Avaya Ethernet Routing Switch 8800/8600 Administration

Release 7.2.22.0
NN46205-605
Issue 10.01
January 2016

Notice

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

Documentation disclaimer

“Documentation” means information published by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya may generally make available to users of its products and Hosted Services. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of documentation unless such modifications, additions, or deletions were performed by Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

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

Warranty

Avaya provides a limited warranty on Avaya hardware and software. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language, as well as information regarding support for this product while under warranty is available to Avaya customers and other parties through the Avaya Support website: https://support.avaya.com/helpcenter/getGenericDetails?detailId=C20091120112456651010 under the link “Warranty & Product Lifecycle” or such successor site as designated by Avaya. Please note that if You acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to You by said Avaya Channel Partner and not by Avaya.

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

Hosted Service

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

Licenses

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

Avaya grants You a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to You. “Software” means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products, pre-installed on hardware products, and any upgrades, updates, patches, bug fixes, or modified versions thereto. “Designated Processor” means a single stand-alone computing device. “Server” means a Designated Processor that hosts a software application to be accessed by multiple users. “Instance” means a single copy of the Software executing at a particular time: (i) on one physical machine; or (ii) on one deployed software virtual machine (“VM”) or similar deployment.

License types

Designated System(s) License (DS). End User may install and use each copy or an Instance of the Software only on a number of Designated Processors up to the number indicated in the order. Avaya may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, Instance, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

Heritage Nortel Software

“Heritage Nortel Software” means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software is the software contained within the list of Heritage Nortel Products located at https://support.avaya.com/LicenseInfo under the link “Heritage

Nortel Products" or such successor site as designated by Avaya. For Heritage Nortel Software, Avaya grants Customer a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

Copyright

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

Virtualization

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

Third Party Components

"Third Party Components" mean certain software programs or portions thereof included in the Software or Hosted Service may contain software (including open source software) distributed under third party agreements ("Third Party Components"), which contain terms regarding the rights to use certain portions of the Software ("Third Party Terms"). As required, information regarding distributed Linux OS source code (for those products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the products, Documentation or on Avaya's website at: https://support.avaya.com/Copyright or such successor site as designated by Avaya. The open source software license terms provided as Third Party Terms are consistent with the license rights granted in these Software License Terms, and may contain additional rights benefiting You, such as modification and distribution of the open source software. The Third Party Terms shall take precedence over these Software License Terms, solely with respect to the applicable Third Party Components to the extent that these Software License Terms impose greater restrictions on You than the applicable Third Party Terms.

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

Service Provider

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

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

Compliance with Laws

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

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

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

Security Vulnerabilities

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

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

Downloading Documentation

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

Contact Avaya Support

See the Avaya Support website: https://support.avaya.com for product or Hosted Service notices and articles, or to report a problem with your Avaya product or Hosted Service. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: https://support.avaya.com (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

Trademarks

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

Contents

Chapter 1: Regulatory Information and Safety Precautions

Read the information in this section to learn about regulatory conformities and compliances.

International Regulatory Statements of Conformity

This is to certify that the Avaya 8000 Series chassis and components installed within the chassis were evaluated to the international regulatory standards for electromagnetic compliance (EMC) and safety and were found to have met the requirements for the following international standards:

- EMC—Electromagnetic Emissions—CISPR 22, Class A
- EMC—Electromagnetic Immunity—CISPR 24
- Electrical Safety—IEC 60950, with CB member national deviations

Further, the equipment has been certified as compliant with the national standards as detailed in the following sections.

National Electromagnetic Compliance (EMC) Statements of Compliance

FCC Statement (USA only)

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the Federal Communications Commission (FCC) rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy. If it is not installed and used in accordance with the instruction manual, it may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to take whatever measures may be necessary to correct the interference at their own expense.

ICES Statement (Canada only)

Canadian Department of Communications Radio Interference Regulations

This digital apparatus (8800/8600 Series chassis and installed components) does not exceed the Class A limits for radio-noise emissions from digital apparatus as set out in the Radio Interference Regulations of the Canadian Department of Communications.

Règlement sur le brouillage radioélectrique du ministère des Communications

Cet appareil numérique (8800/8600 Series chassis) respecte les limites de bruits radioélectriques visant les appareils numériques de classe A prescrites dans le Règlement sur le brouillage radioélectrique du ministère des Communications du Canada.

CE Marking Statement (Europe only)

EN 55022 Statements

This is to certify that the Avaya 8800/8600 Series chassis and components installed within the chassis are shielded against the generation of radio interference in accordance with the application of Council Directive 2004/108/EC. Conformity is declared by the application of EN 55022 Class A (CISPR 22).

Caution:

This device is a Class A product. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users are required to take appropriate measures necessary to correct the interference at their own expense.

EN 55024 Statement

This is to certify that the Avaya 8800/8600 Series chassis is shielded against the susceptibility to radio interference in accordance with the application of Council Directive 2004/108/EC. Conformity is declared by the application of EN 55024 (CISPR 24).

EN 300386 Statement

The Ethernet Routing Switch 8800/8600 Series chassis complies with the requirements of EN 300386 V1.3.3 for emissions and for immunity for a Class A device intended for use in either Telecommunications centre or locations other than telecommunications centres given the performance criteria as specified by the manufacturer.

EC Declaration of Conformity

The Ethernet Routing Switch 8800/8600 Series chassis conforms to the provisions of the R&TTE Directive 1999/5/EC.

VCCI Statement (Japan/Nippon only)

This is a Class A product based on the standard of the Voluntary Control Council for Interference (VCCI) for information technology equipment. If this equipment is used in a domestic environment, radio disturbance may arise. When such trouble occurs, the user may be required to take corrective actions.

この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

KCC Notice (Republic of Korea only)

This device has been approved for use in Business applications only per the Class A requirements of the Republic of Korea Communications Commission (KCC). This device may not be sold for use in a non-business application.

For Class A:

이 기기는 업무용(A급) 전자파적합기기로서 판매자 또는 사용자는 이 점을 주의하시기 바라며, 가정외의 지역에서 사용하는 것을 목적으로 합니다.

Russia Belarus and Kazakhstan Requirement

В целях соблюдения действующего законодательства, продукты Компании Авайя, которые поставляются в Россию, Белоруссию и Казахстан, поставляются с конфигурацией, которая соответствует текущим требованиям нормативных актов. Любые изменения предустановленного программного обеспечения или прошивки программно-аппаратного комплекса, включая установку иной прошивки, запрещаются, а в случае таких изменений, лицо или компания их осуществившие несут ответственность на свой страх и риск. Компания Авайя не несет ответственности за внесение каких-либо изменений в продукт, произведенный на или для использования на территории России, Белоруссии и Казахстана, кроме модификаций, которые выполнены и сертифицированы Компанией Авайя.

In order to comply with existing laws, Avaya's products that are supplied to Russia, Belarus, and Kazakhstan are supplied with a configuration which is in line with existing legislation. Modifications may lead to product certifications becoming invalid. Any modification of preinstalled software and firmware, including installation of other or more current firmware or software, therefore is done at the responsibility of the person or company executing the changes. Avaya is not responsible for any modifications to the product made on or for use on the territory of Russia, Belarus and Kazakhstan other than modifications executed and certified by Avaya itself.

BSMI statement (Taiwan only)

BSMI statement (Taiwan only)

This is a Class A product based on the standard of the Bureau of Standards, Metrology and Inspection (BSMI) CNS 13438 Class A and CNS 14336-1.

警告使用者:
這是甲類的資訊產品，在居住的環境中使用時，可能會造成射頻干擾，在這種情況下，使用者會被要求採取某些適當的對策。

Chinese EMI and safety warnings

Voltage:

Risk of injury by electric shock

Before working on this equipment, be aware of good safety practices and the hazards involved with electrical circuits. Use only power cords that have a good grounding path. Ensure that the switch is properly grounded before powering on the unit.

電壓警告:
觸電受傷的危險性
在此設備上進行作業之前，要認知到良好的安全行為和涉及電子電路可能的危害。使用的電源線需有接地路徑。確保供電給設備之前，有適當的接地。

Warning:

Disconnecting the power cord is the only way to turn off power to this device. Always connect the power cord in a location that can be reached quickly and safely in case of emergency.

警告使用者:
斷開電源線，是關閉該設備電源的唯一方法。始終確保連接電源線的位置，在緊急情況下，是可以快速且安全抵達的一個位置。

Electrostatic alert:

Risk of equipment damage

To prevent damage from electrostatic discharge, always wear an antistatic wrist strap connected to an ESD jack when connecting cables or performing maintenance on this device.

⚠ **靜電提醒：**
設備損壞的風險
為了防止靜電放電的破壞，在此設備上連接纜線或執行維護時，
始終戴上防靜電腕帶並連接到ESD插孔。

National Safety Statements of Compliance

CE Marking Statement (Europe only)

EN 60 950 Statement

This is to certify that the Avaya 8000 Series chassis and components installed within the chassis are in compliance with the requirements of EN 60 950 in accordance with the Low Voltage Directive. Additional national differences for all European Union countries have been evaluated for compliance. Some components installed within the 8000 Series chassis may use a nickel-metal hydride (NiMH) and/or lithium-ion battery. The NiMH and lithium-ion batteries are long-life batteries, and it is very possible that you will never need to replace them. However, should you need to replace them, refer to the individual component manual for directions on replacement and disposal of the battery.

Denan Statement (Japan/Nippon only)

警告

本製品を安全にご使用頂くため、以下のことにご注意ください。

- 接続ケーブル、電源コード、ACアダプタなどの部品は、必ず製品に同梱されております添付品または指定品をご使用ください。添付品・指定品以外の部品をご使用になると故障や動作不良、火災の原因となることがあります。
- 同梱されております付属の電源コードを他の機器には使用しないでください。上記注意事項を守らないと、死亡や大怪我など人身事故の原因となることがあります。

Información NOM (únicamente para México)

La información siguiente se proporciona en el dispositivo o en los dispositivos descritos en este documento, en cumplimiento con los requisitos de la Norma Oficial Mexicana (NOM):

Exportador:	Avaya Inc.
	4655 Great America Parkway
	Santa Clara, CA 95054 USA
Importador:	Avaya Communication de México SA de CV
	Av. Presidente Masarik 111
	Piso 6
	Col Chapultepec Morales
	Deleg. Miguel HIdalgo
	México D.F. 11570
Embarcar a:	Model 8004AC:
	100-240 VCA, 50-60 Hz, 12-6 A max. por fuente de poder
	Model 8005AC:
	100-120 VCA, 50-60 Hz, 16 A max. por fuente de poder
	200-240 VCA, 50-60 Hz, 9.5 A max. por fuente de poder
	Model 8005DI AC:
	100-120 VCA, 50-60 Hz, 16 A max para cada entrada de CA
	200-240 VCA, 50-60 Hz, 9.3 A max para cada entrada de CA
	Model 8005DI DC:
	8005DIDC: 40 to 75 VDC, 48.75 to 32.5 A
	una fuente, una fuente + configuraciones de una fuente redundante, dos
	fuentes o dos + configuraciones de una fuente redundante
	Model 8004DC:
	-48 VCD, 29 A
	Model 8005DC:
	-48 VCD, 42 A

NOM Statement (Mexico only)

The following information is provided on the devices described in this document in compliance with the safety requirements of the Norma Oficial Méxicana (NOM):

Exporter:	Avaya Inc.

Table continues…

	4655 Great America Parkway
	Santa Clara CA 95054 USA
Importer:	Avaya Communication de México, S.A. de C.V.
	Av. Presidente Masarik 111
	Piso 6
	Col Chapultepec Morales
	Deleg. Miguel HIdalgo
	México D.F. 11570
Input:	Model 8004AC:
	100-240 VAC, 50-60 Hz, 12-6 A maximum for each power supply
	Model 8005AC:
	100-120 VAC, 50-60 Hz, 16 A maximum for each power supply
	200-240 VAC, 50-60 Hz, 8.5 A maximum for each power supply
	Model 8005DI AC:
	100-120 VAC, 50-60 Hz, 16 A maximum for each AC inlet
	200-240 VAC, 50-60 Hz, 9.3 A maximum for each AC inlet
	Model 8005DI DC:
	8005DIDC: 40 to 75 VDC, 48.75 to 32.5 A
	single supply, single supply + one redundant supply, two supplies, or two
	supplies + one redundant supply configurations
	Model 8004DC:
	48-60 VDC, 29-23 A
	Model 8005DC:
	48-60 VDC, 42-34 A

European Union and European Free Trade Association (EFTA) Notice

CE

All products labeled with the CE marking comply with R&TTE Directive (1999/5/EEC) which includes the Electromagnetic Compliance (EMC) Directive (2004/108/EC) and the Low Voltage Directive (2006/95/EC) issued by the Commission of the European Community.

Compliance with these directives implies conformity to the following European Norms (ENs). The equivalent international standards are listed in parenthesis.

- EN 55022 (CISPR 22)–Electromagnetic Interference
- EN 55024 (IEC 61000-4-2, -3, -4, -5, -6, -8, -11)–Electromagnetic Immunity
- EN 61000-3-2 (IEC 610000-3-2)–Power Line Harmonics

- EN 61000-3-3 (IEC 610000-3-3)–Power Line Flicker

Safety Messages

This section describes the different precautionary notices used in this document. This section also contains precautionary notices that you must read for safe operation of the Avaya Ethernet Routing Switch 8800/8600.

Notices

Notice paragraphs alert you about issues that require your attention. The following sections describe the types of notices. For a list of safety messages used in this guide and their translations, see "Translations of safety messages".

Attention Notice

Important:

An attention notice provides important information regarding the installation and operation of Avaya products.

Caution ESD Notice

Electrostatic alert:

ESD

ESD notices provide information about how to avoid discharge of static electricity and subsequent damage to Avaya products.

Electrostatic alert:

ESD (décharge électrostatique)

La mention ESD fournit des informations sur les moyens de prévenir une décharge électrostatique et d'éviter d'endommager les produits Avaya.

Electrostatic alert:

ACHTUNG ESD

ESD-Hinweise bieten Information dazu, wie man die Entladung von statischer Elektrizität und Folgeschäden an Avaya-Produkten verhindert.

Electrostatic alert:

PRECAUCIÓN ESD (Descarga electrostática)

El aviso de ESD brinda información acerca de cómo evitar una descarga de electricidad estática y el daño posterior a los productos Avaya.

Electrostatic alert:

CUIDADO ESD

Os avisos do ESD oferecem informações sobre como evitar descarga de eletricidade estática e os conseqüentes danos aos produtos da Avaya.

