Quick Start
Avaya Ethernet Routing Switch 8800/8600

7.1.3
NN46205-310, 06.02
March 2012

© 2012 Avaya Inc.

All Rights Reserved.

Notice

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

Documentation disclaimer

“Documentation” means information published by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya 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.

Preventing Toll Fraud

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

Avaya Toll Fraud Intervention

If you suspect that you are being victimized by Toll Fraud and you need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support Web site: http://support.avaya.com. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Trademarks

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

Avaya is a registered trademark of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners, and “Linux” is a registered trademark of Linus Torvalds.

Downloading Documentation

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

Contact Avaya Support

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

Contents

Chapter 1: Purpose of this document 5
Chapter 2: New in this release 7
Features 7
Other changes 7
Chapter 3: Fundamentals 9
System connections 9
Terminal connection 9
Modem connection 10
System logon 12
hsecure mode 13
Setup utility 15
Secure and nonsecure protocols 18
Management port 19
Static IP entry for the OOB network management interface 19
Compact flash support on 8895 SF/CPU 21
Enterprise Device Manager 21
Chapter 4: Initial steps using the CLI 23
Connecting a terminal 23
Connecting a modem 24
Configuring the switch with the setup utility 31
Configuring system identification 34
Configuring the time zone 36
Configuring the date 37
Specifying the primary SF/CPU 38
Changing passwords 39
Saving the configuration 41
Chapter 5: Initial steps using the ACLI 43
Connecting a terminal 43
Connecting a modem 44
Configuring the switch with the setup utility 50
Configuring system identification 54
Configuring the time zone 56
Configuring the date 58
Specifying the primary SF/CPU 58
Changing passwords 59
Saving the configuration 61
Chapter 6: Initial steps using EDM 63
Configuring the system using the Quick Start wizard 63
Editing system information 65
Configuring the date and time 67
Changing passwords 68
Saving the configuration 70
Chapter 7: Remote connection configuration using the CLI 71
Assigning an IP address to the management port 71

Assigning static routes to the management interface ... 72
Enabling remote access services ... 73
Enabling the Web server for EDM access ... 74
Configuring the remote host logon ... 75
Chapter 8: Remote connection configuration using the ACLI ... 77
Assigning an IP address to the management port ... 77
Assigning static routes to the management interface ... 78
Enabling remote access services ... 79
Enabling the Web server for EDM access ... 80
Configuring the remote host logon ... 81
Chapter 9: Remote connection configuration using EDM ... 85
Assigning an IP address to the management port ... 85
Assigning static routes to the management interface ... 86
Chapter 10: Verification ... 87
Pinging an IP device ... 87
Using Telnet to log on to the device ... 88
Accessing the switch through EDM ... 88
Chapter 11: Customer service ... 91
Getting technical documentation ... 91
Getting Product training ... 91
Getting help from a distributor or reseller ... 91
Getting technical support from the Avaya Web site ... 92

Chapter 1: Purpose of this document

This document includes the minimal, but essential, configuration steps to establish a management interface, begin provisioning, and provide basic security on the Avaya Ethernet Routing Switch 8800/8600.

Chapter 2: New in this release

The following sections detail what's new in *Avaya Routing Switch 8800/8600 Quick Start* (NN46205-310). The Features section describes new features, and the Other changes section describes non-feature changes in Release 7.1.3.

- Features on page 7
- Other changes on page 7

Features

There are no new features for release 7.1.3.

Other changes

There are no other changes to this document in release 7.1.3.

Chapter 3: Fundamentals

This chapter describes some basic concepts to get your switch up and running. The remaining chapters in this document are grouped according to one of the three interfaces: Command Line Interface (CLI), Avaya Command Line Interface (ACLI), and Enterprise Device Manager (EDM).

Important:

Pasting configurations, either via console or telnet/SSH, is not recommended and if performed should only be done one line at a time, versus larger text files. This is independent of any control the user may have over how 'slow' their actual input maybe. The reason for is that neither the console or telnet/SSH functions are high priority, and the switch could be servicing some other task and therefore miss lines in the configuration paste. Optionally, use TFTP/FTP and 'source' the file.

System connections

Connect to the Switch Fabric/Central Processor Unit (SF/CPU) serial ports using one of the following connections:

- Terminal connection on page 9
- Modem connection on page 10

Terminal connection

Connect the serial console interface (an RS-232 port) to a PC or terminal to monitor and configure the switch. The port uses a DB-9 connector that operates as data terminal equipment (DTE) or data communication equipment (DCE). The default communication protocol settings for the console port are listed below:

- 9600 baud
- 8 data bits
- 1 stop bit
- No parity

To use the console port, you need the following equipment:

- A terminal or teletypewriter (TTY)-compatible terminal, or a portable computer with a serial port and terminal-emulation software.
- An Underwriters Laboratories (UL)-listed straight-through or null modem RS-232 cable with a female DB-9 connector for the console port on the switch. The other end of the

cable must use a connector appropriate to the serial port on your computer or terminal. Most computers or terminals use a male DB-25 connector. A null modem cable is shipped with the chassis.

You must shield the cable connected to the console port to comply with emissions regulations and requirements.

Modem connection

You can access the switch through a modem connection to the Avaya Ethernet Routing Switch 8800/8600, 8692 SF/CPU or 8895 SF/CPU modules. Avaya recommends that you use the default settings for the modem port for most modem installations.

To set up modem access, you must use a DTE-to-DCE cable (straight or transmit cable) to connect the Avaya Ethernet Routing Switch 8800/8600 to the modem. The following table shows the DTE-to-DCE pin assignments.

Table 1: DTE-to-DCE straight-through pin assignments

Signal	Switch	Modem	
	Pin number	DCE DB-9 pin number	DCE DB-25 pin number
Received data (RXD)	2	2	3
Transmitted data (TXD)	3	3	2
Data terminal ready (DTR)	4	4	20
Ground (GND)	5	5	7
Data set ready (DSR)	6	6	6
Request to send (RTS)	7	7	4
Clear to send (CTS)	8	8	5

The default communication protocol settings for the modem port are listed below:

- 9600 baud
- 8 data bits
- 1 stop bit
- No parity

Comments? infodev@avaya.com

Because the modem port receives DSR and CTS signals before transmitting, you require control lines in the cables. The modem port supports no inbound flow control. The port does not turn on and turn off control lines to indicate the input buffer is full.

To connect a modem to an Avaya Ethernet Routing Switch 8800/8600, you can configure the modem port first using another type of connection to the command line interface (CLI) or Avaya Command Line Interface (ACLI).

PPP modem connection

You can establish a PPP (Point-to-Point Protocol) link over serial asynchronous lines. PC clients use this link to connect remotely to a switch through a standard dial-up modem and the modem DTE port on the primary switch SF/CPU. You must configure the connection on both the remote client PC and the switch. The following figure shows a standard PPP connection to the Avaya Ethernet Routing Switch 8800/8600.

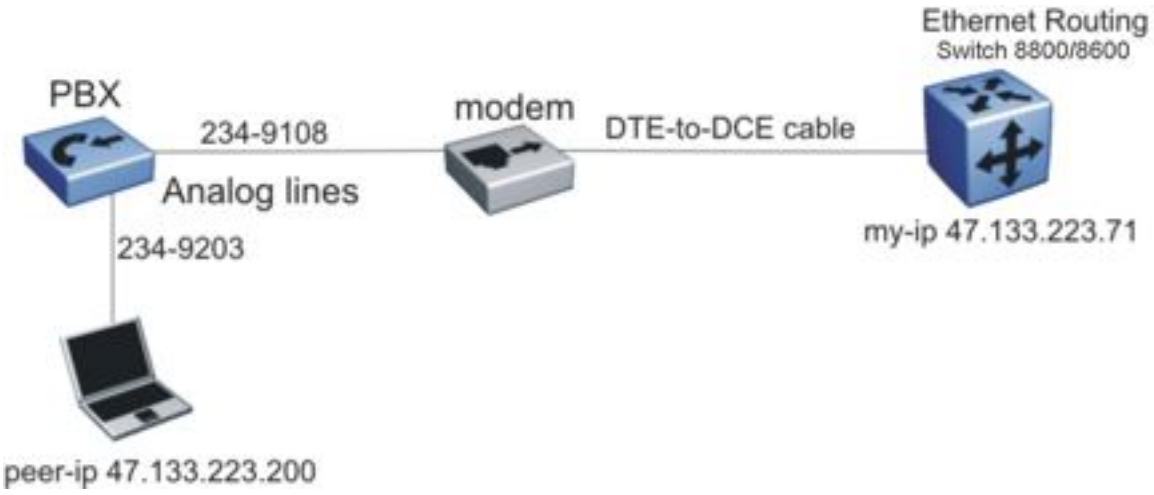


Figure 1: PPP configuration topology

When you configure the modem port on the switch to use PPP, you must also specify a PPP file. The PPP file is a text document that includes all additional PPP configuration parameters to include when the switch restarts. Enter one configuration parameter on each line with required values.

You can configure the connection to use the Challenge-Handshake Authentication Protocol (CHAP) or the Password Authentication Protocol (PAP). Both protocols require a secrets file. The secrets file is a text document that includes the list of all users authorized to use the modem port. You must list one user on each line and include specific parameters. The format for each user is **`client server password IP address`**. The following list explains each option.

- client: the name of the user. This value is the logon name of the authorized user. This value can be the name or ID of the user, similar to a Windows or UNIX logon.
- server: the name of the remote device, which is often the dial-in server. Use an asterisk (*) to indicate any server name is acceptable.

- password: the password for the user.
- IP address: the IP address associated with the user.

The value for the IP address depends on the desired configuration of the modem. If all users must use the same IP address, you must specify the same IP address for all users in the file, and it must be the same IP address that you configure as the peer-ip for the modem port. Configure the IP settings on the client to obtain an IP address automatically.

If each user must use a different IP address, list each user with a different IP address in the file. Configure the client IP settings to use a static IP address that matches what you configure in the secrets file.

An example secrets file looks like the following:

```
long * long 47.133.223.200 william * william 47.133.223.200
```

System logon

After the switch boot sequence is complete, a Login prompt appears. The following table shows the default values for logon and password for the console and Telnet sessions.

Table 2: Access levels and default logon values

Access level	Description	Default logon	Default password
Read-only	Permits view-only configuration and status information. Is equivalent to Simple Network Management Protocol (SNMP) read-only community access.	ro	ro
Layer 1 read/write	View most switch configuration and status information and change physical port settings.	l1	l1
Layer 2 read/write	View and change configuration and status information for Layer 2 (bridging and switching) functions.	l2	l2
Layer 3 read/write (8800/8600 switches only)	View and change configuration and status information for Layer 2 and Layer 3 (routing) functions.	l3	l3
Read/write	View and change configuration and status information across the switch. You cannot change security and password settings. This access level is equivalent to SNMP read/write community access.	rw	rw

Comments? infodev@avaya.com

Access level	Description	Default logon	Default password
Read/write/all	Permits all the rights of Read/Write access and the ability to change security settings, including the CLI and Web-based management user names and passwords and the SNMP community strings.	rwa	rwa

hsecure mode

The Avaya Ethernet Routing Switch 8800/8600 supports a flag called high secure (hsecure). The hsecure flag introduces the following behaviors for the password: 10-character enforcement, aging time, limitation of failed logon attempts, and a protection mechanism to filter certain IP addresses.

After you enable the hsecure flag, the software enforces the 10-character rule for all passwords. After you upgrade from a previous release, if the password does not contain at least 10 characters, you must change your password to the mandatory character length. This password must contain a minimum of two uppercase characters, two lowercase characters, two numbers, and two special characters.

Default passwords and community strings

If the switch starts in hsecure mode as a default factory setting, and you have not configured a password, the default passwords are changed to respect this rule. The following table describes the default passwords.

Table 3: Default setting passwords

User ID	Default password
rwa	rwarwarrwar
rw	rwrwrwrwrw
ro	rororororo
l3	l3l3l3l3l3
l2	l2l2l2l2l2
l1	l1l1l1l1l1
l4admin	l4adminl4a
slbadmin	slbadminsl
oper	operoperop
l4oper	l4operl4op

User ID	Default password
slboper	slboperslb
ssladmin	ssladminss

The following table describes the default community strings.

Table 4: Default community strings

User ID	New community string
ro	`publiconly`
l1	`privateonly`
l2	`privateonly`
l3	`privateonly`
rw	`privateonly`
rwa	`secretonly`

Aging enforcement

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

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

Consider the following after you enable the hsecure flag:

- You cannot enable the Web server.
- You cannot enable the SSH password authentication.

Filtering mechanism

Beginning with Release 4.1, incorrect IP source addresses as network or broadcast addresses are filtered at the virtual router interface. For example, V1 has the network address 192.168.168.0/24.

Comments? infodev@avaya.com

This change is valid for all IP subnets, not only for /24 as mentioned in the example. Source addresses 192.168.168.0 and 192.168.168.255 are discarded.

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

Setup utility

The Setup utility monitors system requirements and obtains the highest system performance. Use the Setup utility to configure your switch by responding to a series of on-screen questions. The Setup utility saves the information in the boot and run-time configuration files. The saved information and files ensure the switch restarts in the desired operating mode. The Setup utility also provides error and warning messages to advise you of the ramifications of certain hardware and software configurations.

