapter provides Terminal Access Controller Access Control Plus (TACACS+) concepts and procedures to complete TACACS+ configuration.

TACACS+ fundamentals

The switch supports the TACACS+ client. TACACS+ is a remote authentication protocol that provides centralized validation of users who attempt to gain access to a router or Network Access Server (NAS).

The TACACS+ feature is a client and server-based protocol that allows the switch to accept a user name and password and send a query to a TACACS+ authentication server, sometimes called a TACACS+ daemon. The TACACS+ server allows access or denies access based on the response by the client.

The TACACS+ feature facilitates the following services:

- Login authentication and authorization for CLI access through rlogin, Secure Shell (SSH), Telnet, or serial port.
- Login authentication for web access through EDM.
- Command authorization for CLI through rlogin, SSH, Telnet, or serial port.
- Accounting of CLI through rlogin, SSH, Telnet, and serial port.

The following figure displays the basic layout of the switch and the TACACS+ server.

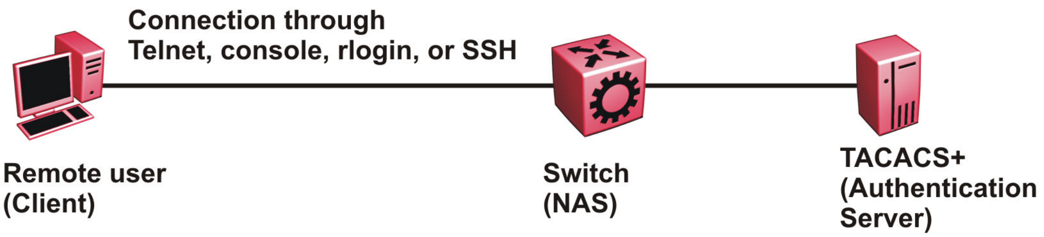


Figure 19: Switch and TACACS+ server

The TACACS+ feature uses Transmission Control Protocol (TCP) for its transport to ensure reliable delivery of packets. TACACS+ provides security by encrypting all traffic between the switch, which acts as the Network Access Server, and the TACACS+ server.

TACACS+ is a newer version of TACACS and provides separate authentication, authorization, and accounting (AAA) services. TACACS+ does not support earlier versions of TACACS.

TACACS+ is a base license feature. The TACACS+ feature is disabled by default.

TACACS+ Operation

The switch acts as an NAS to provide a connection to a single user, to a network, subnetwork or interconnected networks. The switch acts as a gateway to guard access to the TACACS+ server and network. Encryption relies on a secret key that is known to the client and the TACACS+ server.

Similar to the Remote Access Dial-In User Services (RADIUS) protocol, TACACS+ provides the ability to centrally manage the users who want to access a remote device. TACACS+ provides management of remote and local users who try to access a device through:

- rlogin
- Secure Shell (SSHv2)
- Telnet
- serial port
- Web management

A TACACS+ daemon, which typically runs on a UNIX or Windows NT workstation, maintains the TACACS+ authentication, authorization, and accounting services.

You configure users in the TACACS+ server. If you enable authentication, authorization, and accounting services, the following occurs:

- During the logon process, the TACACS+ client initiates the TACACS+ authentication session with the TACACS+ server.
- After successful authentication the TACACS+ client initiates the TACACS+ authorization session with the TACACS+ server. This is transparent to the user. The switch receives the user access level after a successful TACACS+ authorization. The TACACS+ server authorizes every command the user issues if TACACS + command authorization is enabled for that user access level.
- After successful authorization, if you enable TACACS+ accounting, the TACACS+ client sends accounting information to the TACACS+ server.

A TACACS+ session establishes with the server in one of two ways:

- Multi-connection mode (also known as per-session): For every authentication, authorization, and accounting (AAA) request the switch establishes a session with the TACACS+ server, and then once the request finishes, the session is torn down. Multi-connection mode is the default mode.
- Single-connection mode: The first AAA request establishes the session, which is only torn down if TACACS+ is disabled or due to inactivity.

TACACS+ Architecture

You can connect the TACACS+ server to the switch:

- In-band through one of the data ports.
- Out-of-band through the management port, if the physical hardware includes a management port.

Connect the TACACS+ server through a local interface. Management PCs can reside on an out-of-band management Ethernet port, or on the corporate network. Place the TACACS+ server on the corporate network so you can route it to the switch.

Before you configure the switch, you must configure at least one TACACS+ server and a key.

The TACACS+ server and the switch must have the same:

- Encryption key
- Connection mode (single connection or per-session connection. Per-session connection is the same as multi-connection mode.)
- TCP port number

You can configure a secondary TACACS+ server for backup authentication. You specify the primary authentication server when you configure the switch.

Authentication, authorization, and accounting

A fundamental feature of TACACS+ is the separation of authentication, authorization, and accounting (AAA) services, which allows you to selectively implement one or more TACACS + services.

TACACS+ authentication

TACACS+ authentication provides control of authentication through login and password.

Authentication uses a database of users and passwords to determine:

- who a user is
- whether to allow the user access to the NAS

Important:

Prompts for log on and password occur prior to the authentication process. If TACACS+ fails because no valid servers exist, the device uses the user name and password from the local database. If TACACS+ or the local database returns an access denied packet, the authentication process stops. The device attempts no other authentication methods.

The following figure illustrates the authentication process.

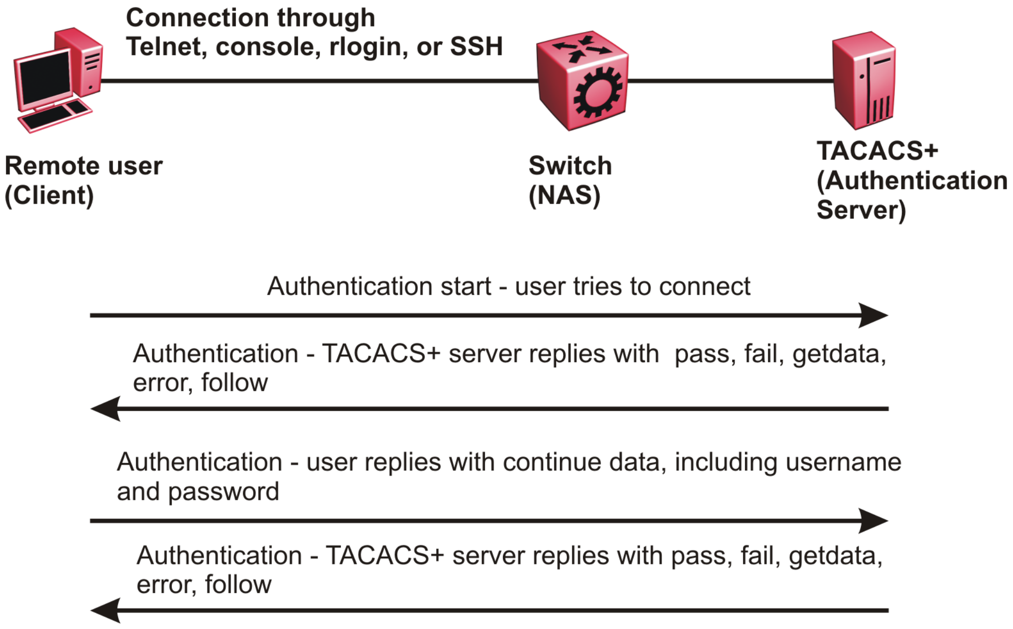

Connection through
Telnet, console, rlogin, or SSH
Remote user
(Client)
Switch
(NAS)
TACACS+
(Authentication
Server)
Authentication start - user tries to connect
Authentication - TACACS+ server replies with pass, fail, getdata, error, follow
Authentication - user replies with continue data, including username and password
Authentication - TACACS+ server replies with pass, fail, getdata, error, follow

Figure 20: Authentication process

TACACS+ authorization

The transition from TACACS+ authentication to the authorization phase is transparent to the user. After successful completion of the authentication session, an authorization session starts with the authenticated user name. The authorization session provides access level functionality.

