Security
Avaya Virtual Services Platform 9000

3.2
NN46250-601, 03.01
February 2012

Notice

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

Documentation disclaimer

“Documentation” means information published by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya generally makes available to users of its products. 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 Web sites 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 its Hardware and Software (“Product(s)”). Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language, as well as information regarding support for this Product while under warranty is available to Avaya customers and other parties through the Avaya Support Web site: http://support.avaya.com. Please note that if you acquired the Product(s) from an authorized Avaya reseller outside of the United States and Canada, the warranty is provided to you by said Avaya reseller and not by Avaya.

Licenses

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

Copyright

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

Third-party components

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

Trademarks

The trademarks, logos and service marks (“Marks”) displayed in this site, the Documentation 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 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, and “Linux” is a registered trademark of Linus Torvalds.

Downloading Documentation

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

Contact Avaya Support

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

Contents

Chapter 1: Purpose of this document

Security documentation provides procedures and conceptual information that you can use to administer and configure the security features for the Avaya Virtual Services Platform 9000.

The security function includes tasks related to product security; for example, the management and protection of resources from unauthorized or detrimental access and use. Security documents include information that supports the configuration and ongoing management of

- communications
- data security
- user security
- access

Chapter 2: New in this release

The following sections describe what is new in *Avaya Virtual Services Platform 9000 Security* , NN46250–601, for Release 3.2.

Features

See the following sections for information about feature-related changes.

RADIUS support of IPv6

Remote Dial-In User Services (RADIUS) is updated to support both IPv4 and IPv6 addresses on Avaya Virtual Services Platform 9000 in Release 3.2. No differences in functionality or configuration exist except in 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.

RADIUS is a distributed client/server system that authenticates the identity of users through a central database. The RADIUS component on VSP is initialized and started as part of the general start sequence. RADIUS allows you to identify remote users before giving access to them. RADIUS accounting enables the server to collect data during a session by a remote user.

See the following sections for more information:

- RADIUS on page 65
- RADIUS configuration using ACLI on page 68
- RADIUS configuration using Enterprise Device Manager on page 86

Other changes

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

ACLI and EDM chapters

ACLI and EDM procedures chapters are grouped together to improve clarity. The Fundamentals chapter is placed at the beginning of the document, followed by ACLI, and then EDM procedures. For major features, for example EAPoL, RADIUS, and SNMP, fundamentals and ACLI and EDM procedures are grouped together into a single chapter by feature.

ACLI Commands

Examples for ACLI commands exist for most commands in the document.

Introduction chapter and navigation

Introduction chapters and navigation are removed.

Purpose of this document

To improve documentation usability, a brief description of the purpose of this document is now the first chapter.

Terminology

Terminology no longer exists in a separate document. Terminology for this document is in a glossary at the end of this document.

Common procedures

Common procedures are incorporated throughout the document.

Chapter 3: Security fundamentals

This section provides conceptual content to help you configure and customize the security services on Avaya Virtual Services Platform 9000.

Security overview

Security is a critical attribute of networking devices such as the Virtual Services Platform 9000. 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
- mechanisms to prevent denial-of-service (DOS) attacks

hsecure mode

Avaya Virtual Services Platform 9000 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 *Avaya Virtual Services Platform 9000 Administration*, NN46250–600.

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.

ACLI passwords

Virtual Services Platform 9000 ships with default passwords assigned for access to Avaya Command Line Interface (ACLI) 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. Avaya strongly recommends that you change the default passwords and community strings immediately after you first log on.

For security purposes, if you fail to log on correctly on the master Control Processor (CP) module in three consecutive instances, the CP module locks for 60 seconds.

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 Virtual Services Platform 9000 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 ACLI.

You can define network stations that can explicitly access Virtual Services Platform 9000 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 Virtual Services Platform 9000 service ports open and in the listen state. No connections are accepted on these ports unless you enable the particular daemon. Avaya 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 *Avaya Virtual Services Platform 9000 Administration*, NN46250–600.

User-based policy support

You can set up a user-based policy (UBP) system by using Avaya Enterprise Policy Manager (EPM), a RADIUS server, and a Virtual Services Platform 9000 with EAP enabled.

EPM is an application designed to manage the traffic prioritization and network access security for business applications. It provides centralized control of advanced packet classification and the ability to priority mark, police, meter, or block traffic.

EPM 5.0 supports UBPs, which allow security administrators to establish and enforce roles and conditions for each user for all access ports in the network. The UBP feature in EPM works in conjunction with Extensible Access Protocol (EAP) technology to enhance the security of the network. Users log on to the networks and are authenticated as the network connection is established.

The UBP feature works as an extension to the Roles feature in EPM. In a UBP environment, role objects are linked directly to specific users (as RADIUS attributes), as opposed to being linked simply to device interfaces. The role object then links the user to specific policies that control the user's access to the network.

When the RADIUS server successfully authenticates a user, the device sends an EAP session start event to the EPM policy server. The policy server then sends user-based policy configuration information for the new user roles to the interface, based on the role attribute that was assigned to that user on the RADIUS server.

Reverse path checking

The reverse path checking feature, when enabled, prevents packet forwarding for incoming IP packets that have incorrect or forged (spoofed) IP addresses. Reverse path checking guarantees that traffic received on one interface was sent by a station from this interface, which prevents address spoofing. With this mode enabled, Virtual Services Platform 9000 performs a reverse path check to determine if the packet IP address is verifiable. If the address is not verifiable, the packet is discarded.

You configure reverse path checking for each IP interface. When you enable reverse path checking, Virtual Services Platform 9000 checks all routing packets that come through that interface. It ensures that the source address and source interface appear in the routing table, and that it matches the interface on which the packet was received.

You can use one of two modes for reverse path checking:

- Exist-only mode: In this mode, reverse path checking checks whether the source IP address of the incoming packet exists in the routing table. If the source IP entry is found, the packet is forwarded as usual; otherwise, the packet is discarded.
- Strict mode: In this mode, reverse path checking checks whether the source IP address of the incoming packet exists in the routing table. If the source IP entry is not found, the packet is dropped. If the source IP entry is found, reverse path checking further checks if the source IP interface matches the incoming interface of the packet. If they match, the packet is forwarded as usual, otherwise, the packet is discarded.

The following figure illustrates how strict mode reverse path checking works.

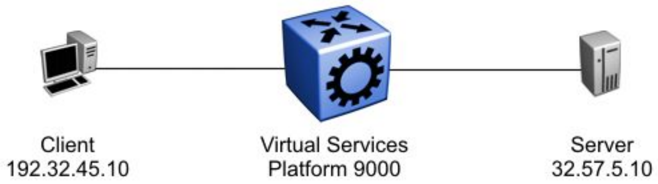


Figure 1: Reverse path checking network configuration

Consider the following parameters:

- Virtual Services Platform 9000 connects a server (32.57.5.10) to a client (192.32.45.10).
- Virtual Services Platform 9000 has reverse path checking enabled.
- The following table details the routing table entries of Virtual Services Platform 9000.

Table 1: Virtual Services Platform 9000 example routing table

Destination address	Next hop address	Forward through port
32.57.5.10	173.56.42.2	3/7
192.32.45.10	145.34.87.2	7/2
192.32.46.10	145.34.88.2	7/1

When a legitimate packet is sent, the following actions occur:

1. The client sends a packet to the server. The packet has a source IP address of 192.32.45.10 and a destination IP address of 32.57.5.10.
2. The packet arrives to Virtual Services Platform 9000 on port 7/2 (brouter); the routing engine performs a destination IP address lookup and finds the destination port is 3/7.
3. Reverse path checking operations begin. The routing engine performs a lookup for the source IP address of 192.32.45.10. It finds an entry in the routing table that specifies that the next-hop port is 7/2, which matches the incoming port of the packet. Because the address and port information matches, the packet is forwarded as usual.

When a spoofed packet is sent, the following actions occur:

1. The client sends a packet to the server with a forged IP address of 192.32.46.10 through port 7/2.
2. Reverse path checking finds that the source IP address next-hop port is 7/1, which does not match the incoming port of the packet of 7/2. In this case, the packet is discarded.

You can also think of reverse path checking as follows. If A sends packets to B through route X ingress port Y, then B sends the return packets to A through egress X through the same port Y. If returning packets take a different path, they are dropped.

Denial-of-service attack prevention

To protect Virtual Services Platform 9000 against IP packets with an illegal source address of 255.255.255.255 from being routed (according to RFC1812 Section 4.2.2.11 and RFC971 Section 3.2), Virtual Services Platform 9000 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.
- 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.

Hsecure is disabled by default. When you enable hsecure, the desired behavior (not routing source packets with an IP address of 255.255.255.255) applies to all ports.

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.

Virtual Services Platform 9000 software supports BaySecure Access Control (BSAC) and the Merit Network 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 (Virtual Services Platform 9000 and Baystack 450, for example) 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 use the following vendor-specific attribute format for ACLI commands:

```
1    1         2                         2+x +----+----+----------------
+----------------------------------------+ |type|len | Vendor-Id
|        value (string)                  | |    |    |
|                                        | +----+----+----------------
+----------------------------------------
+
|                                             |
1    1            v   x                              +----+----
+------------------------------+                           |type|len |
value (cli-command)      |                            |    |
|                              |                             +----+----
+------------------------------+
```

RADIUS on management ports

The management 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. You can hold and synchronize the status of the UDP SRC by a virtual IP flag.

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.

Layer 2 redundancy and High Availability clarifications

Layer 2 (L2) redundancy supports the synchronization of VLAN and QoS software parameters. High Availability (CPU-HA) mode, which is an extension to and includes the Layer 2 redundancy software feature, supports the synchronization of VLAN and QoS software parameters, static and default route records, ARP entries, and LAN virtual interfaces. Specifically, CPU-HA mode passes table information and Layer 3 protocol-specific control packets to the standby CP module.

Layer 2 redundancy and CPU-HA mode saves the boot configuration file onto both the master and the secondary CP modules. The secondary CP module resets automatically. You must manually reset the master CP module.

CPU-HA mode limitations and considerations

The following section describes the limitations and considerations of the CPU-HA feature:

- The CPU-HA mode is not compatible with the Packet Capture Tool (PCAP). Be sure to disable the CPU-HA mode before using PCAP.
- You can use the CPU-HA mode to configure redundant ARP and IP static route tables. For more information about creating ARP and IP static routes, see *Avaya Virtual Services Platform 9000 Configuring — IP Routing, NN46250–505*.
- Enable CPU-HA mode to disable the brouter port capability; you cannot assign IP addresses to Ethernet ports. To assign an IP address, you must create a VLAN, add ports to that VLAN, and then assign the IP address to it.

Interoperability configuration

Avaya Virtual Services Platform 9000 is compatible with RADIUS servers and EAP servers. For more information about Avaya Virtual Services Platform 9000 RADIUS and EAP compatibility, see *Data Networking — Ignition Server PEAP Active Directory Authentication TCG* (Identity Engines Ignition Server — Ethernet Routing Switch 8800 8300 1600 5500 5600 4500 2500), NN48500–626.

You can search the InSite Knowledge Base on the Avaya Support site at www.avaya.com/support. Use the Advanced Search option to narrow your search to specific categories (products) and document types.

Security configuration using ACLI

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 *Avaya Virtual Services Platform 9000 Administration*, NN46250–600.

Enabling hsecure

Before you begin

- For more information about DoS prevention using hsecure, see Denial-of-service attack prevention on page 16.
- You must log on to Global Configuration mode in ACLI.

About this task

Use the boot configuration flag hsecure (high security mode) to prevent denial-of-service (DoS) attacks.