The Setup utility prompts you through the configuration process by asking a series of questions. Answer each question or accept the default by pressing Enter. Each question shows the default in brackets ([ ]) and the acceptable parameter options in parenthesis. For information on configuring the Setup utility, see Configuring the switch with the setup utility on page 31 using the CLI and Configuring the switch with the setup utility on page 50 using the ACLI. You can also use EDM to configure the switch. See Configuring the system using the Quick Start wizard on page 63.

The following figures show sample output from the setup utility. This example uses the default values.

```
ERS-8606:5#
ERS-8606:5# install

######################################################################
Welcome to ERS 8000 setup utility.  You are about to
configure initial configuration of the switch.  Part of the data will
be stored in the file /flash/boot.cfg and part will be stored in
runtime configuration file.  Please reboot the switch after initial
configuration

Several of these commands do not require a reboot and can be
applied dynamically through CLI
######################################################################

Do you want to continue (y/n) ? y
##################
System Parameters
##################
#
Please provide primary config-file path [/flash/SN1.cfg]:
Please provide primary image-file path [/flash/p80a4100.img]:
Please add system prompt [ERS-8606]:
Please select CPU Master slot (5/6) [5]:
Master CPU mgmt port: autonegotiation [n] (y/n) ?
           speed (10/100) [10]:
Do you want to enable automatic savetostandby mode [n] (y/n) ?
Do you want to enable m-mode support [n] (y/n) ?
Do you want to enable enhanced operation mode support [n] (y/n) ?
Do you want to enable CPU High Availability mode [n] (y/n) ?
Do you want to enable vlan-optimization-mode support [n] (y/n) ?
Do you want to enable r-mode support [n] (y/n) ?
#
 1 - Primary configuration file path                (/flash/SN1.cfg)->/flash/
SN1.cfg
 2 - Primary image file path                        (/flash/p80a4100.img)->/
flash/p80a4100.img
 3 - CLI prompt                                     (ERS-8606)->ERS-8606
 4 - Master CPU selection                           (5)->5
```

Figure 2: Setup utility example one

Comments? infodev@avaya.com

```
 5 - Master CPU Mgmt port autonegotiation            (false)->false
‘6 - Master CPU Mgmt port speed                      (10)->10
 7 - Automatic save to Standby                       (false)->false
 8 - Support for M-mode                              (false)->false’
 9 - Support for enhanced operation mode             (false)->false
10 - High Availability mode                          (false)->false
11 - Support for vlan-optimization-mode              (false)->false
12 - Support for R-mode                              (false)->false
#
Please type the line-number you want to change
OR "0" to save & quit at this stage
OR hit return to continue [-1]:


Syncing autoneg
HA-CPU change will be applied at the end of this session only if you choose to
save configuration
##################
System Services
##################
#
Do you want to enable FTP [n] (y/n) ? y
Do you want to enable RLOGIN [n] (y/n) ? y
Do you want to enable TELNET [n] (y/n) ? y
Do you want to enable TFTP [n] (y/n) ? y
Do you want to enable WEB server service [n] (y/n) ? y
#
 1 - FTP server service                              (true)->true
 2 - RLOGIN server service                           (false)->true
 3 - TELNET server service                           (true)->true
 4 - TFTP server service                             (true)->true
 5 - WEB server service                              (false)->true
#

Please type the line-number you want to change
OR "0" to save & quit at this stage
OR hit return to continue [-1]:


########################
IP Network connectivity
########################
```

Figure 3: Setup utility example two

```
IP Address for mgmt port in first CPU Slot [10.127.231.15/255.255.255.0]:
IP Address for mgmt port in second CPU Slot [10.127.231.15/255.255.255.0]:
IP Address for mgmt-virtual-ip [0.0.0.0/0.0.0.0]:
First net mgmt route [172.16.0.0:10.127.231.1]:
Second net mgmt route [134.177.0.0:10.127.231.1]:
Third net mgmt route [10.0.0.0:10.127.231.1]:
Fourth net mgmt route [11.0.0.0:10.127.231.1]:
IP address of the default VLAN [0.0.0.0/0.0.0.0]:
#
 1 - Management port Ip Address for first CPU slot   (10.127.231.15/
255.255.255.0)->10.127.231.15/255.255.255.0
 2 - Management port Ip Address for second CPU slot  (10.127.231.15/
255.255.255.0)->10.127.231.15/255.255.255.0
 3 - Virtual management port Ip Address              (0.0.0.0/0.0.0.0)-
>0.0.0.0/0.0.0.0
 4 - First static route for management port
(172.16.0.0:10.127.231.1)->172.16.0.0:10.127.231.1
 5 - Second static route for management port
(134.177.0.0:10.127.231.1)->134.177.0.0:10.127.231.1
 6 - Third static route for management port          (10.0.0.0:10.127.231.1)-
>10.0.0.0:10.127.231.1
 7 - Fourth static route for management port         (11.0.0.0:10.127.231.1)-
>11.0.0.0:10.127.231.1
 8 - IP address of the default VLAN                  (0.0.0.0/0.0.0.0)-
>0.0.0.0/0.0.0.0
#

Please type the line-number you want to change
OR "0" to save & quit at this stage
OR hit return to continue [-1]:


Do you want to save the changes
[Saving the parameters will update the files
/flash/boot.cfg and /flash/SN1.cfg
] (y/n) ? n

WARNING: The change made will take effect only after
the configuration is saved and the full chassis is rebooted.
This feature is not applicable to 8690SF/CPU cards.
All non-M modules will be taken off-line if m-mode is enabled.

WARNING:The change made will take effect only after
the configuration is saved and the full chassis is rebooted.
```

Figure 4: Setup utility example three

Secure and nonsecure protocols

The following table describes the secure and nonsecure protocols the Avaya Ethernet Routing Switch 8800/8600 supports.

Comments? infodev@avaya.com

Table 5: Secure and nonsecure protocols for IPv4

Nonsecure protocols	Default status	Equivalent secure protocols	Default status
FTP and TFTP	Disabled	SCP	Disabled
Telnet	Disabled	Secure SHell (SSH) v1, v2 Avaya recommends that you use SSHv2 instead of SSHv1.	Disabled
SNMPv1, SNMPv2	Enabled	SNMPv3 You must load the DES/AES image on the switch to use SNMPv3.	Enabled
Rlogin	Disabled	Secure SHell (SSH) v1, v2	Disabled
HTTP	Disabled	No equivalent **Important:** Avaya recommends that you do not use this protocol due to the risk to the security of your network.	

Management port

You must assign an IP address to the management port before you can use it for out-of-band (OOB) management. In a switch with redundant 8692 with super mezz or 8895 modules, each management port uses a specific IP address. In addition, you can create a virtual management port with an IP address available to the master management module.

The master management module replies to all management requests sent to the virtual IP address, and to requests sent to the management port IP address. If the master management module fails and the backup management module takes over, the virtual management port IP address continues to provide management access to the switch.

Static IP entry for the OOB network management interface

The following figure shows the OOB network management port default IP assignment.

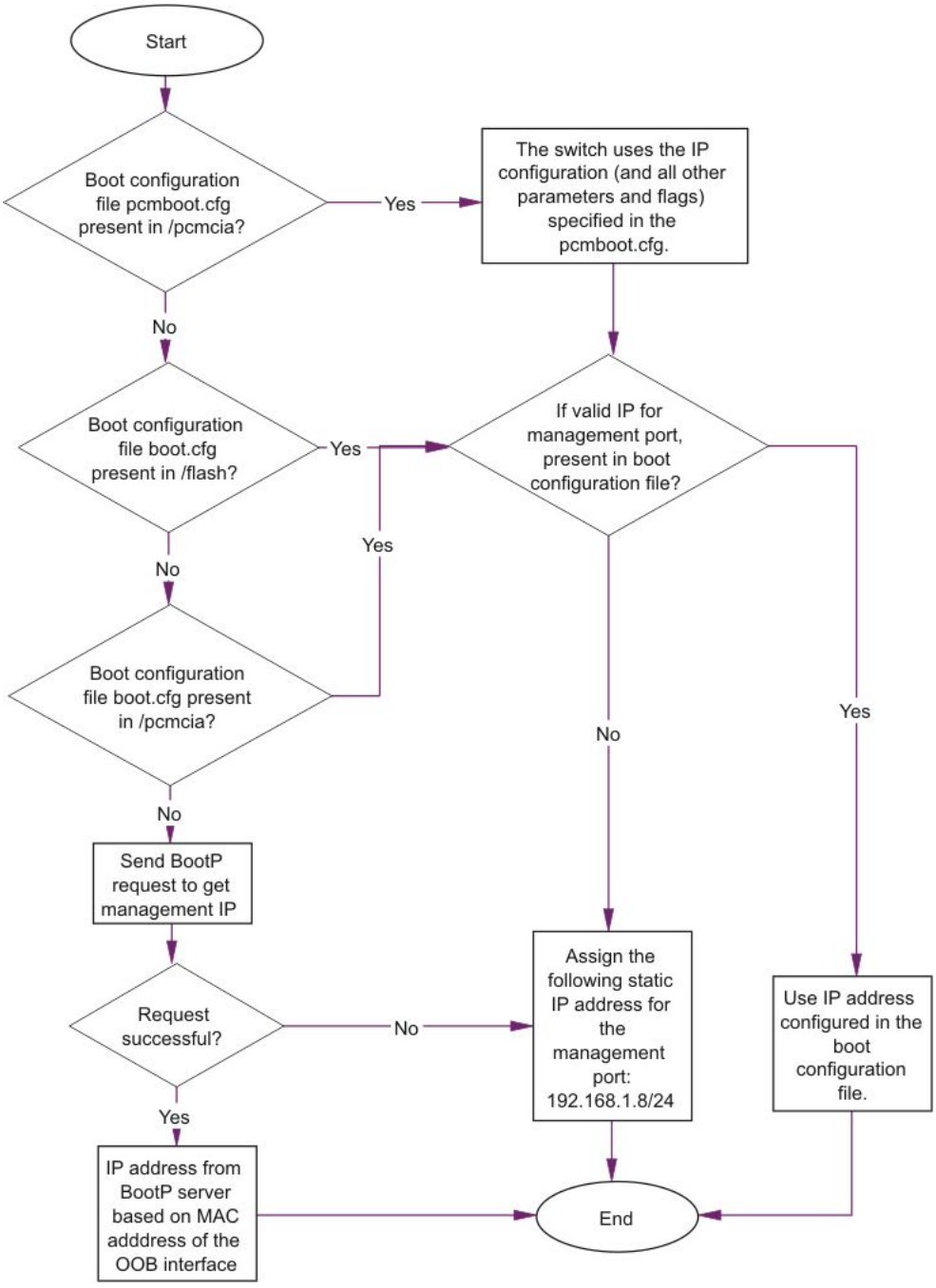


Figure 5: OOB network management port default IP flowchart

The switch first checks for the file pcmboot.cfg in the /pcmcia folder on the external flash (for 8895 SF/CPU) or Personal Computer Memory Card International Association (PCMCIA) (for 8692 SF/CPU). If not found, the switch checks for the file boot.cfg in internal flash (/flash).

Important:

For backwards compatibility, the file naming convention for compact flash card files on the 8895 SF/CPU remains /pcmcia/<filename>.

Important:

If you use the boot configuration file from the external flash or PCMCIA, you must rename the file to pcmboot.cfg The boot.cfg file is no longer saved in external flash or PCMCIA. The file is saved only in internal flash.

Compact flash support on 8895 SF/CPU

Avaya recommends using only the Compact Flash cards listed below with the 8895 SF/CPU since they have been validated for proper operation. Use of any other Compact Flash devices is not recommended as they have not been verified for compatibility on the 8895 SF/CPU.

- SSD-C02G-4000
- SSD-C02G-4007
- SSD-C02G-4300
- SSD-C02G-4500
- SSD-C02G-4600

Enterprise Device Manager

Enterprise Device Manager (EDM) is a Web-based element manager designed to manage single devices. You can use EDM to monitor and configure your Avaya Ethernet Routing Switch 8800/8600 through a Web browser from anywhere on your network.

The EDM interface has the same configuration capabilities as the CLI and the ACLI. For example, you can edit configurations related to the chassis, cards, fans, ports, and all the protocols configured on the switch.

To access EDM, open http://<deviceIP>/login.html from either Microsoft Internet Explorer 7.0, 16 or Mozilla Firefox 3.0.For more information about EDM, see *Avaya Ethernet Routing Switch 8800/8600 User Interface Fundamentals* (NN46205-308).

Note:

To access EDM, you must use the following command to enable the Web server:

```
config web-server enable
```

The default **Username** is **admin** and the default **Password** is **password**.

Chapter 4: Initial steps using the CLI

This chapter describes the basic configuration procedures for the initial provisioning of the switch.

Prerequisites to initial steps

- You must install the hardware.
- You must install at least one cable to set up a remote connection to the switch.
- You must turn on the switch.

Connecting a terminal

Connect a terminal to the serial console interface to monitor and configure the switch.