Authorization cannot occur without authentication.

Authorization:

- determines what a user can do
- allows administrators fine-grained control over the capabilities of users during sessions

The following figure illustrates the authorization process.

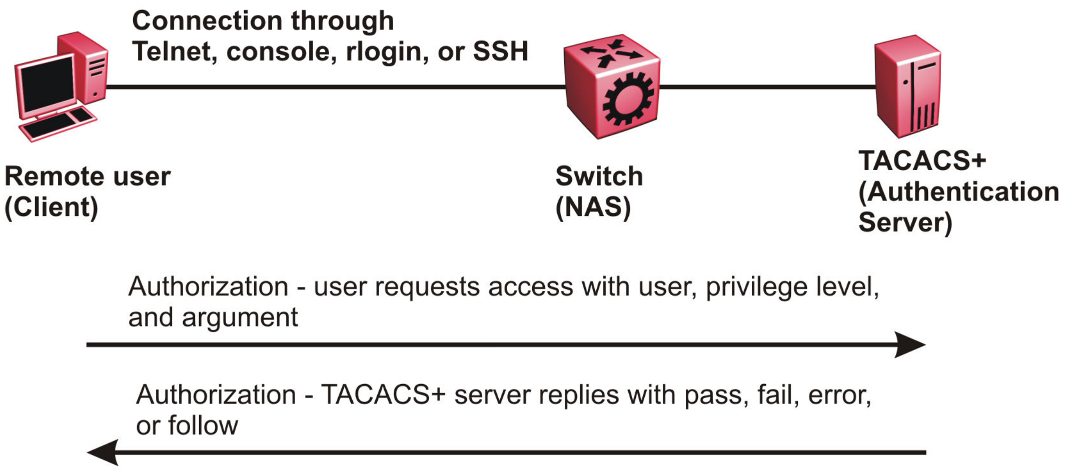

Connection through
Telnet, console, rlogin, or SSH
Remote user
(Client)
Switch
(NAS)
TACACS+
(Authentication
Server)
Authorization - user requests access with user, privilege level, and argument
Authorization - TACACS+ server replies with pass, fail, error, or follow

Figure 21: Authorization process

Authorization determines what a user can do. Authorization gives you the ability to limit network services to certain users and to limit the use of certain commands to certain users. The TACACS+ feature enhances the security by tightly policing the command execution for a particular user. After you enable command authorization, all commands, no matter the access level to which they belong, are sent to the TACACS+ server for authorization. Authorization cannot occur without first enabling authentication. You must configure command authorization globally and at individual access levels.

Two kinds of authorization requests exist:

1. Login authorization: Login authorization happens immediately after authentication and is transparent to the user. When the user logs on to the device, authorization provides the user access level. With log on, the device does not send a command to the TACACS+ server. You cannot configure login authorization.
2. Command authorization: When you configure command authorization for a particular level, all commands that you issue are sent to the TACACS+ server for authorization. The device can only issue the commands the TACACS+ server authorizes. You need to configure command authorization globally and at individual access levels, which are visible to the users.

Note:

You must verify that the switch can reach the TACACS+ server and that you configure TACACS + properly before you enable command authorization.

If a user is TACACS+ authenticated and command authorization is enabled for that level, then if the switch cannot reach the TACACS+ server, the switch does not allow the user to issue any command that has privilege level command authorization enabled. In such a case, the user can only issue logout and exit commands.

If a user tries to log in and the TACACS+ server does not exist or is not reachable, then, as discussed before, a local database in the switch authenticates the user. The switch authorizes a locally authenticated user and a locally authenticated user is not eligible for TACACS+ command authorization.

After the switch requests authorization, the logon credentials are sent to the TACACS+ daemon for authorization. If logon authorization fails, the user receives a permission denied message.

If TACACS+ logon authorization succeeds, the switch uses information from the user profile, which exists in the local user database or on the TACACS+ server, to configure the session for the user.

After you enable TACACS+ command authorization all commands are visible to all users; however, the user can only issue those commands that the TACACS+ server configuration allows.

The switch cannot enforce command access level. The TACACS+ server returns an access level to the switch. The switch allows the user to access the switch according to the access level. The device grants the user access to a command only if the profile for the user allows the access level.

You preconfigure command authorization on the TACACS+ server. You specify a list of regular expressions that match command arguments, and you associate each command with an action to deny or permit.

All members in a group have the same authorization. If you place a user in a group, the daemon looks in the group for authorization parameters if it cannot find them in the user profile.

TACACS+ accounting

TACACS+ accounting enables you to track the services users access and the amount of network resources users consume.

TACACS+ accounting allows you to track:

- what a user does
- when a user does certain actions

The accounting record includes the following information:

- User name
- Date
- Start/stop/elapsed time
- Access server IP address
- Reason

You can use accounting for an audit trail, to bill for connection time or resources used, or for network management. TACACS+ accounting provides information about user sessions using the following connection types: Telnet, rlogin, SSH, and web-based management.

With separation of AAA, accounting can occur independently from authentication and authorization.

The following figure illustrates the accounting process.

