Avaya Virtual Services Platform 7000 Series Configuration Security

10.0
NN47202-501, 01.02
August 2011

© 2011 Avaya Inc.

All Rights Reserved.

Notice

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

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

Licenses

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

Copyright

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

Third-party components

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

Trademarks

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

Avaya is a registered trademark of Avaya Inc.

All other trademarks are the property of their respective owners.

Downloading documents

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

Contact Avaya Support

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

Contents

Chapter 1: New in this Release 5
Chapter 2: Security fundamentals 7
Summary of security features 7
IP Manager 8
User access limitations 8
Password security 9
Custom user names and passwords 9
Password length and valid characters 9
Password retry 10
Password history 10
Password display 10
Password verification 10
Password aging time 10
Logon failure timeout 11
Default passwords 11
Password security enabled or disabled 11
Simple Network Management Protocol 12
SNMP versions 12
SNMP MIB support 13
SNMP trap support 14
SNMP interaction with other features 16
Applications and MIB filenames 16
Chapter 3: User access configuration using ACLI 19
Enabling or disabling password security 19
Creating user names and passwords 19
Configuring password retry attempts 21
Configuring password history 21
Restoring password history to default 22
Displaying password history settings 22
Setting the read-only and write-only passwords 23
Enabling or disabling passwords 23
Enabling or disabling IP Manager 24
Configuring the IP Manager list 25
Removing IP Manager list entries 26
Displaying IP Manager settings 27
Chapter 4: SNMP configuration using ACLI 29
Displaying the SNMP server configuration 29
Enabling SNMP server access 30
Disabling SNMP server access 30
Configuring read or write SNMP server community access 31
Clearing SNMP server community read or write access 32
Configuring an SNMP server system contact 32
Adding or deleting an SNMP trap receiver 33
Displaying SNMP trap destination information 35

Displaying SNMP trap notification information 35
Enabling or disabling SNMP trap notifications 35
Configuring the SNMP system location value 36
Configuring the SNMP system name 37

Chapter 1: New in this Release

This is a new document for Virtual Services Platform 7000 Series Release 10.0.

Comments? infodev@avaya.com

Chapter 2: Security fundamentals

This chapter provides conceptual information about the security features supported by the Avaya Virtual Services Platform 7000 Series to restrict access to your network.

Summary of security features

The tables in this section provide summary information about some of the security features available with the Avaya Virtual Services Platform 7000 Series.

Table 1: Password Authentication security

Password Authentication	Description
Description	Security feature.
What is being secured	User access to a switch or stack.
Layer	Not applicable.
Level of Security	Provides Read Only/Read Write access. The access rights are checked against Local Password.
Violations	Not applicable.
Configuring using interfaces	Console, ACLI, ASCII configuration file.
Restrictions and Limitations	Not applicable.

Table 2: IP Manager security

IP Manager	Description
Description	IP Manager is an extension of Telnet. It provides an option to enable/disable access for TELNET (Telnet On/Off), SNMP (SNMP On/Off), and Web Page Access (Web On/Off) with or without a list of 50 Ipv4 and 50 Ipv6 addresses and masks. **Note:** The IPv6 parameter is valid only for switches that support IPv6.
What is being secured	User access to the switch through Telnet, SNMP, or Web.

IP Manager	Description
Per-Port or Per Switch	For each switch.
Layer	IP.
Level of Security	Access.
Violations	User is not allowed to access the switch.
Requirements for Setup	Optional IP Addresses/Masks, Individual Access (enable/ disable) for TELNET, SNMP, or Web Page.
Configuring using interfaces	Console and ACLI.
Restrictions and Limitations	Not applicable.

IP Manager

You can limit access to the management features of the Avaya Virtual Services Platform 7000 Series by defining the IP addresses that are allowed access to the switch.

Important:

To avoid locking a user out of the switch, Avaya recommends that you configure ranges of IP addresses that are allowed to access the switch.

With IP Manager, you can do the following:

- Define a maximum of 50 Ipv4 addresses, and masks that are allowed to access the switch. No other source IP addresses have management access to the switches.
- Enable or disable access to Telnet and SNMP.

Changes you make to the IP Manager list are reflected only after you restart the system. The sessions that were open at the time of configuring the IP Manager list remain unaffected.

User access limitations

Using ACLI, an administrator can limit user access through the creation and maintenance of passwords for Telnet and Console access. This is a two-step process that requires first creating the password and then enabling it.