Prerequisites

- To use the console port, you need the following equipment:
  - A terminal or teletypewriter (TTY)-compatible terminal, or a portable computer with a serial port and terminal-emulation software.
  - An Underwriters Laboratories (UL)-listed straight-through or null modem RS-232 cable with a female DB-9 connector for the console port on the switch. The other end of the cable must use a connector appropriate to the serial port on your computer or terminal. Most computers or terminals use a male DB-25 connector. A null modem cable is shipped with the chassis.
- You must shield the cable connected to the console port to comply with emissions regulations and requirements.

Procedure steps

1. Configure the terminal protocol as follows:
   - 9600 baud
   - 8 data bits
   - 1 stop bit
   - No parity
2. Connect the RS-232 cable to the console port.
3. Connect the other end of the RS-232 cable to the terminal or computer serial port.
4. Turn on the terminal.
5. Log on to the CLI.

Connecting a modem

Connect a modem to an Avaya Ethernet Routing Switch 8800/8600 to establish a connection with the switch. You can configure the modem port first using another type of connection, such as a terminal connection, to the CLI.

Prerequisites

- You need a DTE-to-DCE cable (straight or transmit cable) to connect the Avaya Ethernet Routing Switch 8800/8600 to the modem.
- You must configure your client dial-up settings to establish the connection to the modem.

Procedure steps

1. In the run-time CLI, configure the modem port by using the following command:

   ```
   config bootconfig sio modem
   ```

   Now you can enter options for this command level without retyping the first part of the command.

Comments? infodev@avaya.com

Important:

Avaya recommends that before you configure the Serial Line Internet Protocol (SLIP) or Point-to-Point Protocol (PPP), you familiarize yourself with these protocols.

2. Configure port parameters based on the modem requirements by using the following commands:

   ```
   baud <rate>

   8databits <true|false>

   mode <ascii|slip|ppp>
   ```

   For more information about the configuration requirements of your modem, see the documentation shipped with the modem.

3. If you configure the port mode to slip, use the following commands to configure other SLIP parameters:

   ```
   slip-compression <true|false>

   slip-rx-compression <true|false>
   ```

4. If you configure the port mode to ppp, use the following commands to configure other PPP parameters:

   ```
   mtu <bytes>

   my-ip <ipaddr>

   peer-ip <ipaddr>

   pppfile <file>
   ```

5. On the modem, turn off echo mode and return code messaging.
6. Connect the modem to the modem port.
7. Save the boot configuration.
8. Restart the switch.

Variable definitions

Use the data in the following table to use the **`config bootconfig sio`** command.

Variable	Value
8databits <true|false>	Specifies either 8 (true) or 7 (false) data bits for each byte for software to interpret. The default is false.

Variable	Value
baud <*rate*>	Configures the baud rate for the port. The default is 9600.
enable <true|false>	Enables or disables the port. The default is true.
info	Displays information about the specified port.
mode <ascii|slip|ppp>	Configures the communication mode for the serial port. The default is American Standard Code for Information Interchange (ASCII). If you are configuring the modem port, you can configure the port to use the SLIP or the PPP communication mode.
mtu <*bytes*>	Configures the size of the maximum transmission unit for a PPP link (0–2048). The default is zero.
my-ip <*ipaddr*>	Configures the IP address for the server side, the Avaya Ethernet Routing Switch 8800/8600, of the point-to-point link. The default is 0.0.0.0. Avaya recommends that you use the current IP address for the management port.
peer-ip <*ipaddr*>	Configures the peer (PC) IP address on the point-to-point link. The default is 0.0.0.0. The switch assigns this value to any PC that connects through the modem port with configured TCP/IP properties to obtain an IP address automatically. If the client uses a static IP address, the Avaya Ethernet Routing Switch 8800/8600 accepts this address. If you use Password Authentication Protocol (PAP) authentication, you must ensure that the client uses the correct IP address.
pppfile <*file*>	Specifies the PPP configuration file you must use to provide details for authentication and other options the switch includes during the boot process. If you configure the port mode to PPP, you must specify a PPP filename. For more information about this file, see Job aid on page 27. The PPP file name is a string value of no more than 64 characters. Identify the file in the format {a.b.c.d:|peer:|/pcmcia/|/flash/}<file>.

Comments? infodev@avaya.com

Variable	Value
	Important: Do not specify a PPP filename with more than 64 characters.
restart	Shuts down and initializes the port.
slip-compression <true|false>	Enables or disables Transmission Control Protocol over IP (TCP/IP) header compression for SLIP mode. The default is false.
slip-rx-compression <true|false>	Enables or disables TCP/IP header compression on the receive packet for SLIP mode. The default is false.

Job aid

Create the PPP file with one option on each line; comment lines start with a pound sign (#). The following table lists the available options.

Option	Description
asyncmap <value>	Configures the desired async map to the value you specify.
chap_file <file>	Obtains Challenge-Handshake Authentication Protocol (CHAP) secrets from the specified file. You require this option if either peer requires CHAP authentication. If your users must use the same IP address, the PAP and CHAP secret files must specify the same IP address for all users and it must match the peer-ip setting on the modem port.
chap_interval <value>	Configures the interval, in seconds, for the CHAP rechallenge to the value you specify.
chap_restart <value>	Configures the timeout, in seconds, for CHAP negotiation to the value you specify.
debug	Activates the PPP daemon debug mode.
default_route	Adds a default route to the system routing table, after successful Internet Protocol Control Protocol (IPCP) negotiation. Use the peer as the gateway. After the PPP connection ends, the system removes this entry.

Option	Description
driver_debug	Activates PPP driver debug mode.
escape_chars <value>	Configures the characters to escape on transmission to the value you specify.
ipcp_accept_local	Accepts what the remote peer uses as the target local IP address, even if the local IP address is specified.
ipcp_accept_remote	Accepts what the remote peer uses as the IP address, even if you specify the remote IP address.
ipcp_max_configure <value>	Configures the maximum number of transmissions for IPCP configuration requests to the value you specify.
ipcp_max_failure <value>	Configures the maximum number of IPCP configuration negative acknowledgements (NAK) to the value you specify.
ipcp_max_terminate <value>	Configures the maximum number of transmissions for IPCP termination requests to the value you specify.
ipcp_restart <value>	Configures the timeout, in seconds, for IPCP negotiation to the value you specify.
lcp_echo_failure <value>	Configures the maximum consecutive Link Control Protocol (LCP) echo failures to the value you specify.
lcp_echo_interval <value>	Configures the interval, in seconds, between LCP echo requests to the value you specify.
lcp_max_configure <value>	Configures the maximum number of transmissions for LCP configuration requests to the value you specify.
lcp_max_failure <value>	Configures the maximum number of LCP configuration NAKs to the value you specify.
lcp_max_terminate <value>	Configures the maximum number of transmissions for LCP termination requests to the value you specify.
lcp_restart <value>	Configures the timeout in seconds for the LCP negotiation to the value you specify.
local_auth_name <name>	Configures the local name for authentication to the specified name.
login	Uses the logon password database for Password Authentication Protocol (PAP) peer authentication.

Comments? infodev@avaya.com

Option	Description
max_challenge <value>	Configures the maximum number of transmissions for CHAP challenge requests to the value you specify.
mru <value>	Configures the maximum receive unit (MRU) size for negotiation to the value you specify.
mtu <value>	Configures the maximum transmission unit (MTU) size for negotiation to the value you specify.
netmask <value>	Configures the netmask value for negotiation to the value you specify.
no_acc	Disables address control compression.
no_all	Does not request or allow options.
no_asyncmap	Disables async map negotiation.
no_chap	Disallows CHAP authentication with peer.
no_ip	Disables IP address negotiation in IPCP.
no_mn	Disables magic number negotiation.
no_mru	Disables MRU negotiation.
no_pap	Disables PAP authentication with the peer.
no_pc	Disables protocol field compression.
no_vj	Disables Van Jacobson (VJ) compression. VJ compression reduces the regular 40-byte TCP/IP header to 3 or 8 bytes.
no_vjccomp	Disables VJ connection ID compression.
pap_file <file>	Obtains PAP secrets from the specified file. You require this option if either peer requires PAP authentication. If your users must use the same IP address, the PAP and CHAP secret files must specify the same IP address for all users and it must match the peer-ip setting on the modem port.
pap_max_authreq <value>	Configures the maximum number of transmissions for PAP authentication requests to the value you specify.
pap_passwd <password>	Configures the password for PAP authentication with the peer to the specified password.
pap_restart <value>	Configures the timeout, in seconds, for PAP negotiation to the value you specify.

Option	Description
pap_user_name <name>	Configures the user name for PAP authentication with the peer to the specified name.
passive_mode	Configures passive mode. PPP waits for the peer to connect after an initial connection attempt.
proxy_arp	Adds an entry to the Address Resolution Protocol (ARP) table with the IP address of the peer and the Ethernet address of the local system.
remote_auth_name <name>	Configures the remote name for authentication to the specified name.
require_chap	Requires CHAP authentication with peer.
require_pap	Requires PAP authentication with peer.
silent_mode	Configures silent mode. PPP does not transmit LCP packets to initiate a connection until it receives a valid LCP packet from the peer.
vj_max_slots <value>	Configures the maximum number of VJ compression header slots to the value you specify.

Table 6: Sample PPP file on page 30 shows example contents from a PPP file.

Table 6: Sample PPP file

```
passive_mode
lcp_echo_interval 30
lcp_echo_failure 10
require_chap
require_pap
no_vj
ipcp_accept_remote
login
chap_file "my_chap"
pap_file "my_pap"
```


Comments? infodev@avaya.com

Configuring the switch with the setup utility

Configure the switch with the setup utility to monitor system requirements and obtain the maximum system performance.

Procedure steps

1. Start the setup utility by using the following command:

   ```
   install
   ```

2. Respond to the series of questions displayed on the screen.

   For more information about the prompted questions, see the following job aid.

3. Restart the switch.

Job aid

The following table lists the questions prompted by the setup utility and provides a description for each.

Prompt	Description and action
Please provide primary config-file path [/flash/config.cfg]:	Description: Indicates the name of the primary configuration file. Action: Press `Enter` to accept the default (/flash/config.cfg), or type a different file name for the primary configuration file. To store your configuration file on the external flash (8895 SF/CPU) or PCMCIA card (8692 SF/CPU), use /PCMCIA/config.cfg. To specify the path to the file is optional.
Please provide primary image-file path [/flash/p80a4100.img]:	Description: Indicates the name of the primary image file. Action: Press `Enter` to accept the default (p80a4100.img), or type a different file name for the primary image file. To specify the path to the file is optional. If your run-time image resides on your external flash (8895 SF/CPU) or PCMCIA card (8692 SF/CPU), you must specify the path as /PCMCIA/ file name.
Please add system prompt [ERS-8606]:	Description: Specifies the text for the prompt.

Prompt	Description and action
	Action: Press `Enter` to accept the default (ERS-8610), or type a different string of up to 20 characters.
Please select CPU primary slot (5/6) [5]:	Description: Indicates the slot number of the primary central processing unit (CPU). The slot can be 5 or 6. Action: Press `Enter` to accept the default (5), or specify 6.
Primary CPU mgmt port: autonegotiation [n] (y/n)?	Description: Specifies if you want the primary CPU to use autonegotiation. Action: Enter **n** to accept the default, or enter **y** to indicate that you want the primary CPU management port to use autonegotiation.
speed (10/100) [10]:	Description: Specifies the line speed in Mb/s. Action: Press `Enter` to accept the default (10 Mb/s), or specify 100 Mb/s.
Do you want to enable automatic savetostandby mode [n] (y/n)?	Description: Specifies if you want the boot and run-time configuration files to be saved on the backup CPU. Action: Enter **y** to save the boot and run-time configuration files on the backup CPU. Accept the default (**n**) to save boot and run-time configuration files on the primary CPU.
Do you want to enable enhanced operation mode support [n] (y/n)?	Description: Specifies if you want to enable enhanced operation mode. Enhanced operation mode increases the maximum number of VLANs when you use MultiLink Trunking (MLT) (1980) and Split MLT (SMLT) (989). Action: Enter **y** to enable enhanced operation mode. Accept the default (**n**), to disable enhanced operation mode.
Do you want to enable CPU High Availability mode [n] (y/n)?	Description: Specifies if you want to enable CPU high availability (HA) mode. Use CPU HA mode to recover switches with two CPUs quickly from a failure of one of the CPUs. In HA mode (hot standby), you synchronize and configure the two CPUs in the same mode, so they are compatible. Action: Specify **y** to enable CPU high availability (HA) mode. Accept the default (**n**), to disable CPU HA mode.
Do you want to enable vlan-optimization-mode support [n] (y/n) ?	Description: Specifies if you want to enable support for the VLAN optimization mode.

