Virtual Services Platform 7000 Series Getting Started

Release 10.0
NN47202-303, 01.01
August 2011

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: New in this release

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

The Avaya VSP 7000 Series is new and supports the following hardware and software features:

Table 1: VSP 7000 hardware

Hardware	Description
AL700001F-E6	VSP 7024XLS chassis, 24 SFP+, Front 2 Back cooling and software (no power supply)
AL700001B-E6	VSP 7024XLS chassis, 24 SFP+, Back 2 Front cooling and software (no power supply)
Note: You must order power supplies separately. The VSP 7000 Series determines the airflow mode based on the primary power supply installed in the chassis. Ensure that all power supplies and fans have matching airflow modes.	
AL7000A0F-E6	VSP 7000 AC power supply, Front 2 Back cooling (NO PC)
AL7000B0F-E6	VSP 7000 AC power supply, Front 2 Back cooling (EU PC)
AL7000C0F-E6	VSP 7000 AC power supply, Front 2 Back cooling (UK PC)
AL7000D0F-E6	VSP 7000 AC power supply, Front 2 Back cooling (JP PC)
AL7000E0F-E6	VSP 7000 AC power supply, Front 2 Back cooling (NA PC)
AL7000F0F-E6	VSP 7000 AC power supply, Front 2 Back cooling (ANZ PC)
AL7000A0B-E6	VSP 7000 AC power supply, Back 2 Front cooling (NO PC)
AL7000B0B-E6	VSP 7000 AC power supply, Back 2 Front cooling (EU PC)
AL7000C0B-E6	VSP 7000 AC power supply, Back 2 Front cooling (UK PC)
AL7000D0B-E6	VSP 7000 AC power supply, Back 2 Front cooling (JP PC)
AL7000E0B-E6	VSP 7000 AC power supply, Back 2 Front cooling (NA PC)
AL7000F0B-E6	VSP 7000 AC power supply, Back 2 Front cooling (ANZ PC)
AL7000A1F-E6	VSP 7000 DC power supply, Front 2 Back cooling
AL7000A1B-E6	VSP 7000 DC power supply, Back 2 Front cooling
AL7000FTB-E6	VSP 7000 Front 2 Back spare fan trays (includes two fan tray kits)
AL7000BTF-E6	VSP 7000 Back 2 Front spare fan trays (includes two fan tray kits)

Hardware	Description
AL7011001–E6	VSP 7000 four post server rack mount kit
AL2011020–E6	Avaya Red DB-9 female to RJ45 adaptor. • converts DB-9 male port to RJ45 serial port. • can be used with CAT5 RJ45 straight cable for console connection.
AL2011021–E6	Avaya Blue DB-9 male to RJ45 adaptor. • converts DB-9 female port to RJ45 serial port. • can be used with CAT5 RJ45 straight cable for console connection.
AL2011022–E6	Avaya RJ45/DB-9 integrated console cable. 1.5 m cable with DB-9 female port and RJ45 console connection.

Software features:

- 128k MAC address table
- 802.1D compliancy
- 802.1D spanning tree
- ASCII Config Generator (ACG)
- ASCII download enhancements
- Autosave configuration
- Backup config file
- Bootp IPv4 address assignment
- Broadcast / Multicast limiting
- CLI quick start (no menu UI)
- CLI support
- CPU utilization
- DHCP client
- Dual Agent support
- Dual syslog server support
- Factory-default command
- Front 2 Back or Back 2 Front airflow support
- Improved syslog capabilities
- IP Manager (IPMGR)
- Memory utilzation

- Multilink Trunking (MLT)
- MLT enable/disable whole trunk
- MLT scaling 12/2 + 1/4
- Ping command and TFTP file support
- Port mirroring (1:1)
- QoS: 8 hardware queues per port
- QoS: 802.1p support
- QoS: DSCP classification
- QoS: enable/disable
- QoS: queue set support
- Reload command
- RMON scaling
- RMON support
- Show environmental
- Show running-config defaults
- Show running-config specific
- SNMP
- SNMP trap notification
- SONMP
- Syslog support IPv4
- Telnet server IPv4 (max 4 sessions)
- TFTP IPv4 (download image, etc)
- USB ASCII config support

  Note:

  USB functionality in Release 10.0 is a technology demonstration feature only. Avaya has determined that some USB devices can cause the USB port to become unresponsive or unusable. For more information, see *Avaya Virtual Services Platform 7000 Series Release 10.0 Release Notes*, NN47202–400.
- Username password history
- Username password security
- VLAN: 802.1p/Q support
- VLAN: port based VLANs
- Write memory and save config commands

Chapter 2: Getting started fundamentals

Use the concepts described in this section to understand the major features of the VSP 7000 Series and to get up and running as fast as possible.

Quick install

Quick Install allows you to take the first configuration from a file found on a USB device or from a minimal configuration menu. If the switch does not obtain an IP address using BootP and a file named `ip.cfg` exists on the USB device, then the switch loads the `ip.cfg` file as its first configuration.

Note:

USB functionality in Release 10.0 is a technology demonstration feature only. Avaya has determined that some USB devices can cause the USB port to become unresponsive or unusable. For more information, see *Avaya Virtual Services Platform 7000 Series Release 10.0 Release Notes*, NN47202–400.

If the switch cannot find an IP address after you press CTRL + Y from the long console menu then it shows a minimal menu. Quick Configuration encompasses multiple menus consolidating them into a single menu for you to access and make the required initial setup modifications.

You must enter the following information into the menu:

- IP address
- Subnet mask
- Default gateway
- Read-only community string
- Read-write community string
- Quick start VLAN

ACLI command modes

ACLI provides the following command modes:

- User EXEC
- Privileged EXEC
- Global Configuration

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

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

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

Command mode and sample prompt	Entrance commands	Exit commands
User EXEC `7024XLS>`	No entrance command, default mode	exit or logout
Privileged EXEC `7024XLS#`	enable	exit or logout
Global Configuration `7024XLS(config)#`	configure	mode, enter: end or exit To exit ACLI completely, enter: logout

See *Avaya Virtual Services Platform 7000 Series Fundamentals* (NN47202-101) for more information about ACLI command modes.

Supported BootP modes

The VSP 7000 Series supports the Bootstrap protocol (BootP).

BootP enables you to retrieve an ASCII configuration file name and configuration server address.