You must be in the Global Configuration mode in ACLI to perform these tasks.

Note:

When you set a *username* and *password* to default, the change is only applied to the switch on which the command was run.

Password security

The Avaya Virtual Services Platform 7000 Series provides password security through a variety of mechanisms. The switch supports both default and customized user names and passwords for accessing a switch with read-only or read-write access, and it supports password security for SNMP access.

The following is a list of the types of password security provided by the switch:

- default switch read-only user name and password
- default switch read-write user name and password
- customized user names and passwords for read-only switch
- customized user names and passwords for read-write switch
- read-only community string (display limitation feature only)
- read-write community string (display limitation feature only)

Custom user names and passwords

The switch provides the ability to create custom user names and passwords for accessing the switch or stack. User names and associated passwords can be defined at any time but only come into effect when password security is enabled. User names and passwords are created only by a user with read-write privileges.

Custom users and passwords cannot have specialized access conferred to them. Custom users have the same privileges as the default read-only or read-write access user. The read-only and read-write passwords cannot be the same.

Password length and valid characters

Valid passwords are between 10 and 15 characters long. The password must contain a minimum of the following:

- 2 lowercase letters
- 2 capital letters

- 2 numbers
- 2 special symbols. For example, !@#$%^&*().

Passwords are case sensitive.

Password retry

If a user fails to provide the correct password after a number of consecutive retries, the switch resets the logon process.

You can configure the maximum number of retries using the Console Interface (TELNET/ SNMP/ Web Access, Login Retries field) or ACLI. The default maximum number of retries is 3.

Password history

The switch stores a maximum of the last 10 passwords used. Stored passwords are not reusable.

Password display

When you type a password, it is not displayed as clear text. Each character of the password is substituted with an asterisk (*****).

Password verification

New passwords must be verified before use. If the two passwords do not match, the password update process fails. In this case, the password change process starts over. There is no limit to the number of password change attempts.

Password aging time

Passwords expire after a specified aging period. The aging period is configurable, with a range of 1 day to approximately 7.5 years (2730 days). The default is 180 days. When a password has aged out, the user is prompted to create a new password. Only users with a valid read-write password can create a new password.

Logon failure timeout

Log on failure timeouts prevent brute force hacking. Following three consecutive password log on failures, all password logon interfaces are disabled for 60 seconds. Logon failure timeouts disable the serial port, Telnet, and Web interfaces.

Log on failure timeouts affect only new log on sessions and do not interfere with sessions already in progress.

Default passwords

For the non-SSH image, the default password for the read–only user is ***user***, and the default password for the read–write user is ***secure***. If your switch supports the SSH software image, the default password for the read–only user is ***userpasswd***, and the default password for the read–write user is ***securepswd*** .

Password security enabled or disabled

By default, password security is disabled for the non-SSH software image. If your switch supports the SSH software image, password security is enabled.

You can enable password security using ACLI only. When password security is enabled, the following occurs:

- Current passwords remain unchanged if they meet the required specifications. If they do not meet the required specifications, the user is prompted to change them to passwords that do meet the requirements.
- An empty password history bank is established. The password bank stores has the capacity to store up to 10 previously used passwords.
- Password verification is required.

You can disable password security using ACLI only. When password security is disabled, the following occurs:

- Current passwords remain valid.
- Password history bank is removed.
- Password verification is not required.

Simple Network Management Protocol

The Avaya Virtual Services Platform 7000 Series supports Simple Network Management Protocol (SNMP).

SNMP is traditionally used to monitor Unix systems, Windows systems, printers, modem racks, switches, routers, power supplies, Web servers, and databases. Any device running software that allows the retrieval of SNMP information can be monitored.

You can also use SNMP to change the state of SNMP-based devices. For example, you can use SNMP to shut down an interface on your switch.

SNMP versions

The SNMP agent for the Avaya Virtual Services Platform 7000 Series supports exchanges using SNMPv1, and SNMPv2c . The following sections provide descriptions for each of these SNMP versions.

SNMP Version 1 (SNMPv1)

SNMP Version 1 (SNMPv1) is an older version of the SNMP protocol that is defined in RFC 1157 and is an Internet Engineering Task Force (IETF) standard. SNMPv1 security is based on communities, which are simply plaintext password strings that allow an SNMP-based application, that knows these strings, to gain access to the management information for a device.