Comments? infodev@avaya.com

Prompt	Description and action
	Action: Specify y to enable VLAN optimization mode support. Accept the default (**n**) to disable VLAN optimization mode support.
Do you want to enable FTP [n] (y/n)?	Description: Specifies if you want users to access the switch by File transfer Protocol (FTP). Action: Enter **y** to enable FTP for remote users. Accept the default (**n**) to disable FTP.
Do you want to enable RLOGIN [n] (y/n)?	Description: Specifies if you want to access the switch by Rlogin. Action: Enter **y** to enable Rlogin for remote users. Accept the default (**n**) to disable Rlogin.
Do you want to enable TELNET [n] (y/n)?	Description: Specifies if you want to access the switch by Telnet. Action: Enter **y** to enable Telnet. Accept the default (**n**) to disable Telnet.
Do you want to enable TFTP [n] (y/n)?	Description: Specifies if you want to access the switch by Trivial FTP (TFTP). Action: Enter **y** to enable TFTP. Accept the default (**n**) to disable TFTP.
Do you want to enable WEB server service [n] (y/n)?	Description: Specifies if you want to enable Web server service. Use the Web server service to monitor statistics for the switch with your Web browser. Action: Enter **y** to enable Web server service. Accept the default (**n**) to disable Web server service.
IP Address for mgmt port in first CPU Slot [192.168.168.168/255.255.2.55.0]:	Description: Indicates the IP address for the management port in the CPU slot you specify. Action: Type the IP address of the management port in the first CPU slot.
IP Address for mgmt port in second CPU Slot [192.168.168.169/255.255.255.0]:	Description: Indicates the IP address for the management port in the CPU slot you specify. Action: Type the IP address of the management port in the second CPU slot.
IP Address for mgmt-virtual-ip [0.0.0.0/0.0.0.0]:	Description: Indicates the IP address for the virtual management port. Action: Type the IP address of the virtual management port. Accept the default (0.0.0.0/0.0.0.0) to not specify an IP address.
First net mgmt route [0.0.0.0:0.0.0.0]:	Description: Specifies the IP address of the first network management route (static route from the network management port to a device in the network). Action: Type the network and gateway IP address of the first network management route.

Prompt	Description and action
Second net mgmt route [0.0.0.0:0.0.0.0]:	Description: Specifies the IP address of the second network management route. Action: Type the IP address of the second network management route (static route from the network management port to a device in the network).
Third net mgmt route [0.0.0.0:0.0.0.0]:	Description: Specifies the IP address of the third network management route. Action: Type the IP address of the third network management route (static route from the network management port to a device in the network).
Fourth net mgmt route [0.0.0.0:0.0.0.0]:	Description: Specifies the IP address of the fourth network management route. Action: Type an IP address of the fourth network management route (static route from the network management port to a device in the network).
IP address of the default VLAN [0.0.0.0/0.0.0.0]:	Description: Specifies the IP address of the default Virtual Local Area Network (VLAN). Action: Type the IP address of the default VLAN.
Do you want to save the changes [Saving the parameters updates the files /flash/boot.cfg and /flash/dvmrp_pol.cfg] (y/n)?	Description: Saves your changes to the boot and run-time configuration files. Action: Enter **y** to save the boot and run-time configuration files. Enter **n** if you do not want to save your changes.

Configuring system identification

Configure system identification to specify the system name, contact person, and location of the switch.

Procedure steps

1. Specify the system name by using the following command:

   ```
   config sys set name <prompt>
   ```

2. Specify the name of the contact person for the switch by using the following command:

   ```
   config sys set contact <contact>
   ```

3. Define the location for the system by using the following command:

Comments? infodev@avaya.com

```
config sys set location <location>
```

Variable definitions

Use the data in the following table to use the **`config sys set`** command.

Variable	Value
clipId-topology-ip <id>	Sets the topology IP from the available CLIP. *id* is the Circuitless IP interface id in the range of 1 to 256.
clock-sync-time <minutes>	Configures the RTC-to-system clock synchronization time. *minutes* is the RTC-to-System clock synchronization time in minutes in the range of 15 to 3600.
contact <contact>	Alters the system contact.*contact* is the system contact. The string length is in the range of 0 to 255.
dot1d-tp-fdb-query <enable|disable>	Enables or disables the dot1d-tp-fdb-query feature.
ecn-compatibility <enable|disable>	Enables or disables ecn-compatibility feature.
force-topology-ip-flag <true|false>	Sets flag to force choice of topology-IP. true|false enables or disables Force Topology IP Flag.
global-filter <enable|disable>	Enables global filter feature.
info	Shows current level parameter settings and next level directories.
location <location>	Changes the system location.
max-vlan-resource-reservation <enable|disable>	Enables MAX-VLAN feature.
mgmt-virtual-ip <ipaddr/mask>	Configures mgmt virtual IP. *ipaddr/mask* is the IP address and network mask {a.b.c.d/x | a.b.c.d/x.x.x.x | default}.
mgmt-virtual-ipv6 <ipv6addr/prefix-len>	Configures mgmt virtual IPV6. *ipv6addr/prefix-len* is the IPV6 address. The string length ranges from 0 to 46.
mroute-stream-limit <enable|disable>	Global mroute stream limit configuration.enable|disable enables or disables mroute stream limit.

Variable	Value
mtu <bytes>	Sets MTU (with CRC) to one of three values: 1522, 1950 and 9600 bytes. The MTU value in the range of 1522 to 9600.
multicast-resource-reservation <value>	Reserves MGIDs for IPMC use. *value* is the number of MGIDs reserved for IPMC use in the range from 64 to 4083.
name <prompt>	Changes the system name. *prompt* is the box or root level prompt . The string length ranges from 0 to 255.
portlock <on|off>	Turns portlock on or off.
sendAuthenticationTrap <true|false>	Sets authentication trap to true or false.
topology <on|off>	Turns topology on/off.
udp-checksum <enable|disable>	Enables or disables UDP Checksum calculation.
udpsrc-by-vip <enable|disable>	Enables or disables the Virtual IP as the UDP source.
vlan-bysrcmac <enable|disable>	Enables or disables the vlan-bysrcmac feature.

Configuring the time zone

Set the time zone to specify the time zone for your location, and configure settings for Daylight Saving Time (DST).

Procedure steps

1. Configure the time zone by using the following command:

   ```
   config bootconfig tz
   ```

2. Save the changed configuration to the boot.cfg and pcmboot.cfg files.
3. Restart the switch.

Variable definitions

Use the data in the following table to use the **`config bootconfig tz`** command.

Comments? infodev@avaya.com

Variable	Value
dst-end <*Mm.n.d/hhmm*|*MMddhhmm*>	Configures the ending date of DST. You can specify the time in one of two ways: • *Mm.n.d/hhmm* specifies an hour on the nth occurrence of a weekday in a month. For example, M10.5.0/0200 means the fifth occurrence of Sunday in the tenth month (October) at 2:00 a.m. • *MMddhhmm* specifies a month, day, hour, and minute. For example, 10310200 means October 31 at 2:00 a.m.
dst-name <*dstname*>	Configures an abbreviated name for the local daylight saving time zone. *dstname* is the name. For example, PDT is Pacific Daylight Time.
dst-offset <*minutes*|*hh:mm*>	Configures the daylight saving adjustment in minutes or in hours and minutes (hh:mm). The default is 60 minutes.
dst-start <*Mm.n.d/hhmm*|*MMddhhmm*>	Configures the starting date of daylight saving time. • *Mm.n.d/hhmm* specifies an hour on the nth occurrence of a weekday in a month. For example, M10.5.0/0200 means the fifth occurrence of Sunday in the tenth month (October) at 2:00 a.m. • *MMddhhmm* specifies a month, day, hour, and minute. For example, 10310200 means October 31 at 2:00 a.m.
info	Displays time zone information.
name <*tz*>	Configures an abbreviated name for the local time zone name. *tz* is the name. For example, PST is Pacific Standard Time.
offset-from-utc <*minutes*|*hh:mm*>	Configures the time zone offset in minutes or in hours and minutes (hh:mm) to subtract from Universal Coordinated Time (UTC), where positive numbers mean west of Greenwich and negative numbers mean east of Greenwich.

Configuring the date

Configure the calendar date and time in the form of month, day, year, hour, minute, and second.

Prerequisites

- You must log on with the rwa credentials to use the command in this procedure.

Procedure steps

Configure the date and time by using the following command:

```
config setdate <MMddyyyyhhmmss>
```

Specifying the primary SF/CPU

Specify the primary SF/CPU to determine which SF/CPU you use as the primary after the switch performs a full power cycle only. When the SF/CPU becomes the primary, the master LED for the SF/CPU is on.

Procedure steps

1. View the current setting for the primary SF/CPU by using the following command:

   ```
   show bootconfig master
   ```

2. Specify the slot of the primary SF/CPU by using the following command:

   ```
   config bootconfig master <cpu-slot>
   ```

3. Save the configuration to the boot.cfg and pcmboot.cfg files.
4. Restart the switch.

Variable definitions

Use the data in the following table to use the **`config bootconfig master`** command.

Variable	Value
<cpu-slot>	Specifies the slot number for the primary SF/CPU. This variable can be 5 or 6. The default primary is slot 5.

Comments? infodev@avaya.com

Changing passwords

Configure new passwords for each access level, or change the logon or password for the different access levels of the switch. After you receive the Avaya Ethernet Routing Switch 8800/8600, use default passwords to initially access the CLI. If you use Simple Network Management Protocol version 3 (SNMPv3), you can change encrypted passwords.

Prerequisites

- You must use an account with read/write/all privileges to change passwords. For security, the switch saves passwords to a hidden file. The optional parameter *password* is the password associated with the user name or logon name.

Procedure steps

Change a password by using the following command:

```
config cli password
```

Variable definitions

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

Variable	Value
access-level <*access-level*> <*enable*|*disable*>	Permits or blocks this access level. • *access level* is an integer from 2–8. • *enable*|*disable* enables or disables the chosen level.
aging <*days*>	Configures the time limit for passwords. *days* is the age-out time as an integer from 1–365.
min-passwd-len <integer>	Configures the minimum length for passwords in high-secure mode. *integer* is in a minimum range of 10–20.
default-lockout-time <*secs*>	Changes the default lockout time after three invalid attempts. *secs* is the lockout time in

Variable	Value
	seconds and is in the 60–6500 range. The default is 60 seconds.
lockout-time <*IPAddress/IPv6Address*> <*secs*>	Configures the host lockout time. • *IP Address/IPv6 Address* is the host IPv4 address in the format {a.b.c.d.} or the IPv6 address in the format {x:x:x:x:x:x:x:x}. • *secs* is the lockout time limit in seconds for passwords lockout in the 60–65000 range. The default is 60 seconds.
info	Shows the level parameter settings and the next level directories.
l1 <*username*> [<*password*>]	Changes the Layer 1 read/write logon or password. • *username* is the logon name • *password* is the password associated with the logon name.
l2 <*username*> <*password*>	Changes the Layer 2 read/write logon or password. *username* is the logon name.
l3 <*username*> [<*password*>]	Changes the Layer 3 read/write logon and/or password (applies only to the Avaya Ethernet Routing Switch 8800/8600). • *username* is the logon name. • *password* is the password associated with the logon name.
l4admin <*username*>	Configures the Layer 4 administrator logon to connect to the Web Switching Module (WSM). This release does not support the WSM module.
l4oper <*username*>	Configures the Layer 4 operator logon to connect to the WSM. This release does not support the WSM module.
oper <*username*>	Configures the operator logon to connect to the WSM. This release does not support the WSM module.
ro <*username*> [<*password*>]	Changes the read-only logon or password. • *username* is the logon name. • *password* is the password associated with the logon name.

Comments? infodev@avaya.com

Variable	Value
rw <*username*> [<*password*>]	Changes the read/write logon or password. • *username* is the logon name. • *password* is the password associated with the logon name.
rwa <*username*> [<*password*>]	Changes the read/write/all logon or password. • *username* is the logon name. • *password* is the password associated with the logon name.
password-history <*number*>	Specifies the number of previous passwords the switch stores. You cannot reuse a password that is stored in the password history. *number* uses a configurable range of 3–32 and the default is 3.

Saving the configuration

After you change the boot configuration, you must save the changes to both the master and the standby management modules. Save the configuration to a file to retain the configuration settings.

Procedure steps

Save to configuration by using the following command:

```
save <savetype> [file <value>] [verbose] [standby <value>]
[backup <value>] [mode <cli|ncli>]
```

Variable definitions

Use the data in the following table to use the **save** command.

Variable	Value
backup <*value*>	Saves the specified file name and identifies the file as a backup file. *value* uses one of the following formats:

Variable	Value
	• /pcmcia/ <file> • /flash/ <file> File is a string of 1–99 characters.
file <*value*>	Specifies the file name in one of the following formats for *value*: • [a.b.c.d]: <file> • peer/<file> • /pcmcia/ <file> • /flash/ <file> File is a string of 1–99 characters.
mode <cli|ncli>	Saves the configuration as CLI or ACLI.
savetype	Specifies what information to save. Possible values for this parameter are, • config • bootconfig • log • trace • clilog • snmplog
standby <*value*>	Saves the specified file name to the standby SF/CPU in the following format for *value*: • filename, /pcmcia/ <file> • /flash/ <file> File is a string of 1–99 characters.
verbose	Saves the default and current configuration. If you omit this parameter, the command saves only parameters you change.

Comments? infodev@avaya.com

Chapter 5: Initial steps using the ACLI

This chapter describes the basic configuration procedures for the initial provisioning of the switch.

Prerequisites to initial steps

- You must install the hardware.
- You must install at least one cable to set up a remote connection to the switch.
- You must turn on the switch.