Electrostatic alert:

ATTENZIONE ESD

Le indicazioni ESD forniscono informazioni per evitare scariche di elettricità statica e i danni correlati per i prodotti Avaya.

Caution Notice

Caution:

Caution notices provide information about how to avoid possible service disruption or damage to Avaya products.

Caution:

ATTENTION

La mention Attention fournit des informations sur les moyens de prévenir une perturbation possible du service et d'éviter d'endommager les produits Avaya.

Caution:

ACHTUNG

Achtungshinweise bieten Informationen dazu, wie man mögliche Dienstunterbrechungen oder Schäden an Avaya-Produkten verhindert.

Caution:

PRECAUCIÓN

Los avisos de Precaución brindan información acerca de cómo evitar posibles interrupciones del servicio o el daño a los productos Avaya.

Caution:

CUIDADO

Os avisos de cuidado oferecem informações sobre como evitar possíveis interrupções do serviço ou danos aos produtos da Avaya.

Caution:

ATTENZIONE

Le indicazioni di attenzione forniscono informazioni per evitare possibili interruzioni del servizio o danni ai prodotti Avaya.

Warning Notice

Warning:

Warning notices provide information about how to avoid personal injury when working with Avaya products.

Warning:

AVERTISSEMENT

La mention Avertissement fournit des informations sur les moyens de prévenir les risques de blessure lors de la manipulation de produits Avaya.

Warning:

WARNUNG

Warnhinweise bieten Informationen dazu, wie man Personenschäden bei der Arbeit mit Avaya-Produkten verhindert.

Warning:

ADVERTENCIA

Los avisos de Advertencia brindan información acerca de cómo prevenir las lesiones a personas al trabajar con productos Avaya.

Warning:

AVISO

Os avisos oferecem informações sobre como evitar ferimentos ao trabalhar com os produtos da Avaya.

Warning:

AVVISO

Le indicazioni di avviso forniscono informazioni per evitare danni alle persone durante l'utilizzo dei prodotti Avaya.

Danger High Voltage Notice

Voltage:

Danger—High Voltage notices provide information about how to avoid a situation or condition that can cause serious personal injury or death from high voltage or electric shock.

Voltage:

La mention Danger—Tension élevée fournit des informations sur les moyens de prévenir une situation ou une condition qui pourrait entraîner un risque de blessure grave ou mortelle à la suite d'une tension élevée ou d'un choc électrique.

Voltage:

GEFAHR

Hinweise mit „Vorsicht – Hochspannung“ bieten Informationen dazu, wie man Situationen oder Umstände verhindert, die zu schweren Personenschäden oder Tod durch Hochspannung oder Stromschlag führen können.

Voltage:

PELIGRO

Los avisos de Peligro-Alto voltaje brindan información acerca de cómo evitar una situación o condición que cause graves lesiones a personas o la muerte, a causa de una electrocución o de una descarga de alto voltaje.

Voltage:

PERIGO

Avisos de Perigo—Alta Tensão oferecem informações sobre como evitar uma situação ou condição que possa causar graves ferimentos ou morte devido a alta tensão ou choques elétricos.

Voltage:

PERICOLO

Le indicazioni Pericolo—Alta tensione forniscono informazioni per evitare situazioni o condizioni che potrebbero causare gravi danni alle persone o il decesso a causa dell'alta tensione o di scosse elettriche.

Danger Notice

Danger:

Danger notices provide information about how to avoid a situation or condition that can cause serious personal injury or death.

Danger:

La mention Danger fournit des informations sur les moyens de prévenir une situation ou une condition qui pourrait entraîner un risque de blessure grave ou mortelle.

Danger:

GEFAHR

Gefahrenhinweise stellen Informationen darüber bereit, wie man Situationen oder Umständen verhindert, die zu schweren Personenschäden oder Tod führen können.

Danger:

PELIGRO

Los avisos de Peligro brindan información acerca de cómo evitar una situación o condición que pueda causar lesiones personales graves o la muerte.

Danger:

PERIGO

Avisos de perigo oferecem informações sobre como evitar uma situação ou condição que possa causar graves ferimentos ou morte.

Danger:

PERICOLO

Le indicazioni di pericolo forniscono informazioni per evitare situazioni o condizioni che potrebbero causare gravi danni alle persone o il decesso.

National Environmental Statements of Compliance

The WEEE Directive 2002/96/EC and RoHS (Restriction of Hazardous Substances) Directive 2002/95/EC sets collection, recycling and recovery targets for various categories of electrical products and their waste.

RoHS Directive Compliance Statement

The Restriction on Hazardous Substances Directive (RoHS) (2002/95/EC), which accompanies the WEEE Directive, bans the use of heavy metals and brominated flame-retardants in the manufacture of electrical and electronic equipment. Specifically, restricted materials under the RoHS Directive are Lead (including solder used in PCB's), Cadmium, Mercury, Hexavalent Chromium, and Bromine.

Avaya declares compliance with the European Union (EU) RoHS Directive (2002/95/EC).

WEEE Directive Compliance Statement

	This product at end of life is subject to separate collection and treatment in the EU Member States, Norway, and Switzerland and therefore is marked with the symbol shown at the left. Treatment applied at end of life of these products in these countries shall comply with the applicable national laws implementing Directive 2002/96/EC on Waste of Electrical and Electronic Equipment (WEEE). Avaya declares compliance with the European Union (EU) WEEE Directive (2002/96/EC).

Chapter 2: Introduction

Purpose of this document

The Avaya Ethernet Routing Switch 8800/8600 is a flexible and multifunctional switch that supports a diverse range of network architectures and protocols. This guide contains conceptual and procedural information to support the administration of the Ethernet Routing Switch 8800/8600. For more information about the available user interfaces and how to use edit commands and special terminal characters, see *Avaya Ethernet Routing Switch 8800/8600 User Interface Fundamentals*, NN46205-308.

Related resources

Documentation

See the *Avaya Ethernet Routing Switch 8800/8600 Documentation Roadmap*, NN46205-103, for a list of the documentation for this product.

Training

Ongoing product training is available. For more information or to register, you can access the website at http://avaya-learning.com/.

Avaya Mentor videos

Avaya Mentor videos provide technical content on how to install, configure, and troubleshoot Avaya products.

About this task

Videos are available on the Avaya Support website, listed under the video document type, and on the Avaya-run channel on YouTube.

Procedure

- To find videos on the Avaya Support website, go to http://support.avaya.com, select the product name, and check the *videos* checkbox to see a list of available videos.
- To find the Avaya Mentor videos on YouTube, go to http://www.youtube.com/AvayaMentor and perform one of the following actions:
  - Enter a key word or key words in the Search Channel to search for a specific product or topic.
  - Scroll down Playlists, and click the name of a topic to see the available list of videos posted on the site.

Note:

Videos are not available for all products.

Support

Visit the Avaya Support website at http://support.avaya.com for the most up-to-date documentation, product notices, and knowledge articles. You can also search for release notes, downloads, and resolutions to issues. Use the online service request system to create a service request. Chat with live agents to get answers to questions, or request an agent to connect you to a support team if an issue requires additional expertise.

Chapter 3: New in this release

The following sections detail what's new in *Avaya Ethernet Routing Switch 8800/8600 Administration* (NN46205-605) for Release 7.2.22.0.

shutdown command for the CP

The syntax of the **shutdown** command changed in this release. The command is now called **sys-shutdown** in the CLI and **sys shutdown** in the ACLI.

For more information, see Shutdown command for the CP on page 52.

Chapter 4: System startup fundamentals

This chapter provides conceptual information on the boot sequence and boot processes of the Avaya Ethernet Routing Switch 8800/8600. Review this content before you make changes to the configurable boot process options.

Boot sequence

The Ethernet Routing Switch 8800/8600 goes through a four-stage boot sequence before it becomes fully operational. After you turn on power to the switch, the SF/CPU module starts its built-in boot loader. In an Ethernet Routing Switch 8800/8600 with redundant switch fabric or switch management modules, the module in slot 5 provides the active SF/CPU functions after the switch powers up or resets. (Use the options in the boot monitor to specify the module that is the active SF/CPU.) The switch fabric subsystems of both modules are active and share the switching functions for the switch.

The boot sequence consists of the following four file loads:

- Stage 1: Loading the boot monitor image on page 32
- Stage 2: Loading the boot configuration on page 32
- Stage 3: Loading the run-time image on page 33
- Stage 4: Loading the switch configuration file on page 34

Stage 1: Loading the boot monitor image

At power-up or reset, the SF/CPU subsystem loads the boot monitor image.

After loading the boot monitor image, the SF/CPU and basic system devices such as the console port, modem port, external flash card slot, and management port initialize. (At this stage, the input/output (I/O) ports are not available; the system does not initialize the I/O ports until later in the boot process.)

Stage 2: Loading the boot configuration

After the boot monitor image loads, if an external card is present the boot configuration loads from a file called /pcmcia/pcmboot.cfg from the external flash card slot. If an external card is not present or file /pcmcia/pcmboot.cfg is not present, then the boot configuration loads from a file called /flash/

boot.cfg on the onboard flash memory (Avaya recommends that you copy the boot.cfg file in the /flash directory). If the /flash/boot.cfg file is not present, and if an external card is present, the Ethernet Routing Switch 8800/8600 searches for the file /pcmcia/boot.cfg.

If the loaded boot configuration file is not found or not read properly, then the switch starts a loop process.

If none of the boot configuration files are present (/pcmcia/pcmboot.cfg or /flash/boot.cfg or /pcmcia/boot.cfg), the Ethernet Routing Switch 8800/8600 starts using the default boot-configuration settings.

Important:

If you are using a PCMCIA card manufactured by Sandisk, the Ethernet Routing Switch 8800/8600 does not consistently access the /pcmcia/pcmboot.cfg or /pcmcia/boot.cfg file during boot-up. This limitation is observed only during boot-up. No limitation is observed if you access the Sandisk device after boot-up.

If the Autoboot flag is disabled or if the boot process is interrupted at the console, the boot process stops. At this stage, you can access the boot monitor at the console. In the boot monitor, you can set the boot configuration and perform upgrades to the boot monitor image and run-time image (loaded in stage 3). Changes made and saved at the boot monitor change the boot configuration.

After you save changes, you can initiate the boot process from the boot monitor using the boot command.

Shutdown command for external compact flash cards

The **sys-shutdown** command helps avoid corrupting an external compact flash card by ensuring that the card is synchronized before it is safely removed. If you do not shutdown the system first, some situations such as power cycling and hard resets might cause flash corruption. There is no risk of flash corruption if you run this command prior to a power cycle or hard reset.

System crashes might also corrupt flash cards so be sure to back up all configurations.

The command is called **sys-shutdown** in the CLI and **sys shutdown** in the ACLI. EDM does not support this command. In the CLI, the command is at the top level; in the ACLI, the command is in the EXEC Mode.

Stage 3: Loading the run-time image

The run-time image loads after the boot configuration. This software image initializes the I/O modules and provides full routing switch functionality. You can load the run-time image from the flash memory, from a PCMCIA card, or from a Trivial File Transfer Protocol (TFTP) server using the management port.

Define the default load order in the boot configuration file (/pcmcia/boot.cfg or /flash/boot.cfg). You can redefine the source and order from where to load the run-time image if you interrupt the autoboot process.

Stage 4: Loading the switch configuration file

The final step of the boot process is to load the switch configuration file (/flash/config.cfg). The switch configuration consists of higher-level functionality, including:

- Chassis configuration
- Port configuration
- Spanning tree group (STG) configuration
- VLAN configuration
- Routing configuration
- IP address assignments
- RMON configuration

The default switch configuration includes the following:

- All ports in a single spanning tree group (STG), STG number 1 (The default Spanning Tree Group is 802.1D compliant, and its Bridge Protocol Data Units (BPDU) are never tagged.)
- A single, port-based default VLAN with a VLAN identification number of 1, bound to the default spanning tree group
- Spanning Tree FastStart disabled on all ports
- No interface assigned IP addresses
- Traffic priority for all ports set to normal priority
- All ports as untagged ports
- Default communication protocol settings for the console port. For more information about these protocol settings, see *Avaya Ethernet Routing Switch 8800/8600 Quick Start, NN46205-310*.

In the configuration file, statements preceded by both the number sign (#) and exclamation point (!) load prior to the general configuration parameters. Statements preceded by only the number sign are comments meant to add clarity to the configuration; they do not load configuration parameters. The following table illustrates the difference between these two statement formats.

Table 1: Configuration file statements

Sample statement	Action
`# software version : 3.7.12.0`	Adds clarity to the configuration by identifying the software version.

Figure 1: Switch boot sequence on page 35 shows a summary of the boot sequence.