A properly configured BootP server enables the switch to automatically learn its assigned IP address, subnet mask and the IP address of the default router (default gateway).

The VSP 7000 Series has a unique 48-bit hardware address, or MAC address, that is printed on a label on the back panel. Use this MAC address when you configure the network BootP server to recognize the VSP 7000 Series BootP requests.

The supported BootP modes are:

- BootP or Last Address mode
- BootP When Needed (This is the default mode.)
- BootP Always
- BootP Disabled (Disabling BootP also disables DHCP.)

Autonegotiation

The VSP 7000 Series are autonegotiating devices:

> The term autonegotiation refers to a standardized protocol (IEEE 802.3u or 802.3z or 802.3ab) that exists between two IEEE-capable devices. Autonegotiation enables the switch to select the best speed and duplex modes.

When autonegotiation-capable devices are attached to the VSP 7000 Series, the ports can negotiate down from 1000 Mb/s speed and full-duplex mode until the attached device acknowledges a supported speed and duplex mode. The VSP 7000 Series supports autonegotiation advertisements of 1000 full and flow control.

Note:

Avaya plans to add support for Custom Autonegotiation Advertisements (CANA) features in a future release.

Chapter 3: Connecting to the switch

Chapter 3: Connecting a terminal to the switch

This procedure describes the steps to connect a terminal to the console port on the switch.

Before you begin

- Terminal with AC power cord and keyboard.
- RJ45 serial cable. The maximum length for the console port cable is 25 feet (8.3 meters).

Procedure

1. Connect one end of serial cable to the connector on the terminal.
2. Connect the other end of the serial cable to the console port on the switch.
3. Turn the terminal on.

Chapter 3: Configuring the terminal

Use this procedure to configure terminal settings.

Before you begin

Use this command in the Privileged EXEC mode.

About this task

Note:

The **`show terminal`** command can be used at any time to display the current terminal settings. This command takes no parameters.

Procedure

Enter the following command:

```
terminal speed {2400|4800|9600|19200|38400} length <0-132>
width <1-132>
```

Variable definitions

The following table outlines the parameters of the **`terminal`** command.

Variable	Value
speed {2400|4800| 9600|19200| 38400}	Sets the transmit and receive baud rates for the terminal. The speed can be set at one of the five options shown. DEFAULT: 9600
length	Sets the length of the terminal display in lines. DEFAULT: 23 **Note:** If the terminal length is set to a value of 0, the pagination is disabled and the display continues to scroll without stopping.
width	Sets the width of the terminal display in characters. DEFAULT: 79

Chapter 4: Configuring the management IP address

Use the procedures in this section to assign, clear, and view IP addresses and gateway addresses.

Setting the IP address

Use this procedure to set the IP address and subnet mask for the switch.

Note:

When the IP address or subnet mask is changed, connectivity to Telnet can be lost.

Before you begin

Use this command in the Global Configuration mode.

Procedure

Enter the following command:

```
ip address <A.B.C.D> [netmask <A.B.C.D>] [default-gateway
<A.B.C.D>]
```

Variable definitions

The following table describes the parameters for the **`ip address`** command.

Variable	Value
<A.B.C.D>	Sets the IP address in dotted-decimal notation; netmask is optional.
netmask	Sets the IP subnet mask for the stack or switch.
default-gateway <A.B.C.D>	Sets the IP address of the default gateway.

Obtaining an IP address automatically

Use this procedure to automatically obtain an IP address, subnet mask and default gateway on the switch.

Before you begin

Use this command in the Global Configuration mode.

About this task

When you use DHCP, the switch can also obtain up to three DNS server IP addresses.

Procedure

Enter the following command:

```
ip address source {bootp-always | bootp-last-address | boot-
pwhen- needed | configured-address | dhcp-always | dhcp-last-
address | dhcp-when-needed}
```

Variable definitions

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

Variable	Value
bootp-always	Always use the BootP server.
bootp-last-address	Use the last BootP server.
bootp-when-needed	Use the BootP server when needed. DEFAULT: bootp-when-needed
configured-address	Use the manually configured IP configuration.
dhcp-always	Always use the DHCP server.
dhcp-last-address	Use the last DHCP server.
dhcp-when-needed	Use DHCP client when needed.

Clearing the IP address

Use this procedure to clear the IP address and subnet mask for a switch.

Note:

When the IP address or subnet mask is changed, connectivity to Telnet can be lost. Any new Telnet connection can be disabled and is required to connect to the serial console port to configure a new IP address.

Before you begin

Use this command in the Global Configuration mode.

About this task

This command sets the IP address and subnet mask to all zeros (0).

Procedure

Enter the following command:

```
no ip address
```

Setting the default IP gateway address

Use this procedure to set the default IP gateway address for a switch.

Note:

When the IP gateway is changed, connectivity to Telnet can be lost.

Before you begin

Use this command in the Global Configuration mode.

Procedure

Enter the dotted-decimal IP address of the default IP gateway.

```
ip default-gateway <A.B.C.D>
```

Deleting the default IP gateway address

Use this procedure to delete the default IP gateway.

Note:

When the IP gateway is changed, connectivity to Telnet can be lost.

Before you begin

Use this command in the Global Configuration mode.

Procedure

Enter the following command:

```
no ip default-gateway
```

Set IP parameters using ip.cfg file on a USB memory device

If the switch does not obtain an IP address through BootP, you can load the IP address and optionally new switch software and configuration from the USB memory device using the `ip.cfg` file.

Note:

The file name, `ip.cfg`, is case-insensitive.

If a properly formatted file exists on a USB port, the switch uses that `ip.cfg` as the first option, rather than the last. You can specify one or more of the optional parameters in the `ip.cfg` file. All of the parameters are optional.

Note:

USB functionality in Release 10.0 is a technology demonstration feature only. Avaya has determined that some USB devices can cause the USB port to become unresponsive or unusable. For more information, see *Avaya Virtual Services Platform 7000 Series Release 10.0 Release Notes*, NN47202–400.