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

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. 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.
   ```

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

Example

```
VSP-9012:1>enable
```

```
VSP-9012:1#configure terminal
```

Enable hsecure mode:

```
VSP-9012:1(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:

```
VSP-9012:1(config)#save config
```

Restart the switch:

```
VSP-9012:1(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 64. 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 ACLI 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
chnage 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

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.
- You must log on to the Global Configuration mode in ACLI.

About this task

Configure new passwords for each access level, or change the logon or password for the different access levels of the switch. After you receive Avaya Virtual Services Platform 9000, use default passwords to initially access ACLI. If you use Simple Network Management Protocol version 3 (SNMPv3), you can change encrypted passwords.

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.

In hsecure mode, the master Control Processor (CP) module synchronizes the password aging time with the secondary CP module. After the password expires, you must change the password in the master CP module to log on to the secondary CP module.

Procedure

1. Change a password:

   `cli password WORD<1–20> {layer1|layer2|layer3|read-only|read-write|read-write-all}`
2. Enter the old password.
3. Enter the new password.
4. Enter the new password a second time.
5. Configure password options:

   `password [access-level WORD<2–8>] [aging-time day <1-365>] [default-lockout-time <60-65000>] [lockout WORD<0–46> time <60-65000>] [min-passwd-len <10-20>] [password-history <3-32>]`

Example

```
VSP-9012:1>enable
```

```
VSP-9012:1#configure terminal
```

Change a password:

```
VSP-9012:1(config)#cli password smith read-write-all
```

Enter the old password:

```
VSP-9012:1(config)#rwa
```

Enter the new password:

```
VSP-9012:1(config)#TestKey1
```

Enter the new password a second time:

```
VSP-9012:1(config)#TestKey1
```

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

```
VSP-9012:1(config)#password access-level rwa aging-time 60
```

Variable definitions

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

Table 2: Variable definitions

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.

Table 3: Variable definitions

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
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.

Variable	Value
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.

Synchronizing the master and standby CP module passwords

Before you begin

- You must log on to the Global Configuration mode in ACLI.

Important:

This procedure does not apply to HA mode, where the system automatically synchronizes the passwords on the master and secondary CP module.

About this task

Synchronize the master and secondary CP module passwords.

The RADIUS protocol is not used on the secondary CP module to authenticate users logging on to the secondary CP module. The command **`save standby`** saves only the configuration file to the secondary CP module, and does not change the runtime configuration on the secondary CP module.

Procedure

1. Change the password on the master CP module.
2. Save the configuration file to the secondary CP module:
   ```
   save config standby WORD<1-99>
   ```
3. Log on to the secondary CP module.
4. Begin a password change:
   ```
   cli password WORD<1-20> {layer1|layer2|layer3|read-only|
   read-write|read-write-all}
   ```
5. At the `Enter the old password :` prompt, enter the old password.
6. At the `Enter the New password :` prompt, enter the new password.

7. At the `Re-enter the New password :` prompt, enter the same new password.

Variable definitions

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

Table 4: Variable definitions

Variable	Value
WORD<1-20>	Specify the user name you require after the password change.
{layer1|layer2|layer3|read-only|read-write|read-write-all}	Specify the access level you require for that user name.

Use the data in the following table to use the `save standby` command.

Table 5: Variable definitions

Variable	Value
<*WORD 1-99*>	Specify the name of the configuration file on the secondary CP module you must save the current configuration to.

Configuring directed broadcast

Before you begin

- You must log on to VLAN Interface Configuration mode in ACLI.

About this task

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

Configure Avaya Virtual Services Platform 9000 to forward directed broadcasts for a VLAN:

```
ip directed-broadcast enable
```

Example

```
VSP-9012:1>enable

VSP-9012:1#configure terminal

VSP-9012:1(config)#interface vlan 2

VSP-9012:1(config-if)#ip directed-broadcast enable
```

Variable definitions

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

Table 6: Variable definitions

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

Before you begin

- You must log on to GigabitEthernet Interface Configuration mode in ACLI.

About this task

Protect Avaya Virtual Services Platform 9000 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. Virtual Services Platform 9000 supports high-secure configurable flag.

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 module.

Procedure

Enable high-secure mode:

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

Example

```
VSP-9012:1>enable
```

```
VSP-9012:1#configure terminal

VSP-9012:1(config)#interface GigabitEthernet 4/16

VSP-9012:1(config-if)#high-secure enable
```

Variable definitions

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

Table 7: Variable definitions

Variable	Value
port {slot/port[-slot/ port][,...]}	Specifies the port on which you want to enable high-secure mode.
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 reverse path checking on a port

Before you begin

- You must log on to the GigabitEthernet Interface Configuration mode in ACLI.

About this task

You can use the unicast reverse path checking feature to reduce the problems that are caused by the introduction of malformed or forged (spoofed) IP source addresses into a network. When you enable reverse path checking, Avaya Virtual Services Platform 9000 performs a reverse path check to determine if the packet IP address is verifiable. If the address is not verifiable, the packet is discarded.

There are two modes for reverse path checking:

- exist-only mode
- strict mode

Procedure

Configure reverse path checking on a port:

```
ip rvs-path-chk mode {exist-only|strict}
```

Example

```
VSP-9012:1>enable
```

```
VSP-9012:1#configure terminal
```

```
VSP-9012:1(config)#interface GigabitEthernet 4/16
```

Check whether the source IP address of the incoming packet exists in the routing table:

```
VSP-9012:1(config-if)#ip rvs-path-chk mode strict
```

Variable definitions

Use the data in the following table to use the `ip rvs-path-chk mode` command.

Table 8: Variable definitions

Variable	Value
mode{exist-only|strict}	Specifies the mode for reverse path checking. In exist-only mode, reverse path checking checks whether the source IP address of the incoming packet exists in the routing table. In strict mode, reverse path checking checks whether the source IP address of the incoming packet exists in the routing table. To set this option to the default value, use the default operator with the command. The default is exist-only.

Configuring reverse path checking on a VLAN

Before you begin

- You must log on to VLAN Interface Configuration mode in ACLI.

Important:

You must assign a valid IP address to the selected port.

About this task

You can use the unicast reverse path checking feature to reduce the problems that are caused by the introduction of malformed or forged (spoofed) IP source addresses into a network. When you enable reverse path checking, Virtual Services Platform 9000 performs a reverse path check to determine if the packet IP address is verifiable. If the address is not verifiable, the packet is discarded.

There are two modes for reverse path checking:

- exist-only mode
- strict mode

Procedure

Configure reverse path checking on a VLAN:

```
ip rvs-path-chk mode {exist-only|strict}
```

Example

```
VSP-9012:1>enable
```

```
VSP-9012:1#configure terminal
```

```
VSP-9012:1(config)#interface vlan 2
```

Check whether the source IP address of the incoming packet exists in the routing table:

```
VSP-9012:1(config-if)#ip rvs-path-chk mode strict
```

Variable definitions

Use the data in the following table to use the `ip rvs-path-chk` command.

Table 9: Variable definitions

Variable	Value
mode {exist-only|strict}	Specifies the mode for reverse path checking. In exist-only mode, reverse path checking checks whether the source IP address of the incoming packet exists in the routing table. In strict mode, reverse path checking checks whether the source IP address of the incoming packet exists in the routing table. To set this option to the default value, use the default operator with the command. The default is exist-only.

Configuring port lock

Before you begin

- You must log on to the Global Configuration mode in ACLI.

About this task

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. Enable port lock globally:
   ```
   portlock enable
   ```
2. Log on to the GigabitEthernet Interface Configuration mode:
   ```
   interface gigabitethernet {slot/port[-slot/port][,...]}
   ```

3. Lock a port:

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

Example

```
VSP-9012:1>enable
```

```
VSP-9012:1#configure terminal
```

Log on to GigabitEthernet Interface Configuration mode:

```
VSP-9012:1(config)#interface GigabitEthernet 4/1
```

Lock port 4/1:

```
VSP-9012:1(config-if)#lock port 4/1 enable
```

Unlock port 4/1:

```
VSP-9012:1(config-if)#no lock port 4/1 enable
```

Variable definitions

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

Table 10: Variable definitions

Variable	Value
{slot/port[-slot/port][,...]}	Specifies the port you want to configure.

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

Table 11: Variable definitions

Variable	Value
{slot/port[-slot/port][,...]}	Specifies the port you want to lock. Use the no form of this command to unlock a port: `no lock port {slot/port[-slot/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 *Avaya Virtual Services Platform 9000 Administration*, NN46250–600.

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.

Configuring reverse path checking on a port

Before you begin

- The system supports reverse path checking only on ports that have a valid IP address.

About this task

Configure reverse path checking on a port to determine if a packet IP address is verifiable. Use reverse path checking to reduce the problems that are caused by the introduction of malformed or forged (spoofed) IP source addresses into a network. After you enable reverse path checking, Avaya Virtual Services Platform 9000 performs a reverse path check to determine if the packet IP address is verifiable. If the address is not verifiable, the system discards the packet.

Reverse path checking operates in one of two modes:

- exist-only mode
- strict mode

Procedure

1. In the Device Physical View tab, select a port.
2. In the navigation tree, open the following folders: **Configuration** > **Edit** > **Port**.
3. Click **IP**.
4. Click the **Reverse Path Checking** tab.
5. Select the **Enable** check box to enable reverse path checking.
6. Select **exist-only** or **strict**.
7. Click **Apply**.

Reverse Path Checking field descriptions

Use the data in the following table to use the **Reverse Path Checking** tab.

Name	Description
Enable	Enables reverse path checking on the selected port. The default is disabled.
Mode	Specifies the mode for reverse path checking. The modes are • exist-only—reverse path checking checks whether the incoming packet source IP address exists in the routing table. If reverse path checking finds the source IP entry, the packet is forwarded; otherwise the packet is discarded. • strict—reverse path checking checks whether the incoming packet source IP address exists in routing table. If reverse path checking does not find the source IP entry, the packet is dropped; otherwise, reverse path checking further checks if the source IP interface matches the incoming interface of the packet. If they match, the packet is forwarded; otherwise the packet is discarded. The default is exist-only.

Configuring reverse path checking on a VLAN

Before you begin

- Before you can configure reverse path checking on a VLAN, you must assign a valid IP address to the selected VLAN.

About this task

Configure reverse path checking on a VLAN to determine if a packet IP address is verifiable. Use reverse path checking to reduce the problems that are caused by the introduction of malformed or forged (spoofed) IP source addresses into a network. After you enable reverse path checking, Avaya Virtual Services Platform 9000 performs a reverse path check to determine if the packet IP address is verifiable. If the address is not verifiable, the system discards the packet.

Reverse path checking operates in one of two modes:

- exist-only mode
- strict mode

Procedure

1. In the navigation tree, open the following folders: **Configuration** > **VLAN**.
2. Click **VLANs**.
3. Click the VLAN on which you want to configure reverse path checking.
4. In the toolbar, click **IP**.
5. Click the **Reverse Path Checking** tab.
6. Select the **Enable** box to enable reverse path checking.
7. Select **exist-only** or **strict**.
8. Click **Apply**.

Reverse Path Checking field descriptions

Use the data in the following table to use the **Reverse Path Checking** tab.

Name	Description
Enable	Enables reverse path checking on the selected VLAN.
Mode	Specifies the mode for reverse path checking. The modes are

Name	Description
	• exist-only—reverse path checking checks whether the incoming packet source IP address exists in the routing table. If reverse path checking finds the source IP entry, the packet is forwarded; otherwise, the packet is discarded. • strict—reverse path checking checks whether the incoming packet source IP address exists in routing table. If reverse path checking does not find the source IP entry, then the packet is dropped. Otherwise, reverse path checking further checks if the source IP interface matches the incoming interface of the packet. If they match, then the packet is forwarded. Otherwise, the packet is discarded. The default is exist-only.

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 an Avaya Virtual Services Platform 9000, 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 tree, open 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.

Name	Description
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.

Chapter 4: 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 connected to Virtual Services Platform 9000 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 it from accessing the network.

Important:

Release 3.2 supports only one EAP Supplicant for each port. If the device receives frames from different MAC addresses on the same port, that port is disabled. Avaya is currently working on a solution to support multiple Supplicants. For more information, contact your local representative. For more information about a list of EAPoL configuration limitations, see System requirements on page 44.

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 Virtual Services Platform 9000 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 Virtual Services Platform 9000, supports the Authenticator functionality.
  - Controlled Port—any port on the device with EAPoL enabled.
- Authentication Server—a RADIUS server that provides authorization 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
  - Port mirroring

- 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 *force-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).

Configuration process

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

The Authenticator also determines the operational state of each controlled port. At system initialization, or when a Supplicant initially connects to one of the controlled ports on the device, the system configures the controlled port state to Blocking. After the Authentication Server notifies the Authenticator PAE about the success or failure of the authentication, the Authenticator changes the controlled port operational state accordingly.

Virtual Services Platform 9000 transmits and receives EAPoL frames regardless of whether the port is authorized or unauthorized. NonEAPoL frames transmit according to the following rules:

- If authentication succeeds, the operational state of the controlled port is set to Forwarding. This means that all the incoming and outgoing traffic is allowed through the port.
- If authentication fails, the controlled port forwards traffic according to how you configure the traffic control for that port. The traffic control command can have one of the following two values:
    - Incoming and Outgoing—All nonEAPoL frames received on the controlled port are discarded, and the state of the controlled port is set to Blocking.
    - Incoming—All nonEAPoL frames received on the port are discarded, but transmit frames are forwarded through the port.

The following figure illustrates how Virtual Services Platform 9000, configured with EAPoL, reacts to a new network connection.

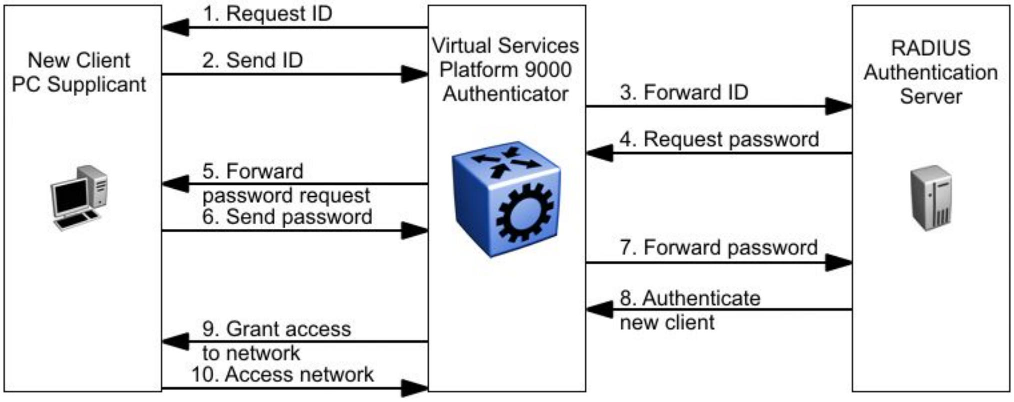


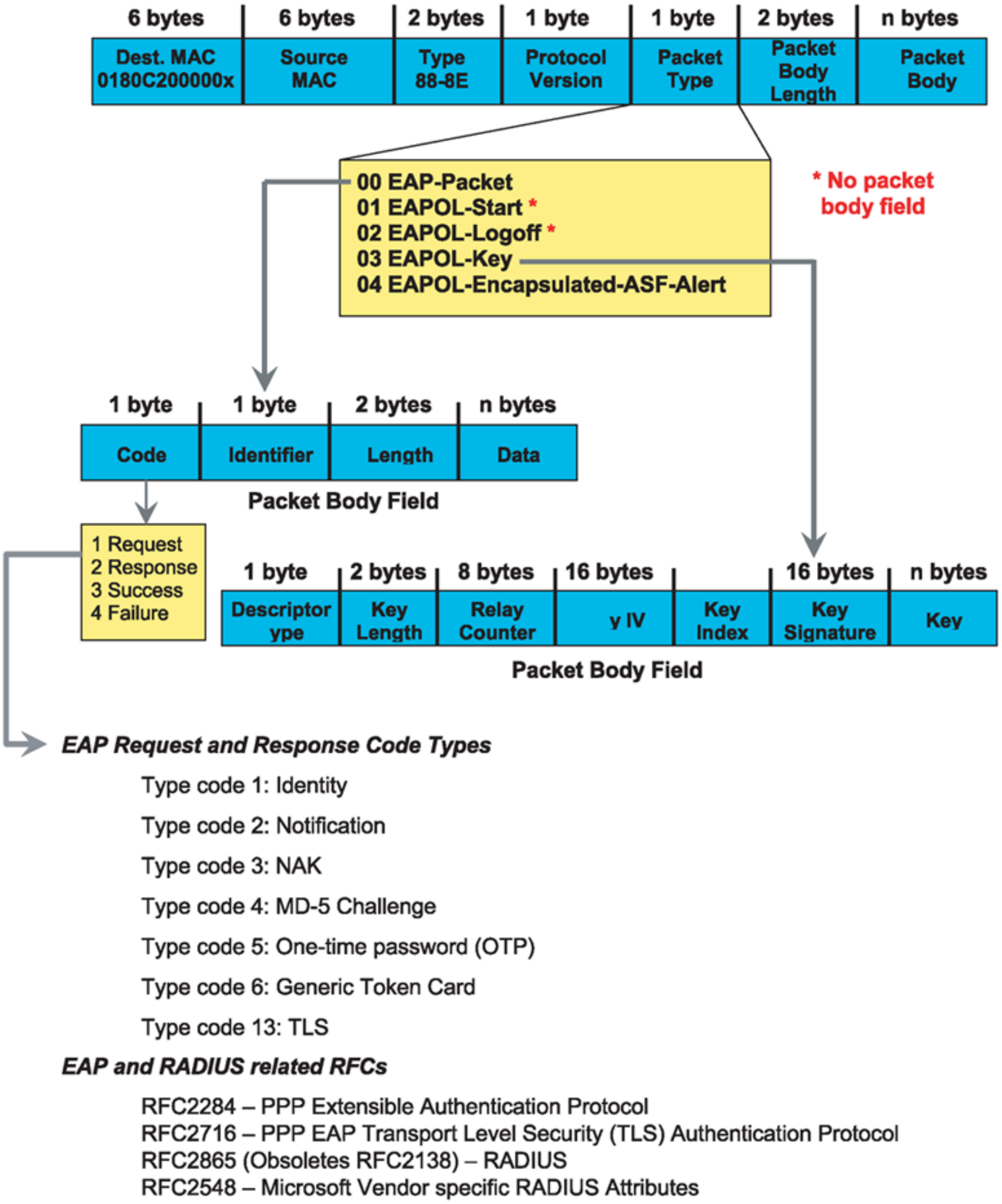
Figure 2: EAPoL configuration example

In Figure 2: EAPoL configuration example on page 40, Virtual Services Platform 9000 uses the following steps to authenticate a new client:

1. Virtual Services Platform 9000 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 Virtual Services Platform 9000.
3. Virtual Services Platform 9000 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. Virtual Services Platform 9000 forwards the request from the RADIUS server to the new client.
6. The new client sends an encrypted password to Virtual Services Platform 9000, within the EAPoL packet.
7. Virtual Services Platform 9000 forwards the EAPoL packet to the RADIUS server.
8. The RADIUS server authenticates the password.
9. Virtual Services Platform 9000 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 3: 802.1x Ethernet frame

The following figure shows the flow diagram for EAPoL on Virtual Services Platform 9000.

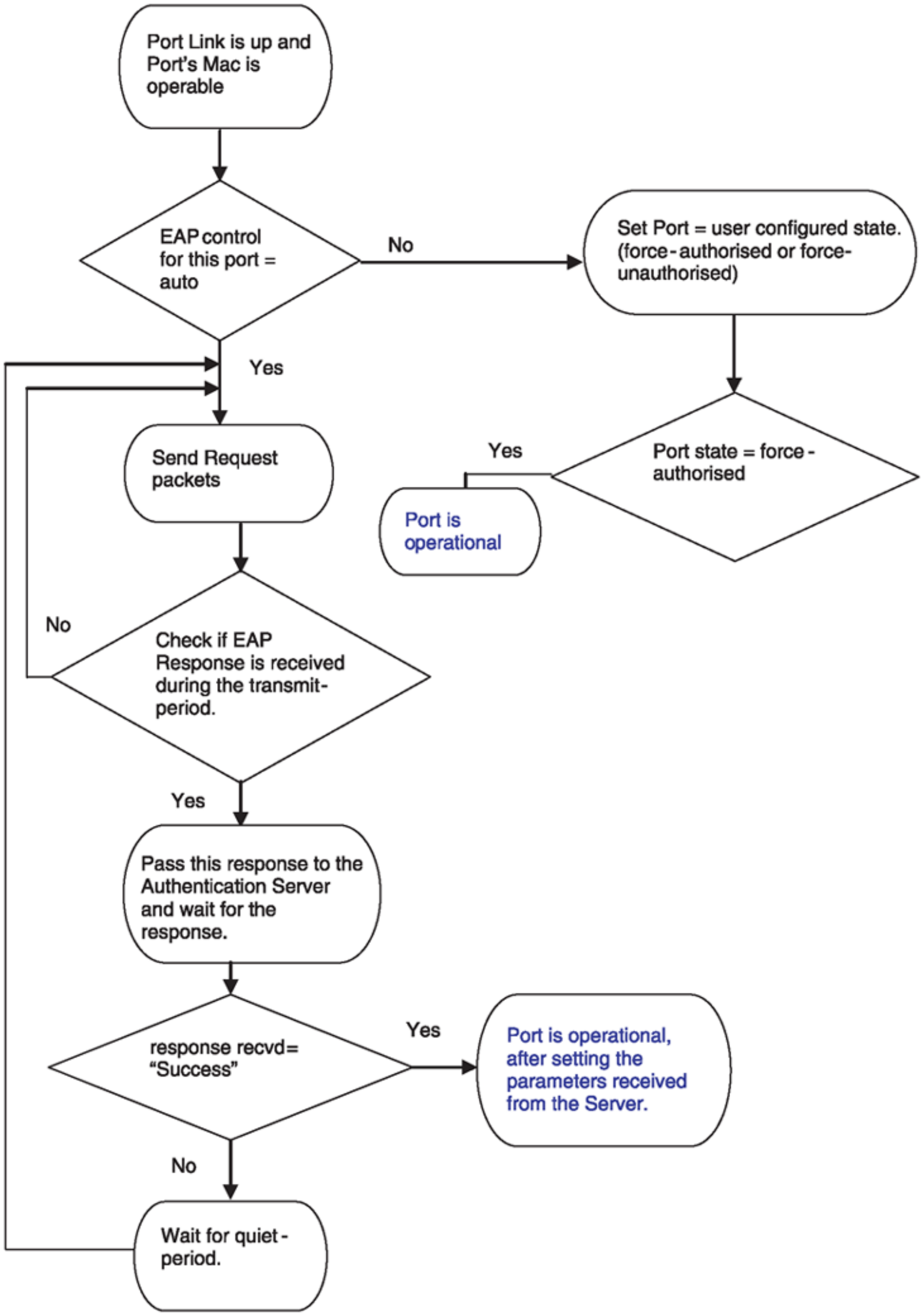

Port Link is up and Port's Mac is operable
EAP control for this port = auto
No
Set Port = user configured state. (force-authorised or force-unauthorised)
Yes
Port state = force-authorised
Yes
Port is operational
Send Request packets
No
Check if EAP Response is received during the transmit-period.
Yes
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 4: Virtual Services Platform 9000 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 Virtual Services Platform 9000 systems. You must configure your Virtual Services Platform 9000 for VLANs and EAPoL security.

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

- You cannot enable EAPoL on tagged ports.
- You cannot enable EAPoL on ports belonging 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.

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 moving it to the VLAN specified.

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 Virtual Services Platform 9000 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.

RADIUS return attributes supported for EAPoL

Virtual Services Platform 9000 uses the RADIUS tunnel attributes to place a port into a particular VLAN to support dynamic VLAN switching based on authentication.

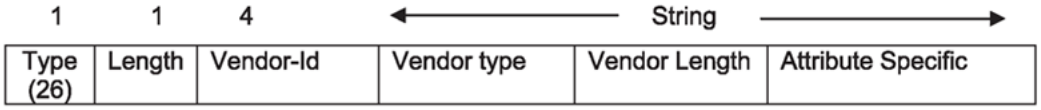
The RADIUS server indicates the desired VLAN by including the tunnel attribute within the Access-Accept message. RADIUS uses the following tunnel attributes:

- 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 to 4096, 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 Virtual Services Platform 9000 Supplicant port a QoS value from 0 to 7.

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



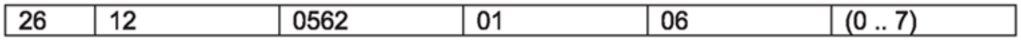
1	1	4	←	String	→
Type (26)	Length	Vendor-Id	Vendor type	Vendor Length	Attribute Specific

Figure 5: RADIUS vendor-specific frame format

Virtual Services Platform 9000 Port Priority frame format

- vendor specific type = 26
- length = 12
- vendor-id = 0562
- string = vendor type = 1 + vendor length = 6 + attribute specific = priority

The following figure shows the port priority frame format.



26	12	0562	01	06	(0 .. 7)

Figure 6: 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 4094 (this value identifies the specified VLAN)
- Port priority (vendor-specific) attributes
  - Vendor ID: value 562, Avaya Vendor ID and value 1584, Bay Networks Vendor ID
  - Attribute Number: value 1, Port Priority

- Attribute Value: value 0 (zero) to 7 (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

Virtual Services Platform 9000 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 12: Summary of accounting events and information logged

Event	Radius attributes	Description
User is authenticated by EAPoL and port enters authorized state	Acct-Status-Type	Start
	Nas-IP-Address	IP address to represent Virtual Services Platform 9000
	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 and port enters unauthorized state	Acct-Status-Type	Stop
	Nas-IP-Address	IP address to represent Virtual Services Platform 9000
	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 RADIUS accounting attribute, see Table 13: 802.1x session termination mapping on page 47.

Event	Radius attributes	Description
	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 13: 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)	—

EAPoL configuration using ACLI

Extensible Authentication Protocol over LAN (EAPoL) is a port-based network access-control protocol. EAPoL provides security to your network by preventing users from accessing network resources before they receive authentication.

You can use EAPoL to set up network access control on internal LANs and to exchange authentication information between any end station or server connected to Avaya Virtual Services Platform 9000 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 PC from accessing the network.

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

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)
- Port mirroring

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 force-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.

Globally enabling EAPoL on the device

Before you begin

- You must log on to the Global Configuration mode in ACLI.

About this task

Enable EAPoL globally on Avaya Virtual Services Platform 9000 before you enable it on a port or interface.

Procedure

Globally configure EAPoL:

```
eapol enable
```

Example

```
VSP-9012:1> enable

VSP-9012:1# configure terminal

VSP-9012:1(config)# eapol enable
```

Configuring EAPoL on an interface

Before you begin

- You must log on to the Interface Configuration mode in ACLI.
- EAPoL must be globally enabled.

About this task

Configure EAPoL on Avaya Virtual Services Platform 9000.

When you configure a port with the EAP status of auto, only one supplicant is allowed on this port. Multiple EAP supplicants are not allowed on the same physical Virtual Services Platform 9000 port.

Procedure

Enable EAPoL on an interface:

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

Example

```
VSP-9012:1> enable

VSP-9012:1# configure terminal

VSP-9012:1(config)# interface GigabitEthernet 3/1

VSP-9012:1(config)# eapol status auto
```

Variable definitions

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

Table 14: Variable definitions

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.
unauthorized	Specifies that the port is always unauthorized. The default value is authorized.

Configuring EAPoL on a port

Before you begin

- You must log on to Interface Configuration mode in ACLI.

About this task

Configure EAPoL on a specific port when you do not want to apply EAPoL to all of the Avaya Virtual Services Platform 9000 ports.

Procedure

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

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

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

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

3. Enable reauthentication:

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

4. Configure the time interval between successive authentications:

   ```
   eapol port {slot/port[-slot/port][,...]} re-authentication-
   period <1-2147483647>
   ```

5. Configure the timer for waiting for a RADIUS response:

   ```
   eapol port {slot/port[-slot/port][,...]} server-timeout
   <1-65535>
   ```

6. Enable an external device to manage the session:

   ```
   eapol port {slot/port[-slot/port][,...]} sess-manage-mode
   enable
   ```

7. Configure which port to open immediately after 802.1x authentication:

   ```
   eapol port {slot/port[-slot/port][,...]} sess-manage-open-
   immediate enable
   ```

8. Configure the EAP authentication status:

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

9. Configure the wait for supplicant response timer for all EAP packets except EAP Request/Identity:

   ```
   eapol port {slot/port[-slot/port][,...]} supplicant-timeout
   <1-65535>
   ```

10. Configure the traffic control level:

    ```
    eapol port {slot/port[-slot/port][,...]} traffic-control
    {in|in-out}
    ```

11. Configure wait time for supplicant :

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

Example

```
VSP-9012:1> enable
```

```
VSP-9012:1# configure terminal
```

```
VSP-9012:1(config)# interface GigabitEthernet 3/1
```

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

```
VSP-9012:1(config-if)# eapol max-request 10
```

Configure the time interval, in seconds, between authentication failure and the start of a new authentication:

```
VSP-9012:1(config-if)# eapol port 3/1 quiet-interval 500
```

Variable definitions

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

Table 15: Variable definitions

Variable	Value
{slot/port[-slot/port][,...]}	Specifies the port or list of ports used by EAPoL.
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 <1-2147483647>	Specifies the time interval in seconds between successive reauthentications. The default is 3600 (1 hour).
server-timeout <1-65535>	Specifies the time in seconds to wait for a response from the RADIUS server. The default is 30.
sess-manage-mode enable	Enables an external device to manage the port session.
sess-manage-open-immediate enable	Specifies the port to be opened immediately after 802.1x authentication.
status {authorized|auto|unauthorized}	Specifies the desired EAP authentication status for this port.

Variable	Value
supplicant-timeout <1-65535>	Specifies the time in seconds to wait for a response from the supplicant for all EAP packets except EAP Request/ Identity.
traffic-control {in|in-out}	Specifies the desired level of traffic control of the port.
transmit-interval <1-65535>	Specifies the time in seconds to wait for a response from the supplicant for EAP Request/Identity packets.

Configuring an EAPoL-enabled RADIUS server

Before you begin

- You must enable EAPoL globally.
- You must log on to the Global Configuration mode in ACLI.

About this task

Avaya Virtual Services Platform 9000 uses RADIUS servers for authentication and accounting services. Use the no form to delete a RADIUS server.

The RADIUS server uses the secret key to validate users.

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

Procedure

Add an EAPoL-enabled RADIUS server:

```
radius server host WORD <0–46> used-by eapol [key WORD<0-20>]
[port 1-65536] [priority <1-10>] [retry <0-6>] [timeout <1-20>]
[enable] [acct-port <1-65536>] [acct-enable] [source-ip WORD
<0–46>]
```

By default, Avaya Virtual Services Platform 9000 uses RADIUS UDP port 1812 for authentication, and port 1813 for accounting. You can change the port numbers or other RADIUS server options.

Example

```
VSP-9012:1> enable
```

```
VSP-9012:1# configure terminal
```

Add an EAPoL RADIUS server:

```
VSP-9012:1(config)# radius server host fe80:0:0:0:21b:4fff:fe5e:73fd
used-by eapol key radiustest
```

Variable definitions

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

Table 16: Variable definitions

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 in ACLI.
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 in ACLI.

Configuring Avaya Virtual Services Platform 9000 for EAPoL and RADIUS

Before you begin

- You must log on to Global Configuration mode in ACLI.

About this task

You must configure Avaya Virtual Services Platform 9000 through which 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 will connect.

Perform the following procedure to set up Virtual Services Platform 9000 for EAPoL and RADIUS.

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

For more information about EPM and UBP, see the user documentation for your Avaya Enterprise Policy Manager (EPM) application.

Procedure

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

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

2. Log on to the Interface Configuration mode:

   `interface vlan <1–4084>`

3. Enable the device to communicate through EAPoL:

   `eapol enable`

4. Globally enable session management:

   `eapol sess-manage enable`

   Important:

   When EPM learns interfaces on the device, it configures the **`eapol sess-manage-mode`** command to **`enable`** on individual interfaces.

5. Exit from VLAN interface mode:

   `exit`

6. Log on to Interface Configuration mode:

   `interface GigabitEthernet <slot/port>`

7. Enable device ports for EAPoL authentication:

   `eapol port <slot/port> status auto`

8. Enable periodic supplicant re-authenticating:

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

9. Save your changes:

   `save config`

Example

```
VSP-9012:1> enable
```

```
VSP-9012:1# configure terminal
```

Create a RADIUS server that is used by EAPoL:

```
VSP-9012:1(config)# radius server host fe90:0:0:0:21b:4eee:fe5e:75fd
used-by eapol key radiustest
```

```
VSP-9012:1(config)# interface vlan 2
```

Enable the device to communicate through EAPoL:

```
VSP-9012:1(config-if)# eapol enable
```

Save your changes:

```
VSP-9012:1(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.

Table 17: Variable definitions

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 in ACLI.
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

Before you begin

- You must log on to the appropriate Interface Configuration mode in ACLI.

About this task

Avaya Virtual Services Platform 9000 authorizes ports by default. This means that the ports are always authorized and are not authenticated by the RADIUS server.

You can change this setting so that the ports are always unauthorized. You can also make the ports controlled so that they are automatically authenticated when you globally enable EAPoL (auto).

Procedure

Configure the authorization status of a port:

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

Example

```
VSP-9012:1> enable
VSP-9012:1# configure terminal
VSP-9012:1(config)# interface GigabitEthernet 3/1
```

Configure the authorization status of a port:

```
VSP-9012:1(config-if)# eapol status authorized
```

Variable definitions

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

Table 18: Variable definitions

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.
unauthorized	Specifies that the port is always unauthorized. The default value is authorized.

Deleting an EAPoL-enabled RADIUS server

Before you begin

- You must log on to Global Configuration mode in ACLI.