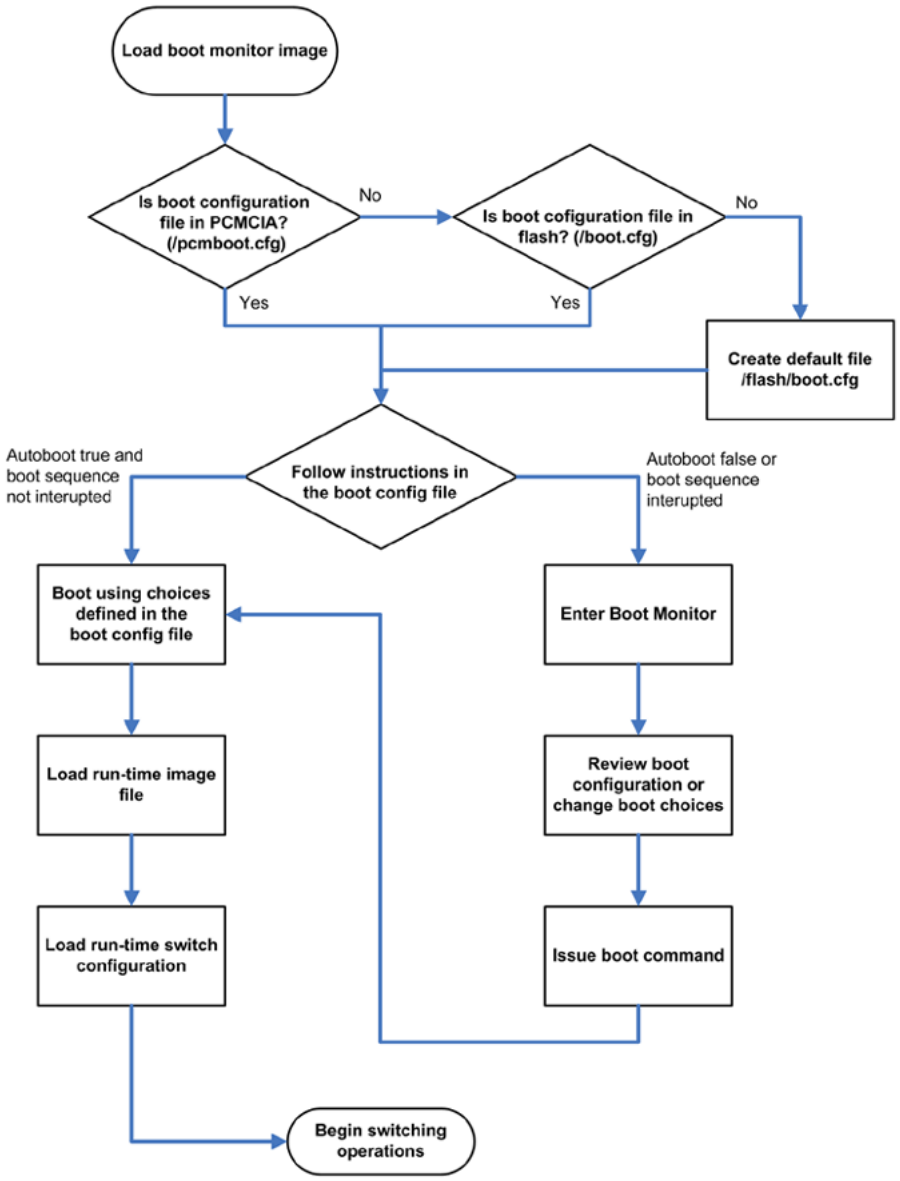


Figure 1: Switch boot sequence

Boot sequence modification

The default boot sequence directs the switch to look for its image and configuration files first on the external flash card, in the onboard flash memory second, and then from a server on the network. That is, the external flash card is the primary source for the files, the onboard flash memory is the secondary source, and the network server is the tertiary source. These source and file name definitions are in the boot configuration file.

Important:

If an Ethernet Routing Switch 8800/8600 loads its secondary software image file because it cannot find its primary software image, during this process, it also loads the secondary configuration file.

You can change the boot sequence in the following ways:

- Change the primary, secondary, and tertiary designations for file sources. For example, you can specify the network as the primary file source and update the configuration file or image file using a single copy of the file on the server.

  Important:

  Each choice of a file source (primary, secondary, or tertiary) specifies an image file and a matching configuration file. When you specify a source, you specify the associated pair of files.
- Change the file names from the default values. You can store several versions of the image or configuration file and specify a particular one by file name after you restart the switch.
- Start the switch without loading a configuration file, so that the switch uses its factory default configuration settings. Bypassing the switch configuration does not affect saved switch configuration; the configuration is simply not loaded.

Whether the switch configuration is loaded or not is controlled by the boot configuration. You can bypass loading the switch configuration.

If the configuration is bypassed, the switch starts with the default switch configuration settings and the boot flag settings that were loaded as the boot configuration file in stage 2.

Figure 2: Boot source text added to the system log file on page 36 shows the boot source text added to the system log file.

```
157: [11/24/2004 10:07:50] INFO: Code=0x0 Task=rcStart: System
is ready

158: [11/24/2004 10:07:51] INFO: Code=0x0 Task=rcStart: BOOTED
WITH TERTIARY BOOT SOURCE - pcmcia:p10ab

159: [11/24/2004 10:07:51] WARNING: Code=0x0 Task=rcStart:
CANNOT ACCESS SECONDARY BOOT SOURCE

160: [11/24/2004 10:07:51] WARNING: Code=0x0 Task=rcStart:
PRIMARY BOOT SOURCE IS NON-EXECUTABLE

161: [11/24/2004 10:07:52] INFO: Code=0x0 Task=tTrapd: Link
Up(1/1)
```

Figure 2: Boot source text added to the system log file

Static IP entry for the OOB network management interface

The default IP for the Out of Band (OOB) network management port is assigned as shown in Figure 3: Flowchart for the default IP for the OOB network management port on page 37.

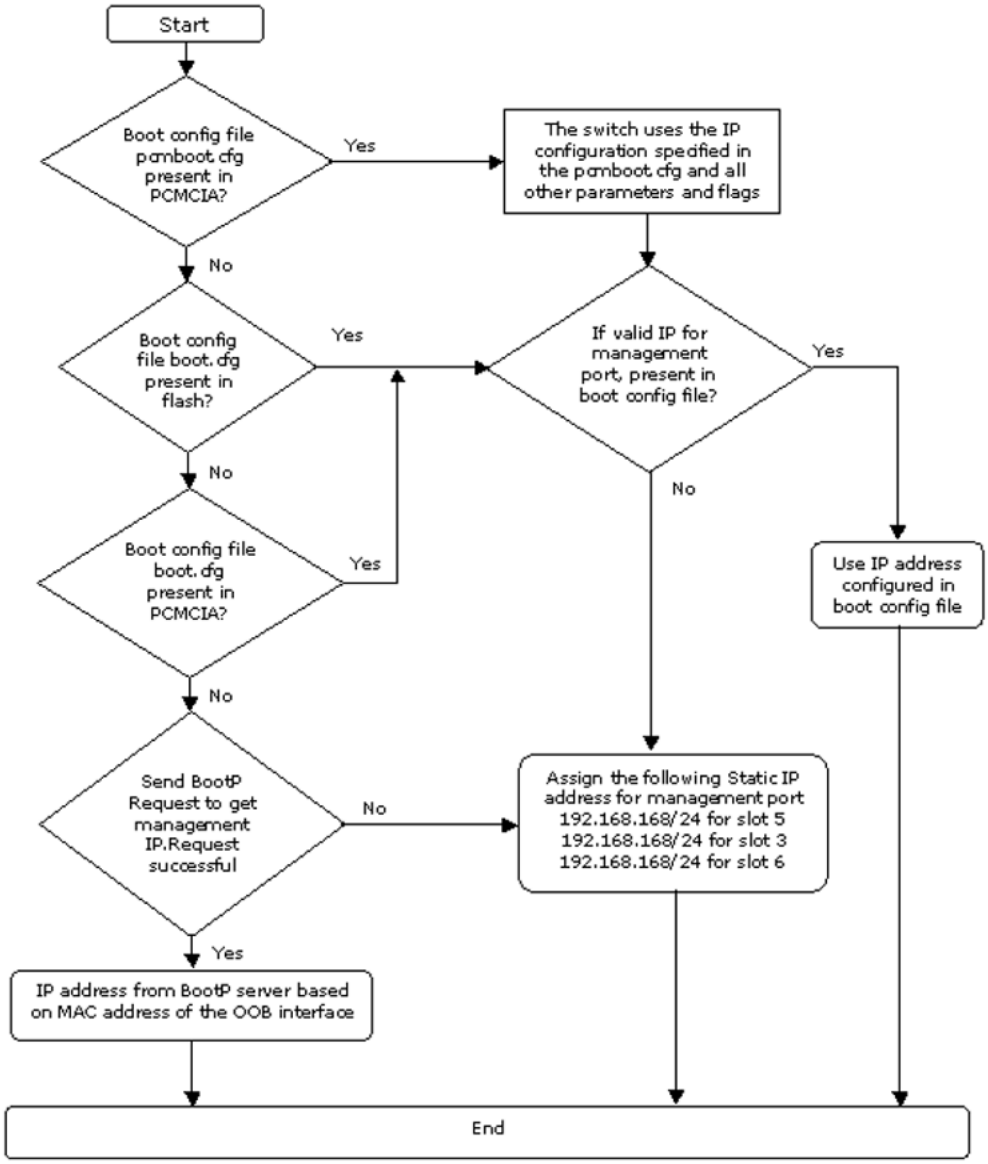


Figure 3: Flowchart for the default IP for the OOB network management port

The switch first checks for the file pcmboot.cfg, in PCMCIA. If not found, the switch checks for the file boot.cfg in flash.

Important:

Users using the boot configuration file from external flash card must rename the file to pcmboot.cfg The boot.cfg file is no longer saved in external flash card. Save the file only in flash.

Boot process and run-time process

You manage the boot process of the switch using the boot monitor.

You access the boot monitor by interrupting the boot process. This interrupt can only be initiated through a direct serial-port connection to the switch, or some remote connection to the serial port such as a remote (out of band) terminal server connection.

A switch placed into the boot monitor state cannot accept peer telnet connections from the master SF/CPU.

After the boot monitor is active, you can change the boot configuration, including boot choices and boot flags, and you can set the flags for Telnet and rlogin to allow remote access, but you cannot access the boot monitor remotely. You can access the boot monitor only through a direct serial-port connection.

You manage the run-time process using the run-time commands. To access the run-time command line interface (CLI) or Avaya command line interface (ACLI), wait until the boot process completes.

Boot image verification

After a switch starts, the switch recognizes the boot source and logs a message in the system log file that informs you about the selected boot source.

Figure 4: Console port boot source messages on page 38 shows the boot source messages observed on the console port.

```
[11/24/2004 10:07:48] ERROR: Code=0x1ff0105 Task=rcStart: unrecognized record
type 60 in alsRead

[11/24/2004 10:07:50] INFO: Code=0x0 Task=rcStart: System is ready

[11/24/2004 10:07:51] INFO: Code=0x0 Task=rcStart: BOOTED WITH TERTIARY BOOT
SOURCE - pcmcia:p10ab

**********************************
* Nortel, Inc.            *
* Copyright (c) 2004
* All Rights Reserved              *
**********************************

Login:
```

Figure 4: Console port boot source messages

Boot monitor

Use the boot monitor to configure and manage the boot process.

Important:

You must use a terminal connected directly to the console port on the switch. If you restart the switch from a remote terminal, the connection is terminated.

After you enter the boot monitor, the

```
monitor#
```

prompt displays.

Run-time

After the Ethernet Routing Switch 8800/8600 is operational, you can use the run-time commands to perform most of the configuration and management functions necessary to manage the switch. These functions include the following:

- Resetting or restarting the Ethernet Routing Switch 8800/8600.
- Adding, deleting, and displaying address resolution protocol (ARP) table entries.
- Pinging another network device.
- Viewing and configuring variables for the entire switch and for individual ports.
- Configuring and displaying STG parameters and enabling or disabling the Spanning Tree Protocol (STP) on an STG.
- Configuring and displaying MultiLink Trunking (MLT) parameters.
- Testing the switching fabric.
- Creating and managing port-based VLANs or policy-based VLANs.

To access the run-time environment you need a connection from a PC or terminal to the switch. You can use a direct connection to the switch through the console or modem port or through Telnet, rlogin, or Secure Shell (SSH) sessions. For more information about SSH, see *Avaya Ethernet Routing Switch 8800/8600 Security, NN46205-601*.

Important:

Before you attempt to access the switch using one of the previous methods, ensure you first enable the corresponding daemon flags.

System flags

After you enable or disable certain modes and functions, you need to save the configuration and reset the switch for your change to take effect. The following tables list parameters and indicate if they require a reset of the switch.

Table 2: Bootconfig flags on page 40 lists parameters you configure in the CLI using the **config bootconfig flags** command and in the ACLI using the **boot config flags** command.

Table 2: Bootconfig flags

CLI flag	ACLI flag	Switch reset
alt-led-enable <true|false>	alt-led	Yes
autoboot <true|false>	autoboot	Yes
block-snmp <true|false>	block-snmp	No
block-warmstandby-switchover <true|false>	block-warmstandby-switchover	Yes
control-record-optimization <true|false> **Important:** This parameter must always be set to false (disabled).	control-record-optimization **Important:** This parameter must always be set to false (disabled).	Yes
daylight-saving-time <true|false>	daylight-saving-time	No
debug-config <true|false>	debug-config	Yes
debugmode <true|false>	debugmode	Yes
factorydefaults <true|false>	factorydefaults	Yes
ftpd <true|false>	ftpd	No
ha-cpu <true|false>	ha-cpu	Yes
hsecure <true|false>	hsecure	No
info	Not applicable	No
logging <true|false>	logging	No
mezz <true|false>	mezz	Yes
acli <true|false>	acli	Yes
reboot <true|false>	reboot	Yes
rlogind <true|false>	rlogind	No
savetostandby <true|false>	savetostandby	No
spanning-tree-mode <mstp|rstp|default>	spanning-tree-mode	Yes
sshd <true|false>	sshd	No
telnetd <true|false>	telnetd	No
tftpd <true|false>	tftpd	No
trace-logging <true|false>	trace-logging	No
verify-config <true|false>	verify-config	Yes
wdt <true|false>	wdt	Yes
cf-pc-compat <true|false>	cf-pc-compat	Yes

You can configure two system flags. Both of the following flags require a system reset:

- global-filter-ordering
- multicast-check-packet

Important:

Avaya recommends that you do not change the configuration of the multicast-check-packet flag.

Table 3: Other system settings on page 41 lists other parameters you configure by using the CLI, ACLI, or Enterprise Device Manager under Configuration, Edit, Chassis, System Flags.

Table 3: Other system settings

Flag	Switch reset	CLI command	ACLI command
AuthenticationTraps	Yes		
WebServer	No	config web-server enable	web-server enable
AccessPolicy	Yes		
MrouteStreamLimit	Yes		
ForceTrapSender	Yes		
ForceIpheaderSender	Yes		
VlanByScrMac	Yes		
DiffServEcnCompatibility	Yes		
TakeIOCardOfflineEnable	Yes	config sys set flags take-iocard-offline <true|false>	sys flags take-iocard-offline
AutoResetFabricEnable	Yes	config sys set flags auto-reset-fabric <true|false>	sys flags auto-reset-fabric
System Monitor	Yes		

8895 SF/CPU compact flash compatibility with Windows PC

Prior to Release 7.1.3, a compact flash card formatted on the 8895 SF/CPU could not be read or written to on a Windows PC and vice-versa.

Release 7.1.3 introduces a new boot configuration flag, which allows a user to format the compact flash in either the Windows PC compatible format or the original format. The Windows PC compatible format allows a compact flash formatted on the 8895 SF/CPU to be read from or written to on a Windows PC and vice-versa.

The new boot configuration flag is `cf-pc-compat` and it can be set to `true` or `false`. The default value is `false` so that there is no impact to usability of compact flash formatted in previous releases after an upgrade to release 7.1.3 or higher. After the flag is set to `true` (Windows PC compatible

mode) and the compact flash formatted on the 8895 SF/CPU, it can be read from or written to on a Windows PC and vice-versa.