The following table describes the `ip.cfg` file parameters:

Parameter	Description
IP <*xx.xx.xx.xx*>	Specifies the IP address for the switch. Example: 192.168.22.1
Mask <*xx.xx.xx.xx*>	Specifies the network mask. Example: 255.255.255.0
Gateway <*xx.xx.xx.xx*>	Specifies the default gateway. Example: 181.30.30.254
SNMPread <*string*>	Specifies the SNMP read community string. Example: public
SNMPwrite <*string*>	Specifies the SNMP write community string. Example: private
VLAN <*number*>	Specifies the management VLAN-ID. Example: VLAN 1
USBdiag <*string*>	Specifies the filename of the diagnostic image to load from the USB. Example: ers5600/ers5600_6.0.0.10.bin
USBascii <*string*>	Specifies the filename of the ASCII config file to load from the USB. Example: customer1.cfg
USBagent <*string*> D NEXTIP, NEXTMask, and NEXTGateway	Specifies the filename of the agent image to load from the USB and specifies IPs for next boot. Example: ers5600/ers5600_6.2.0.0.img

Note:

If you download an ASCII file or diag/image with an `ip.cfg` file, the specific ASCII file or diag/ image must be present on the USB device.

The `ip.cfg` file loads information from the ASCII configuration file in order of precedence. For example, the stack IP becomes 181.30.30.113 no matter what IP address is in the `ip.txt` file if you have an `ip.cfg` file with the following commands:

```
USBascii ip.txt IP 181.30.30.113
Mask 255.255.255.0
Gateway 181.30.30.254
```

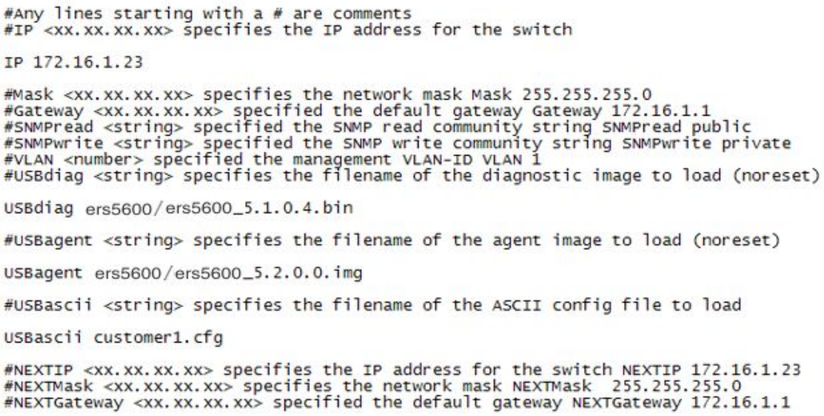
The stack IP will be the IP address defined in the `ip.txt` file if you have an `ip.cfg` file with the following commands:

```
IP 181.30.30.113
Mask 255.255.255.0
Gateway 181.30.30.254
USBascii ip.txt
```

Note:

The `ip.cfg` file runs only on a base or standalone unit. The file cannot be more than 4096 bytes or contain more than 200 lines.

The following figure shows an example of an `ip.cfg` file.



```
#Any lines starting with a # are comments
#IP <xx.xx.xx.xx> specifies the IP address for the switch

IP 172.16.1.23

#Mask <xx.xx.xx.xx> specifies the network mask Mask 255.255.255.0
#Gateway <xx.xx.xx.xx> specified the default gateway Gateway 172.16.1.1
#SNMPread <string> specified the SNMP read community string SNMPread public
#SNMPwrite <string> specified the SNMP write community string SNMPwrite private
#VLAN <number> specified the management VLAN-ID VLAN 1
#USBdiag <string> specifies the filename of the diagnostic image to load (noreset)

USBdiag ers5600/ers5600_5.1.0.4.bin

#USBagent <string> specifies the filename of the agent image to load (noreset)

USBagent ers5600/ers5600_5.2.0.0.img

#USBascii <string> specifies the filename of the ASCII config file to load

USBascii customer1.cfg

#NEXTIP <xx.xx.xx.xx> specifies the IP address for the switch NEXTIP 172.16.1.23
#NEXTMask <xx.xx.xx.xx> specifies the network mask NEXTMask  255.255.255.0
#NEXTGateway <xx.xx.xx.xx> specified the default gateway NEXTGateway 172.16.1.1
```

Figure 1: `ip.cfg` file example

If the `ip.cfg` file specifies an image or agent code, the switch loads the software, even if the same version is already installed on the switch. Ensuring that the appropriate software is always upgraded on the units is the correct operation of `ip.cfg`.

Use the factory default command to reset the switch to the factory default after you insert the USB memory device in the USB port. The USB memory device must contain the properly formatted `ip.cfg` file in the root directory.

Displaying IP-related configuration information

Use this procedure to display the IP configurations, BootP/DHCP mode, switch address, subnet mask, and gateway address.

Before you begin

Use this command in the User EXEC mode.

About this task

This command displays the parameters for what is configured, what is in use, and the last BootP/DHCP. If you do not enter any parameters, this command displays all IPrelated configuration information.

Procedure

Enter the following command:

```
show ip [bootp] [dhcp] [default-gateway] [address]
```

Variable definitions

The following table describes the parameters for the **`show ip`** command.

Variable	Value
bootp	Displays BootP/DHCP-related IP information. The possibilities for status returned are: • BootP Always • BootP or Last Address • BootP When Needed • disabled • DHCP Always • DHCP or Last Address • DHCP When Needed
dhcp client lease	Displays DHCP client lease information. The command displays information about configured lease time and lease time granted by the DHCP server.
default-gateway	Displays the IP address of the default gateway.
address	Displays the current IP address.
address source	Displays the BootP or DHCP client information. The possibilities for status returned are: • BootP Always • BootP or Last Address • BootP When Needed • disabled • DHCP Always

Variable	Value
	• DHCP or Last Address • DHCP When Needed

Chapter 5: Configuring Telnet

Use the procedures in this section to enable Telnet and connect to other switches.

Setting Telnet access

Use this procedure to configure the Telnet connection. Then you can use Telnet to access the ACLI and manage the switch.

Note:

Multiple users can access ACLI system simultaneously, through the serial port, Telnet, and modems. The maximum number of simultaneous users is four, plus, one each at the serial port for a total of 12 users on the stack. All users can configure simultaneously.

Before you begin

- The management port must have an assigned IP address.
- Remote access must be enabled.
- Use this command in the Global Configuration mode.