SNMPv1 uses a proprietary method for configuring SNMP communities and trap destinations for specifying SNMPv1 configuration. This proprietary method includes the following:

- A single read-only community string that can only be configured using the console menus.
- A single read-write community string that can only be configured using the console menus.
- Up to four trap destinations and associated community strings that can be configured either in the console menus, or using SNMP Set requests on the s5AgTrpRcvrTable.

SNMP Version 2 (SNMPv2)

SNMP Version 2 (SNMPv2) is also an older version of the SNMP protocol, which is called SNMPv2c, as defined in RFC 1905, RFC 1906, and RFC 1907. SNMPv2c introduces a standards-based GetBulk retrieval capability using SNMPv1 communities.

SNMP MIB support

The Avaya Virtual Services Platform 7000 Series supports an SNMP agent with industry-standard Management Information Bases (MIB) as well as private MIB extensions, which ensures compatibility with existing network management tools.

Supported MIBs

The IETF standard MIBS supported on the switch include MIB-II (originally published as RFC 1213, then split into separate MIBs as described in RFCs 4293, 4022, and 4113), Bridge MIB (RFC 4188), and the RMON MIB (RFC 2819), which provides access to detailed management statistics.

The following table lists supported SNMP standard MIBs.

MIB	RFC	File name
IF-MIB	2863	rfc2863.mib
SNMPv2-MIB	3418	rfc3418.mib
EtherLike-MIB	2665	rfc2665.mib
ENTITY-MIB	2737	rfc2737.mib
P-BRIDGE-MIB	4363	rfc4363-p.mib
Q-BRIDGE-MIB	4363	rfc4363-q.mib
IEEE8021-PAE-MIB	n/a	eapol-d10.mib
SMIv2-MIB	2578	rfc2578.mib
SMIv2-TC-MIB	2579	rfc2579.mib
SNMPv2-MIB	3418	rfc3418.mib
SNMP-FRAMEWORK-MIB	3411	rfc3411.mib
SNMP-MPD-MIB	3412	rfc3412.mib
SNMP-NOTIFICATION-MIB	3413	rfc3413-notif.mib
SNMP-TARGET-MIB	3413	rfc3413-tgt.mib
SNMP-USER-BASED-MIB	3414	rfc3414.mib
SNMP-VIEW-BASED-ACM-MIB	3415	rfc3415.mib
SNMP-COMMUNITY-MIB	3584	rfc3584.mib

The following table lists supported SNMP proprietary MIBs.

MIB	File name
S5-AGENT-MIB	s5age.mib

MIB	File name
S5-CHASSIS.MIB	s5cha.mib
S5-CHASSIS-TRAP.MIB	s5ctr.trp
S5-ETHERNET-TRAP.MIB	s5etr.trp
RAPID-CITY-MIB	rapidCity.mib
S5-SWITCH--MIB	s5sbs.mib
BN-IF-EXTENSIONS-MIB	s5ifx.mib
BN-LOG-MESSAGE-MIB	bnlog.mib
S5-ETH-MULTISEG-TOPOLOGY-MIB	s5emt.mib
NTN-QOS-POLICY-EVOL-PIB	pibNtnEvol.mib
BAY-STACK-NOTIFICATIONS-MIB	bsn.mib

SNMP trap support

With SNMP management, you can configure SNMP traps (on individual ports) to be generated automatically for conditions such as an unauthorized access attempts or changes in port operating status. You can use ACLI to specify a custom SNMP trap port when a new host receiver is added. The SNMP trap port is stored in NVRAM so that the trap port is saved across switch and stack reboots. The SNMP trap port value is shared among all the units in the stack.

You can configure traps using the SNMPv1 or SNMPv2c format. If you do not identify the SNMP version, the system formats the traps in the SNMPv1 format. A community string can be entered if the system requires one.

The switch supports both industry-standard SNMP traps, as well as private Avaya enterprise traps.

The following table lists supported SNMP traps.

Trap name	Configurable	Sent when
RFC 2863 (industry standard):		
linkUp	For each port	A port link state changes to up.
linkDown	For each port	A port link state changes to down.
RFC 3418 (industry standard):		
authenticationFailure	System wide	An SNMP authentication failure.