Connecting a terminal

Connect a terminal to the serial console interface to monitor and configure the switch.

Prerequisites

- To use the console port, you need the following equipment:
  - a terminal or teletypewriter (TTY)-compatible terminal, or a portable computer with a serial port and terminal-emulation software
  - an Underwriters Laboratories (UL)-listed straight-through or null modem RS-232 cable with a female DB-9 connector for the console port on the switch

    The other end of the cable must use a connector appropriate to the serial port on your computer or terminal. Most computers or terminals use a male DB-25 connector. A null modem cable is shipped with the chassis.
- You must shield the cable connected to the console port to comply with emissions regulations and requirements.

Procedure steps

1. Configure the terminal protocol as follows:
   - 9600 baud
   - 8 data bits
   - 1 stop bit
   - No parity
2. Connect the RS-232 cable to the console port.
3. Connect the other end of the RS-232 cable to the terminal or computer serial port.
4. Turn on the terminal.
5. Log on to the ACLI.

Connecting a modem

Connect a modem to an Avaya Ethernet Routing Switch 8800/8600 to establish a connection with the switch. You can configure the modem port first using another type of connection, such as a terminal connection, to the ACLI.

Prerequisites

- You need a DTE-to-DCE cable (straight or transmit cable) to connect the Avaya Ethernet Routing Switch 8800/8600 to the modem.
- You must configure your client dial-up settings to establish the connection to the modem.
- You must log on to the Global Configuration mode in the ACLI.

Procedure steps

1. Configure port parameters based on the modem requirements by using the following command:

   ```
   boot config sio modem [8databits][baud <rate>] [mode <ascii|slip|ppp>]
   ```


Comments? infodev@avaya.com

For more information about the configuration requirements of your modem, see the documentation shipped with the modem.

Important:

Avaya recommends that before you configure the Serial Line Internet Protocol (SLIP) or the Point-to-Point Protocol (PPP), you familiarize yourself with these protocols.

2. If you configure the port mode to **slip**, use the following command to configure other SLIP parameters:

   ```
   boot config sio modem [slip-compression] [slip-rx-compression]
   ```

3. If you configure the port mode to **ppp**, use the following commands to configure other PPP parameters:

   ```
   boot config sio modem [mtu <bytes>] [my-ip <ipaddr>] [peer-ip <ipaddr>] pppfile <file>
   ```

4. On the modem, turn off echo mode and return code messaging.
5. Connect the modem to the modem port.
6. Save the boot configuration.
7. Optionally, shutdown and reinitialize the port by using the following command:

   ```
   boot config sio modem restart
   ```

8. Restart the switch.

Variable definitions

Use the data in the following table to use the **boot config sio** command.

Variable	Value
8databits	Specifies either 8 (enabled) or 7 (disabled) data bits for each byte for software to interpret. The default is disabled. Use the no operator to remove this configuration. To configure this option to the default value, use the default operator with the command.
baud <*rate*>	Configures the baud rate for the port. The default is 9600. To configure this option to the default value, use the default operator with the command.
mode <ascii|slip|ppp>	Configures the communication mode for the serial port. The default is American Standard Code for Information Interchange (ASCII).

Variable	Value
	If you are configuring the modem port, you can configure the port to use either the SLIP or the PPP communication mode. To configure this option to the default value, use the default operator with the command.
mtu <*bytes*>	Configures the size of the maximum transmission unit for a PPP link (0–2048). The default is 0. To configure this option to the default value, use the default operator with the command.
my-ip <*ipaddr*>	Configures the IP address for the server side, the Avaya Ethernet Routing Switch 8800/8600, of the point-to-point link. The default is 0.0.0.0. Avaya recommends that you use the current IP address for the management port. To configure this option to the default value, use the default operator with the command.
peer-ip <*ipaddr*>	Configures the peer (PC) IP address on the point-to-point link. The default is 0.0.0.0. The switch assigns this value to any PC that connects through the modem port with configured TCP/IP properties to obtain an IP address automatically. If the client uses a static IP address, the Avaya Ethernet Routing Switch 8800/8600 accepts this address. If you use Password Authentication Protocol (PAP) authentication, you must ensure that the client uses the correct IP address. To configure this option to the default value, use the default operator with the command.
pppfile <*file*>	Specifies the PPP configuration file to provide details for authentication and other options to include during the boot procedure of the switch. The PPP file name is a string value of no more than 64 characters. Identify the file in the format {a.b.c.d:|peer:|/pcmcia/|/flash/}<file>. For more information about this file, see Job aid on page 47. **Important:** Do not specify a PPP file name with more than 64 characters. To configure this option to the default value, use the default operator with the command.
restart	Shuts down and initializes the port.
slip-compression	Enables or disables Transmission Control Protocol over IP (TCP/IP) header compression for SLIP mode. The default is false. Use the no operator to remove this configuration. To configure this option to the default value, use the default operator with the command.

Comments? infodev@avaya.com

Variable	Value
slip-rx-compression	Enables or disables TCP/IP header compression on the receive packet for SLIP mode. The default is false. Use the no operator to remove this configuration. To configure this option to the default value, use the default operator with the command.

Job aid

Create the PPP file with one option on each line; comment lines start with a pound sign (#). The following table lists the recognized options.

Option	Description
asyncmap <value>	Configures the desired async map to the value you specify.
chap_file <file>	Obtains Challenge-Handshake Authentication Protocol (CHAP) secrets from the specified file. You require this option if either peer requires CHAP authentication. If your users must use the same IP address, the PAP and CHAP secret files must specify the same IP address for all users and it must match the peer-ip setting on the modem port.
chap_interval <value>	Configures the interval, in seconds, for the CHAP rechallenge to the value you specify.
chap_restart <value>	Configures the timeout, in seconds, for CHAP negotiation to the value you specify.
debug	Activates the PPP daemon debug mode.
default_route	Adds a default route to the system routing table, after successful Internet Protocol Control Protocol (IPCP) negotiation. Use the peer as the gateway. After the PPP connection ends, the system removes this entry.
driver_debug	Activates PPP driver debug mode.
escape_chars <value>	Configures the characters to escape on transmission to the value you specify.
ipcp_accept_local	Accepts what the remote peer uses as the target local IP address, even if the local IP address is specified.

Option	Description
ipcp_accept_remote	Accepts what the remote peer uses as the IP address, even if you specify the remote IP address.
ipcp_max_configure <value>	Configures the maximum number of transmissions for IPCP configuration requests to the value you specify.
ipcp_max_failure <value>	Configures the maximum number of IPCP configuration negative acknowledgements (NAK) to the value you specify.
ipcp_max_terminate <value>	Configures the maximum number of transmissions for IPCP termination requests to the value you specify.
ipcp_restart <value>	Configures the timeout, in seconds, for IPCP negotiation to the value you specify.
lcp_echo_failure <value>	Configures the maximum consecutive Link Control Protocol (LCP) echo failures to the value you specify.
lcp_echo_interval <value>	Configures the interval, in seconds, between LCP echo requests to the value you specify.
lcp_max_configure <value>	Configures the maximum number of transmissions for LCP configuration requests to the value you specify.
lcp_max_failure <value>	Configures the maximum number of LCP configuration NAKs to the value you specify.
lcp_max_terminate <value>	Configures the maximum number of transmissions for LCP termination requests to the value you specify.
lcp_restart <value>	Configures the timeout in seconds for the LCP negotiation to the value you specify.
local_auth_name <name>	Configures the local name for authentication to the specified name.
login	Uses the logon password database for Password Authentication Protocol (PAP) peer authentication.
max_challenge <value>	Configures the maximum number of transmissions for CHAP challenge requests to the value you specify.
mru <value>	Configures the maximum receive unit (MRU) size for negotiation to the value you specify.

Comments? infodev@avaya.com

Option	Description
mtu <value>	Configures the maximum transmission unit (MTU) size for negotiation to the value you specify.
netmask <value>	Configures the netmask value for negotiation to the value you specify.
no_acc	Disables address control compression.
no_all	Does not request or allow options.
no_asyncmap	Disables async map negotiation.
no_chap	Disallows CHAP authentication with peer.
no_ip	Disables IP address negotiation in IPCP.
no_mn	Disables magic number negotiation.
no_mru	Disables MRU negotiation.
no_pap	Disables PAP authentication with the peer.
no_pc	Disables protocol field compression.
no_vj	Disables Van Jacobson (VJ) compression. VJ compression reduces the regular 40-byte TCP/IP header to 3 or 8 bytes.
no_vjccomp	Disables VJ connection ID compression.
pap_file <file>	Obtains PAP secrets from the specified file. You require this option if either peer requires PAP authentication. If your users must use the same IP address, the PAP and CHAP secret files must specify the same IP address for all users and it must match the peer-ip setting on the modem port.
pap_max_authreq <value>	Configures the maximum number of transmissions for PAP authentication requests to the value you specify.
pap_passwd <password>	Configures the password for PAP authentication with the peer to the specified password.
pap_restart <value>	Configures the timeout, in seconds, for PAP negotiation to the value you specify.
pap_user_name <name>	Configures the user name for PAP authentication with the peer to the specified name.
passive_mode	Configures passive mode. PPP waits for the peer to connect after an initial connection attempt.

Option	Description
proxy_arp	Adds an entry to the Address Resolution Protocol (ARP) table with the IP address of the peer and the Ethernet address of the local system.
remote_auth_name <name>	Configures the remote name for authentication to the specified name.
require_chap	Requires CHAP authentication with peer.
require_pap	Requires PAP authentication with peer.
silent_mode	Configures silent mode. PPP does not transmit LCP packets to initiate a connection until it receives a valid LCP packet from the peer.
vj_max_slots <value>	Configures the maximum number of VJ compression header slots to the value you specify.

Table 7: Sample PPP file on page 50 shows example contents from a PPP file.

Table 7: Sample PPP file

```
passive_mode
lcp_echo_interval 30
lcp_echo_failure 10
require_chap
require_pap
no_vj
ipcp_accept_remote
login
chap_file "my_chap"
pap_file "my_pap"
```

Configuring the switch with the setup utility

Configure the switch with the setup utility to monitor system requirements and obtain the maximum system performance.

Comments? infodev@avaya.com

Prerequisites

- You must log on to the Privileged EXEC mode in the ACLI.

Procedure steps

1. Start the setup utility by using the following command:

   ```
   install
   ```

2. Respond to the series of questions displayed on the screen.

   For more information about the prompted questions, see the following job aid.

3. Restart the switch.

Job aid

The following table lists the questions prompted by the setup utility and provides a description for each.

Prompt	Description and action
Please provide primary config-file path [/flash/config.cfg]:	Description: Indicates the name of the primary configuration file. Action: Press `Enter` to accept the default (/flash/config.cfg), or type a different file name for the primary configuration file. To store your configuration file on the external flash (8895 SF/CPU) or PCMCIA card (8692 SF/CPU), use /PCMCIA/config.cfg. To specify the path to the file is optional.
Please provide primary image-file path [/flash/p80a4100.img]:	Description: Indicates the name of the primary image file. Action: Press `Enter` to accept the default (p80a4100.img), or type a different file name for the primary image file. To specify the path to the file is optional. If your run-time image resides on your external flash (8895 SF/CPU) or PCMCIA card (8692 SF/CPU), you must specify the path as /PCMCIA/ file name.
Please add system prompt [ERS-8606]:	Description: Specifies the text for the prompt. Action: Press `Enter` to accept the default (ERS-8610), or type a different string of up to 20 characters.

Prompt	Description and action
Please select CPU primary slot (5/6) [5]:	Description: Indicates the slot number of the primary central processing unit (CPU). The slot can be 5 or 6. Action: Press `Enter` to accept the default (5), or specify 6.
Primary CPU mgmt port: autonegotiation [n] (y/n)?	Description: Specifies if you want the primary CPU to use autonegotiation. Action: Enter **n** to accept the default, or enter **y** to indicate that you want the primary CPU management port to use autonegotiation.
speed (10/100) [10]:	Description: Specifies the line speed in Mb/s. Action: Press `Enter` to accept the default (10 Mb/s), or specify 100 Mb/s.
Do you want to enable automatic savetostandby mode [n] (y/n)?	Description: Specifies if you want the boot and run-time configuration files to be saved on the backup CPU. Action: Enter **y** to save the boot and run-time configuration files on the backup CPU. Accept the default (**n**) to save boot and run-time configuration files on the primary CPU.
Do you want to enable enhanced operation mode support [n] (y/n)?	Description: Specifies if you want to enable enhanced operation mode. Enhanced operation mode increases the maximum number of VLANs when you use MultiLink Trunking (MLT) (1980) and Split MLT (SMLT) (989). Action: Enter **y** to enable enhanced operation mode. Accept the default (**n**), to disable enhanced operation mode.
Do you want to enable CPU High Availability mode [n] (y/n)?	Description: Specifies if you want to enable CPU high availability (HA) mode. Use CPU HA mode to recover switches with two CPUs quickly from a failure of one of the CPUs. In HA mode (hot standby), you synchronize and configure the two CPUs in the same mode, so they are compatible. Action: Specify **y** to enable CPU high availability (HA) mode. Accept the default (**n**), to disable CPU HA mode.
Do you want to enable vlan-optimization-mode support [n] (y/n) ?	Description: Specifies if you want to enable support for the VLAN optimization mode. Action: Specify y to enable VLAN optimization mode support. Accept the default (**n**) to disable VLAN optimization mode support.
Do you want to enable FTP [n] (y/n)?	Description: Specifies if you want users to access the switch by File transfer Protocol (FTP).