Important:

Ensure that you remove the Compact Flash interface card from its slot before you modify the `cf-pc-compat` flag. Otherwise the system displays errors.

Use the following steps to change the format of a compact flash:

1. Back up existing files.
2. Set the `cf-pc-compat` boot configuration flag to `true` or `false`. (This change takes effect immediately so there is no need to reboot.)
3. Format the compact flash.
4. Restore the files that were previously backed up.

Note:

After the `cf-pc-compat` flag is set to `true`, the 8895 SF/CPU will not be able to read a compact flash that was formatted prior to Release 7.1.3 or formatted when the `cf-pc-compat` boot configuration flag was set to `false` and vice versa.

After the `cf-pc-compat` flag is set to `true` and the compact flash formatted on the 8895 SF/CPU, it is compatible with Windows XP, Windows Vista, and Windows 7. It also supports 2GB/FAT16 and 4GB/FAT32 Compact Flash. The 8895 SF/CPU selects the FAT size automatically based on the flash size.

Important:

When using Window PC compatible mode, Avaya recommends formatting the compact flash on the 8895 CPU for it to be recognized by both the 8895 SF/CPU Operating System and Windows. If you format the compact flash on a Windows PC, it may not be recognized by the 8895 SF/CPU.

Clock synchronization

The Ethernet Routing Switch 8800/8600 automatically synchronizes the real-time clocks (hardware) on the primary and secondary SF/CPUs, and synchronizes the real-time and system (software) clocks.

Real-time clock synchronization

After you configure the real-time clock on the master SF/CPU, the slave SF/CPU real-time clock is immediately updated, and both clocks are set to the same time. A log message is added in the log

file stating that clock synchronization is complete. Familiarize yourself with the following conditions regarding SF/CPU clock synchronization:

- If the switch is operating normally with a redundant SF/CPU, the clock synchronizes at 24 hour intervals. If the switch is operating normally with no redundant SF/CPU and a standby SF/CPU card is inserted, the real-time clocks on the master SF/CPU and the standby SF/CPU immediately synchronize. A log message is added in the log file, stating that clock synchronization is complete. If the synchronization process continues successfully, no more log messages are generated and clock synchronization continues at 24 hour intervals.

  At boot time, after the switch is initialized, the clocks on the master SF/CPU and the standby SF/CPU immediately synchronize and clock synchronization continues at 24 hour intervals. If the standby SF/CPU is removed, the SF/CPU clock synchronization process stops. Also, if the clock synchronization process fails, a log message generates in the log file. When the real-time clock synchronization begins to fail, the switch generates a log message for each failed attempt.
- If the Inter SF/CPU Communication (ICC) channel is in use by another process at the time of clock synchronization, the synchronization process is not performed, but attempted again after the scheduled 24 hour interval. The switch adds a log message in the log 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 43
- Modem connection on page 44

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:

- 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. You can find a null modem cable 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 8692 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 Ethernet Routing Switch 8800/8600 to the modem. The following table shows the DTE-to-DCE pin assignments.

Table 4: 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:

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

Because the modem port receives DSR and CTS signals before transmitting, control lines are required 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 Ethernet Routing Switch 8800/8600, you can configure the modem port first using another type of connection to the CLI or 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 master 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 Ethernet Routing Switch 8800/8600.

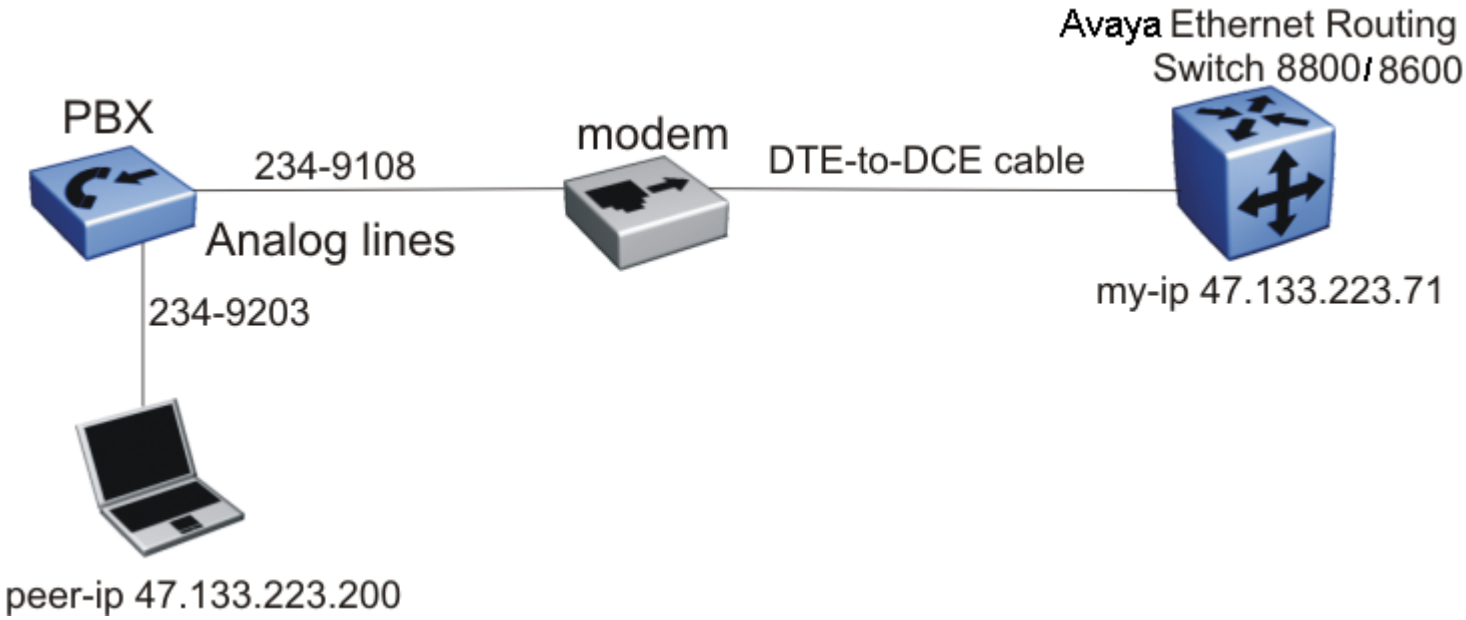


Figure 5: PPP configuration topology

After 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 which includes all additional PPP configuration parameters to include after the switch restarts. Enter one configuration parameter on each line.

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 which 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 is 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
```

Chapter 5: Chassis operations fundamentals

This chapter provides conceptual information for chassis operations such as operating modes, module types, hardware and software compatibility, and power management. Read this section before configuring the chassis operations.

Caution:

Proper handling of compact flash cards and modules can eliminate many potential issues. Please refer to the following sections to avoid unnecessary problems:

- Proper care of external compact flash and PCMCIA cards on page 52
- Proper handling of SF CPU and I O modules on page 53

Operating modes

The Avaya Ethernet Routing Switch 8800/8600 uses hardware records (or table entries) to store Address Resolution Protocol (ARP) entries. In addition, hardware records are used to store information pertaining to MACs, multicast, VLANs, IP routes, IP filters, and IPX entries. Each hardware record type, such as ARP or MAC, has a defined minimum number of reserved records.

The Ethernet Routing Switch 8800/8600 interface modules can support up to:

- 256 000 IP routes
- 64 000 MAC entries
- 32 000 ARP entries

SF/CPU High Availability mode

CPU High Availability (CPU-HA) mode enables switches with two CPUs to recover quickly from a failure of the master SF/CPU. HA and non-HA mode characteristics are as follows:

- In HA mode, also called “hot standby,” the two CPUs are synchronized. This means the CPUs have the same configuration and forwarding tables, with the master automatically updating the forwarding tables of the secondary in real time. When the master SF/CPU fails, the secondary takes over "master" responsibility very quickly, thereby minimizing traffic interruption for the failure condition.

- In non-HA mode, also called “warm standby,” the two CPUs are not synchronized. In this mode, when the master fails, the secondary SF/CPU must boot before taking "master" responsibility, and then must also re-learn the forwarding table information. This operation causes an interruption to traffic.

SF/CPU failure has no effect on the SF portion of the SF/CPU module. The switchover of traffic to the single functioning SF is always sub-second. The preceding list of characteristics refers to failures and their effect on the CPU portion of the SF/CPU module, as this is a dual-purpose module. Failures to the secondary or standby SF/CPU have no effect on CPU operation within the system while the primary SF/CPU is operational.

Important:

When operating in HA mode, if the Standby and Master SF/CPUs are rebooted quickly in succession within a few seconds in that order, a race condition can occur in which R, RS, and 8800 modules do not get rebooted as part of the Standby and Master reboot process. Instead they get rebooted in a delayed fashion during the new Master SF/CPU initialization. However, they would function normally after that. To avoid this delayed reboot condition and an unnecessary alarm, Avaya recommends that you avoid rebooting both the Standby and Master SF/CPUs in quick succession or simultaneously. By leaving a gap of around 10 seconds, this problem could be avoided.

The following table identifies which features support HA mode.

Table 5: Feature support for HA in specified software release versions

Release/ Feature	3.5.0	3.7.0	4.0.0	4.1.0	5.0	5.1	7.0	7.1
Modules	Classic	Classic	Classic and R	Classic and R	Classic, R, and RS	Classic, R, and RS	R and RS only.	R, RS, and 8800 Series
Platform	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Layer 2	Yes	Yes	Yes (3.5 based)	Yes	Yes	Yes	Yes	Yes
Layer 3	Yes (Static/ ARP)	Yes (3.5 + RIP, OSPF, VRRP, Filters, Route Policies) No BGP	No, 3.5 based	Yes (3.7.0 +, ACE/ ACLs) No BGP	Yes as in 4.1.0 and BGP	Yes BGP, BFD	Yes BGP, BFD	Yes BGP, BFD, SPBM
Multicast	No	No	No	No	Yes, DVMRP and PIM No PGM	Yes DVMRP, PIM, MSDP, Multicast virtualization of IGMP,	Yes DVMRP, PIM, MSDP, Multicast virtualization of	Yes DVMRP, PIM, MSDP, Multicast virtualization of

Table continues…

Release/ Feature	3.5.0	3.7.0	4.0.0	4.1.0	5.0	5.1	7.0	7.1
						and PIM-SM/SSM	IGMP, and PIM-SM/SSM	IGMP, and PIM-SM/SSM
IPv6	NA	NA	NA	Yes, Restart	Yes, Restart	Yes	Yes	Yes
Security	Yes	Yes	Yes (3.5 based)	Yes	Yes	Yes TACACS+	Yes TACACS+ DHCP Snooping ARP Inspection IP Source Guard	Yes TACACS+ DHCP Snooping ARP Inspection IP Source Guard

Important:

Partial HA support

In partial HA support, the synchronization of the configuration takes place between the Master and Slave SF/CPU and not between the learned routes. Hence convergence must take place and learning happens after a failover.

HA synchronization also applies to various configuration and software parameters, and may also be dependent on software release. The following table shows which features are supported in Release 3.5 and later.

Table 6: Release 3.5 and later synchronization capabilities in HA mode

Synchronization of:	3.5	3.7	4.0 (HA Layer 2 not supported)	4.1	5.0	5.1	7.0	7.1
Layer 1								
Port configuration parameters	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Layer 2								
VLAN parameters	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
STP parameters	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
RSTP/MSTP parameters	N/A	N/A	N/A	Yes	Yes	Yes	Yes	Yes
SMLT parameters	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

Table continues…

Synchronization of:	3.5	3.7	4.0 (HA Layer 2 not supported)	4.1	5.0	5.1	7.0	7.1
QoS parameters	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Layer 3								
Virtual IP (VLANs)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
ARP entries Note 3	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Static and default routes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
VRRP	No	Yes	No	Yes	Yes	Yes	Yes	Yes
RIP	No	Yes	No	Yes	Yes	Yes	Yes	Yes
OSPF	No	Yes	No	Yes	Yes	Yes	Yes	Yes
Layer 3 Filters/ACE/ACLs	No	Yes	No	Yes	Yes	Yes	Yes	Yes
BGP	No	No	No	No	Yes	Yes	Partial HA	Partial HA
DVMRP	No	No	No	No	Yes	Yes	Partial HA	Partial HA
PIM-SM/SSM	No	No	No	No	No Note 1	Yes Note 2	Partial HA	Partial HA
MSDP	No	No	No	No	No	Yes	Yes	Yes
Multicast	No	No	No	No	No	Yes	Partial HA	Partial HA
BFD	No	No	No	No	No	Yes	Yes	Yes
IPv6	No	No	No	Partial HA	Partial HA	Partial HA	Partial HA	Partial HA
SPBM	N/A	N/A	N/A	N/A	N/A	N/A	N/A	Yes Note 4

Note 1: In Release 5.0, PIM-SM and SSM have partial HA support with GRT only, no virtualization.

Note 2: In Release 5.1, PIM-SM and SSM are virtualized and have partial HA support.

Note 3: With HA enabled, the switch does not flush the VR ARP entry from the ARP table when you delete the VR ID from both switches.

Note 4: There is a 6–7 second gap between the active CPU going down and the standby CPU coming up. To avoid IS-IS adjacency bounce during the switchover, Avaya recommends a hello interval of 9 seconds and a hello multiplier of 3.

HA mode support

In the following configurations, assume that SF/CPU High Availability mode is activated. However, in some cases HA mode is impossible because one of the SF/CPUs is offline due to a hardware or software incompatibility.

HA mode support for Dual SF/CPU

If your switch supports Dual SF/CPU modules, see Table 7: Boot mode at startup for Dual SF/CPU configurations on page 51 to use the SF/CPU High Availability mode. The boot mode is determined by the types of SF/CPUs in the chassis and whether the SF/CPU High Availability mode is activated.

When using the command line interface (CLI) or Avaya command line interface (ACLI) on a dual-SF/CPU system with HA mode enabled, do not enter configuration commands on the Standby SF/CPU. Execute all configuration commands on the Master SF/CPU only.

Table 7: Boot mode at startup for Dual SF/CPU configurations

If the configuration is:	And SF/CPU high- availability mode is:	Then:
Two dual SF/CPU modules	Activated	System starts in SF/CPU High Availability mode.
One dual SF/CPU module and one single SF/CPU module	Activated	If the single SF/CPU starts first, the SF/CPU restarts so the dual SF/CPU is the master and the single SF/CPU goes offline. If the dual SF/CPU starts first, the system starts in SF/CPU High Availability mode and the single SF/CPU goes offline.
Two single SF/CPU modules	Activated	System does not start and stays in monitor mode.
Two dual SF/CPU modules	Disabled	System starts in single SF/CPU mode.
One dual SF/CPU module and one single SF/CPU module	Disabled	System starts in single SF/CPU mode.
Two single SF/CPU modules	Disabled	System starts in single SF/CPU mode.

After you insert a module into a running chassis, the SF/CPU High Availability mode status determines the initialization mode of the module.

Table 8: Inserting single and dual SF/CPU modules into running chassis

If you insert this module into a running chassis:	And SF/CPU High Availability mode status is:	Then:
Dual SF/CPU module	Activated	The module is activated as a backup.
Single SF/CPU module	Activated	The module is not activated. A trap is sent and the system logs an error to the console.
Dual SF/CPU module	Disabled	The module is activated in single SF/CPU mode.
Single SF/CPU module	Disabled	The module is activated in single SF/CPU mode.

Shutdown command for the CP

The **sys-shutdown** command shuts down the CP by dismounting both the internal and external file systems. After you enter this command, the following message appears on the serial console:

```
It is now safe to reset, remove, or power off this CP.
```

Use this command whenever you have to shut down the CP and when you are working with external flash cards. For more information on flash cards, see Proper care of external compact flash and PCMCIA cards on page 52.

The command is called **sys-shutdown** in the CLI and **sys shutdown** in the ACLI. EDM does not support this command. In the CLI, the command is at the top level; in the ACLI, the command is in the EXEC Mode.

Important:

The command for shutting down modules is different than for shutting down the CP. For information about shutting down a module, see Proper handling of SF CPU and I O modules on page 53.

Proper care of external compact flash and PCMCIA cards

To ensure proper software cleanup on the CP and to prevent corruption of the external compact flash card or the PCMCIA card, **do not remove the external memory card without first entering the following command:**

- **dos-stop /pcmcia**

Be sure to back up all configurations, as all files can be lost if the card becomes corrupted.

To check and optionally repair a file system, you can use the **dos-chkdsk <device> repair** command.

If the file system cannot be repaired, you can attempt to reformat the device using the **dos-format <device>** command. Otherwise, you may need to replace the card.

Both of the preceding commands delete all information on the memory, so be sure to backup all information before using either of the commands.

The above commands are available in the CLI, ACLI, and the boot monitor.

Note:

When the number of files stored on the PCMCIA card exceeds 100, the I/O modules may continuously reset after rebooting the chassis. If there are more than 100 files on the PCMCIA card, delete any unnecessary files and reboot the chassis.

For more information, see Shutting down external compact flash cards on page 115 using the CLI and Shutting down external compact flash cards on page 243 using the ACLI.

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

Proper handling of SF/CPU and I/O modules

Caution:

Avaya strongly recommends that you disable any module (SF/CPU or I/O) before you remove it. Use one of the following commands.

- **config slot <slotnum> state disable** (CLI command)
- **slot shutdown <slotnum>** (ACLI command)

Do not remove any module without first entering one of the preceding commands.

For more information on using these commands for specific tasks, see the following topics in *Upgrades* (NN46205–400):

- Upgrading from 8692 SF/CPU with SuperMezz to 8895 SF/CPU
- Hot swapping the Master SF/CPU module in a dual CPU chassis
- Hot swapping the Secondary SF/CPU module in a dual CPU chassis
- Hot swapping an I/O module

Module types

The Ethernet Routing Switch 8800/8600 modules include the following types:

- R modules support greater bandwidth and routing table memory. R modules use an R suffix, which identifies them as R modules. R modules support:
  - 256 000 IP routes
  - 64 000 MAC entries
  - 32 000 ARP entries
  - Custom AutoNegotiation Advertisement (CANA)
- RS modules support extended mirroring over R modules. RS modules use an RS suffix, which identifies them as RS modules. RS modules support:
  - All features supported by R modules as well as new features.
  - Multiple ports for each lane for both ingress and egress mirroring.
  - Improved port behavior to provide for faster link state detection than R modules.
- 8800 series modules also support extended mirroing over R modules. 8800 modules support:
  - All features supported by R and RS modules.

Table 9: Avaya Ethernet Routing Switch 8800/8600 modules on page 54 lists the supported modules.

Table 9: Avaya Ethernet Routing Switch 8800/8600 modules

R modules	RS modules	8800 modules
N/A	8612XLRS	8812XL
8630GBR		N/A
N/A	8634XGRS	8834XG
N/A	8648GBRS	8848GT
8648GTR	8648GTRS	8848GB
8683XIR		N/A

R, RS and 8800 module support for 8010co chassis

The 8010co chassis supports R, RS, and 8800 modules with a High Performance Backplane. Identify the High Performance Backplane by the chassis revision number in the CLI. The CLI display of the **`show sys info`** command shows a revision number of 02 or higher in the hardware configuration (H/W Config) field to indicate the new high performance chassis. Additionally, you can examine the hardware revision field (HwRev) to determine whether a chassis is high performance or standard, see Table 10: Chassis revision number on page 55.

Table 10: Chassis revision number

Chassis Mode	HwRev
8010	06 or greater
8006	05 or greater
8010 co chassis	05 or greater

SF/CPU warm standby

The Avaya Ethernet Routing Switch 8800/8600 supports up to two 8692 or 8895 SF/CPU modules in slots 5 or 6 in either a 6-slot or 10-slot chassis. If you start the switch with SF/CPU modules in slots 5 and 6, slot 5 becomes the master SF/CPU, and slot 6 becomes the backup (warm standby) by default. You can change this default behavior.

The 8692 and 8895 SF/CPU modules provide two functions: SF/CPU and switching. Switching fabrics are always active, providing load sharing for input/output (I/O) modules. One SF/CPU remains active, while the other SF/CPU is the backup.

Important:

Release 7.0 and above supports the 8692 SF/CPU with SuperMezz card and the 8895 SF/CPU only.

Important:

A Dual SF/CPU system configuration supports two modes of SF/CPU operation: warm standby or hot standby. Hot standby, or High Availability (HA) uses the two SF/CPUs as synchronizing tables – Layer 2, Layer 3, or both. HA is not activated by default. You must enable a specific flag to enable HA.

Important:

A dual SF/CPU chassis does not operate when the same type of SF/CPU is not installed. For example, a chassis cannot operate when you install 8692 SF/CPU with SuperMezz and 8895 SF/CPU simultaneously.

Hardware and software compatibility

The following tables describe the hardware and the minimum Avaya Ethernet Routing Switch 8800/8600 software version required to support the hardware.

Table 11: Hardware and minimum software version

Chassis and switching fabric			Minimum software version	Part number
	8010co chassis	10-slot chassis	3.1.2	DS1402004-E5 DS1402004- E5GS
	8010 chassis	10-slot chassis	3.0.0	DS1402001-E5 DS1402001- E5GS
	8006 chassis	6-slot chassis	3.0.0	DS1402002-E5 DS1402002- E5GS
	8003-R chassis	3-slot chassis	7.0.0	DS1402011-E5
	8692 SF/CPU with SuperMezz	Switching fabric	3.5.6, 3.7.3, 4.0.0, 5.0.0, 5.1, 7.0, 7.1, 7.1.1.	DS1404066-E5
	8895 SF/CPU	switching fabric	7.0.0, 7.1, 7.1.1.	DS1404120-E5
Power Supplies				
	8004AC	850W AC Power Supply	3.1.2	DS1405E08-E5
	8004DC	850W DC Power Supply	3.1.2	DS1405007-E5
	8005AC	1462W AC Power Supply	4.0.0	DS1405012-E5
	8005DC	1462W DC Power Supply	4.0.x	DS1405011-E5
	8005DI AC	1462W AC Power Supply	5.0	DS1405E18-E6
	8005DI DC	1462W DC Power Supply	5.0	DS1405E17-E6
Upgrade Kits				
	256MB SF/CPU upgrade kit	The 8692 SF/CPU must be upgraded to 256MB with Software Release 3.5, 3.7, 4.0 and 4.1. This memory upgrade is required for the 3.5 and 3.7 software to run properly.	3.5.0	DS1404016
	MAC upgrade kit	Use this kit to add Media Access Control (MAC) addresses to your system. This kit is required for routed interface scaling beyond 500.	3.5.0	DS1404015

Table 12: Hardware and minimum software version continued

8800/8600 modules and components			Minimum software version	Part number
Ethernet R modules				
	8630GBR module	30-port Gigabit Ethernet SFP	4.0.0	DS1404063
	8648GTR module	48-port 10/100/1000 TX	4.0.x	DS1404092
	8683XLR module	3-port 10Gigabit Ethernet XFP (10.3125 Gb/s LAN PHY)	4.0.0	DS1404101
	8683XZR module	3-port 10Gigabit Ethernet XFP (10.3125 Gb/s LAN PHY and 9.953 Gb/s WAN PHY)	4.1.0	DS1404064
Ethernet RS modules				
	8612XLRS	12 port 10 GE	5.0	DS1404097
	8634XGRS	2 port 10GE, 32 port 100/1000	5.0	DS1404109
	8648GBRS	48 port 100/1000Gb/s SFP	5.0	DS1404102
	8648GTRS	48 port 10 Base-T/100 Base -TX/1000 Base-T	5.0	DS1404110
Ethernet 8800 modules				
	8834XG	2 port 10GE, 32 port 100/1000	7.1	DS1404123-E6
	8848GB	48 port 100/1000Gb/s SFP	7.1.	DS1404122-E6
	8848GT	48 port 10 Base-T/100 Base -TX/1000 Base-T	7.1	DS1404124-E6
	8812XL	12 port 10Gb/s SFP+	7.1.3	DS1404121-E6
8800/8600 compatible GBICs, SFPs, SFP+s and XFPs				
GBICs **Important:** GBICs are not supported in release 7.1.3 and later.				
	1000BASE-SX GBIC	850 nm, short wavelength, Gigabit Ethernet	3.0.0	AA1419001
	1000BASE-LX GBIC	1300 nm, long wavelength, Gigabit Ethernet	3.0.0	AA1419002
	1000BASE-T GBIC	Category 5 copper unshielded twisted pair (UTP)	3.5.0	AA1419041

Table continues…

8800/8600 modules and components			Minimum software version	Part number
	1000BASE-XD GBIC	50k, SC duplex SMF, Gigabit Ethernet	3.0.0	AA1419003
	1000BASE-ZX GBIC	70k, SC duplex SMF, Gigabit Ethernet	3.0.0	AA1419004
	Gray CWDM GBIC	Discontinued, see Gray CWDM APD GBIC	3.1.2	AA1419005
	Violet CWDM GBIC	Discontinued, see Violet CWDM APD GBIC	3.1.2	AA1419006
	Blue CWDM GBIC	Discontinued, see Blue CWDM APD GBIC	3.1.2	AA1419007
	Green CWDM GBIC	Discontinued, see Green CWDM APD GBIC	3.1.2	AA1419008
	Yellow CWDM GBIC	Discontinued, see Yellow CWDM APD GBIC	3.1.2	AA1419009
	Orange CWDM GBIC	Discontinued, see Orange CWDM APD GBIC	3.1.2	AA1419010
	Red CWDM GBIC	Discontinued, see Red CWDM APD GBIC	3.1.2	AA1419011
	Brown CWDM GBIC	Discontinued, see Brown CWDM APD GBIC	3.1.2	AA1419012
	Gray CWDM APD GBIC	1470nm	3.1.4	AA1419017
	Violet CWDM APD GBIC	1490nm	3.1.4	AA1419018
	Blue CWDM APD GBIC	1510nm	3.1.4	AA1419019
	Green CWDM APD GBIC	1530nm	3.1.4	AA1419020
	Yellow CWDM APD GBIC	1550nm	3.1.4	AA1419021
	Orange CWDM APD GBIC	1570nm	3.1.4	AA1419022
	Red CWDM APD GBIC	1590nm	3.1.4	AA1419023
	Brown CWDM APD GBIC	1610nm	3.1.4	AA1419024
SFPs				
	1000BASE-SX SFP	850nm, Gigabit Ethernet, LC connector	4.0.0	AA1419013

Table continues…

8800/8600 modules and components			Minimum software version	Part number
	1000BASE-SX SFP	850nm, Gigabit Ethernet, MT-RJ connector	4.0.0	AA1419014
	1000BASE-LX SFP	1310nm, Gigabit Ethernet, LC connector	4.0.0	AA1419015
	1000BASE-T SFP	Category 5 copper unshielded twisted pair (UTP), RJ-45 connector	4.0.0	AA1419043
	1000BASE-BX bidirectional SFP	1310nm, Gigabit Ethernet, single fiber LC fiber-optic connector	4.1.0	AA1419069
	1000BASE-BX bidirectional SFP	1490nm, Gigabit Ethernet, single fiber LC fiber-optic connector	4.1.0	AA1419070
SFP+s				
	10GBASE-LR	1310 nm	7.1.3	AA1403011-E6
	10GBASE-ER	1530 to 1565 nm; 1550 nm nominal	7.1.3	AA1403013-E6
	10GBASE-SR	840 to 860 nanometers (nm); 850 nm nominal	7.1.3	AA1403015-E6
	10GBASE-LRM	1260 to 1355 nm; 1310 nm nominal	7.1.3	AA1403017-E6
	10GBASE-CX SFP+ direct attach cable; length 10 m.	N/A	7.1.3	AA1403018–E6
	10GBASE-CX SFP+ direct attach cable; length is 3 m.	N/A	7.1.3	AA1403019–E6
	10GBASE-CX SFP+ direct attach cable; length is 5 m.	N/A	7.1.3	AA1403020–E6
XFPs				
	10GBASE-LR/LW XFP	1-port 10km, 1310nm SMF, LC connector	4.0.0	AA1403001-E5
	10GBASE-SR XFP	1-port 300m, 850nm MMF, LC connector	4.0.0	AA1403005-E5
	10GBASE-ER/EW XFP	1-port 40km, 1550nm SMF, LC connector	4.0.x	AA1403003-E5

Table continues…

8800/8600 modules and components			Minimum software version	Part number
	10GBASE-ZR/ZW XFP	1550nm SMF, 80km, LC connector	4.1.0	AA1403006-E5
	10GBASE-LRM	1310 nm, DDI, up to 220 m, LC connector	4.1.0	AA1403007-E6

Power management

Power management identifies the available power in the chassis, called the power budget, and determines if enough power is available to operate the installed components.

During system boots, by default, switch fabrics are allotted highest priority and always power up. I/O modules power up if there is sufficient power remaining to do so. If there is insufficient power to bring all I/O modules online, they are powered up based on slot priority. By default, I/O modules are powered up starting at slot 1 until there is insufficient power to bring the next module online.

If you configure slot priorities, the slot with the lowest priority will not be powered up when there is insufficient power. After a power over-usage occurs, the system uses an SNMP trap to send a message to the user interface.

In redundancy mode, the system compares the total chassis power consumed against the total chassis power available and verifies that if one power supply fails, enough power still remains to operate the chassis and components. If, after one power supply failure, not enough power is available to operate the chassis and all components, the system sends an SNMP trap to the receiver and a message to the CLI to inform you that the switch is no longer operating in redundant mode. By default, the trap notification for redundancy is disabled.

Note:

In a redundant power supply configuration, that is, a +1 configuration where the system has one or more power supplies above the actual requirement, the power management logic automatically employs load-sharing across all active power supplies. This load-sharing ensures that the switch draws power equally from all available power supplies to support the system requirements in a fully active model.

Software lock-up detection

The software lock-up detect feature monitors processes on the master SF/CPU to limit situations where the switch stops functioning because of a software process issue. Monitored issues include:

- software entering a dead-lock state
- a software process entering an infinite loop

This feature monitors processes to ensure that software is functioning within expected time limits. After an issue that can potentially lock up the master SF/CPU is encountered, the master ends the process and restarts. In redundant configurations, the standby SF/CPU takes over from the master.