Procedure

Enter the following command:

```
telnet-access [enable | disable] [login-timeout <1-10>] [retry
<1-100>] [inactive-timeout <0-60>] [logging {none | access |
failures | all}] [source-ip <1-50> <51-100> <A.B.C.D> <WORD>]
[mask <A.B.C.D>]
```

Variable definitions

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

Variable	Value
enable | disable	Enables or disables Telnet connection. DEFAULT: disable

Variable	Value
login-timeout <1-10>	Specify in minutes the time to wait for Telnet and Console login before the connection closes. Enter an integer between 1 and 10.
retry <1-100>	Specify the number of times the user can enter an incorrect password before closing the connection. Enter an integer between 1 and 100.
inactive-timeout <0-60>	Specify in minutes the duration for an inactive session to be terminated.
logging {none | access | failures | all}	Specify the events whose details you want to store in the event log: • none — Do not save access events in the log. • access — Save only successful access events in the log. • failure — Save failed access events in the log. • all — Save all access events in the log.
[source-ip <1-50. <51-50> *<A.B.C.D>*]	Specify the source IP address from which connections are allowed. Enter the IP address in dotted-decimal notation.
mask *<A.B.C.D>*	Specify the subnet mask from which connections are allowed; enter IP mask in dotted-decimal notation.
no telnet-access [source-ip [<1-50>]]	Set the no form of this command, which disables the Telnet connection for an IPv4 address and mask pair. When you do not use the optional parameter, the source-ip list is cleared, meaning the first index is set to 0.0.0.0/0.0.0.0, the second to fiftieth indexes are set to 255.255.255.255/255.255.255.255. When you specify a source-ip address, the specified pair is set to 255.255.255.255/255.255.255.255 for indexes between 1 and 50.
no telnet-access [source-ip [<51-100>]]	Set the no form of this command, which disables the Telnet connection for an IPv6 address and mask pair. When you do not use the optional parameter, the source-ip list is cleared, meaning the fiftyfirst index is set to ::/0, and the fiftysecond

Variable	Value
	to hundredth indexes are set to ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff/128. When you specify a source-ip address, the specified pair is set to ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff/ 128 for indexes between 51 and 100.
default telnet-access	Set the Telnet settings to the default values.

Using ping to communicate with another switch

Use this procedure to determine if communication with another switch can be established.

Before you begin

Use this command in the User EXEC mode.

Procedure

Use the following command to specify the IP address of the unit to test.

```
ping <A.B.C.D> [datasize <64-4096>] [{count <1-9999>} |
continuous] [{timeout | -t} <1-120>] [interval <1-60>] [debug]
```

Variable definitions

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

Variable	Value
<A.B.C.D>	Specify the IP address of the unit to test.
datasize <64– 4096>	Specify the size of the ICMP packet to be sent. The data size range is from 64 to 4096 bytes.
count <1–9999> | continuous	Set the number of ICMP packets to be sent. The continuous mode sets the ping running until the user interrupts it by entering Ctrl +C.
timeout | -t | <1–120>	Set the timeout using either the timeout with the -t parameter followed by the number of seconds the switch must wait before timing out.

Variable	Value
interval <1–60>	Specify the number of seconds between transmitted packets.
debug	Provide additional output information such as the ICMP sequence number and the trip time.

Chapter 6: Configuring the switch

Use the procedures in this section to configure your switch for the first time, copy the configuration to a storage device, or retrieve a saved configuration. There are also procedures for displaying or modifying the current configuration on the switch or for restoring the factory default configuration.

Displaying the stored configurations

Use this procedure to show the configurations currently stored on the switch.

Before you begin

Use this command in the Global Configuration mode.

Procedure

Enter the following command:

```
show nvram block
```

Restoring the factory default configuration

Use this procedure to reset the switch or stack back to its default configuration.

Before you begin

Use this command in the Global Configuration mode.

Procedure

Enter the following command:

```
restore factory-default [-y]
```

The [-y] parameter instructs the switch not to prompt for confirmation.

Copying a configuration to flash memory

Use this procedure to copy the current configuration to one of the flash memory spots.

Before you begin

Use this command in the Global Configuration mode.

Procedure

Enter the following command:

```
copy config nvram block <1-2> name <block_name>
```

Variable definitions

The following table describes the parameters for the **copy config nvram block** command.

Variable	Value
<1–2>	The flash memory location to store the configuration.
name <block_name>	The name to attach to this block. Names can be up to 40 characters in length with no spaces.

Copying a configuration from flash memory

Use this procedure to copy the configuration stored in flash memory at the specified location and make it the active configuration.

Before you begin

Use this command in the Global Configuration mode.

About this task

Substitute <1-2> with the configuration file to load. This command causes the switch to reset so that the new configuration can be loaded.

Procedure

Enter the following command:

```
copy nvram config block <1-2>
```

Restoring a system configuration from a USB device

Use this procedure to restore a configuration file stored on a USB mass storage device.

Note:

USB functionality in Release 10.0 is a technology demonstration feature only. Avaya has determined that some USB devices can cause the USB port to become unresponsive or unusable. For more information, see *Avaya Virtual Services Platform 7000 Series Release 10.0 Release Notes*, NN47202–400.

Before you begin

Use this command in the Privileged EXEC mode.

Procedure

Enter the following command:

```
copy usb config filename <name>
```

Note:

The only parameter for this command is the name of the file to be retrieved from the USB device.

Restoring a system configuration from a TFTP server

Use this procedure to restore a configuration file stored on a TFTP server.

Before you begin

Use this command in the Privileged EXEC mode.

Procedure

Enter the following command:

```
copy tftp config address <A.B.C.D> filename <name>
```

Variable definitions

The following table describes the parameters for the **`copy tftp config`** command.

Variable	Value
address <A.B.C.D>	The IP address of the TFTP server to be used.
filename <name>	The name of the file to be retrieved.

Displaying the current configuration

Use this procedure to display the current configuration of a switch or a stack for switches that support stacking.

Before you begin

Use this command in the Privileged EXEC mode.

Procedure

Enter the following command:

```
show running-config [verbose | module <value>]
```

Note:

If the switch CPU is busy performing other tasks, the output of this command can appear to intermittently start and stop. This is a normal operation to ensure that the switch management tasks receive appropriate priority.

Variable definitions

The following table describes the parameters for the **`show running-config`** command.

Variable	Value
verbose	Displays all the configuration parameters including defaults and non-defaults.
module <value>	Displays the configuration of an application for any of the following parameter values that the switch supports: [banner] [core] [interface] [ip] [ipmgr] [logging] [mlt] [port-mirroring] [qos] [rate-limit] [rmon] [rtc] [snmp] [stp] [vlan] **Note:** Not all switches support the above features.