Comments? infodev@avaya.com

Prompt	Description and action
	Action: Enter **y** to enable FTP for remote users. Accept the default (**n**) to disable FTP.
Do you want to enable RLOGIN [n] (y/n)?	Description: Specifies if you want to access the switch by Rlogin. Action: Enter **y** to enable Rlogin for remote users. Accept the default (**n**) to disable Rlogin.
Do you want to enable TELNET [n] (y/n)?	Description: Specifies if you want to access the switch by Telnet. Action: Enter **y** to enable Telnet. Accept the default (**n**) to disable Telnet.
Do you want to enable TFTP [n] (y/n)?	Description: Specifies if you want to access the switch by Trivial FTP (TFTP). Action: Enter **y** to enable TFTP. Accept the default (**n**) to disable TFTP.
Do you want to enable WEB server service [n] (y/n)?	Description: Specifies if you want to enable Web server service. Use the Web server service to monitor statistics for the switch with your Web browser. Action: Enter **y** to enable Web server service. Accept the default (**n**) to disable Web server service.
IP Address for mgmt port in first CPU Slot [192.168.168.168/255.255.2.55.0]:	Description: Indicates the IP address for the management port in the CPU slot you specify. Action: Type the IP address of the management port in the first CPU slot.
IP Address for mgmt port in second CPU Slot [192.168.168.169/255.255.255.0]:	Description: Indicates the IP address for the management port in the CPU slot you specify. Action: Type the IP address of the management port in the second CPU slot.
IP Address for mgmt-virtual-ip [0.0.0.0/0.0.0.0]:	Description: Indicates the IP address for the virtual management port. Action: Type the IP address of the virtual management port. Accept the default (0.0.0.0/0.0.0.0) to not specify an IP address.
First net mgmt route [0.0.0.0:0.0.0.0]:	Description: Specifies the IP address of the first network management route (static route from the network management port to a device in the network). Action: Type the network and gateway IP address of the first network management route.
Second net mgmt route [0.0.0.0:0.0.0.0]:	Description: Specifies the IP address of the second network management route. Action: Type the IP address of the second network management route (static route from the network management port to a device in the network).

Prompt	Description and action
Third net mgmt route [0.0.0.0:0.0.0.0]:	Description: Specifies the IP address of the third network management route. Action: Type the IP address of the third network management route (static route from the network management port to a device in the network).
Fourth net mgmt route [0.0.0.0:0.0.0.0]:	Description: Specifies the IP address of the fourth network management route. Action: Type an IP address of the fourth network management route (static route from the network management port to a device in the network).
IP address of the default VLAN [0.0.0.0/0.0.0.0]:	Description: Specifies the IP address of the default Virtual Local Area Network (VLAN). Action: Type the IP address of the default VLAN.
Do you want to save the changes? [Saving the parameters updates the files /flash/boot.cfg and /flash/dvmrp_pol.cfg] (y/n)?	Description: Saves your changes to the boot and run-time configuration files. Action: Enter **y** to save the boot and run-time configuration files. Enter **n** if you do not want to save your changes.

Configuring system identification

Configure system identification to specify the system name, contact person, and location of the switch.

Prerequisites

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

Procedure steps

1. Change the system name by using the following command:

   ```
   sys name <word 0-255>
   ```

2. Configure the system location by using the following command:

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


Comments? infodev@avaya.com

Variable definitions

Use the data in the following table to use system-level commands.

Variable	Value
agent-conformance	Enables agent conformance mode.
authentication-trap	Enables or disables generation of authentication traps.
bootstrap	Sets SNMP initial user entry.
community	Sets community table.
contact <word>	Identifies the contact person who manages the node. To include blank spaces in the contact, use quotation marks (") around the text. Use the no operator to remove this configuration. To configure this option to the default value, use the default operator with the command. The default is support@avaya.com.
force-iphdr-sender	Sets same SNMP and IP sender flag.
force-trap-sender	Sets SNMP trap sender IP.
group	Sets SNMP v3 group access table.
host	Specifies hosts to receive SNMP notifications.
location <word>	Identifies the physical location of the node. To include blank spaces in the location, use quotation marks (") around the text. Use the no operator to remove this configuration. To configure this option to the default value, use the default operator with the command. The default is an Avaya address.
log	Specifies the SNMP log feature.
name <*word*>	Configures the system or root level prompt name for the switch. *word* is an ASCII string from 1 to 255 characters (for example, LabSC7 or Closet4).
notify-filter	Creates new entry for notify filter table.
sender-ip	Sets SNMP trap sender IP.
user	Creates or modifies SNMPv3 user.
view	Creates or modifies an SNMP access view.

Example of configuring system identification

Procedure steps

1. Change the system name by using the following command:

   ```
   ERS-8610:5(config)# sys name ERS-8610
   ```

2. Configure the system location by using the following command:

   ```
   ERS-8610:5(config)# snmp-server location "12 Main St,
   Vancouver, BC"
   ```

Configuring the time zone

Configure the time zone to specify the time zone for your location and configure settings for Daylight Saving Time (DST).

Prerequisites

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

Procedure steps

1. Configure the time zone by using the following command:

   ```
   boot config tz
   ```

2. Save the changed configuration to the boot.cfg and pcmboot.cfg files.
3. Restart the switch.

Variable definitions

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

Variable	Value
dst-end <*Mm.n.d/hhmm*|*MMddhhmm*>	Configures the ending date of DST. You can specify the time in one of two ways:

Comments? infodev@avaya.com

Variable	Value
	• *Mm.n.d/hhmm* specifies an hour on the nth occurrence of a weekday in a month. For example, M10.5.0/0200 means the fifth occurrence of Sunday in the tenth month (October) at 2:00 a.m. • *MMddhhmm* specifies a month, day, hour, and minute. For example, 10310200 means October 31 at 2:00 a.m.
dst-name <*WORD 1-7*>	Configures an abbreviated name for the local daylight saving time zone. *dstname* is the name. For example, PDT is Pacific Daylight Time. To configure this option to the default value, use the default operator with the command. *WORD <1-7>* daylight saving timezone abbreviation.
dst-offset <*WORD 0-6*>	Configures the daylight saving adjustment in minutes or in hours and minutes (hh:mm). The default is 60 minutes. To configure this option to the default value, use the default operator with the command *WORD<0-6>*. Daylight saving adjustment {hh:mm{-4:00-4:00}/minutes{-240-240}}.
dst-start <*Mm.n.d/hhmm*|*MMddhhmm*>	Configures the starting date of DST. • *Mm.n.d/hhmm* specifies an hour on the nth occurrence of a weekday in a month. For example, M10.5.0/0200 means the fifth occurrence of Sunday in the tenth month (October) at 2:00 a.m. • *MMddhhmm* specifies a month, day, hour, and minute. For example, 10310200 means October 31 at 2:00 a.m.
name <*WORD 1-7*>	Configures an abbreviated name for the local time zone name. *tz* is the name. For example, PST is Pacific Standard Time. To configure this option to the default value, use the default operator with the command. <*WORD 1-7*> is the timezone abbreviation.
offset-from-utc <*WORD 0-6*>	Configures the time zone offset in minutes or in hours and minutes (hh:mm) to subtract from Universal Coordinated Time (UTC), where positive numbers mean west of Greenwich and negative numbers mean east of Greenwich. To configure this option to the default value, use the default operator with the command.

Configuring the date

Configure the calendar date and time in the form of month, day, year, hour, minute, and second.

Prerequisites

- You must log on to the Privileged EXEC mode in the ACLI.

Procedure steps

Configure the calendar date and time by using the following command:

```
clock set <MMddyyyyhhmmss> MMddyyyyhhmmss
```

Specifying the primary SF/CPU

Specify the primary SF/CPU to determine which SF/CPU you use as the master after the switch performs a full power cycle only. When the SF/CPU becomes the primary, the master LED for the SF/CPU is on.

Prerequisites

- You must log on to at least Privileged EXEC mode to use the show command.
- You must log on to the Global Configuration mode in the ACLI to use the configuration command in this procedure.

Procedure steps

1. View the current setting for the primary SF/CPU by using the following command:

   ```
   show boot config master
   ```

2. Specify the slot of the primary SF/CPU by using the following command:

Comments? infodev@avaya.com

```
boot config master <cpu-slot>
```

3. Save the configuration to the boot.cfg and pcmboot.cfg files.
4. Restart the switch.

Variable definitions

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

Variable	Value
<*cpu-slot*>	Specifies the slot number for the primary SF/CPU. This variable can be 5 or 6. The default primary is slot 5.

Changing passwords

Configure new passwords for each access level, or change the logon or password for the different access levels of the switch. After you receive the Avaya Ethernet Routing Switch 8800/8600, use default passwords to initially access the ACLI. If you use Simple Network Management Protocol version 3 (SNMPv3), you can change encrypted passwords.

Prerequisites

- You must use an account with read/write/all privileges to change passwords. For security, the switch saves passwords to a hidden file.
- You must log on to the Global Configuration mode in the ACLI.

Procedure steps

1. Change a password by using the following command:

   ```
   cli password <word 1-20> <access-level>
   ```

2. Configure password options by using the following command:

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

Variable definitions

Use the data in the following table to use the password commands.

Variable	Value
access level <word>	Permits or blocks this access level. The available access level values are: • l4admin • l4oper • layer1 <word> • layer2 • layer3 <word> • oper • read-only <word> • read-write <word> • read-write-all <word> • slbadmin • slboper • ssladmin <*word*> represents the new password with 0–20 characters.
aging-time day <*1-365*>	Configures the expiration period for passwords in days, from 1–365.
default-lockout-time <*60-65000*>	Changes the default lockout time after three invalid attempts. Configures the lockout time, in seconds, and is in the 60–65000 range. The default is 60 seconds. To configure this option to the default value, use the default operator with the command.
lockout <*word*> *time* <*time*>	Configures the host lockout time. • *word* is the host IP address in the format a.b.c.d. • *time* is the lockout-out time, in seconds, in the 60–65000 range. The default is 60 seconds.
min-passwd-len <*10-20*>	Configures the minimum length for passwords in high-secure mode.

Comments? infodev@avaya.com

Variable	Value
	To configure this option to the default value, use the default operator with the command.
password-history <*3-32*>	Specifies the number of previous passwords the switch stores. You cannot reuse a password that is stored in the password history. The default is 3. To configure this option to the default value, use the default operator with the command.

Saving the configuration

After you change the boot configuration, you must save the changes to both the master and the standby management modules. Save the configuration to a file to retain the configuration settings.

Prerequisites

- You must log on to the Privileged EXEC mode in the ACLI.

Procedure steps

1. Save to boot configuration by using the following command:

   ```
   save boot config [file <word 1-99>] [verbose] [standby <word
   1-99>] [backup <word 1-99>] [mode <cli|ncli>]
   ```

2. Save the running configuration by using the following command:

   ```
   save config [file <word 1-99>] [verbose] [standby <word
   1-99>] [backup <word 1-99>] [mode (cli|ncli)]
   ```

Variable definitions

Use the data in the following table to use the **`save boot config`** and **`save config`** commands.

Variable	Value
backup <word>	Saves the specified file name and identifies the file as a backup file. *word* uses one of the following formats: • [a.b.c.d]:<file> • peer/<file> • /pcmcia/ <file> • /flash/ <file> File is a string of 1–99 characters.
file <word>	Specifies the file name in one of the following formats for *word*: • [a.b.c.d]: <file> • peer/<file> • /pcmcia/ <file> • /flash/ <file> File is a string of 1–99 characters.
mode <cli|ncli>	Saves the boot configuration in CLI or ACLI format.
standby <word>	Saves the specified file name to the standby SF/CPU in the following format for *word*: • filename, /pcmcia/ <file> • /flash/ <file> File is a string of 1–99 characters.
verbose	Saves the default and current configuration. If you omit this parameter, the command saves only parameters you change.

Comments? infodev@avaya.com

Chapter 6: Initial steps using EDM

This chapter describes the basic configuration procedures for the initial provisioning of the switch.

EDM software is bundled with the switch code. However, to access EDM help files, you must install these separately. For more information about EDM, including instructions for installing the EDM help, see *Avaya Ethernet Routing Switch 8800/8600 User Interface Fundamentals, NN46205-308*.

Prerequisites to initial steps using EDM

- You must install the hardware.
- You must install at least one cable to set up a remote connection to the switch.
- You must turn on the switch.
- The switch must be configured with an IP address.
- Connect to the switch IP address using one of the following browsers:
  - Mozilla Firefox, version 3.0
  - Microsoft Internet Explorer, version 7.0

Log on to EDM using rwa/rwa/GlobalRouter as the default credentials.

Important:

If you configured a username and password for Web server access in a previous release, these configured values remain unchanged in this release. To access EDM, use these previously configured username and password values. In this case, the user: `admin` and password: `password` default values do not apply.

Configuring the system using the Quick Start wizard

Configure the system by using the Quick Start wizard for the initial configuration of the switch. The Quick Start wizard uses a series of questions to guide you through the configuration process.