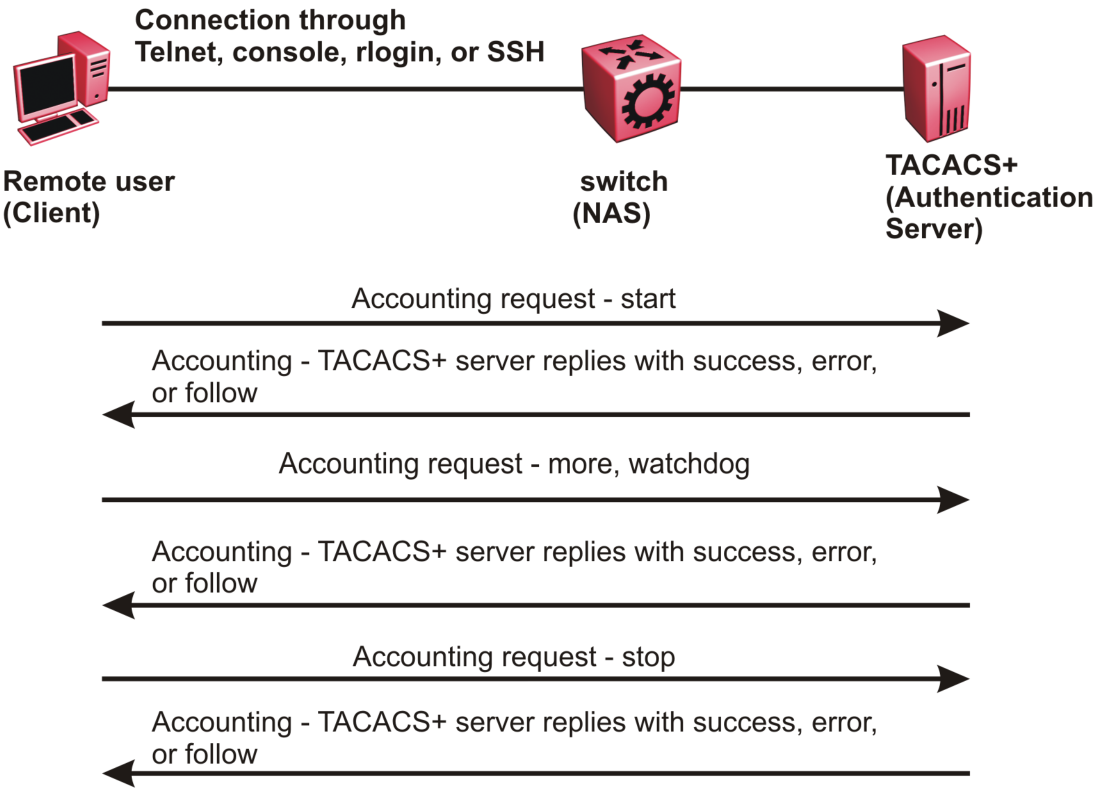

Connection through
Telnet, console, rlogin, or SSH
Remote user
(Client)
switch
(NAS)
TACACS+
(Authentication
Server)
Accounting request - start
Accounting - TACACS+ server replies with success, error, or follow
Accounting request - more, watchdog
Accounting - TACACS+ server replies with success, error, or follow
Accounting request - stop
Accounting - TACACS+ server replies with success, error, or follow

Figure 22: Accounting process

After you enable accounting, the switch reports user activity to the TACACS+ server in the form of accounting records. Each accounting record contains accounting attribute value (AV) pairs. AV pairs are strings of text in the form “attribute-value” sent between the switch and a TACACS+ daemon as part of the TACACS+ protocol. The TACACS+ server stores the accounting records.

You cannot customize the set of events the switch monitors and logs with TACACS+ accounting. TACACS+ accounting logs the following events:

- User logon and logoff
- Logoff generated because of activity timeout
- Unauthorized command
- Telnet session closed (not logged off)

Privilege level changes at runtime

You can change your privilege level at runtime with the **`tacacs switch level`** command.

You need to configure separate profiles in the TACACS+ server configuration file for the switch level. The switch supports only levels 1 to 6 and level 15. The switch uses the profile when you issue the command **tacacs switch level <1–15>**. As part of the profile, you specify a user name, level, and password. To preconfigure a dummy user for that level on the TACACS+ daemon, the format of the user name for the dummy user is **$enab<n>$**, where <*n*> is the privilege level to which you want to allow access.

The following is an example of a TACACS+ server profile, which you configure on the TACACS + server:

```
user = $enab6$ {
member = level6
login = cleartext get-me-on-6
}
```

The following table maps user accounts to TACACS+ privilege level.

Switch access level	TACACS+ privilege level	Description
NONE	0	If the TACACS+ server returns an access level of 0, the user is denied access. You cannot log into the device if you have an access level of 0.
READ ONLY	1	Permits you to view only configuration and status information.
LAYER 1 READ WRITE	2	Permits you to view most of the switch configuration and status information and change physical port settings.
LAYER 2 READ WRITE	3	Permits you to view and change configuration and status information for Layer 2 (bridging and switching) functions.
LAYER 3 READ WRITE	4	Permits you to view and change configuration and status information for Layer 2 and Layer 3 (routing) functions.
READ WRITE	5	Permits you to view and change configuration and status information across the switch. This level does not allow you to change security and password settings.
READ WRITE ALL	6	Permits you to have all the rights of read-write access and the ability to change security settings, including command line interface (CLI) and web-based management user names and passwords, and the SNMP community strings.

Table continues…

Switch access level	TACACS+ privilege level	Description
NONE	7 to 14	If the TACACS+ server returns an access level of 7 to 14, the user is denied access. You cannot log into the device if you have an access level of 7 to 14.
READ WRITE ALL	15	Permits you to have all the rights of read-write access and the ability to change security settings, including command line interface (CLI) and Web-based management user names and passwords, and the SNMP community strings. **Note:** Access level 15 is internally mapped to access level 6, which ensures consistency with other vendor implementations. The switch does not differentiate between an access level of 6 and an access level of 15.

Note:

If you enable enhanced secure mode with the **`boot config flags enhancedsecure-mode`** command, you enable new access levels, along with stronger password complexity, length, and minimum change intervals. With enhanced secure mode enabled, the switch supports the following access levels for RADIUS authentication:

- Administrator
- Privilege
- Operator
- Auditor
- Security

The switch associates each username with a certain role and appropriate authorization rights to view and configure commands. For more information on system access fundamentals and configuration, see *Administering*.

TACACS+ command authorization

After you enable TACACS+ authorization, the current privilege-level to command mapping on the switch is no longer relevant because the TACACS+ server has complete responsibility for command authorization. TACACS+ authorization provides access to the system based on username, not based on privilege level.

After you enable TACACS+ command authorization for a particular privilege level, and a user with that privilege level logs on, the user can access commands based on his user name.

TACACS+ switch level and TACACS+ switch back commands

The user can only issue the **`tacacs switch level`** command after TACACS+ authenticates the user. Locally authenticated users, which means users authenticated only by the switch and not by the TACACS+ server, cannot use the **`tacacs switch level`** command.

Consider a user, called X, with a privilege level of 4, who uses the **`tacacs switch level <1-15>`** command to change the privilege level from 4 to 6.

If user X successfully changes the switch level to 6, the user name changes from X to “$enab6$”, and the privilege level changes from 4 to 6. If TACACS+ command authorization is enabled for privilege level 6, then the TACACS+ server authorizes commands issued based on the rules defined for (dummy) user “$enab6$”.

If TACACS+ command authorization is not enabled for privilege level 6, then the switch locally authorizes the user X based on the privilege level of the user.

The user can return to his previous privilege level using the **`tacacs switch back`** command. In the preceding scenario, if the user issues the **`tacacs switch back`** command, the user name changes for user X from “$enab6$” to X, and the privilege level changes from 6 to 4.

TACACS+ switch level supports up to eight levels, and TACACS+ switch level allows a user to switch level up to eight times from his original privilege level. The switch stores all of the previous privilege levels in the same order in which the user switches levels. After switching eight times, if the user tries to switch a level the ninth time, the following error message displays:

```
Only allowed to switch level 8 times!
```

The user can switch back to his previous privilege levels using the **`tacacs switch back`** command. The **`tacacs switch back`** command switches back in the reverse order in which you issued the **`tacacs switch level`** command. Consider a user who switched levels from 4 to 5, and then to 6. If the user used the **`tacacs switch back`** command, the user first moves from 6 to 5, and then using the **`tacacs switch back`** command again moves from 5 to 4.