Comments? infodev@avaya.com

Trap name	Configurable	Sent when
coldStart	Always on	The system is powered on.
warmStart	Always on	The system restarts due to a management reset.
s5CtrMIB (Avaya proprietary traps):		
s5CtrUnitUp	Always on	A unit is added to an operational stack.
s5CtrUnitDown	Always on	A unit is removed from an operational stack.
s5CtrHotSwap	Always on	A unit is hot-swapped in an operational stack.
s5CtrProblem	Always on	• Base unit fails. • AC power fails or is restored. • RPSU (DC) power fails or is restored. • Fan fails or is restored.
s5EtrSbsMacAccessViolation	Always on	A MAC address security violation is detected.
entConfigChange	Always on	Any hardware change—unit added or removed from stack, GBIC inserted or removed.
risingAlarm fallingAlarm	Always on	An RMON alarm threshold is crossed.
bsnConfigurationSavedToNvram	Always on	Each time the system configuration is saved to NVRAM.
bsnEapAccessViolation	Always on	An EAP access violation occurs.
bsnStackManagerReconfiguration	System-wide	A stack is configured.
RAPID-SPANNING-TREE-MIB:		
nnRstGeneralEvent	Always on	Any general event, such as protocol up or protocol down, occurs.
nnRstErrorEvent	System-wide	Any error event occurs. Error events include memory failure, buffer failure, protocol migration, new root, and topology change.

Trap name	Configurable	Sent when
nnRstNewRoot	System-wide	A new root bridge is selected in the topology.
nnRstTopologyChange	System-wide	A topology change is detected.
nnRstProtocolMigration	For each port	Port protocol migration occurs.

SNMP interaction with other features

This section provides information about how SNMP interacts with other switch features.

If your switch supports Dynamic Host Control Protocol (DHCP) and DHCP is disabled globally, SNMP traps for DHCP Snooping cannot be generated.

Applications and MIB filenames

The following table shows supported applications, related MIBs, and the MIB filenames.

Table 3: Application and related MIBs

Application	Related MIBs	File name
Autotopology	S5-ETH-MULTISEGTOPOLOGY-MIB	s5emt.mib
	S5-SWITCH--MIB	s5sbs.mib
MIB-2	RFC1213-MIB	rfc1213.mib
MultiLink Trunking (MLT)	RAPID-CITY-MIB (rcMlt group)	rcMlt.mib
RMON-MIB	RMON-MIB	rfc2819.mib
Spanning Tree	BRIDGE-MIB	rfc4188.mib
System log	BN-LOG-MESSAGE-MIB	bnlog.mib
VLAN	RAPID-CITY-MIB (rcVlan group)	rcVlan.mib

Comments? infodev@avaya.com

Table 4: New MIBs

MIB name	RFC	File name
BAY-STACK-ERRORMESSAGE-MIB	1271	Rfc1271.mib

Comments? infodev@avaya.com

Chapter 3: User access configuration using ACLI

You can use the information in this chapter to configure and manage user access limitations for the Avaya Virtual Services Platform 7000 Series.

Enabling or disabling password security

Use this procedure to enable or disable password security for the switch.

Before you begin

Use this command in the Global Configuration mode.

Procedure

Enter the following command:

```
[no] password security
```

Variable definitions

The following table describes the parameters for the **`password security`** command.

Variable	Value
[no]	Disables password security for the switch.

Creating user names and passwords

Use this procedure to create custom user names and assign read-only and read-write passwords to the user names.

These custom user names apply to local authentication only.

Before you begin

Use this command in the Global Configuration mode.

Procedure

Enter the following command:

```
username <user_name> {ro | rw}
```

Next steps

After entering this command, the switch prompts you to enter a password for the new user. For more information about rules regarding password length and composition, see the *Password length and valid characters*.

Custom users cannot have custom access rights and limitations. Use of the associated read-only password confers the same rights and limitations as the default read-only user. Use of the associated read-write password confers the same rights and limitation as the default read-write user. For more information, see *Default password and default password security* and *Summary of password security features and requirements* .

Variable definitions

The following table describes the parameters for the **username** command.

Variable	Value
<user_name>	Specifies the character string you use for the custom user name.
ro|rw	Specifies the read-only (ro) user name or the read-write (rw) user name. The *ro|rw* variable is optional. If you omit this variable, the command applies to both read-only and read-write users.

Comments? infodev@avaya.com

Configuring password retry attempts

Use this procedure to configure the number of times a user can retry a password.