Copying the running configuration to a TFTP server

Use this procedure to copy the running configuration file to a TFTP server.

Before you begin

Use this command in the Privileged EXEC mode.

Procedure

Enter the following command:

```
copy running-config tftp address {<A.B.C.D> } {[module <value>]
| [verbose]} filename <WORD>
```

Variable definitions

The following table describes the parameters for the **`copy running-config tftp`** command.

Variable	Value
address {<A.B.C.D>}	Specifies the address of the TFTP server to be used: *A.B.C.D* specifies the IP address.
verbose	Copies all the configuration parameters including defaults and non-defaults.
module <value>	Copies the configuration of an application for any of the following parameter values that the switch supports: [banner] [core] [interface] [ip] [ipmgr] [logging] [mlt] [port-mirroring] [qos] [rate-limit] [rmon] [rtc] [snmp] [stp] [vlan] **Note:** Not all switches support the above features.
filename <WORD>	Specifies the name of the file that is created when the configuration is saved to the TFTP server.

Copying the running configuration to a USB device

Use this procedure to copy the running configuration file to a USB mass storage device.

> **Note:**
> USB functionality in Release 10.0 is a technology demonstration feature only. Avaya has determined that some USB devices can cause the USB port to become unresponsive or

unusable. For more information, see *Avaya Virtual Services Platform 7000 Series Release 10.0 Release Notes*, NN47202–400.

Before you begin

Use this command in the Privileged EXEC mode.

Procedure

Enter the following command:

```
copy running-config usb {[module <value>] | [verbose]} filename
<WORD>
```

Variable definitions

The following table describes the parameters for the **`copy running-config usb`** command.

Variable	Value
module <value>	Copies the configuration of an application for any of the following parameter values that the switch supports: [banner] [core] [interface] [ip] [ipmgr] [logging] [macsecurity] [mlt] [port-mirroring] [qos] [rate-limit] [rmon] [rtc] [snmp] [stack] [stp] [vlan] **Note:** Not all switches support the above features.
verbose	Copies all the configuration, including defaults and non-defaults, to the USB.
filename <WORD>	Specifies the name of the file that is created when the configuration is saved to the USB mass storage device.

Downloading a configuration file automatically at startup

Use this procedure to enable a script to be loaded and executed immediately as well as configure parameters to automatically download a configuration file when the switch or stack is booted.

Note:
To view the current switch settings relevant to this process, use **show config-network**.

Before you begin

Use this command in the Privileged EXEC mode.

Procedure

Enter the following command:

```
configure network load-on-boot {disable | use-bootp |
useconfig} address <A.B.C.D> filename <name>>
```

Configuring Autosave

Use this procedure to enable the Autosave feature.

Before you begin

Use this command in the Global Configuration mode.

Procedure

1. To enable Autosave, enter the following command:

   ```
   autosave enable
   ```

   With Autosave enabled the system checks every minute to see if there is any new configuration data. If there is, it will automatically be saved to NVRAM. While Autosave is enabled, the AUR feature should perform normally.

2. To disable Autosave, enter the following command:

   ```
   no autosave enable
   ```

   With Autosave disabled, the unit will not save the new configuration data to NVRAM. The user can use AUR to restore all the configuration data that is configured before the feature is disabled. The user can also restore via AUR all the configuration data that is configured before ACLI command **copy config nvram** is executed. When resetting a stack with Autosave disabled, the stack will form with the configuration from NVRAM of each unit in the stack. The original configuration of a unit should be restored if the user replaces that unit in the stack without having to use the **copy config nvram** command.

Displaying interfaces

Use this procedure to display the current configuration and status of all interfaces or for a specific port. The status of all interfaces on the switch or stack can be viewed, including Multi-Link Trunk membership, link status, autonegotiation and speed.

Before you begin

Use this command in the User EXEC mode.

Procedure

Enter the following command:

```
show interfaces [names] [<portlist>]
```

Displaying hardware information

Use this procedure to display hardware information about the status of the switch.

Procedure

Enter the following command in any command mode:

```
show system [verbose]
```

Note:

The verbose option enables you to display additional information such as fan status, power status, and the switch serial number.

Configuring the Simple Network Management Protocol (SNMP)

Use this procedure to configure SNMP to monitor devices running software that supports the retrieval of SNMP information.

Before you begin

Use these commands in the Global Configuration mode.

Procedure

1. Enter the following command to enable SNMP. (The default setting is disabled.)
   ```
   snmp-server enable
   ```
2. Enable authentication traps.
   ```
   snmp-server authenticationtrap enable
   ```
3. Set the read-only community name (requirement: enter community string twice).
   ```
   snmp-server community ro
   ```
4. Set the read-write community name (requirement: enter community string twice).
   ```
   snmp-server community rw
   ```
5. Set contact information.
   ```
   snmp-server contact "whatever you want"
   ```
6. Set building name and closet information.
   ```
   snmp-server location <Building/Closet-number>
   ```
7. Maintain coherent Syslog messages.
   ```
   snmp-server name <switch_ipaddress>
   ```
8. Set IP address of trap receiver.
   ```
   snmp-server host <host IP>> <community>>
   ```
9. Verify configuration.
   ```
   show sys-info
   ```
10. Verify configuration.
    ```
    show snmp host
    ```

Configuring VLANs and tagged uplinks

Use the following procedure to configure Virtual Local Area Networks (VLAN) and tagged uplinks, .

Before you begin

Use this command in the Global Configuration mode.

Procedure

1. Enter the following command to automatically remove an untagged port from current VLAN and update PVID when the port is added to a different VLAN. (The setting appears at the bottom of the VLAN configuration information.)
   ```
   vlan configcontrol automatic
   ```
2. Enable tagging on the uplink.
   ```
   vlan ports <uplink port> tagging tagall
   ```
3. Discard untagged frames.
   ```
   vlan ports <uplink port> filter-untagged-frame enable
   ```
4. Break Spanning Tree Protocol (STP) for Voice over Internet Protocol (VoIP).
   ```
   vlan ports ALL filter-unregistered-frame disable
   ```
5. Create the port based VLAN and assign the 802.1q identifier.
   ```
   vlan create <vid> type port
   ```
6. Name the VLAN according to conventions.
   ```
   vlan name <vid> <name>
   ```
7. Add ports to appropriate VLANs.
   ```
   vlan members add <vid> <port_listing>
   ```
8. Set the management VLAN.
   ```
   vlan mgmt <vid>
   ```
9. Remove all ports from VLAN 1.
   ```
   vlan members remove 1 ALL
   ```
10. Set the PVID on the uplink.
    ```
    vlan ports <uplink_port> pvid <vid>
    ```
11. Verify VLAN configuration.
    ```
    show vlan
    ```
12. Verify configuration of PVID and port type.

```
show vlan interface info
```

Setting the real-time clock

Use this procedure to set the real-time clock (RTC), providing the switch with time information.