Note:

If you want to switch to a privilege level 'X' using **`tacacs switch level <1-15>`** command, you must create a user "$enabX$" on the TACACS+ server. X is the privilege level that you want to change.

TACACS+ switch level functionality:

The following table explains TACACS+ switch level functionality.

User logs in with	TACACS+ server available	Result
TACACS+ authentication	Yes	The user can issue the **`tacacs switch level <1–15>`** command.
Local authentication	No	The user cannot issue the **`tacacs switch level <1–15>`** command.

Table continues…

User logs in with	TACACS+ server available	Result
Local authentication	Yes	Even if a TACACS+ server becomes reachable, the user remains locally authenticated and cannot issue the **`tacacs switch level <1-15>`** command.

TACACS+ command authorization functionality:

The following table explains TACACS+ command authorization functionality.

User logs in with	Command authorization	Result
Local authentication	—	The switch authorizes the user locally.
TACACS+ authentication	Not enabled for the logged-in level.	The switch authorizes the user locally. If the server connection is lost, the switch authorizes the user locally.
TACACS+ authentication	Enabled for the logged-in level.	The TACACS+ server authorizes the user. If the server connection is lost, the user can only issue **`exit`** and **`logout`** commands.

Note:

A user who configures TACACS+ is locally authenticated and authorized by the switch, so even after the user configures TACACS+, the switch continues to locally authorize the user.

TACACS+ and RADIUS differences

TACACS+ and RADIUS are security protocols that you can use on network devices.

You can enable TACACS+ and RADIUS together. However, TACACS+ has a higher priority. If the TACACS+ server is not available the authentication is sent to RADIUS, if RADIUS is enabled. However, if TACACS+ authentication fails, then requests are not sent to RADIUS.

Following is a list of differences between TACACS+ and RADIUS.

TACACS+	RADIUS
Separates Authorization, Authentication and Accounting (AAA). As a result, you can selectively implement one or more TACACS+ services. With TACACS+ you can use different servers for each service.	Combines authentication and authorization.
Uses TCP. TCP is connection-oriented.	Uses UDP. UDP is best-effort delivery.

Table continues…

TACACS+	RADIUS
TCP immediately indicates if a server crashes or is not running. TCP offers an acknowledgement that a request has been received.	RADIUS uses re-transmit attempts and timeouts to make up for the support TCP has.
Encrypts the entire body of the packet, which includes the password and username.	Encrypts only the password from the client to the server.
Used for administrator access. Usually used for administrator access to network devices.	Used for subscriber access. Usually used to authenticate remote users to a network.
Can control which access level of commands a user or group can access.	Cannot control which access level of commands can be used.

TACACS+ feature limitations

The current implementation of TACACS+ does not support the following features:

- Point-to-Point Protocol (PPP) authentication and accounting
- IPv6 for TACACS+
- S/KEY (One Time Password) authentication
- PAP/CHAP/MSCHAP authentication methods
- The FOLLOW response of a TACACS+ server, in which the AAA services are redirected to another server. The response is interpreted as an authentication failure.
- User capability to change passwords at runtime over the network. The system administrator must change user passwords locally, on the server.
- TACACS+ command authorization when the user accesses the switch through EDM and SNMP.
- Restriction of command authorization for a specific kind of access. After you enable command authorization, command authorization applies for Telnet, SSH, rlogin, and serial-port access. You cannot restrict command authorization to just one kind of access.

If a user is TACACS+ authenticated and command authorization is enabled for that level, then if the switch cannot reach the TACACS+ server, the switch does not allow the user to execute any command that has privilege level command authorization enabled.

TACACS+ configuration using CLI

Enabling TACACS+

Enable TACACS+ globally on the switch.

The switch supports the TACACS+ client. TACACS+ is a security application implemented as a client and server-based protocol that provides centralized validation of users who attempt to gain access to a router or network access server (the switch).

By default, TACACS+ is disabled.

Before you begin

- You must have access to and you must configure a TACACS+ server before the TACACS+ features on your switch are available.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Enable TACACS+ globally:

   ```
   tacacs protocol enable
   ```

3. Disable TACACS+ globally:

   ```
   no tacacs protocol enable
   ```

   ```
   default tacacs protocol enable
   ```

Example

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#tacacs protocol enable
```

Adding a TACACS+ server

Add a primary and secondary TACACS+ server and specify the authentication process.

If you have a backup server configured, the AAA request goes to the backup server if the primary server is not available.

About this task

The TACACS+ server and the switch must have the same:

- Encryption key

- Connection mode (single connection or per-session connection. Per-session connection is the same as multi-connection mode)
- TCP port number

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Add a primary TACACS+ server with an encryption key:

   ```
   tacacs server host {A.B.C.D} key WORD<0-128>
   ```

3. **(Optional)** Configure the parameters for the primary TACACS+ server as required.

   a. **(Optional)** Specify a single connection. The single connection parameter maintains a constant connection between the switch and the TACACS+ daemon:

      ```
      tacacs server host {A.B.C.D} single-connection
      ```

      Note:

      The TACACS+ daemon must also support this mode. If you do not configure this, the switch uses the default connection type, which is the per-session connection. Per-session is the same as multi-connection mode.

   b. **(Optional)** Specify the TCP port to use when the switch connects to the TACACS+ daemon:

      ```
      tacacs server host {A.B.C.D} port <1-65535>
      ```

      The default port is 49.

   c. **(Optional)** Specify the period of time (in seconds) the switch waits for a response from the TACACS+ daemon before it times out and shows an error:

      ```
      tacacs server host {A.B.C.D} timeout <10-30>
      ```

   d. **(Optional)** Designate a fixed source IP address for all outgoing TACACS+ packets and enable this option:

      ```
      tacacs server host {A.B.C.D} source {A.B.C.D}source-ip-interface
      enable
      ```

4. Specify the IP address of the secondary TACACS+ server and specify an encryption key:

   ```
   tacacs server secondary-host {A.B.C.D} key WORD<0-128>
   ```

5. **(Optional)** Configure the optional parameters on the secondary TACACS+ server as required.

   a. **(Optional)** Specify a single connection for the secondary TACACS+ server. The single connection parameter maintains a constant connection between the switch and the TACACS+ daemon:

      ```
      tacacs server secondary-host {A.B.C.D} single-connection
      ```

Note:

The TACACS+ daemon must also support this mode. If you do not configure this, the switch uses the default connection type, which is the per-session connection. Per-session is the same as multi-connection mode.

b. **(Optional)** Specify the TCP port to use when the switch connects to the TACACS+ daemon:

```
tacacs server secondary-host {A.B.C.D} port <1-65535>
```

c. **(Optional)** Specify the period of time (in seconds) the switch waits for a response from the TACACS+ daemon before it times out and shows an error:

```
tacacs server secondary-host {A.B.C.D} timeout<10-30>
```

d. **(Optional)** Designate a fixed source IP address for all outgoing TACACS+ packets and enable this option:

```
tacacs server secondary-host {A.B.C.D} source {A.B.C.D} source-ip-interface enable
```

6. Display the status of the TACACS+ configuration:

```
show tacacs
```

7. **(Optional)** Delete a primary TACACS+ server:

```
no tacacs server host{A.B.C.D} [single-connection][source source-ip-interface enable]
```

8. **(Optional)** Delete a backup TACACS+ server:

```
no tacacs server secondary-host{A.B.C.D} [single-connection][source source-ip-interface enable]
```

9. **(Optional)** Configure a primary TACACS+ server or secondary TACACS+ server to the default settings:

```
default tacacs server {A.B.C.D} [port][single-connection][source source-ip-interface enable][timeout]
```

Example

Configure the primary server with the IP address 192.0.2.1 and the encryption key 1dt41y. Configure the secondary server with the IP address 198.51.100.2 with the same encryption key 1dt41y. Display the configuration to ensure proper configuration.

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#tacacs server host 192.0.2.1 key 1dt4ly
Switch:1(config)#tacacs server secondary-host 198.51.100.2 key 1dt4ly
Switch:1(config)#show tacacs

Global Status:

   global enable : true

   authentication enabled for : cli

   accounting enabled for : none
   authorization : disabled

   User privilege levels set for command authorization : None

Server:
                  create :

Prio      Status  Key         Port  IP address      Timeout Single Source
SourceEnabled
Primary   Conn    ******     49    192.0.2.1       10      false  0.0.0.0
false
Backup    NotConn ******     49    198.51.100.2    10      false  0.0.0.0
false


Switch:1(config)#no tacacs server host 192.0.2.1
Switch:1(config)#no tacacs server secondary-host 198.51.100.2
```

Variable definitions

Use the data in the following table to use the **`tacacs server host`** and the **`tacacs server secondary-host`** commands.

Variable	Value
{A.B.C.D}	Specifies the IP address of the TACACS+ server you want to add. For the current release, only IPv4 addresses are valid.
key *WORD <0-128>*	Configures the authentication and encryption key for all TACACS+ communications between the device and the TACACS+ server. If the key length is zero, that indicates no encryption is used. You must configure the same encryption key for the TACACS+ server and the switch.
port *<1-65535>*	Configures the TCP port, on which the client establishes a connection to the server. A value of 0 indicates the system specified default value is used. The default is 49. You must configure the same TCP port for the TACACS+ server and the switch.
single-connection	Specifies if the TCP connection between the device and the TACACS+ server is a single connection. If you specify the single connection parameter, the connection between the switch and the TACACS+ daemon remains open, which is more efficient because it allows the daemon to handle a higher number of TACACS+ operations. The single-connection is torn down if TACACS+ is disabled due to inactivity.

Table continues…

Variable	Value
	If you do not configure this, the switch uses the default connection type, which is the multi-connection. With the multi-connection, the connection opens and closes each time the switch and TACACS+ daemon communicate. **Note:** You must configure the same connection mode for the TACACS+ server and the switch. To enable single-connection, the TACACS+ daemon has to support this mode as well.
source *{A.B.C.D}*	Designates a fixed source IP address for all outgoing TACACS+ packets, which is useful if the router has many interfaces and you want to make sure all TACACS+ packets from a certain router have the same IP address. If you do not configure an address, the system uses 0.0.0.0 as the default. For the current release, only IPv4 addresses are valid. **Note:** If you configure a valid source IP address that is not 0.0.0.0 without enabling source-ip-interface, the source IP address returns to 0.0.0.0.
source-ip-interface enable	Enables the source address. You must enable this parameter if you configure a valid source IP address. The default is disabled.
timeout *<10-30>*	Configures the maximum time, in seconds, to wait for this TACACS+ server to reply before it times out. The default value is 10 seconds.

Job aid

The following table describes the fields in the output for the **`show tacacs`** command.

Name	Description
`Global Status`	
`global enable`	Displays if the TACACS+ feature is enabled globally.
`authentication enabled for`	Displays which application is authenticated by TACACS+. The possibilities are CLI, web, or all.
`accounting enabled for`	Displays if accounting is enabled. You can only enable accounting for CLI. By default, accounting is not enabled.

Table continues…

Name	Description
authorization	Displays if authorization is enabled.
User privilege levels set for command authorization	Displays the privilege levels set for command authorization. When you configure command authorization for a particular level, all commands that you execute are sent to the TACACS+ server for authorization. The device can only execute the commands the TACACS+ server authorizes. The user privilege levels are: • 0: denied access • 1: read only (ro) access • 2: Layer 1 read and write (l1) access • 3: Layer 2 read and write (l2) access • 4: Layer 3 read and write (l3) access • 5: read and write (rw) access • 6: read and write all (rwa) access • 7-14: denied access • 15: read and write all (rwa) access
Server	
Prio	Displays the priority of the TACACS+ server. The switch attempts to use the primary server first, and the secondary server second.
Status	Displays the connection status between the server and the switch – connected or not connected.
Key	Displays as ****** instead of the actual key. The key is secret and is not visible.
Port	Displays the TCP port used to establish the connection to the server. The default port is 49.
IP address	Displays the IP address for the primary and secondary TACACS+ servers.
Timeout	Displays the period of time, in seconds, the switch waits for a response from the TACACS+ daemon before it times out and declares an error. The default is 10 seconds.
Single	Displays if a single open connection is maintained between the switch and TACACS+ daemon, or if the switch opens and closes the TCP connection to the TACACS+ daemon each time they communicate. The default is false, which means the device does not maintain the single open connection.

Table continues…

Name	Description
`Source`	Displays the fixed source IP address, if you configure one, for all outgoing TACACS+ packets.
`SourceEnabled`	Displays if the fixed source IP address is enabled for all outgoing TACACS+ packets.

Configuring TACACS+ authentication

Configure what application TACACS+ authenticates: CLI, web, or all.

TACACS+ authentication provides control of authentication through login and password.

By default, CLI authentication is enabled.

Before you begin

- You must enable TACACS+ globally for TACACS+ authentication to function.

Procedure

1. Enter Global Configuration mode:

   `enable`

   `configure terminal`

2. Configure TACACS+ authentication:

   `tacacs authentication` *`<all/cli/web>`*

3. **(Optional)** Disable TACACS+ authentication:

   `no tacacs authentication` *`<all/web>`*

4. **(Optional)** Configure TACACS+ authentication to the default settings (default is cli authentication enabled):

   `default tacacs authentication` *`<all/cli/web>`*

5. Display the configuration:

   `show tacacs`

Example

Configure TACACS+ to authenticate CLI and display the configuration.