Before you begin

Use this command in either the Global or Interface Configuration mode.

Procedure

Enter the following command:

```
telnet-access retry <number>
```

Variable definitions

The following table describes the parameters for the **`telnet-access retry`** command.

Variable	Value
<*number*>	Specifies a value ranging from 1 to 100 for the allowed number of failed logon attempts. The default value is 3.

Configuring password history

Use this procedure to

Before you begin

Use this command in the Global Configuration mode.

Procedure

Enter the following command:

```
password password-history <3-10>
```

Variable definitions

The following table describes the parameters for the **password password-history** command.

Variable	Value
<3-10>	Specifies the number of passwords to store in the history table.

Restoring password history to default

Use this procedure to return the number of passwords stored in the password history table to the default value of 3.

Before you begin

Use this command in the Global Configuration mode.

Procedure

Enter the following command:

```
default password password-history
```

Displaying password history settings

Use this procedure to display the number of passwords currently stored in the password history table.

Before you begin

Use this command in the Privileged EXEC Configuration mode.

Procedure

Enter the following command:

```
show password password-history
```


Comments? infodev@avaya.com

Setting the read-only and write-only passwords

Use this procedure to set the read-only and read-write passwords.

Before you begin

Use this command in the Privileged EXEC Configuration mode.

About this task

The first step to requiring password authentication when the user logs in to the switch is to edit the password settings.

Procedure

Enter the following command:

```
cli password {read-only | read-write} <password>
```

Variable definitions

The following table describes the parameters for the **`cli password`** command.

Variable	Value
{read-only | read-write}	Specifies if the password is for read-only access or read-write access.
<password>	Specifies the character string for the password.

Enabling or disabling passwords

Use this procedure to enable or disable passwords.

Before you begin

Use this command in the Privileged EXEC Configuration mode.

About this task

After the read-only and read-write passwords are set, they can be individually enabled or disabled for the various switch access methods. When enabled, password security prompts you for a password and the value is hidden.

Procedure

Enter the following command:

```
cli password {telnet | serial} {none | local }
```

Variable definitions

The following table describes the parameters for the **`cli password`** command.

Variable	Value
{telnet | serial}	Specifies if the password is enabled or disabled for Telnet or the console.
{none | local}	Specifies if the password is to be disabled (none), or if the password to be used is the locally stored password created in *Setting the read-only and write-only passwords*.

Enabling or disabling IP Manager

Use this procedure to enable or disable the control of Telnet and SNMP access using IP Manager.

Before you begin

Use this command in the Global Configuration mode.

Procedure

Enter the following command:

```
[no] ipmgr {telnet|snmp}
```

Variable definitions

The following table describes the parameters for the **`ipmgr`** command.

Variable	Value
[no]	Disables IP Manager.

Comments? infodev@avaya.com

Variable	Value
snmp	Enables the IP Manager list check for SNMP, including Enterprise Device Manager.
telnet	Enables the IP Manager list check for Telnet access.

Configuring the IP Manager list

Use this procedure to list specific source IPv4 or IPv6 addresses that can access a switch or stack when IP Manager is enabled.

Before you begin

Use this command in the Global Configuration mode.

Procedure

1. Enter the following command to list specific source IPv4 addresses:
   `ipmgr source-ip <list ID> <Ipv4addr> [mask <mask>]`
2. Enter the following command to list specific source IPv6 addresses:
   `ipmgr source-ip <list ID> <Ipv6addr/prefix>`

Note:
The IPv6 parameter is valid only for switches that support IPv6.

Variable definitions

The following table describes the parameters for the **`ipmgr source-ip`** command.

Variable	Value
<list ID>	Specifies a value ranging from 1 to 50 that uniquely identifies the Ipv4 entry in the IP Manager list. **OR** Specifies a value ranging from 51 to 100 that uniquely identifies the Ipv6 entry in the IP Manager list.

Variable	Value
	Note: The IPv6 parameter is valid only for switches that support IPv6.
<*Ipv4addr*>	Specifies the source IPv4 address from which access is allowed.
mask<*mask*>	Specifies the subnet mask from which access is allowed.
<*Ipv6addr/prefix*>	Specifies the source IPv6 address and prefix from which access is allowed. **Note:** The IPv6 parameter is valid only for switches that support IPv6.