About this task

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

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

Procedure

Delete an EAPoL-enabled RADIUS server:

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

Example

```
VSP-9012:1> enable

VSP-9012:1# configure terminal

VSP-9012:1(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.

Table 19: Variable definitions

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 in ACLI.
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.

EAPoL configuration using Enterprise Device Manager

Extensible Authentication Protocol over LAN (EAPoL) is a port-based network access-control protocol. EAPoL provides security to your network by preventing users from accessing network resources before they receive authentication.

You can use EAPoL to set up network access control on internal LANs and to exchange authentication information between any end station or server connected to Avaya Virtual Services Platform 9000 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 PC from accessing the network.

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)
  - Port mirroring
- 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 59. 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 that is configured for EAPoL. If you attempt to add additional clients on the EAPoL authorized port, the port goes to force-unauthorized mode.

Globally configuring EAPoL on the server

About this task

Use SystemAuthControl to 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, open the following folders: **Configuration** > **Security** > **Data Path**.
2. Click **802.1x - EAPOL**.
3. Click the **Global** tab.
4. From the SystemAuthControl options, select **enabled**.

5. Click **Apply**.

Global field descriptions

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

Name	Description
SystemAuthControl	Enables system authentication control. EAPoL is disabled by default.

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. You can also make the ports controlled so that they are automatically authenticated when you globally enable EAPoL.

Procedure

1. In the Device Physical View tab, select the port you need to configure.
2. In the navigation tree, open the following folders: **Configuration** > **Edit** > **Port**.
3. Click **General**.
4. Click the **EAPOL** tab.
5. Select the **PortInitialize** check box if desired.
6. Select the **PortReauthenticate** check box if desired.
7. Select the desired **AdminControlledDirections** option.
8. Select the desired **AuthControlledPortControl** option.
9. In the **QuietPeriod** field, type the time interval.
10. In the **TxPeriod** field, type the time.
11. In the **SuppTimeout** field, type the response time.
12. In the **ServerTimeout** field, type the time.
13. In the **MaxReq** field, type the number of times.
14. In the **ReAuthPeriod** field, type the time between reauthentications.
15. Select the **ReEAuthEnabled** field if desired.

16. Click **Apply**.

EAPoL field descriptions

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

Name	Description
portProtocolVersion	Shows the protocol version number of the EAPoL implementation supported by the port.
portCapabilities	Shows 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.
PortInitialize	Initializes EAPoL authentication on this port. After the port initializes, this field reverts to its default, which is disabled.
PortReauthenticate	Reauthenticates the supplicant connected to this port immediately. The default is disabled.
PaeState	Shows the current Authenticator PAE state. The possible states are initialized, disconnected, connecting, authenticating, authenticated, aborting, held, forceAuth, forceUnauth The default state is forceAuth.
BackendAuthState	Shows the current state of Backend Authentication. The possible states are request, response, success, fail, timeout, idle, initialize The default state is idle.
AdminControlDirections	Determines whether the port exerts control over communication in both directions (both incoming and outgoing) or only in the incoming direction. The default value is both.
OperControlledDirections	Shows the current direction of control over communications exerted on the port.
AuthControlledPortStatus	Shows the current state of the port: unauthorized, auto, or authorized. The default value is authorized.
AuthControlledPortControl	Configures the authentication status for this port. The default is forceAuthorized. forceUnauthorized—port is always unauthorized. auto—configures the port to match the global EAPoL authentication setting.

Name	Description
	forceAuthorized—port is always authorized. The default value is forceAuthorized.
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.
TxPeriod	Configures the time in seconds to wait for a response from a supplicant for EAP Request/Identity packets. The allowed range is 1–65535; the default is 30.
SuppTimeout	Configures the time (in seconds) to wait for a response from a supplicant for all EAP packets except EAP Request/Identity packets. The allowed range is 1–65535; the default is 30.
ServerTimeout	Configures the time (in seconds) to wait for a response from the RADIUS server. The allowed range is 1–65535; the default is 30.
MaxReq	Configures the maximum number of times to retry sending packets to the supplicant. The allowed range is 1–10; the default is 2.
ReAuthPeriod	Configures the time interval (in seconds) between successive reauthentications. The allowed range is 1–2147483647; the default is 3600 (1 hour).
ReAuthEnabled	Reauthenticates an existing supplicant at the time interval specified in ReAuthPeriod.
SessionId	Shows a unique identifier for the session, in the form of a printable ASCII string of at least three characters.
SessionAuthenticMethod	Shows the authentication method used to establish the session.
SessionTime	Shows the duration of the session in seconds.
SessionTerminateCause	Shows the reason for the session termination.
SessionUserName	Shows the user name representing the identity of the supplicant PAE.
LastEapolFrameVersion	Shows the protocol version number carried in the most recently received EAPoL frame.
LastEapolFrameSource	Shows the source MAC address carried in the most recently received EAPoL frame.

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, open 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.
PortProtocolVersion	Indicates the protocol version associated with this port.
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.
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.
PortReauthenticate	Specifies the reauthentication control for this port. Setting this attribute true causes the Authenticator PAE state machine for the port to reauthenticate the Supplicant. Setting this attribute false has no effect. This attribute always returns false when it is read.

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 tree, open 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.
PAEState	Indicates the current value of the authenticator Port Access Entity (PAE) state machine.
BackendAuthState	Indicates the current state of the Backend Authentication state machine.
AdminControlledDirections	Indicates the current value of the administrative controlled directions parameter for the port.
OperControlledDirections	Indicates the current value of the operational controlled directions parameter for the port.
AuthControlledPortStatus	Indicates the current value of the controlled port status parameter for the port.
AuthControlledPortControl	Indicates the current value of the controlled port control parameter for the port.
QuietPeriod	Indicates the value, in seconds, of the QuietPeriod constant currently in use by the Authenticator PAE state machine. The range is 1 to 65535. The default is 60 seconds.
TxPeriod	Indicates the value, in seconds, of the TxPeriod constant currently in use by the Authenticator PAE state machine. The range is 1 to 65535. The default is 30 seconds.

Name	Description
SuppTimeout	Indicates the value, in seconds, of the SuppTimeout constant currently in use by the Backend Authentication state machine. The range is 1 to 65535.
ServerTimeout	Indicates the server timeout value, in seconds, currently in use by the Backend Authentication state machine. The range is 1 to 65535. The default is 30 seconds.
MaxReq	Indicates the value of the maxReq constant currently in use by the Backend Authentication state machine. The range is 1 to 10. The default is 2.
ReAuthPeriod	Indicates the value, in seconds, of the reauthentication interval currently in use by the Reauthentication Timer state machine (8.5.5.1). The default is 3600 seconds.
ReAuthEnabled	Indicates whether reauthentication is enabled (true) or disabled (false). The default is false.

Chapter 5: 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 users 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: RFC2865, Accounting: RFC2866). With Virtual Services Platform 9000, you use RADIUS authentication to get secure access to the system (console/Telnet/SSH/EDM), and RADIUS accounting to track the management sessions (ACLI only).

RADIUS support for IPv6

RADIUS supports both IPv4 and IPv6 addresses on Virtual Services Platform 9000. There are no differences in functionality or configuration for all except 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.

Virtual Services Platform 9000 software supports BaySecure Access Control (BSAC) and the Merit Network servers. 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.

Important:

RADIUS Authentication is supported in HA mode.

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

RADIUS authentication on secondary CP modules

Secondary CP modules support RADIUS authentication. To connect to a secondary CP module using RADIUS, you must configure the management port on the secondary CP module with an out-of-band IP address, and a route must exist from the management port to the RADIUS server. In addition, you must configure an entry on the RADIUS server that contains the IP address of the secondary CP module.

However, if you configure the RADIUS source-ip option to use a CLIP address or the management virtual IP address on Virtual Services Platform 9000, then you cannot connect to the secondary CP module using RADIUS.

Use of RADIUS to modify user access to ACLI commands

Virtual Services Platform 9000 provides ACLI command access based on a user’s configured access level. However, you can use RADIUS to override ACLI command access provided by Virtual Services Platform 9000.

To override user access to ACLI commands, you must configure the command-access-attribute on Virtual Services Platform 9000 and on the RADIUS server. (Virtual Services Platform 9000 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.

Regardless of the RADIUS server configuration, you must configure the user’s access on Virtual Services Platform 9000 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 20: 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 ACLI commands are executed	• Accounting interim request: NAS IP address • Session ID • ACLI commands • User name
User logs off	• Accounting stop request: NAS IP address • Session ID • Session duration

Event	Accounting information logged at server
	• 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 • ACLI 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 ACLI

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, with no difference in functionality or configuration using ACLI.

RADIUS is a fully open and standard protocol, defined by RFCs (Authentication: RFC2865, accounting RFC2866). With Avaya Virtual Services Platform 9000, you use RADIUS authentication to secure access to the device (console/Telnet/SSH), and RADIUS accounting to track the management sessions for Avaya Command Line Interface (ACLI) 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.

Direct RADIUS authentication is supported on secondary CP modules and in High-Availability (HA) mode.

Configuring RADIUS attributes

Before you begin

- You must log on to the Global Configuration mode in ACLI.

About this task

Configure RADIUS to authenticate user identity through a central database.

Procedure

1. Configure RADIUS access priority:
   `radius access-priority-attribute <192-240>`
2. Configure RADIUS accounting:
   `radius accounting {attribute-value <192-240>|enable|include-cli-commands}`
3. Configure the RADIUS authentication info attribute value:
   `radius auth-info-attr-value <0-255>`
4. Clear RADIUS statistics:
   `radius clear-stat`
5. Configure the value of the CLI commands:
   `radius cli-commands-attribute <192-240>`
6. Configure the value of the command access attribute:
   `radius command-access-attribute <192-240>`
7. Configure the maximum number of servers allowed:
   `radius maxserver <1-10>`
8. Configure the multicast address attribute:
   `radius mcast-addr-attr-value <0-255>`

Example

```
VSP-9012:1> enable
```

```
VSP-9012:1# configure terminal
```

Configure RADIUS access priority:

```
VSP-9012:1(config)# radius access-priority-attribute 192
```

Configure RADIUS accounting to include CLI commands:

```
VSP-9012:1(config)# radius accounting include-cli-commands
```

Variable definitions

Use the data in the following table to use the `radius` command.

Table 21: Variable definitions

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 ACLI 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 ACLI commands attribute in the range of 192 to 240. The default is 195.
cli-profile	Enable RADIUS CLI profiling. ACLI profiling grants or denies access to users being authenticated by way of the RADIUS server. You can add a set of ACLI 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 Avaya Virtual Services Platform 9000.
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|eapol|web} [acct-enable] [acct-port *<1–65536>*] [enable] [port *<1–65536>*] [priority *<1–10>*] [retry	• host *WORD<0–46>* Creates a host server. WORD<0–46> signifies an IP address. • key *WORD<0–32>*

Variable	Value
<0–6>] [source-ip *WORD<0–46>*] [timeout *<1–60>*]	Specifies a secret key in the range of 0–32 characters. • used-by *{cli|snmp|eapol|web}* Specifies how the server functions. Configures the server for authentication for • cli • snmp • eapol • 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.
sourceip-flag	Enable the source IP so Avaya Virtual Services Platform 9000 uses a configured source IP address. If the outgoing interface on Avaya Virtual Services Platform 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

Variable	Value
	configure Avaya Virtual Services Platform 9000 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 Avaya Virtual Services Platform with multiple CLIP interfaces. **Note:** If you configure the RADIUS source-ip option to use a CLIP address on Virtual Services Platform 9000, then you cannot connect to the secondary CP module using RADIUS. By default, Avaya Virtual Services Platform 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

Before you begin

- You must log on to the Global Configuration mode in ACLI.

About this task

Use RADIUS ACLI profiling to grant or deny ACLI command access to users being authenticated by way of the RADIUS server. You can add a set of ACLI 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

Enable RADIUS ACLI profiling:

```
radius cli-profile
```

Example

```
VSP-9012:1> enable

VSP-9012:1# configure terminal

VSP-9012:1(config)# radius cli-profile
```

Enabling RADIUS authentication

Before you begin

- You must log on to the Global Configuration mode in ACLI.

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

Enable RADIUS authentication globally on Avaya Virtual Services Platform 9000:

```
radius enable
```

```
no radius enable
```

```
default radius enable
```

Enabling the source IP flag for the RADIUS server

Before you begin

- You must log on to the Global Configuration mode in ACLI.
- 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 Virtual Services Platform 9000. 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, Avaya Virtual Services Platform 9000 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 Virtual Services Platform 9000 uses a configured source IP address instead. Therefore, if the outgoing interface on Virtual Services Platform 9000 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 ACLI.

To simplify RADIUS Server configuration, you can configure Virtual Services Platform 9000 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 Virtual Services Platform 9000 with multiple CLIP interfaces.

Note:

If you configure the RADIUS source-ip option to use a CLIP address on Virtual Services Platform 9000, then you cannot connect to the secondary CP module using RADIUS.

The default for **`radius sourceip-flag`** is false.

Procedure

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.
- You must log on to the Global Configuration mode in ACLI.

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. Enable RADIUS accounting globally:
   ```
   radius accounting enable
   ```
2. Include or exclude CLI commands in RADIUS accounting updates:
   ```
   radius accounting include-cli-commands
   ```
3. Specify the integer value of the CLI commands attribute:
   ```
   radius accounting attribute-value <192–240>
   ```

Example

```
VSP-9012:1> enable

VSP-9012:1# configure terminal

VSP-9012:(config)# radius accounting enable

VSP-9012:(config)# radius accounting include-cli-commands
```

Variable definitions

Use the data in the following table to use the `radius accounting` command.

Table 22: 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.
- You must log on to the Global Configuration mode in ACLI.

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. Enable RADIUS Simple Network Management Protocol (SNMP) accounting globally:

   ```
   radius-snmp acct-enable
   ```

2. Set a timer to send a stop accounting message for RADIUS Simple Network Management Protocol (SNMP):

   ```
   radius-snmp abort-session-timer <30–65535>
   ```

3. Set the timer for re-authentication of the SNMP session:

   ```
   radius-snmp re-auth-timer <30–65535>
   ```

4. Specify the user name for SNMP access:

```
radius-snmp user WORD <0–20>
```

Example

```
VSP-9012:1> enable
VSP-9012:1# configure terminal
VSP-9012:(config)# radius-snmp acct-enable
VSP-9012:(config)# radius-snmp abort-session-timer 30
```

Variable definitions

Use the data in the following table to use the `radius-snmp` command.

Table 23: 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

Before you begin

- You must log on to the Global Configuration mode in ACLI.

About this task

Configure RADIUS accounting interim requests to create a log whenever a user executes more than the number of ACLI 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. Configure RADIUS accounting interim requests:
   `radius cli-cmd-count <1-40>`
2. 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

```
VSP-9012:1>enable

VSP-9012:1#configure terminal

VSP-9012:1(config)#radius cli-cmd-count 30

VSP-9012:1(config)#radius accounting include-cli-commands
```

Variable definitions

Use the data in the following table to use the `radius cli-cmd-count` command.

Table 24: Variable definitions

Variable	Value
<1-40>	Specifies how many ACLI 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

Before you begin

- You must log on to the Global Configuration mode in ACLI.

About this task

Configure RADIUS authentication and RADIUS accounting attributes to determine the size of the packets received.

Procedure

1. Configure the RADIUS authentication attribute value:
   `radius command-access-attribute <192-240>`
2. Configure the RADIUS accounting attribute value:
   `radius accounting attribute-value <192-240>`

Example

```
VSP-9012:1> enable

VSP-9012:1# configure terminal

VSP-9012:1(config)# radius command-access-attribute 192

VSP-9012:1(config)# radius accounting attribute-value 192
```

Variable definitions

Use the data in the following table to use the `radius` command.

Table 25: Variable definitions

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 ACLI 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 ACLI commands attribute in the range of 192 to 240. The default is 195.
cli-profile	Enable RADIUS CLI profiling. ACLI profiling grants or denies access to users being authenticated by way of the RADIUS server. You can add a set of ACLI commands to the configuration on the RADIUS server,

Variable	Value
	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 Avaya Virtual Services Platform 9000.
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|eapol|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*|*eapol*|*web}* Specifies how the server functions. Configures the server for authentication for • cli • snmp • eapol • 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>*

Variable	Value
	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 Avaya Virtual Services Platform 9000 uses a configured source IP address. If the outgoing interface on Avaya Virtual Services Platform 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 Avaya Virtual Services Platform 9000 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 Avaya Virtual Services Platform with multiple CLIP interfaces. **Note:** If you configure the RADIUS source-ip option to use a CLIP address on Virtual Services Platform 9000, then you cannot connect to the secondary CP module using RADIUS. By default, Avaya Virtual Services Platform 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

Before you begin

- You must log on to the Global Configuration mode in ACLI.

About this task

Add a RADIUS server to allow RADIUS service on Avaya Virtual Services Platform 9000.

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

Procedure

Add a RADIUS server:

```
radius server host WORD <0–46> key WORD<0-32> [used-by {cli|
snmp|eapol|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>]
```

Example

```
VSP-9012:1> enable
```

```
VSP-9012:1# configure terminal
```

Add a RADIUS server:

```
VSP-9012:1(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.

Table 26: Variable definitions

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 ACLI.
key *WORD<0-32>*	Specifies a secret key in the range of 0–32 characters.
used-by {cli|snmp|eapol|web}	Specifies how the server functions • cli—configure the server for CLI authentication. • snmp—configure the server for SNMP authentication. • eapol—configure the server for EAPoL authentication. • web—configure the server for http(s) authentication Use the no option to remove a host server: **`no radius server host WORD<0–46>`**

Variable	Value
	used-by {cli|snmp|eapol|web}. The default is cli. The default command is: **default radius server host WORD<0–46> used-by {cli|snmp|eapol|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. **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 ACLI.
timeout *<1-60>*	Specifies the number of seconds before the authentication request times out. The default is 3.

Modifying RADIUS server settings

Before you begin

- You must log on to the Global Configuration mode in ACLI.

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 ACLI.

Procedure

Modify a RADIUS server:

```
radius server host WORD <0–46> [used-by {cli|eapol|snmp|web}]
[key WORD<0-20>] [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

```
VSP-9012:1> enable
```

```
VSP-9012:1# configure terminal
```

Modify a RADIUS server:

```
VSP-9012:1(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.

Table 27: Variable definitions

Variable	Value
used-by {cli|eapol|snmp| web}	Specifies how the server functions • cli—configure the server for CLI authentication. • snmp—configure the server for SNMP authentication. • eapol—configure the server for EAPoL authentication. • web—configure the server for Web authentication.

Variable	Value
	Use the no option to remove a host server: **`no radius server host WORD<0-46> used-by {cli|snmp|eapol|web}`**. The default is cli. The default command is: **`default radius server host WORD<0-46> used-by {cli|snmp|eapol|web}`**.
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 ACLI.
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 <0–20>*	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 ACLI.
timeout *<1–20>*	Configures the number of seconds before the authentication request times out (1 to 20). The default is 3.

Showing RADIUS information

About this task

Display the global status of RADIUS information to ensure you configured the RADIUS feature according to the needs of the network.

Procedure

Display the global status of RADIUS information:

```
show radius
```

Example

```
VSP-9012:1>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
                        maxserver : 10
            mcast-addr-attr-value : 90
                    sourceip-flag : false
```

Displaying RADIUS server information

About this task

If your system is configured with a RADIUS server you can display the RADIUS server information.

Procedure

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

```
VSP-9012:1>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

About this task

Display current RADIUS SNMP configurations.

Procedure

Display the current RADIUS server SNMP configurations:

```
show radius snmp
```

Example

```
VSP-9012:1>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: RFC2865, accounting RFC2866). With Avaya Virtual Services Platform 9000, you use RADIUS authentication to secure access to the device (console/Telnet/SSH), and RADIUS accounting to track the management sessions for Avaya Command Line Interface (ACLI) 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.

Direct RADIUS authentication is supported on secondary CP modules and in High-Availability (HA) mode.

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. Avaya recommends the default setting of 192 for Virtual Services Platform 9000.

Name	Description
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. Avaya recommends the default setting of 192 for Virtual Services Platform 9000.
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

Name	Description
	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.

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. Avaya recommends the default setting of 192 for Virtual Services Platform 9000.
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

Name	Description
	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 Virtual Services Platform 9000. 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 94.

Important:

Use the source IP option only for the RADIUS servers connected to the in-band network.

About this task

By default, Avaya Virtual Services Platform 9000 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 Virtual Services Platform 9000 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 Virtual Services Platform 9000 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 Virtual Services Platform 9000 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 value set in the dictionary file on the

Name	Description
	RADIUS server. The valid values are 192 through 240. Avaya recommends the default setting of 192 for Virtual Services Platform 9000.
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 Avaya Virtual Services Platform 9000.

Remote Dial-In User Services (RADIUS) is updated to support both IPv4 and IPv6 addresses. There are 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 EAP PAE Authenticator • 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 (1 to 10). The default is 10.

Name	Description
TimeOut	Specifies the time interval in seconds before the client retransmits the packet (1 to 20).
Enable	Enables or disables authentication on the server. The default is true.
MaxRetries	Specifies the maximum number of retransmissions allowed (1 to 6). The default is 1.
UdpPort	Specifies the UDP port that the client uses to send requests to the server (1 to 65536). 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 (1 to 65536). 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.
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 EAP PAE Authenticator • 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 (1 to 10). The default is 10.
TimeOut	Specifies the time interval in seconds before the client retransmits the packet (1 to 20).
Enable	Enables or disables authentication on the server. The default is true.
MaxRetries	Specifies the maximum number of retransmissions allowed (1 to 6). The default is 1.
UdpPort	Specifies the UDP port that the client uses to send requests to the server (1 to 65536). 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 (1 to 65536). 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

Name	Description
	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 6: 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).

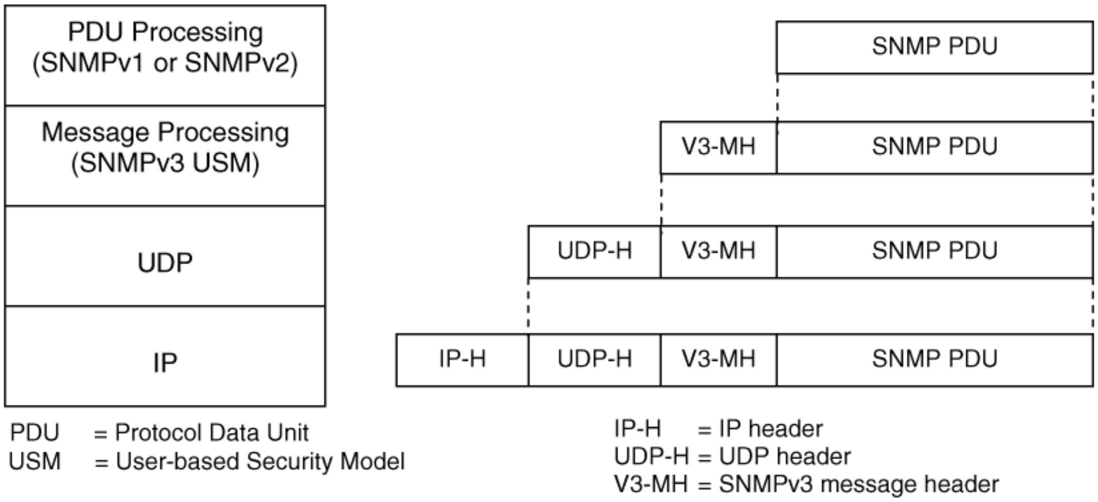

PDU Processing (SNMPv1 or SNMPv2)
Message Processing (SNMPv3 USM)
UDP
IP
SNMP PDU
V3-MH
SNMP PDU
UDP-H
V3-MH
SNMP PDU
IP-H
UDP-H
V3-MH
SNMP PDU
PDU = Protocol Data Unit
USM = User-based Security Model
IP-H = IP header
UDP-H = UDP header
V3-MH = SNMPv3 message header

Figure 7: 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 103
- Message processing subsystem on page 103
- Security subsystem on page 103
- Access control subsystem on page 104

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.

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.

Security

The SNMPv3 security protects against the following:

- 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—protection against delaying or replaying messages
- disclosure—protects against eavesdropping
- 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 Virtual Services Platform 9000 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.