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#tacacs authentication cli
Switch:1(config)#show tacacs
Global Status:

   global enable : true

   authentication enabled for : cli

   accounting enabled for : none
```

```
Server:
                  create :

Prio     Status   Key     Port  IP address  Timeout  SingleSource Source  Enabled
Primary  Conn     ******  49    192.0.2.1       10   false        0.0.0.0 false
Backup   NotConn ******  49    198.51.100.2    10   false        0.0.0.0 false
```

Variable definitions

Use the data in the following table to use the **`tacacs authentication`** command.

Variable	Value
all	Specifies TACACS+ authentication for all applications. By default, CLI authentication is enabled.
cli	Specifies TACACS+ authentication for command line connections. By default, CLI authentication is enabled.
web	Specifies TACACS+ authentication for web connections. By default, CLI authentication is enabled.

Configuring TACACS+ accounting

Determines for which applications TACACS+ collects accounting information. Use TACACS+ accounting to track the services that users access and the amount of network resources that users consume. If unassigned, TACACS+ does not perform the accounting function.

If enabled, TACACS+ accounting logs the following events:

- User log on and log off
- Log off generated because of activity timeout
- Unauthorized command
- Telnet session closed (not logged off)

If unassigned, TACACS+ does not perform the accounting function. No default value exists.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Enable TACACS+ accounting:

   ```
   tacacs accounting enable cli
   ```

3. **(Optional)** Disable TACACS+ accounting:

```
no tacacs accounting cli
```

```
tacacs accounting disable [cli]
```

Example

Enable TACACS+ accounting:

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#tacacs accounting enable cli
```

Configuring command authorization with TACACS+

Use this procedure to enable TACACS+ authorization for a particular privilege level. Use this option to limit the use of certain commands to certain users.

If command authorization fails, the following log message displays: `Command <command> not authorized for user <username>.`

By default, command authorization is disabled on the switch. The default for the command authorization level is none.

Before you begin

- You must have access to and you must configure a TACACS+ server before the TACACS+ features on your switch are available. You must verify that the switch can reach the TACACS+ server and that you configure TACACS+ properly before you enable command authorization. If a user is TACACS+ authenticated and command authorization is enabled for that level, then if the switch cannot reach the TACACS+ server, the switch does not allow you to issue any command that has privilege level command authorization enabled. If the switch cannot reach the TACACS+ server, you can only issue logout and exit commands.
- To use TACACS+ authorization, you must enable TACACS+ authentication.

About this task

Two kinds of authorization requests exist:

1. Login authorization: Login authorization happens immediately after authentication when the user logs on to the device, authorization provides the user access level. You cannot configure login authorization.
2. Command authorization: When you configure command authorization for a particular level, all commands that you issue are sent to the TACACS+ server for authorization. You need to configure command authorization globally and at individual access levels.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Enable TACACS+ authorization:

   ```
   tacacs authorization enable
   ```

3. Configure TACACS+ privilege level for TACACS+ command authorization:

   ```
   tacacs authorization level <1-6>
   ```

   ```
   tacacs authorization level all
   ```

   ```
   tacacs authorization level none
   ```

4. **(Optional)** Disable TACACS+ authorization:

   ```
   tacacs authorization disable
   ```

   ```
   default tacacs authorization
   ```

Example

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#tacacs authorization enable
Switch:1(config)#tacacs authorization level 6
```

Variable definitions

Use the data in the following table to use the **`tacacs authorization`** command.

Variable	Value
level *<1–6>*	Enables command authorization for a specific privilege level. The default for the command authorization level is none.
level all	Enables command authorization for all privilege levels. The default for the command authorization level is none.
level none	Disables command authorization for all privilege levels. The default for the command authorization level is none.

Changing privilege levels at runtime

Users can change their privilege levels at runtime. The privilege level determines what commands a user can access through TACACS+ server authorization.

A user can only use the **`tacacs switch level`** command, after TACACS+ authenticates the user. Locally authenticated users, which means users authenticated only by the switch and not by the TACACS+ server, cannot use the **`tacacs switch level`** command.

Before you begin

- You need to configure separate profiles in the TACACS+ server configuration file for switch level. As part of the profile, you specify a user name, level, and password.

About this task

After you enable TACACS+ authorization, the current privilege-level to command mapping on the switch is no longer relevant because the TACACS+ server has complete responsibility for command authorization. TACACS+ authorization provides access to the system based on username, not based on privilege level.

After you enable TACACS+ command authorization for a particular privilege level, and a user with that privilege level logs on, the user can access commands based on his user name.

Note:

If you want to switch to a privilege level 'X' using **`tacacs switch level <1-15>`** command, you must create a user "$enabX$" on the TACACS+ server. X is the privilege level to which you want to change.

Procedure

1. Enter Global Configuration mode:

   ```
   enable
   ```

   ```
   configure terminal
   ```

2. Change the privilege level for a user at runtime:

   ```
   tacacs switch level <1-15>
   ```

3. Return to the original privilege level:

   ```
   tacacs switch back
   ```

Example

Change the privilege level for a user at runtime. Return to the original privilege level:

```
Switch:1>enable
Switch:1#configure terminal
Switch:1(config)#tacacs protocol enable
Switch:1(config)#tacacs switch level 5
Password:******
```

Return to the original privilege level:

```
Switch:1(config)#tacacs switch back
```

Variable definitions

Use the data in the following table to use the **`tacacs switch`** command.

Variable	Value
level <*1–15*>	Specifies the privilege level you want to access. You can change your privilege level at runtime by using this parameter. You are prompted to provide the required password. If you do not specify a level in the command, the administration level is selected by default. **Note:** For switch level, you need to configure separate profiles in the TACACS+ server configuration

Table continues…

Variable	Value
	file. As part of the profile, you specify a username, level, and password. To preconfigure a dummy user for that level on the TACACS+ daemon, the format of the username for the dummy user is **`$enab<n>$`**, where *<n>* is the privilege level to which you want to allow access.
back	Specifies that you want to return to the original privilege level.

TACACS+ configuration using EDM

Configuring TACACS+ globally

Enable TACACS+ globally on the switch. TACACS+ is a security application implemented as a client and server-based protocol that provides centralized validation of users. By default, TACACS+ is disabled.

Before you begin

- You must have access to and you must configure a TACACS+ server before the TACACS+ features on your switch (network access server) are available.

  You must verify that the switch can reach the TACACS+ server and that you configure TACACS+ properly before you enable command authorization.

- If a user is TACACS+ authenticated and command authorization is enabled for that level, then if the switch cannot reach the TACACS+ server, the switch does not allow the user to issue any command that has privilege level command authorization enabled. In such a case, the user can only issue logout and exit commands.
- You must enable TACACS+ globally for TACACS+ authentication to function.
- You must enable TACACS+ authentication for TACACS+ authorization to function.

About this task

Configure what application TACACS+ authenticates. TACACS+ authentication provides control of authentication through login and password dialog, challenge and response. By default, CLI authentication is enabled.

After authentication is complete, the switch starts the authorization process. By default, command authorization is disabled on the switch. The default for the command authorization level is none. If command authorization fails, the following log message displays: `Command <command> not authorized for user <username>.`

Two kinds of authorization requests exist:

1. Login authorization: Login authorization happens immediately after authentication when the user logs on to the device, authorization provides the user access level. You cannot configure login authorization.
2. Command authorization: When you configure command authorization for a particular level, all commands that you issue are sent to the TACACS+ server for authorization. You need to configure command authorization globally and at individual access levels.

Enable TACACS+ accounting function and determine which application TACACS+ accounts. After you enable accounting, the switch reports user activity to the TACACS+ server in the form of accounting records. The default for accounting is none.

Procedure

1. In the navigation pane, expand the following folders: **Configuration** > **Security** > **Control Path**.
2. Click **TACACS+**.
3. Click the **TACACS+ Globals** tab.
4. Select the **GlobalEnable** check box to enable TACACS+ globally.
5. Select the **cli** check box to enable the **Accounting** option.
6. Select the **cli** or **web** check box to enable the **Authentication** option.
7. Click the **AcliCommandAuthorizationEnabled** box to enable TACACS+ authorization.
8. Select the level in the **AcliCommandAuthorizationLevels** box.
9. Click **Apply**.

TACACS+ Globals field descriptions

Use the data in the following table to use the **TACACS+ Globals** tab.

Name	Description
GlobalEnable	Enables or disables the TACACS+ feature globally.
Accounting	Determines for which applications TACACS+ collects accounting information. Use TACACS+ accounting to track the services that users access and the amount of network resources that users consume. If unassigned, TACACS+ does not perform the accounting function. The default is none. If enabled, TACACS+ accounting logs the following events: • User log on and log off • Log off generated because of activity timeout • Unauthorized command

Table continues…

Name	Description
	• Telnet session closed (not logged off)
Authentication	Configures what application TACACS+ authenticates. The options include: • cli • web TACACS + authentication provides control of authentication through login and password dialog, challenge and response. By default, CLI authentication is enabled.
LastUserName	Displays the last user for which the system attempted authentication.
LastAddressType	Displays the type of address to access the TACACS + server.
LastAddress	Displays the last address to access the TACACS+ server.
AcliCommandAuthorizationEnabled	Enables TACACS+ authorization for a particular privilege level. Use this option to limit the use of certain commands to certain users. To use TACACS + authorization, you must also use TACACS+ authentication. The switch allows the user to access the switch according to the access level. The default is disabled.
AcliCommandAuthorizationLevels	Enables command authorization for a specific privilege level. The default for the command authorization level is none.

Adding a TACACS+ server

Add a TACACS+ server, configure the TACACS+ server, and specify the authentication process.

If you have a secondary server configured, the AAA request goes to the backup server if the primary server is not available.

Before you begin

You must have access to and you must configure a TACACS+ server before the TACACS+ features on your switch are available.

About this task

The TACACS+ server and the switch must have the same:

- Encryption key

- Connection mode (single connection or per-session connection. Per-session is the same as multi-connection mode.)
- TCP port number

Procedure

1. In the navigation pane, expand the following folders: **Configuration** > **Security** > **Control Path**.
2. Click **TACACS+**.
3. Click the **TACACS+ Servers** tab.
4. Click **Insert**.
5. In the **AddressType** box, select **ipv4**.
6. In the **Address** field, type the IP address of the TACACS+ server.
7. **(Optional)** In the **PortNumber** field, type the TCP port on which the client establishes a connection to the TACACS+ server.
8. **(Optional)** In the **ConnectionType** box, select either **singleConnection** or **perSessionConnection** to specify the TCP connection type between the switch and TACACS+ server.
9. **(Optional)** In the **Timeout** field, type the period of time (in seconds) the switch waits for a response from the TACACS+ server.
10. In the **Key** field, enter the key that the switch and the TACACS+ server share.
11. **(Optional)** Select **SourceIpInterfaceEnabled**, if you want to enable the switch to designate a fixed source IP address for all outgoing TACACS+ packets.
12. In the **SourceIPInterfaceType** box, select **ipv4**.
13. **(Optional)** In the **SourceIpInterface** field, type a fixed source IP address if you want to designate a fixed source IP address for all outgoing TACACS+ packets.
14. In the **Priority** box, select either **primary** or **backup** to determine the order the switch uses the TACACS+ servers.
15. Click **Insert**.
16. If you want to delete an existing TACACS+ configuration perform the following procedure. In the navigation pane, expand the following folders: **Configuration** > **Security** > **Control Path**.
17. Click **TACACS+**.
18. In the **TACACS+** tab, click **TACACS+ Servers** tab.
19. Identify the configuration to delete by clicking anywhere in the row.
20. Click **Delete**.

TACACS+ Servers field descriptions

Use the data in the following table to use the **TACACS+ Servers** tab.

Name	Description
AddressType	Specifies the type of IP address to use on the TACACS+ server. For the current release, you must set the value to IPv4.
Address	Specifies the IP address of the TACACS+ server.
PortNumber	Configures the TCP port on which the client establishes a connection to the server. The default is 49. A value of 0 indicates that the system specified default value is used. You must configure the same TCP port for the TACACS+ server and the switch.
ConnectionType	Specifies if the TCP connection between the device and the TACACS+ server is a single connection. If you specify the single connection parameter, the connection between the switch and the TACACS+ daemon remains open, which is more efficient because it allows the daemon to handle a higher number of TACACS+ operations. The single-connection session is torn down if TACACS+ is disabled due to inactivity. If you do not configure this parameter, the switch uses the default connection type, which is the multi-connection. With the multi-connection, the connection opens and closes each time the switch and TACACS+ daemon communicate. **Note:** You must configure the same connection mode for the TACACS+ server and the switch. To enable single-connection, the TACACS+ daemon has to support this mode as well.
ConnectionStatus	Specifies if the TCP connection between the device and TACACS+ server is connected or not connected.
Timeout	Configures the maximum time, in seconds, to wait for this TACACS+ server to reply before it times out. The default value is 10 seconds.
Key	Configures the authentication and encryption key for all TACACS+ communications between the device and the TACACS+ server. If the key length is zero, that indicates no encryption is used. You must configure the same encryption key for the TACACS+ server and the switch.
SourceIpInterfaceEnabled	Enables the source address specification. If **SourceIpInterfaceEnabled** is true (the check box is

Table continues…

Name	Description
	selected), and you change **SourceIpInterfaceEnabled** to false (the check box is cleared), the **SourceIpInterface** is reset to 0.0.0.0. The default is disabled. You must enable this parameter if you configure a valid source IP address
SourceIpInterfaceType	Specifies the type of IP address to use on the interface that connects to the TACACS+ server. **Note:** For the current software release, you must set the value to IPv4.
SourceIpInterface	Designates a fixed source IP address for all outgoing TACACS+ packets, which is useful if the router has many interfaces and you want to make sure all TACACS+ packets from a certain router have the same IP address. If you do not configure an address, the system uses 0.0.0.0 as the default. For the current release, only IPv4 addresses are valid. **Note:** If you configure a valid source IP address that is not 0.0.0.0 without enabling source-ip-interface, the source IP address returns to 0.0.0.0.
Priority	Determines the order in which the switch uses the TACACS+ servers, where 1 is the highest priority. The priority values are primary and backup. If more than one server shares the same priority, the device uses the servers in the order they exist in the table.

Modifying a TACACS+ configuration

Modify an existing TACACS+ configuration to customize the server.

Procedure

1. In the navigation tree, expand the following folders: **Configuration** > **Security** > **Control Path**.
2. Click **TACACS+**.
3. Click **TACACS+ Servers** tab.

4. Double-click in the fields that you want to modify.

   In some of the fields, the text becomes bold, which indicates that you can edit them. In other fields, a list appears.

5. In the fields that you can edit, type the desired values.
6. In the fields with lists, select the desired option.
7. Click **Apply**.

TACACS+ configuration examples

This section provides a configuration example to configure the switch to use TACACS+.

TACACS+ configuration on the switch

The following section shows the steps required to configure TACACS+ on the switch.

The example displays how to:

- Configure a key to be used by the TACACS+ server and the switch. In the example, the key is configured to the word `secret`.
- Configure an IP address for the TACACS+ server. In the example the IP address for the primary server is 192.0.2.8, which is accessible by the Management Router VRF.
- Configure the TACACS+ server to authenticate CLI sessions.
- Enable TACACS+.

Switch