The SF/CPU logs details about suspended tasks in the log file. The log file is saved only on an installed external flash card. Installation of an external flash card on all SF/CPU modules is a best practice. Ensure that the external flash card provides sufficient space to write the log file. For additional information about this log file, see *Avaya Ethernet Routing Switch 8800/8600 Logs Reference, NN46205-701*.

Loop prevention and CP limit

Split MultiLink Trunking (SMLT) based network designs form physical loops for redundancy that logically do not function as a loop. Under certain adverse conditions, incorrect configurations or cabling, loops can form.

The two solutions to detect loops are Loop Detect and Simple Loop Prevention Protocol (SLPP). Loop Detect and SLPP detect a loop and automatically stop the loop. Both solutions determine on which port the loop is occurring and shuts down that port.

Control packet rate limit (CP Limit) controls the amount of multicast and broadcast traffic sent to the SF/CPU from a physical port. CP Limit protects the SF/CPU from being flooded with traffic from a single, unstable port. The CP Limit functionality only protects the switch from broadcast and control traffic with a QoS value of 7.

Do not use only the CP Limit for loop prevention. Avaya recommends the following loop prevention and recovery features in order of preference:

- SLPP
- Extended CP Limit (Ext-CP Limit) HardDown
- Loop Detect with ARP-Detect activated, when available

Beginning with Software Release 4.1, Avaya recommends using SLPP to protect the network against Layer 2 loops. SLPP is used to prevent loops in an SMLT network. SLPP is focused on SMLT networks but works with other configurations. This functionality provides active protection against network loops. When you configure and enable SLPP, the switch sends a test packet to the VLAN. A loop is detected if the switch or if a peer aggregation switch on the same VLAN receives the original packet. If a loop is detected, the switch disables the port. To enable the port requires manual intervention. As an alternative, you can use port Auto Recovery to reenable the port after a predefined interval. In addition to using SLPP for loop prevention, you can use the extended CP Limit softdown feature to protect the SF/CPU against DOS attacks where required.

The Loop Detection feature is used at the edge of a network to prevent loops. It detects whether the same MAC address appears on different ports. This feature can disable a VLAN or a port. The Loop Detection feature can also disable a group of ports if it detects the same MAC address on two different ports five times in a configurable amount of time.

On a individual port basis, the Loop Detection feature detects MAC addresses that are looping from one port to other ports. After a loop is detected, the port on which the MAC addresses were learned is disabled. Additionally, if a MAC address is found to loop, the MAC address is disabled for that VLAN.

The ARP-Detect feature is an enhancement over Loop Detect to account for ARP packets on IP configured interfaces. For network loops involving ARP frames on routed interfaces, Loop-Detect does not detect the network loop condition due to how ARP frames are copied to the SF/CPU . Use ARP-Detect on Layer 3 interfaces. The ARP-Detect feature supports only the vlan-block and port-down options.

For more information about designing your network with CP Limit and SLPP, see *Avaya Ethernet Routing Switch 8800/8600 Planning and Engineering — Network Design, NN46205-200*. For more information about loop detection, see *Avaya Ethernet Routing Switch 8800/8600 Configuration — VLANs and Spanning Tree, NN46205-517*.

The following table provides the Avaya recommended CP Limit values.

Table 13: CP Limit recommended values

	CP Limit Values when using the 8895 SF/CPU		CP Limit Values when using the 8692 SF/CPU with SuperMezz	
	Broadcast	**Multicast**	**Broadcast**	**Multicast**
Aggressive				
Access SMLT/SLT	1000	1000	1000	1000
Server	2500	2500	2500	2500
Core SMLT	7500	7500	3000	3000
Moderate				
Access SMLT/SLT	2500	2500	2500	2500
Server	5000	5000	3000	3000
Core SMLT	9000	9000	3000	3000
Relaxed				
Access SMLT/SLT	4000	4000	3000	3000
Server	7000	7000	3000	3000
Core SMLT	10 000	10 000	3000	3000

Important:

The 8692 SF/CPU with SuperMezz requires additional processing to send control packets from the CP to the SuperMezz and to program any hardware records in the I/O modules. Both operations now require an additional hop because they require CP involvement. To accommodate this additional processing, you must use the **`cp-limit broadcast-limit <value>`** and **`cp-limit multicast-limit <value>`** commands to lower the broadcast and multicast thresholds to 3000 packets per second.

The following table provides the Avaya recommended SLPP values.

Table 14: SLPP recommended values

	Setting
Enable SLPP	
Access SMLT	Yes
Access SLT	Yes
Core SMLT	No
IST	No
Primary switch	
Packet Rx threshold	5
Transmission interval	500 milliseconds (ms) (default)
Ethertype	Default
Secondary switch	
Packet Rx threshold	50
Transmission interval	500 ms (default)
Ethertype	Default

SLPP configuration considerations

Use the information in this section to understand the considerations and guidelines when configuring SLPP in an SMLT network.

- In Release 7.1, the default SLPP protocol ID Ethertype changed from 0x8104 to 0x8102. The new Ethertype is backward compatible and supports upgrade scenarios. For example, consider two IST peers with one running Release 7.0 and the other running Release 7.1. If you set both peers to use the default SLPP Ethertype, the protocol ID's will be different but they are compatible.
- In SMLT designs, you must enable SLPP packet receive on a port to detect a loop.
- Vary the SLPP packet receive threshold between the two IST peer switches so that if a loop is detected, the SMLT/SLT ports on each switch do not simultaneously go down, such that SMLT client isolation is avoided.
- SLPP packets (SLPP-PDU) are forwarded for each VLAN associated with any SLPP-Tx enabled ports.
- Within a VLAN, ports that should not be running SLPP should have either or both of their Rx or Tx settings disabled.
- The SLPP-PDU destination MAC address is the switch base MAC address, and the source MAC address is the switch base MAC address appended with the VLAN ID.
- The SLPP-PDU is sent out as a Layer 2 multicast packet and is constrained to the VLAN on which it is sent.
- If one port of an MLT is shut down because it received SLPP-PDUs that exceed the receive threshold of the port, then all ports of the MLT are shut down.

- In SMLT designs, a SLPP-PDU can be received by either the originating switch or the IST peer switch. All other switches treat the SLPP-PDU as a normal multicast packet and forward it within the VLAN.
- SLPP-PDU transmission and reception operates only on ports for which STP is in a forwarding state (if STP is enabled on one switch in the path).
- SLPP is port-based, so a port is disabled if it receives SLPP-PDU on one or more VLANs on a tagged port. For example, if the SLPP packet receive threshold is set to 5, a port is shut down if it receives 5 SLPP-PDU from one or more VLANs on a tagged port.
- SLPP operates and is configured at the VLAN level, but functions at a port level. This means that the SLPP receive threshold can be exceeded by packets from multiple different VLANs, not just packets from one VLAN. This is normally seen with tagged (trunk) ports.
- The SLPP receive count for a port is currently only reset upon port disable/enable, slot reset, or switch reset.
- SLPP prevents loops by shutting down the ports where the SLPP packet is received. However, if SLPP cannot find out where the loop is, it shuts down all SMLT ports. In some configurations, this can isolate an edge switch where a loop was detected.

SLPP and Spanning Tree Protocol

If you enable SLPP with any form of Spanning Tree (STP, RSTP, or MSTP), configure your network carefully to avoid potential issues. Consider the following example.

Figure 6: SLPP and Spanning Tree

In this example, with Rapid Spanning Tree enabled in the network, a loop condition is detected and a port on ERS2 is declared alternate. The alternate port is not part of the topology and does not forward any user traffic.

If SLPP is then enabled on ERS2, ERS2 sends out an SLPP-PDU on the active connection. However, it then receives the same SLPP-PDU on the alternate port. Because ERS2 receives an SLPP-PDU originated by itself, it disables the alternate port as there is a loop from an SLPP point of view.

This scenario arises because the switch can process SLPP network control packets received on a discarding port. This is due to the fact that, to conform with STP, the port must not forward traffic on the alternate port. However, the alternate port must continue to process certain network control packets (for example, if the discarding port could not read BPDUs, the port would never transition into the designated state). The processed control packets include those for LACP, VLACP, and, in this example, SLPP.

To run SLPP over Spanning Tree, configure the pathcosts such that the switch generating the SLPP PDUs does not have any ports in Alternate/Discarding state. Then SLPP will not shut down any interfaces unless Spanning Tree fails and there is a genuine loop.

Important:

SLPP and any form of STP are both used as loop prevention or protection protocols. Running both protocols at the same time on the same port is not recommended. It is recommended that users choose a design in which one or the other is enabled.

Extended CP Limit

The CP Limit function protects the SF/CPU by shutting down ports that send traffic to the SF/CPU at a rate greater than desired through one or more ports. You can configure the Extended CP Limit functionality to prevent overwhelming the switch with high traffic. To use the Extended CP Limit functionality, configure CP Limit at the chassis and port levels.

Important:

The Extended CP Limit feature differs from the rate-limit feature by monitoring packets that are only sent to the SF/CPU (control plane), instead of all packets that are forwarded through the switch (data plane).

The set of ports to check for a high rate of traffic must be predetermined, and configured as either SoftDown or HardDown.

HardDown ports are disabled immediately after the SF/CPU is congested for a certain period of time.

SoftDown ports are monitored for a specified time interval, and are disabled only if the traffic does not subside. The user configures the maximum number of monitored SoftDown ports.

To enable this functionality and set its general parameters, configuration must take place at the chassis level first. After you enable this functionality at the chassis level, configure each port individually to make use of it.

CP Limit Statistics

CP Limit protects the CPU from being flooded by traffic from a single, unstable port. You configure CP Limit by specifying thresholds on specified port within the chassis. If an unstable port reaches this threshold, CP Limit logs the current port statistics and then shuts down the port.

The CP Limit statistics feature captures traffic details such as the type of traffic and their queue priority. This information helps the designer debug issues with the network. To access these details, enter the following command to see the logs: **`more /pcmcia/rxstats.txt`**.

- For more information about CP Limit using EDM, see Configuring CP Limit on page 383
- For more information about CP Limit using the CLI, see Configuring CP Limit on page 163

- For more information about CP Limit using the ACLI, see Configuring CP Limit on page 291

Switch reliability

As system resources become more widely distributed, the reliability of network nodes is even more important because it affects connectivity in the entire network. Although software and hardware components of a node are reliable, they are still prone to failures. Protecting the node from failure of one of its components makes the node highly available.

The Ethernet Routing Switch 8800/8600 supports many High Availability features at all levels, including the following:

- Hardware
  - hot-swappable Input/Output (I/O) modules
  - hot-swappable Service Delivery Modules
  - passive backplane
  - Silicon Switch Fabric redundancy and load-sharing
  - redundant fans and power supply units
- Software
  - port-level and slot-level redundancy in the form of link aggregation
  - Split Link Aggregation
  - Split MulitLink Trunking (SMLT)
  - Routed Split MultiLink Trunking (RSMLT)
  - basic Central Processing Unit (SF/CPU) availability— warm standby
  - high SF/CPU availability—hot standby
  - router redundancy through Virtual Router Redundancy Protocol (VRRP)

If the primary SF/CPU module fails, the backup SF/CPU assumes the primary role.

Important:

During a SF/CPU failover, do not hot swap I/O modules until the new SF/CPU becomes the master SF/CPU.

You can configure SF/CPU redundancy to provide either basic availability or High Availability.

In warm standby redundancy mode, if the primary SF/CPU fails, the backup SF/CPU must initialize all input/output modules and load switch configurations, causing delays and disrupting operations. In hot standby redundancy mode, both SF/CPUs maintain synchronized configuration and operational databases, enabling very quick recovery and High Availability.

If you enable HA, also called CPU-HA, you automatically disable all non-HA features, that is features not supported by HA.

After you enable HA, both the primary and secondary SF/CPUs synchronize their database structures following initialization. After this complete table synchronization, only topology changes are exchanged between the primary and secondary SF/CPU.

Fabric (FAB) Memory Full error handling