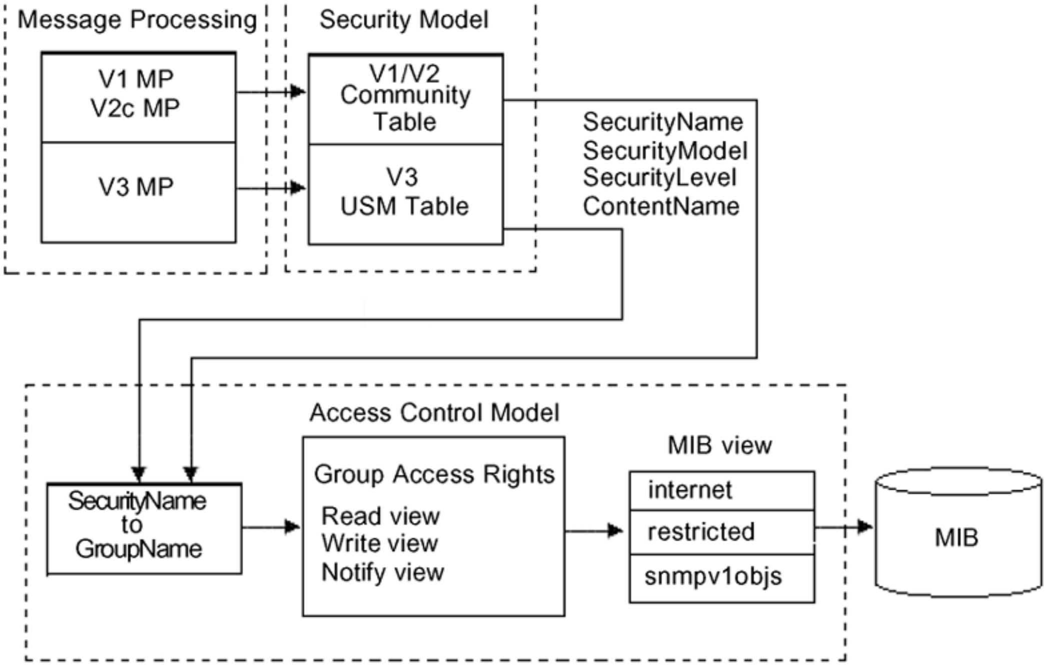


Figure 8: USM association with VACM

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 the following:

- 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 module for SNMPv3 is defined as a security subsystem within an SNMP engine. Currently Virtual Services Platform 9000 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 (FIPS-197) 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.

Important:

Due to export restrictions, the SNMPv3 encryption capability is separate from the main image. For more information about downloading and enabling the SNMPv3 encryption image, see Downloading the SNMPv3 encryption software on page 110 and Loading the SNMPv3 encryption modules on page 112. SNMPv3 does not function properly without the use of this image.

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

Virtual Services Platform 9000 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

Virtual Services Platform 9000 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 *Avaya Virtual Services Platform 9000 Troubleshooting, NN46250-700*.

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 ACLI . 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).

Avaya provides community strings 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 101.

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 blowfish algorithm. Community strings do not appear on the device and are not stored in the configuration file.

⚠ **Caution:**

Security risk

For security reasons, Avaya recommends that you set the community strings to values other than the factory defaults.

Virtual Services Platform 9000 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 (Virtual Services Platform 9000). 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 ACLI

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.

- Before you can use SNMPv3 with Data Encryption Standard (DES) or Advanced Encryption Standard (AES) to access the device, you must load the appropriate SNMPv3 encryption module. For more information, see Loading the SNMPv3 encryption modules on page 112.
- To perform the procedures in this section, you must log on to the Global Configuration mode in ACLI. For more information about how to use ACLI, see *Avaya Virtual Services Platform 9000 User Interface Fundamentals*, NN46250–103.

This task flow shows you the sequence of procedures you perform to configure basic elements of SNMP when using ACLI.

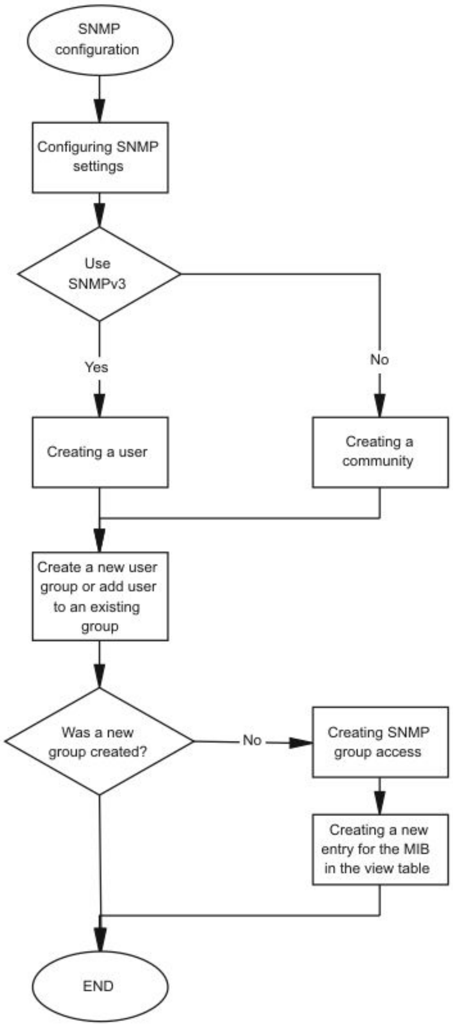

SNMP configuration
Configuring SNMP settings
Use SNMPv3
Yes
No
Creating a user
Creating a community
Create a new user group or add user to an existing group
Was a new group created?
No
Creating SNMP group access
Creating a new entry for the MIB in the view table
END

Figure 9: SNMP configuration procedures

Downloading the SNMPv3 encryption software

Before you begin

- For more information about downloading Avaya Virtual Services Platform 9000 software, go to the Avaya Web site: www.avaya.com/support.

About this task

Download the Advanced Encryption Standard (AES) and Data Encryption Standard (DES) software before you enable the encryption algorithms and use SNMPv3.

Due to export restrictions, the encryption capability is separate from the main software image. SNMPv3 does not function properly without the use of this image.

The AES and DES encryption modules exist in a single file and you can enable them when the file is stored on flash. The file containing the security encryption modules is VSP9K.3.2.0.0_modules.tgz.

Procedure

1. From an Internet browser, browse to www.avaya.com/support.
2. Click **Products** on the left navigation pane.
3. Type **Virtual Services Platform 9000** into the text box, and then select the link that appears below in the text box.
4. Click **Downloads** on the left navigation pane.
5. To filter for a specific release number, select the release you want from the drop down arrow at the top middle part of the page.
6. Click the release name.
7. Click the **Downloads** tab.
8. Download the required software release.
9. Use a FTP client in binary mode to transfer the file to Virtual Services Platform 9000, or transfer it using an external flash or USB device.

   Important:

   You must load the security encryption modules on the device before you can use the protocol.

Downloading the SSH encryption software

Before you begin

- For more information about downloading Avaya Virtual Services Platform 9000 software, go to the Avaya Web site: www.avaya.com/support.

About this task

Download the SSH encryption software before you enable the 3DES encryption module and use SSH.

Due to export restrictions, the encryption capability is separate from the main software image. The SSH server does not function properly without the use of this image.

The file containing the security encryption modules is VSP9K.3.2.0.0_modules.tgz.

Procedure

1. From an Internet browser, browse to www.avaya.com/support.
2. Click **Products** on the left navigation pane.
3. Type **Virtual Services Platform 9000** into the text box, and then select the link that appears below in the text box.
4. Click **Downloads** on the left navigation pane.
5. To filter for a specific release number, select the release you want from the drop down arrow at the top middle part of the page.
6. Click the release name.
7. Click the **Downloads** tab.
8. Download the required software release.
9. Use a FTP client in binary mode to transfer the file to Virtual Services Platform 9000, or transfer it using an external flash or USB device.

   Important:

   You must load the security encryption modules on the device before you can use the protocol.

Loading the SNMPv3 encryption modules

Before you begin

- Download the file containing the SNMPv3 encryption software. For more information about downloading the SNMPv3 encryption software, see Downloading the SNMPv3 encryption software on page 110.

  Important:

  Due to export restrictions, the SNMPv3 encryption capability is separate from the main image. You must copy the SNMPv3 encryption software to Avaya Virtual Services Platform 9000 before you can load the SNMPv3 encryption modules. SNMPv3 does not function properly without this image.

- You must log on to the Global Configuration mode in ACLI.

About this task

Before you can use SNMPv3 with Data Encryption Standard (DES) or Advanced Encryption Standard (AES) to access the device, you must load the appropriate SNMPv3 encryption module.

Procedure

Load the encryption module file on the device:

```
load-encryption-module <DES|AES>
```

Important:

You must load the AES and DES encryption routines by issuing two separate load-encryption-module commands. If you issue the load-encryption-module command for AES, the image is loaded into memory and only the AES routines are enabled; the DES routines are not enabled. To enable the DES routines, you must issue a separate load-encryption-module command for DES.

Example

```
VSP-9012:1>enable
```

```
VSP-9012:1#configure terminal
```

Load the Advanced Encryption Standard security encryption image:

```
VSP-9012:1(config)#load-encryption-module AES
```

Variable definitions

Use the data in the following table to use the `load-encryption-module` command.

Table 28: Variable definitions

Variable	Value
{DES|AES}	Loads the AES or DES SNMPv3 encryption module.

Configuring SNMP settings

Before you begin

- You must log on to the Global Configuration mode in ACLI.

About this task

Configure Simple Network Management Protocol (SNMP) to define or modify the SNMP settings, and specify how secure you want SNMP communications.

Procedure

1. Enable agent conformance mode:

   ```
   snmp-server agent-conformance enable
   ```

2. Enable the generation of authentication traps:

   `snmp-server authentication-trap enable`

3. Create an initial set of SNMPv3 configuration data:

   `snmp-server bootstrap {min-secure|semi-secure|very-secure}`

4. Configure the contact information for the system:

   `snmp-server contact WORD<0-255>`

5. Configure the SNMP and IP sender flag to the same value:

   `snmp-server force-iphdr-sender enable`

6. Send the configured source address (sender IP) as the sender network in the notification message:

   `snmp-server force-trap-sender enable`

7. Create an SNMPv1 server host:

   ```
   snmp-server host WORD<1-256> [port <1-65535>] v1 WORD<1-32>
   [filter WORD<1-32>]
   ```

8. 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>]
   ```

9. 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>]
   ```

10. Configure the system location:

    `snmp-server location WORD<0-255>`

11. Configure the system name:

    `snmp-server name WORD<0-255>`

12. Create a new entry in the notify filter table:

    `snmp-server notify-filter WORD<1-32> WORD<1-32>`

13. Configure the SNMP trap receiver and source IP addresses:

    `snmp-server sender-ip {A.B.C.D} {A.B.C.D}`

Example

```
VSP-9012:1>enable
```

```
VSP-9012:1#configure terminal
```

Enable agent conformance mode:

```
VSP-9012:1(config)#snmp-server agent-conformance enable
```

Enable the generation of authentication traps:

```
VSP-9012:1(config)#snmp-server authentication-trap enable
```

Create an initial set of SNMPv3 configuration data to very-secure:

```
VSP-9012:1(config)#snmp-server bootstrap very-secure
```

```
VSP-9012:1(config)#snmp-server contact xxxx@avaya.com
```

```
VSP-9012:1(config)#snmp-server force-iphdr-sender enable
```