Removing IP Manager list entries

Use this procedure to deny access to the switch or stack for specified source IPv4 or IPv6 addresses.

Before you begin

Use this command in the Global Configuration mode.

About this task

The command sets both the IP address and mask for the specified entry to 255.255.255.255 for Ipv4 entries and to ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff/128 for Ipv6 entries. If you do not specify a <*list ID*> value, the command resets the whole list to factory defaults.

Note:
The IPv6 parameter is valid only for switches that support IPv6.

Procedure

Enter the following command:

```
no ipmgr source-ip [<list ID>]
```


Comments? infodev@avaya.com

Variable definitions

The following table describes the parameters for the **no ipmgr source-ip** command.

Variable	Value
<list ID>	Specifies a value ranging from 1 to 50 that uniquely identifies the Ipv4 entry in the IP Manager list. **OR** Specifies a value ranging from 51 to 100 that uniquely identifies the Ipv6 entry in the IP Manager list. **Note:** The IPv6 parameter is valid only for switches that support IPv6.

Displaying IP Manager settings

Use this procedure to display information about the IP Manager list.

Before you begin

Use this command in the Privileged EXEC Configuration mode.

About this task

The command displays the following information:

- If Telnet, SNMP, and Web access are enabled.
- Whether the IP Manager list is being used to control access to Telnet and SNMP.
- The current IP Manager list configuration.

Procedure

Enter the following command:

```
show ipmgr
```

Comments? infodev@avaya.com

Chapter 4: SNMP configuration using ACLI

You can use the information in this chapter to monitor devices running software that supports the retrieval of SNMP information.

Displaying the SNMP server configuration

Use this procedure to display SNMP server configuration information.

Before you begin

Use this command in the Privileged EXEC Configuration mode.

Procedure

Enter the following command:

```
show snmp-server {host|user|view}
```

Variable definitions

The following table describes the parameters for the **`show snmp-server`** command.

Variable	Value
host	Displays the trap receivers configured in the SNMPv3 MIBs.
user	Displays the SNMPv3 users, including views accessible to each user.
view	Displays SNMPv3 views.

Enabling SNMP server access

Use this procedure to enable SNMP server access to the switch.

Before you begin

Use this command in the Global Configuration mode.

Procedure

Enter the following command:

```
snmp-server enable
```

Disabling SNMP server access

Use this procedure to disable SNMP server access to the switch.

Important:
If you disable SNMP server access to the switch, you cannot use Enterprise Device Manager (EDM) for the switch.

Before you begin

Use this command in the Global Configuration mode.

Procedure

Enter either of the following commands:

```
snmp-server disable
```

OR

```
no snmp-server
```

Configuring read or write SNMP server community access

Use this procedure to configure a single read-only or a single read-write community string for SNMPv1 and SNMPv2c access.

Before you begin

Use this command in the Global Configuration mode.

About this task

The community strings created by this command are controlled by the SNMP Configuration screen in the console interface. These community strings have a fixed MIB view.

Procedure

Enter the following command:

```
[default] snmp-server community [ro|rw]
```

Variable definitions

The following table describes the parameters for the **`snmp-server community`** command.

Variable	Value
[default]	Restores the read-only (ro) community to **Public**, or the read-write (rw) community to **Private**.
ro|*rw*	Specifies read-only (ro) or read-write (rw) access for an SNMP server community. When you select either *ro* or *rw* access for an SNMP community, the switch prompts you to enter and confirm a community string. If you do not specify read-only or read-write access for an SNMP server community, the switch applies the default value (read-only). Stations with read-only access can only retrieve MIB objects and stations with read-write access can retrieve, and modify MIB objects.

Clearing SNMP server community read or write access

Use this procedure to clear the SNMP server community read or write access configuration.

Before you begin

Use this command in the Global Configuration mode.

Procedure

Enter the following command:

```
no snmp-server community {ro|rw|}
```

Variable definitions

The following table describes the parameters for the **`no snmp-server community`** command.

Variable	Value
ro|rw	Clears the SNMP server community read—only or write—only access configuration. If you do not specify read-only or read-write, all community strings are removed. If you specify read-only or read-write, then just the read-only or read-write community is removed.

Configuring an SNMP server system contact

Use this procedure to add or remove a contact person name for a managed SNMP server system node.

Before you begin

Use this command in the Global Configuration mode.