Before you begin

Use this command in the Privileged EXEC mode.

Procedure

Enter the following command:

```
clock set {<LINE> | <hh:mm:ss>}
```

Setting the default clock source

Use this procedure to set the default clock source for the switch.

Before you begin

Use this command in the Global Configuration mode.

Procedure

Enter the following command:

```
clock source {rtc | sysUpTime}
```

Resetting the clock source to factory default

Use this procedure to set the clock source to factory defaults.

Before you begin

Use this command in the Global Configuration mode.

Procedure

Enter the following command:

```
default clock source
```

Configuring boot parameters

Use this procedure to perform a soft-boot of the switch or stack.

Before you begin

Use this command in the Privileged EXEC mode.

Procedure

Enter the following command:

```
boot [default] [partial default]
```

Note:

When you reset to factory defaults, the switch or stack retains the last reset count and reason for last reset; these two parameters do not default to factory defaults. Stack operational mode is retained only when resetting to partial-default.

Configuring DHCP modes

Use this procedure to configure DHCP modes and automatically obtain an IP address, subnet mask and default gateway on the switch or stack. When you use DHCP, the switch or stack can also obtain up to three DNS server IP addresses.

Before you begin

Use this command in the Global Configuration mode.

Procedure

Enter the following command:

```
ip address source {configured-address | dhcp-always | dhcp-lastaddress | dhcp-when-needed}
```

Configuring BootP parameters

Use this procedure to configure BootP on the current instance of the switch or server. This command is used to change the value of BootP from the default value, which is BootPwhen-needed.

Before you begin

Use this command in the Global Configuration mode.

About this task

The BootP default value is BootP-when-needed. This enables the switch to be booted and the system to automatically seek a BootP server for the IP address.

- If an IP address is assigned to the device and the BootP process times out, the BootP mode remains in the default mode of BootP-when-needed.
- If the device does not have an assigned IP address and the BootP process times out, the BootP mode automatically changes to BootP disabled. But this change to BootP disabled is not stored, and the BootP reverts to the default value of BootP-when-needed after rebooting the device.

When the system is upgraded, the switch retains the previous BootP value. When the switch is defaulted after an upgrade, the system moves to the default value of BootP-when-needed.

Procedure

Enter the following command:

```
ip bootp server {always | disable | last | needed}
```

Displaying BootP and DHCP modes

Use this procedure to display the IP configurations, BootP/DHCP mode, stack address, switch address, subnet mask, and gateway address.

Before you begin

Use this command in the User EXEC mode.

Procedure

Enter the following command:

```
show ip [bootp] [dhcp] [default-gateway] [address]
```

Chapter 7: Configuring and testing ports

Use the procedures in this section to configure port features such as the port speed, duplex operation, and autotopology.

Enabling Autotopology

Use this procedure to enable the Autotopology protocol.

Before you begin

Use this command in the Global Configuration mode.

About this task

Autotopology enables a network management system (NMS) to reconstruct the network topology by collecting topology tables from each device that implements the autotopology network management module (NMM) behavior. NMM behavior is comprised of two activities:

- listening for SynOptics Network Management Protocol (SONMP) packets that are used to construct the topology table
- generating SONMP packets that other NMMs are listening for

The switch sends out two types of multicast packets every 10 seconds to all forwarding ports: Flatnet hello and Segment hello. It listens for only one type of multicast, Flatnet hello. The SONMP packets received are used to construct a topology table. The switch supports a maximum of 100 NMM topology table entries and 50 bridge topology table entries.

Procedure

1. Enter the following command:
   ```
   autotopology
   ```
2. To disable Autotopology, enter the following command:
   ```
   no autotopology
   ```
3. To reset Autotopology to the factory default, enter the following command:
   ```
   default autotopology
   ```

Displaying Autotopology settings

Use this procedure to display the global autotopology settings.

Before you begin

Use this command in the Privileged EXEC mode.

Procedure

Enter the following command:

```
show autotopology settings
```

Displaying the Autotopology nmm table

Use this procedure to display the Autotopology network management module (NMM) table.

Before you begin

Use this command in the Privileged EXEC mode.

Procedure

Enter the following command:

```
show autotopology nmm-table
```

Configuring flow control

Use this procedure to control the traffic rates on ports during congestion.

Before you begin

Use this command in the Interface Configuration mode.

Procedure

Enter the following command:

```
flowcontrol [port <portlist>] {asymmetric | symmetric | auto |
disable}
```

Variable definitions

The following table describes the parameters for the `flowcontrol` command.

Variable	Value
port<*portlist*>	Specifies the port numbers to configure for flow control.
asymmetric | symmetric | auto | disable	Sets the mode for flow control: • asymmetric means PAUSE frames can only flow in one direction. • symmetric means PAUSE frames can flow in either direction. • auto sets the port to automatically determine the flow control mode. • disable disables flow control on the port. DEFAULT: auto no flowcontrol [port <*portlist*>] disables flow control. default flowcontrol [port <*portlist*>] set the flow control to auto, which automatically detects the flow control.

Note:

If you omit either of these parameters, the system uses the ports you specified in the interface command but only those ports that have speed set to 1000/full.

Chapter 8: Updating switch software

Use the procedures in this section to update the switch software, which is a necessary part of switch configuration and maintenance.

Before you begin

- The switch has been given a valid IP address.
- A Trivial File Transfer Protocol (TFTP) server is present on the network that is accessible by the switch and that has the desired software version loaded.
- If you change the switch software with software stored on a USB mass storage device, ensure that the mass storage device has the desired software version loaded on it and is inserted into the front panel USB port.