```
TACACS CONFIGURATION

tacacs server  host 192.0.2.8 key ******
tacacs protocol enable
tacacs accounting enable cli
tacacs authorization enable
tacacs authorization level 6
```

Verify your configuration

The **`show tacacs`** output must show as `global enable: true` to confirm TACACS is enabled.

The output for the **`show tacacs`** command must display the IP addresses for the TACACS+ server. The IP addresses must be accessible to the Management Router VRF on the switch.

If you want to use the TACACS+ server to authenticate sessions in CLI, the output must display as `authentication enabled for: cli`. If you want to authenticate EDM sessions, the output must display as `authentication enabled for: web`.

Ensure the other parameters match what you have configured.

```
Global Status:

   global enable : true

   authentication enabled for : cli

   accounting enabled for : cli

   authorization : enabled

   User privilege levels set for command authorization : rwa

Server:
                  create :

Prio      Status  Key         Port  IP address      Timeout Single Source
SourceEnabled
Primary   Conn    ******      49    192.0.2.8       10      false  0.0.0.0
false
```

Glossary

American Standard Code for Information Interchange (ASCII)

A code to represent characters in computers. ASCII uses uppercase and lowercase alphabetic letters, numeric digits, and special symbols.

authentication server

A RADIUS server that provides authorization services to the authenticator, which is software that authorizes or rejects a supplicant attached to the other end of the LAN segment.

Authentication, Authorization, and Accounting (AAA)

Authentication, Authorization, and Accounting (AAA) is a framework used to control access to a network, limit network services to certain users, and track what users do. Authentication determines who a user is before allowing the user to access the network and network services. Authorization allows you to determine what you allow a user to do. Accounting records what a user is doing or has done.

Challenge Handshake Authentication Protocol (CHAP)

An access protocol that exchanges a random value between the server and the client and is encrypted with a challenge password.

command line interface (CLI)

A textual user interface. When you use CLI, you respond to a prompt by typing a command. After you enter the command, you receive a system response.

controlled port

In relation to EAPoL, any port on the device with EAPoL enabled.

daemon/server

A daemon is a program that services network requests for authentication and authorization, verifies identities, grants or denies authorizations, and logs accounting records.

Data Encryption Standard (DES)access control entry (ACE)

A cryptographic algorithm that protects unclassified computer data. The National Institute of Standards and Technology publishes the DES in the Federal Information Processing Standard Publication 46-1.

Global routing engine (GRE)

The base router or routing instance 0 in the Virtual Routing and Forwarding (VRF).

Institute of Electrical and Electronics Engineers (IEEE)

An international professional society that issues standards and is a member of the American National Standards Institute, the International Standards Institute, and the International Standards Organization.

Internet Engineering Task Force (IETF)

A standards organization for IP data networks.

Layer 2

Layer 2 is the Data Link Layer of the OSI model. Examples of Layer 2 protocols are Ethernet and Frame Relay.

Layer 3

Layer 3 is the Network Layer of the OSI model. An example of a Layer 3 protocol is Internet Protocol (IP).

Local Area Network (LAN)

A data communications system that lies within a limited spatial area, uses a specific user group and topology, and can connect to a public switched telecommunications network (but is not one).

management information base (MIB)

The MIB defines system operations and parameters used for the Simple Network Management Protocol (SNMP).

mask

A bit string that the device uses along with an IP address to indicate the number of leading bits in the address that correspond with the network part.

Media Access Control (MAC)

Arbitrates access to and from a shared medium.

Message Digest 5 (MD5)

A one-way hash function that creates a message digest for digital signatures.

MultiLink Trunking (MLT)

A method of link aggregation that uses multiple Ethernet trunks aggregated to provide a single logical trunk. A multilink trunk provides the combined bandwidth of multiple links and the physical layer protection against the failure of a single link.

network access server (NAS)

A network access server (NAS) is a single point of access to a remote device. The NAS acts as a gateway to guard the remote device. A client connects to the NAS and then the NAS connects to another device to verify the credentials of the client. Once verified the NAS allows or disallows access to the device. Network access servers are almost exclusively used with Authentication, Authorization, and Accounting (AAA) servers.

next hop

The next hop to which a packet can be sent to advance the packet to the destination.

Point-to-Point Protocol (PPP)

Point-to-Point Protocol is a basic protocol at the data link layer that provides its own authentication protocols, with no authorization stage. PPP is often used to form a direct connection between two networking nodes.

port
A physical interface that transmits and receives data.

Port Access Entity (PAE)
Software that controls each port on the switch. The PAE, which resides on the device, supports authenticator functionality. The PAE works with the Extensible Authentication Protocol over LAN (EAPoL).

Protocol Data Units (PDUs)
A unit of data that is specified in a protocol of a specific layer and that consists of protocol-control information of the specific layer and possibly user data of that layer.

quality of service (QoS)
QoS features reserve resources in a congested network, allowing you to configure a higher priority for certain devices. For example, you can configure a higher priority for IP deskphones, which need a fixed bit rate and split the remaining bandwidth between data connections if calls in the network are more important than the file transfers.

Read Write All (RWA)
An access class that lets users access all menu items and editable fields.

remote login (rlogin)
An application that provides a terminal interface between hosts (usually UNIX) that use the TCP/IP network protocol. Unlike Telnet, rlogin assumes the remote host is, or behaves like, a UNIX host.

Routing Information Protocol (RIP)
A distance vector protocol in the IP suite, used by IP network-layer protocol, that enables routers in the same AS to exchange routing information by means of periodic updates. You often use RIP as a very simple interior gateway protocol (IGP) within small networks.

Secure Copy (SCP)
Secure Copy securely transfers files between the switch and a remote station.

Simple Network Management Protocol (SNMP)
SNMP administratively monitors network performance through agents and management stations.

supplicant
A device, such as a PC, that applies for access to the network.

User Datagram Protocol (UDP)
In TCP/IP, a packet-level protocol built directly on the Internet Protocol layer. TCP/IP host systems use UDP for application-to-application programs.

user-based policies (UBP)
Establishes and enforces roles and conditions on an individual user basis for access ports in the network.

view-based access control model (VACM)
Provides context, group access, and group security levels based on a predefined subset of management information base (MIB) objects.

virtual router forwarding (VRF)
Provides traffic isolation between customers operating over the same node. Each virtual router emulates the behavior of a dedicated hardware router by

providing separate routing functionality, and the network treats each VRF as a separate physical router.