Procedure

Enter the following command:

Comments? infodev@avaya.com

```
[default] [no] snmp-server contact <name>
```

Variable definitions

The following table describes the parameters for the **`snmp-server contact`** command.

Variable	Value
default	Restores SNMP server system contact to default.
no	Disables SNMP server system contact.
<name>	Specifies an alphanumeric character string that identifies a contact person for a managed SNMP server system node.

Adding or deleting an SNMP trap receiver

Use this procedure to add SNMP trap receivers to the trap receiver table or remove trap receivers from the table.

Before you begin

Use this command in the Global Configuration mode.

About this task

With the proprietary method, the table has a maximum of four entries, and these entries can generate only SNMPv1 traps. This command controls the contents of the s5AgTrpRcvrTable, which is the set of trap destinations controlled by the SNMP Configuration screen in the console interface.

Using the standards-based SNMP method, you can create several entries in SNMP MIBs. Each can generate v1 or v2c traps.

Important:
Before using the desired community string or user in this command, ensure that it is configured with a notify-view.

Procedure

1. To use the proprietary method, enter the following command:

```
[default] [no] snmp-server host <host-ip> <community-string>
```

2. To use the standards-based SNMP method, enter the following command:

```
[default] [no] snmp-server host <host-ip> [port <trap-port>]
{v1 <community-string> | v2c <community-string> }
```

Variable definitions

The following table describes the parameters for the **`snmp-server host`** command.

Variable	Value
[default]	Clears the SNMP trap receiver table.
host-ip	Specifies the IP address of a host for the trap destination.
community-string	If you use the proprietary method for SNMP, this parameter specifies a community string that works as a password and permits access to the SNMP protocol.
[no]	Deletes the specified SNMP trap receiver from the trap-receiver table.
port<*trap-port*>	Specifies a value for the SNMP trap port between 1 and 65535.
v1<*community-string*>	To configure the standards-based tables, using v1 creates trap receivers in the SNMP MIBs. Multiple trap receivers with varying access levels can be created.
v2c<*community-string*>	To configure the new standards-based tables, using v2c creates trap receivers in the SNMP MIBs. Multiple trap receivers with varying access levels can be created.

Comments? infodev@avaya.com

Displaying SNMP trap destination information

Use this procedure to display the current SNMP host trap destination information.

Before you begin

Use this command in the Privileged EXEC Configuration mode.

Procedure

Enter the following command:

```
show snmp-server host
```

Displaying SNMP trap notification information

Use this procedure to display a list of SNMP trap notification types and the status of each type.

Before you begin

Use this command in the Privileged EXEC Configuration mode.

Procedure

Enter the following command:

```
show snmp-server notification-control
```

Enabling or disabling SNMP trap notifications

Use this procedure to enable or disable SNMP trap notifications by notification type.

Before you begin

Use this command in the Global Configuration mode.

Procedure

Enter the following command:

```
[default] [no] snmp-server notification-control <WORD/1-128>
```

Variable definitions

The following table describes the parameters for the **`snmp-server notification-control`** command.

Variable	Value
[default]	Restores the specified SNMP trap notification to the default value (Disabled).
[no]	Disables the specified SNMP trap notification.
<*WORD/1-128*>	Specifies an alphanumeric description or the OID of a supported notification type.

Configuring the SNMP system location value

Use this procedure to configure the SNMP system location value.

Before you begin

Use this command in the Global Configuration mode.

Procedure

Enter the following command:

```
[default] [no] snmp-server location <location_value>
```

Variable definitions

The following table describes the parameters for the **`snmp-server location`** command.

Variable	Value
[default]	Restores the SNMP system location value to default.
[no]	Clears the SNMP system location value.

Comments? infodev@avaya.com

Variable	Value
<*location_value*>	Specifies an alphanumeric value, with a maximum of 255 characters, for the SNMP system location.

Configuring the SNMP system name

Use this procedure to configure a value for the SNMP system name.

Before you begin

Use this command in the Global Configuration mode.

Procedure

Enter the following command:

```
[default] [no] snmp-server name <name_value>
```

Variable definitions

The following table describes the parameters for the **`snmp-server name`** command.

Variable	Value
[default]	Restores the the SNMP system name to default.
[no]	Clears the SNMP system name.
<*name_value*>	Specifies an alphanumeric value, with a maximum of 255 characters, for the SNMP system name.

Comments? infodev@avaya.com