  Note:

  USB functionality in Release 10.0 is a technology demonstration feature only. Avaya has determined that some USB devices can cause the USB port to become unresponsive or unusable. For more information, see *Avaya Virtual Services Platform 7000 Series Release 10.0 Release Notes*, NN47202–400.

- Ensure that ACLI is in Privileged EXEC mode.

About this task

The VSP 7000 Series supports the Dual Agent feature. This feature provides two agent images: the Agent Primary image and the Agent Secondary image. The Agent Primary image represents the agent image used for the next boot. You can select either image for the next boot. The Dual Agent Boot flag determines which agent image is the boot image. The diagnostics and agent software must use the same value for the Dual Agent Boot flag. If the Dual Agent Boot flag is not set, the unit will boot from Agent 1 (default).

During the software download process, the port LEDs light one after another in a chasing pattern. This chasing pattern is initially fast as the software image is downloaded but gradually slows as the switch erases the flash memory. This pattern speeds up again as the switch programs the new image into the flash memory. When the process is complete, the port LEDs are no longer lit and the switch resets.

Changing switch software

Use this procedure to specify the download target image and change the software version running on the switch.

Before you begin

Use this command in the Global Configuration mode.

About this task

You can update either active image or non-active image. Once the image download is done, the unit resets and restarts with the new image regardless of the value of the Next Boot image indicator. In case of image download without reset, the new image in the flash will be the Next Boot image.

The software download process occurs automatically without user intervention. This process deletes the contents of the flash memory and replaces it with the desired software image. Do not interrupt the download process. Depending on network conditions, this process may take up to 10 minutes.

When the download process is complete, the switch automatically resets unless the `no-reset` parameter was used. The software image initiates a self-test and returns a message when the process is complete.

The following shows an example of this message.

```
Download Image [/]
Saving Image [-]
Finished Upgrading Image
```

The switch is not operational during the download process. You can track the progress of the download process by observing the front panel LEDs.

Procedure

1. Enter the following command:

   ```
   download [address <a.b.c.d>] {primary | secondary} {image
   <image_name> | image–if–newer <image_name> | diag
   <image_name>} [no-reset] [usb]
   ```

2. Press `Enter`.

Variable definitions

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

Variable	Value
address <*a.b.c.d*>	Specifies the IP address of the TFTP server to be used. The address <ip> parameter is optional and if omitted the switch defaults to the TFTP server specified by the `tftpserver` command unless software download is to take place using a USB mass storage device.
primary | secondary	Specifies the image to download: primary or secondary.
image <*image_name*>	Specifies the name of the software image to be downloaded from the TFTP server.
image—if—newer <*image_name*>	Specifies the name of the software image to be downloaded from the TFTP server if newer than the currently running image.
diag <*image_name*>	Specifies the name of the diagnostic image to be downloaded from the TFTP server.
no-reset	Stops the switch from resetting after the software download is complete.
usb	Specifies that the software download is performed using a USB mass storage device.
Note: The `image`, `image-if-newer`, and `diag` parameters are mutually exclusive and only one can be executed at a time.	

Using the Dual Agent next boot image

Use this procedure to toggle the next boot image.

Note:
You must restart the switch or stack after this command to use the next boot image as the new primary image.

Before you begin

Use this command in the Global Configuration mode.

About this task

The Next Boot image in Dual Agent is an agent image that is stored in the flash memory to be used for the next boot. In Dual Agent, there are two agent images in the flash memory, but only one image is assigned as the Next Boot image at a time.

When an agent image is downloaded to the switch, the unit resets and boots up with the newly downloaded image regardless of the value of the Next Boot image indicator. If an agent image is downloaded to the switch without a reset of the unit, the newly downloaded image becomes the Next Boot image.

You can change the Next Boot image at any time. The Next Boot image indicator (a value to indicate which agent image in the flash memory is used in the next boot) is stored in the NVRAM. This value, combined with other factors in the stack discovery process, determines which Dual Agent image the switch uses.

Procedure

Enter the following command:

```
toggle-next-boot-image
```

Using the Dual Agent secondary boot image

Use this procedure to use the secondary boot image.

Note:
The switch or stack will restart automatically with the new image.

Before you begin

Use this command in the Global Configuration mode.

Procedure

Enter the following command:

```
boot secondary
```

Displaying agent images

Use this procedure to show the agent image information for agent images stored in the flash memory.

Before you begin

Use this command in the Global Configuration mode.

Procedure

Enter the following command:

```
show boot image
```

Chapter 9: Shutting down and resetting a switch

Use the procedures in this section to use the `shutdown` command for safely shutting down a switch or stack and the `reload` command to configure remote devices.

About this task

The `shutdown` command proves a mechanism for safely shutting down a switch or stack without interfering with device processes or corrupting the software image. After this command is issued, the configuration is saved, auto-save functionality is temporarily disabled, and configuration changes are not allowed until the switch or stack restarts. If the shutdown is cancelled, auto-save functionality returns to the state in which it was previously functioning.

The `reload` command operates in a similar fashion to the `shutdown` command. However, the `reload` command is intended more to be used by system administrators using the command functionality to configure remote devices and reset them when the configuration is complete.

The `reload` command differs from the `shutdown` command in that the configuration is not explicitly saved after the command is issued. This means that any configuration changes must be explicitly saved before the switch or stack reloads. The `reload` command does temporarily disable auto-save functionality until the reload occurs. Cancelling the reload returns auto-save functionality to any previous setting.

Shutting down the switch

Use this procedure to shut down a switch or stack.

Before you begin

Use this command in the Privileged EXEC mode.

Procedure

Enter the following command:

```
shutdown [force] [minutes-to-wait <1-60>] [cancel]
```

Variable definitions

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

Variable	Value
force	Forces the shutdown without confirmation.
minutes-to-wait <1-60>	Specifies the number of minutes to wait before the shutdown occurs. DEFAULT: 10
cancel	cancels a scheduled shutdown any time during the time period specified by the minutes-to-wait parameter.

Reloading remote devices

Use this procedure to reload a switch or stack.

Before you begin

Use this command in the Privileged EXEC mode.

Procedure

Enter the following command:

```
reload [force] [minutes-to-wait <1-60>] [cancel]
```

Variable definitions

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

Variable	Value
force	Forces the reload without confirmation.
minutes-to-wait <1-60>	Specifies the number of minutes to wait before the reload occurs. DEFAULT: 10

Variable	Value
cancel	cancels a scheduled reload any time during the time period specified by the minutes-to-wait parameter.