The wizard offers the following setup configurations:

- Basic
- Management

- Remote access
- File

Procedure steps

1. Power up the system.
2. Log into the switch using Enterprise Device Manager. For more information, see *Avaya Ethernet Routing Switch 8800/8600 User Interface Fundamentals* (NN46205-308).
3. In the navigation tree, open the following folders: **Configuration** > **Device** > **Quick Start**
4. Click **Quick Start**.

   A Welcome Step message appears.
5. To continue, click **Start**
6. Follow the Quick Start wizard prompts.

Job aid

The following table describes the Quick Start wizard prompts.

Prompt	Action
System Prompt String	Specifies the system prompt string of up to 20 characters.
Default VLAN IP address	Specifies the IP address of the default VLAN.
CPU Master Slot	Specifies the slot containing the master CPU.
1st CPU IP Address	Specifies the IP address of the management port in the first CPU slot. For example, 192.168.168.168/255.255.255.0.
2nd CPU IP Address	Specifies the IP address of the management port in the second CPU slot.
Virtual IP Address	Specifies the IP address of the virtual management port.
1st Net Management Route	Specifies the IP address of the first network management route. The default is 0.0.0.0/0.0.0.0.
2nd Net Management Route	Specifies the IP address of the second network management route.
3rd Net Management Route	Specifies the IP address of the third network management route.
4th Net Management Route	Specifies the IP address of the fourth network management route.

Comments? infodev@avaya.com

Prompt	Action
Enable Ftp Server	Enables (Yes) or disables (No) the FTP server on the switch.
Enable R-Login	Enables (Yes) or disables (No) R-login on the switch.
Enable Telnet	Enables (Yes) or disables (No) Telnet connections to the switch.
Enable TFTP	Enables (Yes) or disables (No) TFTP on the switch.
Configure-File Path	Specifies the path of the primary switch configuration file. The default is /flash/config.cfg. To store the configuration file on the external compact flash or PCMCIA card, specify /pcmcia/config.cfg.

Editing system information

You can edit system information, such as the contact person, the name of the device, and the location by performing this procedure.

Procedure steps

1. In the navigation tree, open the following folders: **Configuration** > **Edit**.
2. Click **Chassis**.

   The Chassis dialog box appears with the System tab displayed.
3. Type the contact information.
4. Type the system name.
5. Type the location information.
6. Type the Virtual IP address information.
7. Type the Virtual Net mask address information.
8. Type the Virtual IPv6 address information.
9. Type the Virtual IPv6 prefix length information.
10. Click **Apply**.

Variable definitions

Use the data in the following table to configure the System tab.

Variable	Value
sysDescr	Shows the system assigned name and the software version
sysUpTime	Shows the time since the system last started
sysContact	Configures the contact information (in this case, an e-mail address) for the Avaya support group
sysName	Configures the name of this device
sysLocation	Configures the physical location of this device
VirtualIpAddr	Configures the virtual IP address that is advertised by the primary SF/CPU and stored in the switch configuration file and not the boot configuration file
VirtualNetMask	Configures the net mask of the virtual management IP address
VirtualIpv6Address	Configures the virtual IPv6 address that is advertised by the primary SF/CPU. and stored in the switch configuration file and not the boot configuration file
VirtualIPv6Prefix Length	Configures the length of the virtual IPv6 prefix entry
DnsDomainName	Configures the default domain for querying the DNS server
LastChange	Displays the time since the last configuration change
LastVlanChange	Displays the time since the last VLAN change
LastStatisticsReset	Displays the time since the statistics counters were last reset
LastRunTimeConfigSave	Displays the last run-time configuration saved
LastRunTimeConfigSaveToSlave	Displays the last run-time configuration saved to the standby device
LastBootConfigSave	Displays the last boot configuration saved
LastBootConfigSaveOnSlave	Displays the last boot configuration saved on the standby device
DefaultRuntimeConfigFileName	Displays the default run-time configuration file directory name
DefaultBootConfigFileName	Displays the default boot configuration file directory name
ConfigFileName	Specifies the name of a new configuration file
ActionGroup1	Can be one of the following actions:

Comments? infodev@avaya.com

Variable	Value
	• resetCounters—resets all statistic counters • saveRuntimeConfig—saves the current run-time configuration • saveRuntimeConfigToSlave—saves the current run-time configuration to the standby SF/CPU • saveBootConfig—saves the current boot configuration • saveSlaveBootConfig—saves the current boot configuration to the standby SF/CPU • loadLicense—loads a software license file to enable features
ActionGroup2	resetIstStatCounters—resets the IST statistic counters
ActionGroup3	flushIpRouteTbl—flushes IP routes from the routing table
ActionGroup4	Can be one of the following actions: • hardReset—resets the device and runs power-on tests. • softReset—resets the device without running power-on tests • cpuSwitchOver—switch control from one SF/CPU to another • resetConsole—reinitializes the hardware UART drivers. Use only if the console or modem connection is hung • resetModem—reinitializes the UART drivers on the modem port. Use only if the console or modem connection is hung
Result	Displays a message after you click Apply.

Configuring the date and time

Use the User Set Time tab to configure the date and time.

Procedure steps

1. In the navigation tree, open the following folders: **Configuration** > **Edit**.
2. Click **Chassis**.

   The Chassis dialog box appears with the System tab displayed.
3. Click the **User Set Time** tab.
4. Type the correct details.
5. Click **Apply**.

Variable definitions

Use the data in the following table to configure the User Set Time tab.

Variable	Value
Year	Configures the year (integer 1998–2097)
Month	Configures the month
Date	Configures the day (integer 1–31)
Hour	Configures the hour (integer 0–23)
Minute	Configures the minute (integer 0–59)
Second	Configures the second (integer 0–59)

Changing passwords

Configure new passwords for each access level, or change the logon or password for the different access levels of the switch. After you receive the Avaya Ethernet Routing Switch 8800/8600, use default passwords to initially access the CLI. If you use Simple Network Management Protocol version 3 (SNMPv3), you can change passwords that are in encrypted format.

Procedure steps

1. In the navigation tree, open the following folders: **Configuration** > **Security** > **Control Path**.
2. Click **General**.

   The Port Lock dialog box appears with the System tab displayed.
3. Click the **CLI** tab.
4. Specify the user name and password for the appropriate access level.
5. Click **Apply**.

Variable definitions

Use the data in the following table to configure the CLI tab.

Variable	Value
RWAUserName	Specifies the user name for the read/write/all CLI account.
RWAPassword	Specifies the password for the read/write/all CLI account.
RWEnable	Activates the read/write access level.
RWUserName	Specifies the user name for the read/write CLI account.
RWPassword	Specifies the password for the read/write CLI account.
RWL3Enable	Activates the read/write Layer 3 access level.
RWL3UserName	Specifies the user name for the Layer 3 read/write CLI account.
RWL3Password	Specifies the password for the Layer 3 read/write CLI account.
RWL2Enable	Activates the read/write Layer 2 access level.
RWL2UserName	Specifies the user name for the Layer 2 read/write CLI account.
RWL2Password	Specifies the password for the Layer 2 read/write CLI account.
RWL1Enable	Activates the read/write Layer 1 access level.
RWL1UserName	Specifies the user name for the Layer 1 read/write CLI account.
RWL1Password	Specifies the password for the Layer 1 read/write CLI account.

Variable	Value
ROEnable	Activates the read/only CLI account level.
WebUserName	Specifies the user name for the read-only CLI account.
WebPassword	Specifies the password for the read-only CLI account.
MaxTelnetSessions	Indicates the maximum number of concurrent Telnet sessions (0–8).
MaxRloginSessions	Indicates the maximum number of concurrent Rlogin sessions (0–8).
Timeout	Indicates the number of seconds of inactivity for a Telnet or Rlogin session before automatic timeout and disconnect (30–65535 seconds).
NumAccessViolations	Indicates the number of CLI access violations detected by the system. This field is a read-only field.

Saving the configuration

After you change the boot configuration, you must save the changes to both the master and the standby management modules. Save the configuration to a file to retain the configuration settings.

Procedure steps

1. In the navigation tree, open the following folders: **Configuration** > **Edit**.
2. Click **Chassis**.

   The Chassis dialog box appears with the System tab displayed.
3. Scroll down to the ActionGroup1 section and select **saveBootConfig** to save the boot configuration.
4. Click **Apply**.
5. Select **saveRuntimeConfig** to save the current configuration.
6. Click **Apply**.

Comments? infodev@avaya.com

Chapter 7: Remote connection configuration using the CLI

This section contains the minimum information required to configure a management interface to set up a remote connection.

Assigning an IP address to the management port

Assign an IP address to the management port to use it for out-of-band (OOB) management. The standby IP must be in the same subnet as the master IP. Create a virtual management port in addition to the physical management ports on the switch management modules.

Procedure steps

1. Assign an IP address to the management port by using the following command:

   ```
   config bootconfig net mgmt ip <ipaddr/mask> [cpu-slot <value>]
   ```

2. Assign an IP address to a virtual management port by using the following command:

   ```
   config sys set mgmt-virtual-ip <ipaddr/mask>
   ```

3. Save the changes to the boot.cfg and config.cfg files.

Variable definitions

Use the data in the following table to use the **`config bootconfig net mgmt ip`** and **`config sys set mgmt-virtual-ip`** commands.

Variable	Value
cpu-slot <value>	Specifies the Switch Fabric/Central Processor Unit (SF/CPU) module (8692 SF/CPU or 8895 SF/CPU), slot 5 or slot 6. If you do not specify a slot number for the IP address, the switch assigns the slot number to the currently active management module.
ipaddr/mask	Specifies the IP address and subnet mask of the management port (for example,

Variable	Value
	10.127.231.15/255.255.255.0). You cannot assign an address of 0.0.0.0/0.

Assigning static routes to the management interface

Assign a static route to specify a gateway address route for the management interface. You can specify up to four static routes for the management interface. For more information about static routes, see *Avaya Ethernet Routing Switch 8800/8600 Configuration — IP Routing, NN46205-523*.

Procedure steps

1. Specify a gateway address route by using the following command:

   ```
   config bootconfig net mgmt route [add|del] <netaddr/mask>
   <gateway>
   ```

2. Save the changes to the boot.cfg and config.cfg files.

Variable definitions

Use the data in the following table to use the **`config bootconfig net mgmt route [add|del]`** command.

Variable	Value
[add|del]	Adds or deletes a route.
gateway	Configures the IP address of the default gateway.
netaddr/mask	Configures the IP address and mask of the destination network in the formats a.b.c.d/x | a.b.c.d/x.x.x.x | default.

Example of assigning a static route to the management interface

Procedure steps

If you locate a management station on the network of 11.0.0.0/255.0.0.0, and the next hop to that network from the management interface is 10.127.231.1, enter the following command to configure the management port:

```
config bootconfig net mgmt route add 11.0.0.0/255.0.0.0
10.127.231.1
```

The value 11.0.0.0/255.0.0.0 represents the target subnet; the value 10.127.231.1 represents the gateway you use to point to the target subnet.

Important:

The **`config bootconfig net mgmt route add`** command uses the natural mask of the target subnet. Therefore, in the preceding example, what you implement is the command: **`config bootconfig net mgmt route add 13.0.0.0 10.125.2.1`**. Additionally, this route does not appear in the routing table of the Avaya Ethernet Routing Switch 8800/8600. If you configure a 13.x.x.x network for output using the I/O modules, the switch can experience connectivity issues.

Enabling remote access services

Enable the remote access service to provide multiple methods of remote access.

Prerequisites

- When you enable an Rlogin flag, you must configure an access policy and specify the user name of who can access the switch. For more information about the access policy commands, see *Avaya Ethernet Routing Switch 8800/8600 Security, NN46205-601*.

Procedure steps

1. Enable or disable the access service, in the run-time CLI, by using the following command:

   ```
   config bootconfig flags <access-service> <true|false>
   ```

2. Save the configuration.

Alternatively, you can configure remote access services from the boot monitor CLI.

1. Reboot the switch.
2. While the switch is starting, press any key to interrupt the autoboot process and access the boot-monitor CLI.
3. Enable or disable the access service by using the following command:

   ```
   flags <access-service> <true|false>
   ```

4. Save the boot configuration.

Variable definitions

Use the data in the following table to use the **flags** command.

Variable	Value
access-service	Specifies the type of remote access service as one of the following: • ftpd • rlogind • telnetd • tftpd • sshd
true|false	True enables the service. False disables the service.

Enabling the Web server for EDM access

Enable the Web server to provide management access to the switch using Enterprise Device Manager (EDM). For more information about EDM, see *Avaya Ethernet Routing Switch User Interface Fundamentals, NN46205-308*.

Procedure steps

1. Enable the Web server by using the following command:

   ```
   config web-server enable
   ```

2. Configure the access password by using the following command:

   ```
   config web-server password <rwa> <username> <password>
   ```

Variable definitions

Use the data in the following table to use the **config web-server** command.

Variable	Value
enable	Enables the Ethernet Routing Switch Web server.

Comments? infodev@avaya.com

Variable	Value
password <rwa> <username> <password>	Configures the password for access to EDM. **username** is the user logon name (up to 20 characters). **password** is the password associated with the logon name (up to 20 characters). Default values are rwa/rwa.