Configure hosts to receive SNMP notifications

```
VSP-9012:1(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.

Table 29: Variable definitions

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 RFC3515 Appendix A for details. • very-secure—a maximum security configuration that allows no access to the users.

Variable	Value
	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 Virtual Services Platform 9000. 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 • 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

Variable	Value
	(from an IP routing table perspective) to the destination SNMP server.

Creating a user

Before you begin

- You must log on to Global Configuration mode in ACLI.
- Before you can use SNMPv3 with Data Encryption Standard (DES) or Advanced Encryption Standard (AES) to access the device, you must load the appropriate SNMPv3 encryption module. For more information, see Loading the SNMPv3 encryption modules on page 112.

About this task

Create a new user in the USM table to authorize a user on a particular SNMP engine

Procedure

1. Create a user on a remote system:

   ```
   snmp-server user WORD<1-32> [engine-id WORD<1-32>] [{md5|sha} WORD<1-32>] [{aes|des} WORD<1-32>]
   ```

2. Create a user on the local system:

   ```
   snmp-server user WORD<1-32> [read-view WORD<1-32>] [write-view WORD<1-32>] [notify-view WORD<1-32>] [[{md5|sha} WORD<1-32>] [read-view WORD<1-32>] [write-view WORD<1-32>] [notify-view WORD<1-32>] [{aes|des|3des} WORD<1-32> [read-view WORD<1-32>] [write-view WORD<1-32>] [notify-view WORD<1-32>]]
   ```

3. 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

```
VSP-9012:1> enable
```

```
VSP-9012:1# configure terminal
```

Create a local user test1 with MD5:

```
VSP-9012:1(config)# snmp-server user test1 md5 auth-password
```

Variable definitions

Use the data in the following table to use the `snmp-server user` command.

Table 30: 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, des, or 3des. *WORD<1-32>* assigns a privacy password. If no value is entered, no privacy capability exists. The range is 1–32 characters. **Important:** You must set authentication before you can set the privacy option.
engine-id *WORD<1-32>*	Assigns an SNMPv3 engine ID. The range is 10–64 characters. 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<1-32>	Specifies the view name in the range of 0–32 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<1-32>	Specifies the view name in the range of 0–32 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<1-32>	Specifies the view name in the range of 0–32 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

Before you begin

- You must log on to Global Configuration mode in ACLI.

About this task

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.

Procedure

Create a new user group:

```
snmp-server group WORD <1-32> WORD<1-32> {auth-no-priv|auth-
priv|no-auth-no-priv} [notify-view WORD<1-32>] [read-view
WORD<1-32>] [write-view WORD<1-32>]
```

Example

```
VSP-9012:1> enable
```

```
VSP-9012:1# configure terminal
```

Create a new user group:

```
VSP-9012:1(config)# snmp-server group Grouptest1 auth-priv auth-priv
```

Variable definitions

Use the data in the following table use the `snmp-server group` command.

Table 31: Variable definitions

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.

Variable	Value
group WORD<1-32> WORD<1-32>	The first WORD<1–32> specifies the group name for data access. The range is 1–32 characters. Use the no operator to remove this configuration. The second WORD<1–32> specifies the context name. The range is 1–32 characters. 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<1-32>	Specifies the view name in the range of 0–32 characters.
read-view WORD<1-32>	Specifies the view name in the range of 0–32 characters.
write-view WORD<1-32>	Specifies the view name in the range of 0–32 characters.

Creating a new entry for the MIB in the view table

Before you begin

- You must log on to Global Configuration mode in ACLI.

About this task

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

Create a new entry:

```
snmp-server view WORD<1-32> WORD<1-32>
```

Example

```
VSP-9012:1> enable
```

```
VSP-9012:1# configure terminal
```

Create MIB views:

```
VSP-9012:1(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 32: 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

Before you begin

- You must log on to Global Configuration mode in ACLI.

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 to access the system using an SNMP-based management software.

Procedure

Create a community:

```
snmp-server community WORD<1-32> [group WORD<1-32>] [index
WORD<1-32>] [secname WORD<1-32>]
```

Important:

You cannot use the `@` character or the string `::` when you create community strings.

Example

```
VSP-9012:1> enable
```

```
VSP-9012:1# configure terminal
```

```
VSP9012:1(config)# snmp-server community third secname public
```

Variable definitions

Use the data in the following table to use the `snmp-server community` command.

Table 33: 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

Before you begin

- You must log on to Global Configuration mode in ACLI.

About this task

Add a user to a group to logically group users who require the same level of access.

Procedure

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

```
VSP-9012:1> enable
```

```
VSP-9012:1# configure terminal
```

Add a user to a group to logically group users who require the same level of access:

```
VSP-9012:1(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 34: 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, des, or 3des. *WORD<1-32>* assigns a privacy password. If no value is entered, no privacy capability exists. The range is 1–32 characters. **Important:** You must set authentication before you can set the privacy option.
engine-id *WORD<1-32>*	Assigns an SNMPv3 engine ID. The range is 10–64 characters. 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<1-32>	Specifies the view name in the range of 0–32 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<1-32>	Specifies the view name in the range of 0–32 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<1-32>	Specifies the view name in the range of 0–32 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

Before you begin

- You must log on to Global Configuration mode in ACLI.

About this task

Disable SNMP by using the SNMP block flag. By default, SNMP access is enabled.

Procedure

Disable SNMP:

```
boot config flags block-snmp
```

Example

```
VSP-9012:1> enable
```

```
VSP-9012:1# configure terminal
```

Disable SNMP:

```
VSP-9012:1(config)# boot config flags block-snmp
```

Variable definitions

Use the data in the following table to use the `boot config flags` command.

Table 35: 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

About this task

Display SNMP system information to view trap and authentication profiles. For a comprehensive set of SNMP-related `show` commands, see *Avaya Virtual Services Platform 9000 Commands Reference — ACLI*, NN46250–104.

Procedure

Display SNMP system information:

```
show snmp-server
```

Example

```
VSP-9012:1>show snmp-server

                 trap-sender :
           force-trap-sender : FALSE
          force-iphdr-sender : FALSE
           agent-conformance : DISABLED
                     contact : http://support.avaya.com/
                    location : 211 Mt. Airy Road,Basking Ridge,NJ 07920
                        name : VSP-9012
          AuthenticationTrap : false
            LoginSuccessTrap : false
                   bootstrap : unknown level
```

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.

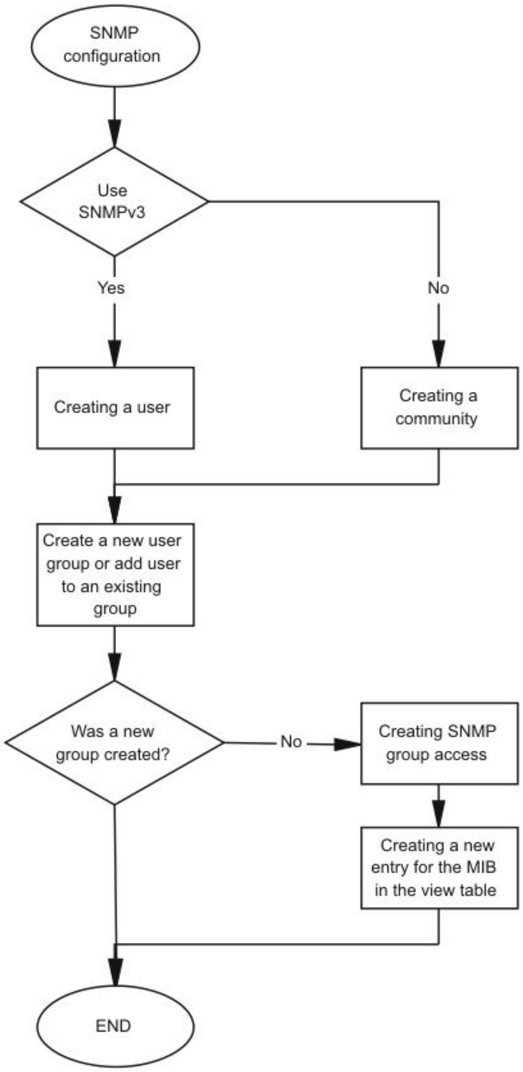

SNMP configuration
Use SNMPv3
Yes
No
Creating a user
Creating a community
Create a new user group or add user to an existing group
Was a new group created?
No
Creating SNMP group access
Creating a new entry for the MIB in the view table
END

Figure 10: 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 ACLI 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 tree, open 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.

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.

Name	Description
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 Avaya Virtual Services Platform 9000 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 *Avaya Virtual Services Platform 9000 Administration*, NN46250–600.

Procedure

1. In the navigation tree, open the following folders: **Configuration** > **Security** > **Control Path**.
2. Click **Access Policies**.
3. Click the **Access Policies-SNMP Groups** tab.
4. Click **Insert**.
5. Beside the **ID** box, click the ellipsis (**...**) button.
6. Select a policy ID from the ID list, and then click **Ok**.
7. In the **Name** box, type a name.
8. From the **Model** options, select a security model.
9. 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	Description
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.

Name	Description
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 Avaya Virtual Services Platform 9000 using an SNMP-based management software.

Procedure

1. In the navigation tree, open 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.

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 7: Customer service

Visit the Avaya Web site to access the complete range of services and support that Avaya provides. Go to www.avaya.com or go to one of the pages listed in the following sections.

Getting technical documentation

To download and print selected technical publications and release notes directly from the Internet, go to www.avaya.com/support.

Getting product training

Ongoing product training is available. For more information or to register, you can access the Web site at www.avaya.com/support. From this Web site, you can locate the Training contacts link on the left-hand navigation pane.

Getting help from a distributor or reseller

If you purchased a service contract for your Avaya product from a distributor or authorized reseller, contact the technical support staff for that distributor or reseller for assistance.

Getting technical support from the Avaya Web site

The easiest and most effective way to get technical support for Avaya products is from the Avaya Technical Support Web site at www.avaya.com/support.

Glossary

American Standard Code for Information Interchange (ASCII)
A code for representing 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.

authenticator
Software on Virtual Services Platform 9000 that authorizes or rejects a supplicant, such as a PC, attached to the other end of a LAN segment.

Avaya command line interface (ACLI)
A textual user interface. When you use ACLI, you respond to a prompt by typing a command. After you enter the command, you receive a system response.

Control Processor Unit High Availability (CPU-HA)
Activates two CP modules simultaneously. The CP modules exchange topology data so, if a failure occurs, either CP module can take precedence in less than 1 second with the most recent topology data.

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.

controlled port
In relation to EAPoL, any port on the device with EAPoL enabled.

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.

Extensible Authentication Protocol over LAN (EAPoL)
A port-based network access control protocol. EAPoL provides security in that it prevents users from accessing network resources before they are authenticated.

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 The Data Link Layer of the OSI model. Examples of Layer 2 protocols are Ethernet and Frame Relay.

Layer 3 The Network Layer of the OSI model. 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) Defines system operations and parameters used for the Simple Network Management Protocol (SNMP).

mask A bit string that is used 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.

next hop The next hop to which a packet can be sent to advance the packet to the destination.

Packet Capture Tool (PCAP) A data packet capture tool that captures ingress and egress (on Ethernet modules only) packets on selected ports. You can analyze captured packets for troubleshooting purposes.

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 given layer and that consists of protocol-control information of the given layer and possibly user data of that layer.

quality of service (QoS) Use QoS features to reserve resources in a congested network. For example, you can configure a higher priority to IP deskphones, which need a fixed bit rate, and, split the remaining bandwidth between data connections if calls in the network are important than the file transfers.

Read Write All (RWA) An access class that lets users access all menu items and editable fields.

Remote Authentication Dial-in User Service (RADIUS) A protocol that authenticates, authorizes, and accounts for remote access connections that use dial-up networking and Virtual Private Network (VPN) functionality.

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. The RIP is most often used as a very simple IGP within small networks.

Secure Copy (SCP) Securely transfers files between the switch and a remote station.

Simple Network Management Protocol (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-based policies (UBP) Establishes and enforces roles and conditions on an individual user basis for access ports in 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.

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.