Chapter 10: Configuring a TFTP server

Use the procedures in this section to configure a default Trivial File Transfer Protocol (TFTP) server. These procedures include setting a default server, displaying the default configuration, and clearing the default configuration.

Configuring a default TFTP server

Use this procedure to specify a default TFTP server.

Before you begin

Use this command in the Privileged EXEC mode.

About this task

The switch processes that make use of a TFTP server often give the switch administrator the option of specifying the IP address of a TFTP server to be used. Instead of entering this address every time it is needed, you can store a default IP address on the switch.

Procedure

Use the following command to enter the IP address of the default TFTP server:

```
tftp-server <A.B.C.D>
```

Displaying the default TFTP server

Use this procedure to display the default TFTP server configured for the switch.

Before you begin

Use this command in the Privileged EXEC mode.

Procedure

Enter the following command:

```
show tftp-server
```

Clearing the default TFTP server

Use this procedure to clear the default TFTP server from the switch and reset it to 0.0.0.0.

Before you begin

Use this command in the Global Configuration mode.

Procedure

Enter the following commands:

```
no tftp-server
default tftp-server
```

Appendix A: Factory default configuration

Factory default configuration settings

Setting	Factory Default Configuration Value
Unit Select switch	non-Base
Unit	1
BootP Request Mode	BootP When Needed
In-Band Stack IP Address	0.0.0.0 (no IP address assigned)
In-Band Switch IP Address	0.0.0.0 (no IP address assigned)
In-Band Subnet Mask	0.0.0.0 (no subnet mask assigned)
Default Gateway	0.0.0.0 (no IP address assigned)
Read-Only Community String	public
Read-Write Community String	private
Trap IP Address	0.0.0.0 (no IP address assigned)
Community String	Zero-length string
Authentication Trap	Enabled
Autotopology	Enabled
sysContact	Zero-length string
sysName	Zero-length string
sysLocation	Zero-length string
Aging Time	300 seconds
Find an Address	00-00-00-00-00-00 (no MAC address assigned)
Select VLAN ID [1]	
Trunk	blank field
Security	Disabled
Port List	blank field
Find an Address	blank field
MAC Address	00-00 00-00 -00-00
Allowed Source	blank field

Setting	Factory Default Configuration Value
Display/Create MAC Address	00-00-00-00-00-00
Create VLAN	1
Delete VLAN	blank field
VLAN Name	VLAN #
Management VLAN	Yes (VLAN #1)
VLAN Type	Port-based
Protocol ID (PID)	None
User-Defined PID	0x0000
VLAN State	Active (VLAN # 1)
Port Membership	All ports assigned as members of VLAN 1
Unit	1
Port	1
Filter Untagged Frames	No
Filter Unregistered Frames	Yes
Port Name	Unit 1, Port 1
PVID	1
Port Priority	0
Tagging	Untag All
AutoPVID	Enabled
Unit	1
Port	1
PVID	1 (read only)
Port Name	Unit 1, Port 1 (read only)
Unit	1
Status	Enabled (for all ports)
Linktrap	On
Autonegotiation	Enabled (for all ports)
Speed/Duplex	(Refer to Autonegotiation)
Trunk	1 to 12 (depending on configuration status)
Trunk Members (Unit/Port)	Blank field
STP Learning	Normal

Setting	Factory Default Configuration Value
Trunk Mode	Basic
Trunk Status	Disabled
Trunk Name	Trunk #1 to Trunk #12
Traffic Type	Rx and Tx
Port	1
Monitoring Mode	Disabled
Monitor/Unit Port	Zero-length string
Unit/Port X	Zero-length string
Unit/Port Y	Zero-length string
Rate Limit Packet Type	Both
Limit	None
VLAN	1
Unit	1
Port	1
Console Port Speed	9600 Baud
Console Switch Password type	None
Console Stack Password type	None
Telnet Stack Password type	None
Telnet Switch Password type	None
Console Read-Only Switch Password	Passwords are user for non-SSH software images and userpasswd for SSH software images.
Console Read-Write Switch Password	Passwords are secure for non-SSH software images and securepasswd for SSH software images.
Console Read-Only Stack Password	Passwords are user for non-SSH software images and userpasswd for SSH software images.
Console Read-Write Stack Password	Passwords are secure for non-SSH software images and securepasswd for SSH software images.
Radius password/server	secret
New Unit Number	Current stack order
Renumber units with new setting?	No
Group	1

Setting	Factory Default Configuration Value
Bridge Priority	8000
Bridge Hello Time	2 seconds
Bridge Maximum Age Time	20 seconds
Bridge Forward Delay	15 seconds
Add VLAN Membership	1
Tagged BPDU on tagged port	• STP Group 1--No • Other STP Groups--Yes
STP Group State	• STP Group 1--Active • Other STP Groups--InActive
VID used for tagged BPDU	4001-4008 for STGs 1-8, respectively
STP Group	1
Participation	Normal Learning
Priority	128
Path Cost	1
STP Group	1
STP Group	1
TELNET Access/SNMP	By default, SNMP access is disabled in the SSH image and enabled in the non-SSH image. Telnet is enabled by default in both SSH and non-SSH images. Use list: Yes
Login Timeout	1 minute
Login Retries	3
Inactivity Timeout	15 minutes
Event Logging	All
Allowed Source IP Address (50 user-configurable fields)	First field: 0.0.0.0 (no IP address assigned)
	Remaining 49 fields: 255.255.255.255 (any address is allowed)
Allowed Source Mask (50 user-configurable fields)	First field: 0.0.0.0 (no IP address assigned)
	Remaining 49 fields: 255.255.255.255 (any address is allowed)
	Remaining 49 fields: ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff/128 (any IPv6 address is allowed)
Image Filename	Zero-length string

Setting	Factory Default Configuration Value
Diagnostics image filename	Zero-length string
TFTP Server IP Address	0.0.0.0 (no IP address assigned)
Start TFTP Load of New Image	No
Configuration Image Filename	Zero-length string
Copy Configuration Image to Server	No
Retrieve Configuration Image from Server	No
ASCII Configuration Filename	Zero-length string
Retrieve Configuration file from Server	No
Auto Configuration on Reset	Disabled
High Speed Flow Control Configuration	
VLAN Configuration Control	Strict