Configuring the remote host logon

Configure the remote host logon to modify parameters for FTP and TFTP access. Use the default parameters for TFTP transfers. If you want to use FTP as the transfer mechanism, you need to change the password to a valid value.

Procedure steps

1. Define conditions for the remote host logon by using the following command:

   ```
   config bootconfig host
   ```

2. Save the changed configuration to the boot.cfg and pcmboot.cfg files.
3. Restart the switch.

Variable definitions

Use the data in the following table to use the **config bootconfig host** command.

Variable	Value
ftp-debug <true|false>	Enables or disables debug mode on FTP. If you enable debug mode, debug messages appear on the management console screen. The default is false.
info	Displays the current remote host logon settings.
password <*value*>	Configures the password to enable FTP transfers. *value* is the password, up to 16 characters long. After you configure this password, use only FTP for remote host logon. **Important:** This password must match the password for the FTP server, or the FTP operation fails. Also, if you configure the password to a valid value, then all copying to and from the network uses FTP instead of TFTP. If the user name or password is incorrect, copying over the network fails.

Variable	Value
tftp-debug <true|false>	Enables or disables debug mode on TFTP/TFTPD. If you enable debug mode, debug messages appear on the management console screen. The default is false.
tftp-hash <true|false>	Enables or disables the TFTP hash bucket display. The default is false.
tftp-rexmit <*seconds*>	Configures the TFTP retransmission timeout. The default value is 2 seconds. *seconds* is the number of seconds (1–2147483647).
tftp-timeout <*seconds*>	Configures the TFTP timeout. The default value is 6 seconds. *seconds* is the number of seconds (1–120).
user <*value*>	Configures the remote user logon. *value* is the user logon name (up to 16 characters).

Comments? infodev@avaya.com

Chapter 8: Remote connection configuration using the ACLI

This section contains the minimum information to configure a management interface to set up a remote connection.

Assigning an IP address to the management port

Assign an IP address to the management port to use it for out-of-band (OOB) management. The standby IP must be in the same subnet as the master IP. Create a virtual management port in addition to the physical management ports on the switch management modules.

Prerequisites

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

Procedure steps

1. Assign an IP address to the management port by using the following command:

   ```
   boot config net mgmt ip <ipaddr> <mask> <value>
   ```

2. Assign an IP address to a virtual management port by using the following command:

   ```
   sys mgmt-virtual-ip <ipaddr/mask>
   ```

3. Save the changes to the boot.cfg and config.cfg files.

Variable definitions

Use the data in the following table to use the **`boot config net mgmt ip`** and **`sys mgmt-virtual-ip`** commands.

Variable	Value
cpu-slot <value>	Specifies the Switch Fabric/Central Processor Unit (SF/CPU) module (8692 SF/CPU or 8895 SF/CPU), slot 5 or slot 6. If you do not specify a slot number for the IP address, the switch assigns the slot number to the currently active management module.
<ipaddr> <mask>	Specifies the IP address and subnet mask of the management port (for example, 10.127.231.15 255.255.255.0). **Important:** You cannot assign an address of 0.0.0.0/0.

Assigning static routes to the management interface

Assign a static route to specify a gateway address route for the management interface. You can specify up to four static routes for the management interface. For more information about static routes, see *Avaya Ethernet Routing Switch 8800/8600 Configuration — OSPF and RIP, NN46205-522*.

Prerequisites

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

Procedure steps

1. Specify a gateway address route by using the following command:

   ```
   boot config net mgmt route <netaddr/mask> <gateway>
   ```

2. Save the changes to the boot.cfg and config.cfg files.

Variable definitions

Use the data in the following table to use the **`boot config net mgmt route`** command.

Comments? infodev@avaya.com

Variable	Value
gateway	Configures the IP address of the default gateway.
netaddr/mask	Configures the IP address and mask of the destination network in the formats a.b.c.d/x | a.b.c.d/x.x.x.x | default.

Example of assigning a static route to the management interface

Procedure steps

If you locate a management station on the network of 11.0.0.0/255.0.0.0, and the next hop to that network from the management interface is 10.127.231.1, enter the following command to configure the management port:

```
ERS-8606:5(config)# boot config net mgmt route
11.0.0.0/255.0.0.0 10.127.231.1
```

The value 11.0.0.0/255.0.0.0 represents the target subnet; the value 10.127.231.1 represents the gateway used to point to the target subnet.

Important:

The **`config net mgmt route`** command uses the natural mask of the target subnet. Therefore, in the preceding example, what you implement is the command: **`config net mgmt route 13.0.0.0 10.125.2.1`**. Additionally, this route does not appear in the routing table of the Avaya Ethernet Routing Switch 8800/8600. If you configure a 13.x.x.x network for output using the I/O modules, the switch can experience connectivity issues.

Enabling remote access services

Enable the remote access service to provide multiple methods of remote access.

Prerequisites

- When you enable an Rlogin flag, you must configure an access policy to specify the user name of who can access the switch. For more information about the access policy commands, see *Avaya Ethernet Routing Switch 8800/8600 Security, NN46205-601*.
- You must log on to the Global Configuration mode in the ACLI.

Procedure steps

1. Enable the access service by using the following command:

   ```
   boot config flags <access-service>
   ```

2. Save the boot configuration.

Variable definitions

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

Variable	Value
access-service	Specifies one of the following remote-access service types to enable: • ftpd • rlogind • sshd • telnetd • tftpd Use the no operator to remove this configuration. To configure this option to the default value, use the default operator with the command.

Enabling the Web server for EDM access

Enable the Web server to provide management access to the switch using Enterprise Device Manager.

Comments? infodev@avaya.com

Prerequisites

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

Procedure steps

1. Enable the Web server by using the following command:

   ```
   web-server enable
   ```

2. Configure the access password by using the following command:

   ```
   web-server password <rwa> <username> <passwd>
   ```

Variable definitions

Use the data in the following table to use the **`web-server`** command.

Variable	Value
def-display-rows	Sets internet server default display row width.
enable	Enables the internet interface.
help-tftp	Sets internet server HTML directories.
http-port	Sets internet server HTTP port.
password	Sets internet web server password. Default username and password combination is rwa/rwa.

Configuring the remote host logon

Configure the remote host logon to modify parameters for FTP and TFTP access. Use the default parameters for TFTP transfers. If you want to use FTP as the transfer mechanism, you must change the password to a valid value.

Prerequisites

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

Procedure steps

1. Define conditions for the remote host logon by using the following command:

   ```
   boot config host
   ```

2. Save the changed configuration to the boot.cfg and pcmboot.cfg files.
3. Restart the switch.

Variable definitions

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

Variable	Value
ftp-debug	Enables or disables debug mode on FTP. If you enable debug mode, debug messages appear on the management console screen. The default is disabled. Use the no operator to later remove this configuration. To configure this option to the default value, use the default operator with the command.
password <*WORD 0-16*>	Configures the password to enable FTP transfers. <*WORD 0-16*> is the remote host user logon password, enables FTP transfers and is up to 16 characters long. After you configure this password, only FTP is used for remote host logon. **Important:** This password must match the password for the FTP server, or the FTP operation fails. Also, if you configure the password to a valid value, then all copying to and from the network uses FTP instead of TFTP. If the user name or password is incorrect, copying over the network fails.
tftp-debug	Enables or disables debug mode on TFTP/TFTPD. If you enable debug mode, debug messages display on the management console screen. The default is disabled. Use the no operator to remove this configuration. To configure this option to the default value, use the default operator with the command.

Comments? infodev@avaya.com

Variable	Value
tftp-hash	Enables or disables the TFTP hash bucket display. The default is disabled. Use the no operator to remove this configuration. To configure this option to the default value, use the default operator with the command.
tftp-rexmit <*seconds*>	Configures the TFTP retransmission timeout. The default value is 2 seconds. *seconds* is the number of seconds (1–120). To configure this option to the default value, use the default operator with the command.
tftp-timeout <*seconds*>	Configures the TFTP timeout. The default value is 6 seconds. *seconds* is the number of seconds (1–120). To configure this option to the default value, use the default operator with the command.
user <*value*>	Configures the remote user logon. *value* is the user logon name (up to 16 characters). To configure this option to the default value, use the default operator with the command.

Comments? infodev@avaya.com

Chapter 9: Remote connection configuration using EDM

This section contains the minimum information required to configure a management interface for the purposes of setting up a remote connection.

Assigning an IP address to the management port

Assign an IP address to the management port to use it for out-of-band (OOB) management. The standby IP must be in the same subnet as the master IP. Create a virtual management port in addition to the physical management ports on the switch management modules.

Procedure steps

1. In the Device Physical View, select the management port.
2. In the navigation tree, open the following folders: **Configuration** > **Edit**.
3. Click **Mgmt Port**.

   The Mgmt Port dialog box appears with the Mgmt Port-IP tab displayed.
4. In the **Addr** box, type the required IP address for the management port.
5. In the **Mask** box, type the subnet mask.
6. Click **Apply**.
7. In the Device Physical View, select the chassis.
8. In the navigation tree, open the following folders: **Configuration** > **Edit**.
9. Click **Chassis**.

   The Chassis dialog box appears with the System tab displayed.
10. In the **VirtualIPAddr** box, enter the IP address you want to configure as the virtual address.
11. In the **VirtualNetMask** box, enter the subnet mask.
12. Click **Apply**.

Assigning static routes to the management interface

Assign static routes to the management interface to specify network and gateway IP addresses used to remotely manage the device. You can specify up to four static routes for the management interface.

Procedure steps

1. In the Device Physical View, select the management port.
2. In the navigation tree, open the following folders: **Configuration** > **Edit**.
3. Click **Mgmt Port**.
4. Click the **CPU Route Table** tab.
5. Click **Insert**.
6. Enter the new Network and Gateway IP addresses.
7. Click **Insert**.

Variable definitions

Use the data in the following table to configure the Insert CPU Route Table tab.

Variable	Value
Network	Specifies the network IP address.
Gateway	Specifies the device gateway IP address.

Comments? infodev@avaya.com

Chapter 10: Verification

This section contains information about how to verify your provisioning procedures result in a functional switch.

Pinging an IP device

Ping a device to test the connection between the Avaya Ethernet Routing Switch 8800/8600 and another network device. After you ping a device, the switch sends an Internet Control Message Protocol (ICMP) packet to the target device. If the device receives the packet, it sends a ping reply. After the switch receives the reply, a message appears indicating you can reach the specified IP address. If the switch does not receive a reply, the message indicates the address is not responding.

Procedure steps

Ping an IP network connection by using the following command:

```
ping <HostName/ipv4address/ipv6address> [scopeid <value>]
[datasize <value>] [count <value>][-s] [-I <value>] [-t
<value>] [-d] [vrf <WORD 0–64>]
```

Variable definitions

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

Variable	Value
count value	Specifies the number of times to ping (for IPv4) (1–9999).
-d	Configures ping debug mode (for IPv4).
datasize value	Specifies the size of ping data sent in bytes (for IPv4) (16–4076).
HostName/ipv4address/ipv6address	Specifies the host name or IPv4 (a.b.c.d) or IPv6 (x:x:x:x:x:x:x:x) address (string length 1–256).

Variable	Value
-I	Specifies the interval between transmissions in seconds (1–60).
-s	Configures the continuous ping at the interval rate defined by the [-I] parameter (for IPv4).
scopeid value	Specifies the circuit ID (for IPv6) (1–9999).
-t	Specifies the no-answer timeout value in seconds (1–120) for IPv4.
vrf <WORD 0–64>	Specifies the virtual router and forwarder (VRF) name from 1–64 characters.

Using Telnet to log on to the device

Use Telnet to log on to the device and remotely manage the switch.

Procedure steps

1. From a PC or terminal, start a Telnet session by using the following command:

   ```
   telnet <ipv4 or ipv6 address>
   ```

2. Enter the logon and password when prompted.

Accessing the switch through EDM

You can configure and monitor the switch through EDM from anywhere on your network. EDM uses a 15-minute timeout period. If no activity occurs for 15 minutes, the system logs off EDM, and you must reenter the password information.

Procedure steps

1. Start one of the following Web browsers.

   • Mozilla Firefox, version 3.0

Comments? infodev@avaya.com

- Microsoft Internet Explorer, version 7.0

2. Type the switch IP address as the URL in the Web address field.

   The EDM logon page appears.

3. In the **User Name** and **Password** boxes, type the user name and password. The default login is user: `admin` and password: `password`.

   Important:

   If you configured a username and password for Web server access in a previous release, these configured values remain unchanged in this release. To access EDM, use these previously configured username and password values. In this case, the default login user: `admin` and password: `password` do not apply.

4. Click **Log On**.

   EDM displays the device view, which provides a picture of the switch.

Comments? infodev@avaya.com

Chapter 11: Customer service

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

Navigation

- Getting technical documentation on page 91
- Getting Product training on page 91
- Getting help from a distributor or reseller on page 91
- Getting technical support from the Avaya Web site on page 92

Getting technical documentation

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

Getting Product training

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

Getting help from a distributor or reseller

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

Getting technical support from the Avaya Web site

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

Comments? infodev@avaya.com