This feature resolves the `Fab Memory Full` error that appears when I/O modules reset many times. Typically, the recovery action is to either reset the switch or replace the I/O module. Fabric (FAB) Memory Full error handling provides two commands that support these actions.

You can configure this feature to take a problematic I/O card offline, or to reset the switch fabric when the Fab Memory Full error is reported. For redundant network designs, resetting the switch fabric will divert network traffic around the affected switch and allow the network to recover with minimal interruption. If the network design does not support redundancy, then there will be network interruption while the switch is reset.

For configuration information using the CLI, see Enabling Fabric (FAB) Memory Full error handling on page 166

For configuration information using the ACLI, see Enabling Fabric (FAB) Memory Full error handling on page 295

For configuration information using the EDM, see Enabling Fabric (FAB) Memory Full error handling on page 368

Switch fabric failure detection

Each I/O module connects to the switch fabric on the CPU, and all ingress and egress traffic passes through the switch fabric. The Switch Fabric Failure Detection feature improves the parity-error detection and recovery mechanisms by monitoring the I/O modules' TAPs for parity errors and acting when errors exceed a specified threshold.

Caution:

The improper use of this feature may cause serious network problems. Avaya strongly recommends contacting Avaya Support before you enable it.

- For configuring the Switch Fabric Failure Detection feature using the CLI, see Detecting a switch fabric failure on page 132.
- For configuring the Switch Fabric Failure Detection feature using the ACLI, see Detecting a switch fabric failure on page 260.

Note:

This feature has CLI and ACLI support only. There is no EDM support in this release.

Important:

The following behavior occurs only when **parity-errors** is set to enabled and **action-869xSF-disable** is set to true:

- If there is only one CPU in the chassis and excess parity errors are detected, the I/O module with excess errors is powered off and the CPU is rebooted into boot monitor mode.
- If there are dual CPUs in the chassis and excess parity errors are detected on the Secondary CPU, the Switch Fabric Failure Detection feature sets the **autoboot** flag to false in boot.cfg on the Secondary CPU. Then the Switch Fabric Failure Detection feature reboots the Secondary CPU into boot monitor mode, thereby taking it out of service.
- If there are dual CPUs in the chassis and excess parity errors are detected on the Primary CPU, the Switch Fabric Failure Detection feature sets the **autoboot** flag to false on both the Primary and Secondary boot.cfg files. Then the Switch Fabric Failure Detection feature reboots the Primary CPU into boot monitor mode. The Secondary CPU now becomes the Primary CPU.

  If there is another failure on the new Primary, it will reboot and stop at boot monitor. To prevent this, you must manually set the **autoboot** flag to true in the new Primary CPU boot.cfg file. When excess parity errors occur on the Primary CPU, the Secondary CPU that becomes the new Primary initializes the failed Switch Fabric so it can remain in service.

Jumbo frames

The standard 1518 bytes Ethernet frame size was designed to protect against the high bit error rates of older physical-layer Ethernet components but increases in computer processing power and the use of switched Ethernet over unshielded twisted pair or fiber media significantly lowers Ethernet errors.

In addition, the speed and capacity of the Ethernet are expanding the processor limits of many installed servers, and more data is transferred between servers. For these reasons, increasing Ethernet frame size is a logical option. The Ethernet Routing Switch 8800/8600 now supports Ethernet frames as large as 9600 bytes, compared to the standard 1518 bytes, to transmit large amounts of data efficiently and minimize the task load on a server SF/CPU.

Tagged VLAN support

A port with VLAN tagging activated can send tagged frames. If you plan to use Jumbo frames in a VLAN, make sure that the ports in the VLAN are configured to accept Jumbo frames and that the server or hosts in the VLAN do not send frames that exceed 9600 bytes. For more information about configuring VLANs, see *Avaya Ethernet Routing Switch 8800/8600 Configuration — VLANs and Spanning Tree, NN46205-517*.

Modules and interfaces that support Jumbo frames

As a minimum, Jumbo frame support requires Gigabit speed. Although the system allows larger MTU settings, modules with 10/100 interfaces do not support Jumbo frames.

The following Ethernet Routing Switch 8800/8600 devices and interfaces support Jumbo frames:

- All RS and 8800 modules.
- Gigabit fiber and Gigabit copper ports in 8608GBIC, 8608GBIC-E, 8632TX, 8630GBR, and 8648GTR.
- 10 Gigabit interfaces 8683XLR and 8683XZR.
- IPv6—if you enable IPv6 Jumbo frame support you must set the port interface MTU size to 9600 bytes.

The following IPv4 and IPv6 control plane applications do not support Jumbo frames:

- Ping
- Telnet
- Domain Name Service (DNS)
- Secure Shell (SSH)
- Secure Copy Protocol (SCP)
- Simple Network Management Protocol (SNMP)
- Open Shortest Path First (OSPF) versions 2 and 3
- Routing Internet Protocol (RIP)

If you enable Jumbo frame support on the chassis, then you must set the port interfaces that support the Jumbo frames feature to an MTU size of 9600 bytes. Retain the default MTU size of 1950 bytes on port interfaces that do not support the Jumbo frames feature. Changes that you make to the MTU size take place immediately.

Important:

On the 8648GTR module, ports operating at 100 Mbit/s support a maximum frame size of 9188 bytes.

Link Layer Discovery Protocol

Link Layer Discovery Protocol (LLDP) enables stations connected to a LAN to advertise their capabilities to each other, enabling the discovery of physical topology information for network management. LLDP-compatible stations can consist of any interconnection device including PCs, switches, and routers. Each LLDP station stores LLDP information in a standard Management Information Base (MIB), making it possible for a network management system (NMS) or application to access the information.

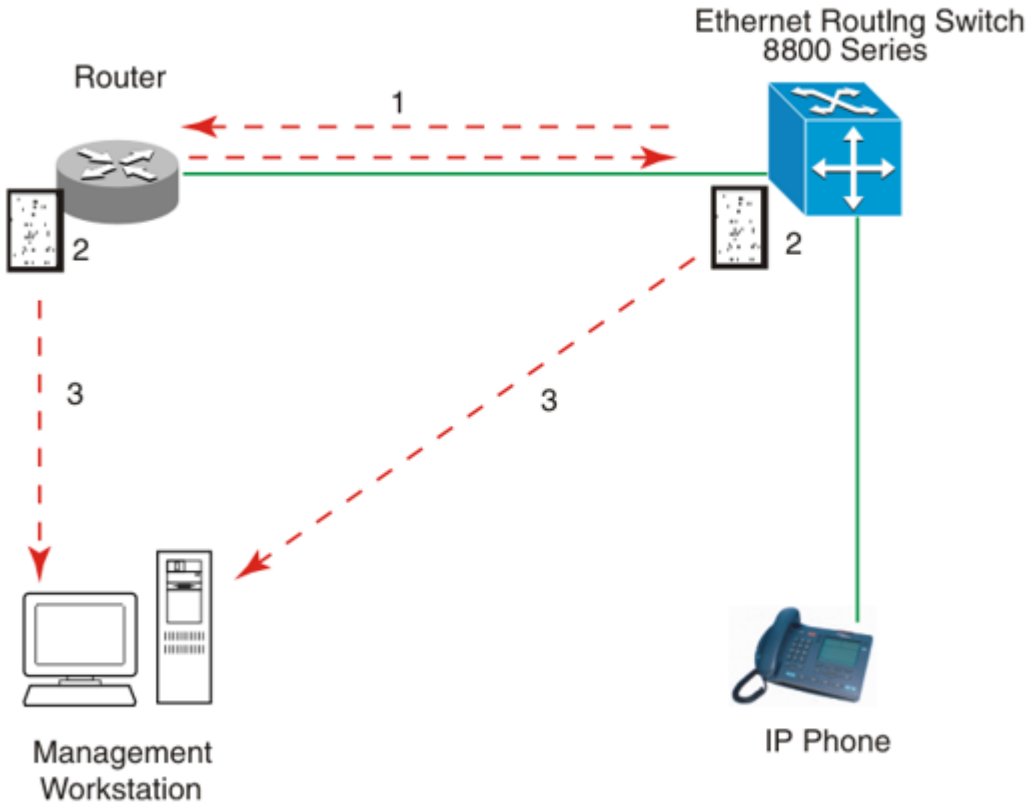
Each LLDP station:

- advertises connectivity and management information about the local station to adjacent stations on the same 802 LAN (802.3 Ethernet with 8300 Series).
- receives network management information from adjacent stations on the same LAN.

LLDP also makes it possible to discover certain configuration inconsistencies or malfunctions that can result in impaired communications at higher layers. For example, it can be used to discover duplex mismatches between a router and the connected switch.

LLDP is compatible with IETF PROTO MIB (IETF RFC 2922).

The following image shows an example of how LLDP works in a network.



1. The Ethernet Routing Switch and LLDP-enabled router advertise chassis/port IDs and system descriptions to each other.
2. The devices store the information about each other in local MIB databases, accessible by using SNMP.
3. A network management system retrieves the data stored by each device and builds a network topology map.

LLDP operational modes

LLDP is a one-way protocol. An LLDP agent can transmit information about the capabilities and current status of the system associated with its MAC service access point (MSAP) identifier. The LLDP agent also can receive information about the capabilities and current status of the system associated with a remote MSAP identifier. However, LLDP agents cannot solicit information from each other.

You can set the local LLDP agent to transmit only, receive only, or to both transmit and receive LLDP information. You can configure the state for LLDP reception and transmission using SNMP, CLI, or ACLI commands.

Connectivity and management information

The information parameters in each LLDP frame are in a Link Layer Discovery Protocol Data Unit (LLDPDU) as a sequence of short, variable length information elements known as TLVs (type, length, value).

Each LLDPDU includes the following four mandatory TLVs:

- Chassis ID TLV
- Port ID TLV
- Time To Live TLV
- End Of LLDPDU TLV

The chassis ID and the port ID values are concatenated to form a logical MSAP identifier that the recipient uses to identify the sending LLDP agent and port.

- A non-zero value in the Time to Live (TTL) field of the TTL TLV indicates to the receiving LLDP agent how long the LLDPDU information from the MSAP identifier remains valid. The receiving LLDP agent automatically discards all LLDPDU information, if the sender fails to update it in a timely manner.
- A zero value in TTL field of Time To Live TLV tells the receiving LLDP agent to discard the information associated with the LLDPDU MSAP identifier.

In addition to the four mandatory TLVs, the ERS 8800/8600 software supports the TLV extension set consisting of Management TLVs and organizationally-specific TLVs. Organizationally-specific TLVs are defined by either the professional organizations or the individual vendors that are involved with the particular functionality being implemented. You can specify which of these optional TLVs to include in the transmitted LLDPDUs for each port.

For more information about the supported TLV extension set, refer to the following sections:

- Management TLVs on page 72
- IEEE 802.1 organizationally-specific TLVs on page 72
- IEEE 802.3 organizationally-specific TLVs on page 72

Management TLVs

The optional management TLVs are as follows:

- Port Description TLV
- System Name TLV
- System Description TLV
- System Capabilities TLV (indicates both the system supported capabilities and enabled capabilities, such as end station, bridge, or router)
- Management Address TLV

IEEE 802.1 organizationally-specific TLVs

The optional IEEE 802.1 organizationally specific TLVs are:

- Port VLAN ID TLV contains the local port PVID.
- Port And Protocol VLAN ID contains the VLAN IDs of the port and protocol VLANs that contain the local port. (If the port is a part of multiple protocol based VLANs then the lowest protocol based VLAN ID is advertised.)
- VLAN Name TLV contains the VLAN names of the VLANs that contain the local port. (If the port is tagged and is a member of multiple VLANs, including a voice VLAN, then the voice VLAN ID is advertised. If the port is tagged and is part of multiple VLANs, but not a voice VLAN, then the Default VLAN ID is advertised.)
- Protocol Identity TLV advertises the protocol supported. The following values are used for supported protocols:
  - STP protocol string {0x00,0x26,0x42,0x42,0x03, 0x00, 0x00, 0x00}
  - MSTP protocol string {?????}
  - RSTP protocol string {?????}
  - EAP protocol string {0x88, 0x8E, 0x01}
  - LLDP protocol string {0x88, 0xCC}

IEEE 802.3 organizationally-specific TLVs

The optional IEEE 802.3 organizationally specific TLVs are:

- MAC/PHY Configuration/Status TLV indicates the autonegotiation capability and the speed and duplex status of IEEE 802.3 MAC/PHYs.
- Link Aggregation TLV indicates the current link aggregation status of IEEE 802.3 MACs.
- Maximum Frame Size TLV indicates the maximum supported 802.3 frame size.

Transmitting LLDPDUs

When a transmit cycle is initiated, the LLDP manager extracts the managed objects from the LLDP local system MIB and formats this information into TLVs. TLVs are inserted into the LLDPDU.

LLDPDU are regularly transmitted at a user-configurable transmit interval (tx-interval) or when any of the variables in the LLPDU is modified on the local system (such as system name or management address).

Tx-delay is "the minimum delay between successive LLDP frame transmissions."

TLV system MIBs

The LLDP local system MIB stores the information for constructing the various TLVs to be sent. The LLDP remote systems MIB stores the information received from remote LLDP agents.

LLDPDU and TLV error handling

LLDPDUs and TLVs that contain detectable errors are discarded. TLVs that are not recognized, but that also contain no basic format errors, are assumed to be validated and are stored for possible later retrieval by network management.

LLDP considerations and limitations

Keep the following points in mind when configuring LLDP on an ERS 8800/8600 switch:

- Discovery of IP handsets is not supported.
- Power over Ethernet (PoE) is not supported.
- Media Endpoint Discovery (MED) is not supported.
- High Availability (HA) is not supported.
- EDM support for LLDP is not supported in this release.

Chapter 6: System access fundamentals

This chapter contains conceptual information about accessing the Avaya Ethernet Routing Switch 8800/8600 and creating users and user passwords for access.

Logging on to the system

After the switch startup sequence is complete, the login prompt appears. The default values for login and password for the console and Telnet sessions are shown in the following table .

Table 15: 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; does not allow changing security and password settings. This access level is equivalent to SNMP read-write community access.	rw	rw
Read/write/all	Permits all the rights of Read-Write access and the ability to change security settings, including the command line interface (CLI) and Web-based management user names and passwords and the SNMP community strings.	rwa	rwa

You can enable or disable users with particular access levels on the Ethernet Routing Switch 8800/8600, eliminating the need to of maintain large numbers of access levels and passwords for each user.

A user with a disabled access level who attempts to log on is denied access to the switch. The following error message appears after a user attempts to log on with a blocked access level:

```
Code=0x1ff0009 Blocked unauthorized cli access.
```

The system logs the following message to the log file:

```
User <user-name> tried to connect with blocked access level <access-level> from <src-
ipaddress> via <login type>.
```

The system logs the following message for the console or modem port:

```
User <user-name> tried to connect with blocked access level <access-level> from <console/
modem> port.
```

RADIUS authentication takes precedence over the local configuration. If you enable RADIUS authentication on the switch, the user can access the switch even if an access level is blocked on the switch.

If you disable an access level all running sessions, except FTP sessions, with that access level to the switch terminate.

Important:

Only the RWA user can disable an access level on the switch. You cannot disable the RWA access level on the switch.

These configurations are preserved across restarts.

hsecure bootconfig flag

The Ethernet Routing Switch 8800/8600 supports a configurable flag called High Secure (hsecure). Use the hsecure flag to enable the following password features:

- 10 characters enforcement
- aging time
- limitation of failed login attempts
- protection mechanism to filter designated IP addresses

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

For more information about the hsecure flag, see *Avaya Ethernet Routing Switch 8800/8600 Security, NN46205-601*.

Managing the switch using different VRF contexts

You can use Enterprise Device Manager to manage the switch using different VRF contexts. When you open a switch using Enterprise Device Manager in the GlobalRouter (VRF 0) context, you can manage the entire switch. When you open a switch using EDM in a different VRF context, you have limited capability for managing the switch. For example, you can manage only the ports that were assigned to this VRF. In addition, many of the EDM management functions are not available to you.

With the use of user names and context names (SNMPv3), and community strings (SNMPv1/v2) , administrators can assign different VRFs to manage selected components, such as ports and VLANs. For more information about context names and community strings, see *Avaya Ethernet Routing Switch 8800/8600 Security, NN46205-601*.

CLI passwords

The switch ships with default passwords set for access to the CLI through a console or Telnet session. If you possess read/write/all access authority, and you are using SNMPv3, you can change passwords that are in encrypted format. If you are using EDM, you can also specify the number of allowed Telnet sessions and rlogin sessions.

Important:

Be aware that the default passwords and community strings are documented and well known. Avaya strongly recommends that you change the default passwords and community strings immediately after the first logon.

For security, if you fail to log on correctly on the master central processing unit (CPU) in three consecutive instances, the CPU locks for 60 seconds.

Password encryption

In the Avaya Ethernet Routing Switch 8800/8600 software Release 4.1 and later, passwords are stored in encrypted format and are no longer stored in the configuration file.

Caution:

Security risk

If you load a configuration file saved prior to Release 3.7.6, saved passwords from the configuration file are not recognized. If you start the switch for the first time with Release 3.7.6 or higher image, the password resets to default values and the system generates a log, indicating changes.

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

Subscriber or administrative interaction

As a network administrator, you can configure the RADIUS server for user authentication to override user access to commands. You must still provide access based on the existing six access levels in the Ethernet Routing Switch 8800/8600, but you can customize user access by allowing and disallowing specific commands.

You must configure the following three returnable attributes for each user:

- Access priority (single instance)–the access levels currently available on Ethernet Routing Switch 8800/8600 ro, l1, l2, l3, rw, rwa.
- Command access (single instance)–indicates whether the commands configured on the RADIUS server are allowed or disallowed for the user.
- CLI commands (multiple instances)–the list of commands that the user can or cannot use.

Access policies for services

You can control access to the switch by creating an access policy. An access policy specifies the hosts or networks that can access the switch through various services, such as Telnet, Simple Network Management Protocol (SNMP), Hypertext Transfer Protocol (HTTP), Secure Shell (SSH), and remote login (rlogin). You can enable or disable access services by configuring flags.

You can define network stations that are explicitly allowed to access the switch or stations that are explicitly forbidden to access the switch. For each service you can also specify the level of access, such as read-only or read/write/all.

When you configure access policies, you can either:

Globally enable the access policy feature, and then create and enable individual policies. Each policy takes effect immediately after you enable it.

or

Create and enable individual access policies, and then globally enable the access policy feature to activate all the policies at the same time.

For more information about configuring access policies on IPv6, see *Avaya Ethernet Routing Switch 8800/8600 Configuration — IPv6 Routing, NN46205-504*.

Enterprise Device Manager passwords

The Ethernet Routing Switch 8800/8600 includes a Web-based management interface, Enterprise Device Manager, that you can use to configure and monitor your switch through a Web browser from anywhere on your network.

Enterprise Device Manager is protected by a security mechanism that requires you to log in to the device using a user name and password. The switch ships with the default user name of **admin** and the password is **password**.

Important:

For security reasons, the Web interface is disabled by default. For instructions about how to enable the interface, see *Avaya Ethernet Routing Switch 8800/8600 User Interface Fundamentals, NN46205-308*

Web server password

Web-server passwords authenticate the user who is accessing the device using Enterprise Device Manager. The passwords are encrypted using the blowfish algorithm and are stored in a hidden file. The passwords are not visible on the device through any show command and are not stored in the configuration file.

Password reset

You can selectively reset login username and passwords, web-server passwords, and SNMP community strings. This reset is implemented as a hidden command in the CLI and Avaya command line interface (ACLI) and you can access the command only if you are assigned the rwa access level.

Password encryption

The Avaya Ethernet Routing Switch 8800/8600 handles password encryption in the following manner:

- When the device starts, the web-server passwords and community strings are restored from the hidden file.
- When the web-server username/password or SNMP community strings are modified, the modifications are updated to the hidden file.

Password recovery

Use the following CLI commands to recover your password. Only a user with rwa access can access these hidden commands.

- **ERS-8606:5/config/sys/set/reset-passwd# login-user <l1|l2|l3|ro|rw>**

The preceding command resets the login usernames and passwords selectively. You can reset the following access levels: l1, l2, l3, ro, rw.

Important:

You cannot reset the rwa community string.

- The following command resets the web server username/password for "rwa" access:
  ERS-8606:5/config/sys/set/reset-passwd# web-server-passwd <rwa>
- The following command resets the following SNMP community strings: l1, l2, l3, ro, rw :
  ERS-8606:5/config/sys/set/reset-passwd# snmp-community-strings <l1|l2|l3|ro|rw>

Chapter 7: Ethernet Routing Switch 8800/8600 licensing fundamentals

This chapter provides conceptual information about the feature licensing for the Avaya Ethernet Routing Switch 8800/8600. Review this section before you make changes to the license configuration.

Feature licensing

Enabling features on a Ethernet Routing Switch 8800/8600 requires the generation and installation of a license file that contains the authorized MAC addresses of the switches that the license file will be installed on.

In addition to a Base Software License, the Ethernet Routing Switch 8800/8600 supports optional Advanced and Premier feature licenses to provide access to additional switch features contained within those licensing levels. These licenses are purchased separately in the form of either an Advanced License Kit or Premier License Kit. The Premier License Kit contains all Advanced License Kit features. When you purchase either an Advanced License Kit or a Premier License Kit, all current and future features are covered under the license. If you currently have an Advanced License Kit, there is no discounted price to move to a Premier License Kit, you must purchase a complete Premier License Kit. If you purchase a Premier License Kit at any time, you are licensed for all features for the life of the product. For more information, contact your Avaya sales representative.

You must purchase one Base software license for each chassis to obtain access to those features.

Advanced and Premier License level features use a software-based licensing mechanism to unlock specific features.

You must specify the name and location of your license file in the boot configuration file. If you do not specify the location of your license file, you can encounter issues with your licensed features.

For more information see, Boot parameter configuration using the CLI on page 105 and Boot parameter configuration using the ACLI on page 235.

Base License

The features enabled by the Base License are as follows:

- Avaya VENA Unified Access
- IP Multinetting
- IP Source guard
- DHCP Snooping
- Dynamic ARP Inspection
- BPDU Filtering
- IGMP Querier for L2
- PIM-SSM for SMLT
- Multicast/VLAN Registration
- LLDP

Advanced License

The features enabled by the Advanced License are as follows:

- Border Gateway Protocol version 4 (BGP4) for more than 10 Peers
- Bidirectional Forwarding Detection
- Multicast Source Discovery Protocol (MSDP)
- Packet Capture function (PCAP)
- IPv6 Features
  - IP Routing
  - IPv6 over SMLT and RSMLT
  - DHCPv6 Relay
  - VRRPv3
  - BGP+
  - RADIUSv6
  - BFD over IPv6

Premier License

The features enabled by the Premier License are as follows:

- All Advanced License features

- Virtual Routing and Forwarding, Lite version (VRF-Lite)
- Multicast virtualization for VRF-Lite (IGMP & PIM-SM/SSM)
- Multi-Protocol Border Gateway Protocol (MP-BGP)
- IP-Virtual Private Network, Multi-Protocol Label Switching (RFC2547) (IP-VPN MPLS RFC2547)
- IP-Virtual Private Network-Lite (IP-VPN-Lite – IP-in-IP)
- Shortest Path Bridging (SPB) Features:
  - SPB L2 VSNs (VLAN Extensions)
  - SPB GRT Shortcuts (VRF0 shortcuts)
  - SPB L3 VSN (VRF Extensions)
  - IP VPN Lite over SPB IP shortcuts
  - Inter-VSN Routing
  - IEEE 802.ag Connectivity Fault Management
  - IP Multicast over SPBM

The Premier License enables all licensed features on the Ethernet Routing Switch 8800.

Important:

Avaya recommends that you purchase the Premier License if you anticipate growth in your network. If you purchase the Advanced License, and later require features available only if you have the Premier License, you must also purchase the Premier License. If you purchase the Premier License initially, you have access to all features enabled by the Advanced License and the Premier License (there is no need to purchase the Advanced License separately).

You must purchase the Base software license for each chassis. You can install an Advanced or Premier License on each chassis after you have installed the Base software license, but the Advanced and Premier Licenses are optional.

Premier Trial License

The Ethernet Routing Switch 8800/8600 provides a trial period of 60 days during which you have access to all features. In the trial period you can configure all features without restriction, including system console and log messages.

System console and log messages alert you to the expiry of the 60 day trial period. The message `Trial Period for Automatic Premier Feature usage will expire in ## days` first appears when 30 days of the trial period remain. You receive periodic notification until fewer than 10 days remain in the trial period, at which point you receive notification every 24 hours until the expiry date.

At the end of the trial period, the following message appears: `The automatic Premier feature trial period has now expired. Any Advanced or Premier features that were used or enabled will continue to work but will be disabled`

`after any switch reboot. Please buy the proper license if you wish to continue to use these features.` This message is the last notification recorded.

The switch logs the preceding messages even if no license features are used or tested during the trial period. If any valid license is loaded on the switch at any time, none of the preceding messages will be recorded.

Note:

If you need to extend your trial license to complete testing of Premier License features, contact your Avaya representative who can obtain the procedure from product management to extend the trial license for a single additional 60 day period.

Licensing enhancements

Release 7.2.10 includes the following licensing enhancements.

Warning messages

The ERS 8800/8600 switch generated a Warning message every 24 hours to notify customers that their feature license was not installed or the trial period expired.

This enhancement stops the display of erroneous messages by checking to see if the Advanced or Premier feature is actually configured on the switch before generating the Warning message.

VRF security risk

If a VRF Premier license was not installed or the trial period expired, there was a potential security risk because the VLANs of VRFs were added to the Global Router (Vrf 0).

This enhancement allows the VRF configurations to load properly, but you cannot enable or create any new Advanced or Premier features configurations until you install a valid license.

SuperMezz failure

If a SuperMezz card failed, it caused the switch to boot in Non-Mezz mode. This was a potential security risk because the VLANs of VRFs were added to the Global Router (Vrf 0).

This enhancement allows the Mezz configuration to load properly even if the Mezz card fails. The switch logs a Warning messages every 15 minutes indicating the Mezz failure until it is resolved.

PCAP and port mirroring

If a PCAP Advanced license trial period expired, there was no way to remove the PCAP configuration. Because the PCAP filters could not be removed, the switch blocked any new port mirroring configurations.

This enhancement generates a log messages every hour indicating that the PCAP license is invalid. However, it also enables you to delete the PCAP configuration if you no longer want to use that feature. This enables you to continue to use port mirroring.

License type and part numbers

The following table provides the part number for the various licenses supported on the Ethernet Routing Switch 8800/8600.

Table 16: Supported licenses for the Ethernet Routing Switch 8800/8600

Part number/ Order code	License type and description	Number of chassis supported
DS1410021	Ethernet Routing Switch 8800/8600 Advanced License Kit for one chassis. Enabled features: BGP4 (above 10 peers), IPv6 Routing, PCAP, MSDP and BFD. (One license required per chassis.)	1
DS1410022	Ethernet Routing Switch 8800/8600 Advanced License Kit for up to 10 chassis. Enabled features: BGP4 (above 10 peers), IPv6 Routing, PCAP, MSDP, and BFD. (One license required per chassis.)	10
DS1410023	Ethernet Routing Switch 8800/8600 Advanced License Kit for up to 50 chassis. Enabled features: BGP4 (above 10 peers), IPv6 Routing, PCAP, MSDP, and BFD. (One license required per chassis.)	50
DS1410024	Ethernet Routing Switch 8800/8600 Advanced License Kit for up to 100 chassis. Enabled features: BGP4 (above 10 peers), IPv6 Routing, PCAP, MSDP, and BFD. (One license required per chassis.)	100
DS1410026	Ethernet Routing Switch 8800/8600 Premier License kit for one chassis. Enabled features: Advanced License features, plus, VRF-Lite, MP-BGP, IP-VPN MPLS RFC4364/2547, IP-VPN-Lite (IP-in-IP), and Multicast Virtualization for VRF-lite (IGMP, PIM-SM/SSM). (One license required per chassis.)	1
DS1410027	Ethernet Routing Switch 8800/8600 Premier License Kit for up to 10 chassis. Enabled features: Advanced License features, plus, VRF-Lite, MP-BGP, IP-VPN MPLS RFC4364/2547, IP-VPN-Lite (IP-in-IP), and Multicast Virtualization for VRF-lite (IGMP, PIM-SM/SSM). (One license required per chassis.)	10
DS1410028	Ethernet Routing Switch 8800/8600 Premier License Kit for up to 50 chassis. Enabled features: Advanced License features, plus, VRF-Lite, MP-BGP, IP-VPN MPLS RFC4364/2547, IP-VPN-Lite (IP-in-IP), and Multicast Virtualization for VRF-lite (IGMP, PIM-SM/SSM). (One license required per chassis.)	50
DS1410029	Ethernet Routing Switch 8800/8600 Premier License Kit for up to 100 chassis. Enabled features: Advanced License features, plus, VRF-Lite, MP-BGP, IP-VPN	100

Table continues…

Part number/ Order code	License type and description	Number of chassis supported
	MPLS RFC4364/2547, IP-VPN-Lite (IP-in-IP), and Multicast Virtualization for VRF-lite (IGMP, PIM-SM/ SSM). (One license required per chassis.)	

License certificates

Each Advanced or Premier License Kit contains a License Certificate with a License Authorization Code (LAC) that enables a specific number of licenses for one or multiple Ethernet Routing Switch 8800/8600 switches. Each Ethernet Routing Switch 8800/8600 switch requires and uses only one license file to unlock features associated with that license. A single license file can contain up to 100 Base MAC addresses for installation on multiple Ethernet Routing Switch 8800/8600 switches.

The License Certificate has printed instructions detailing how to deposit license entitlements (LACs) into a license bank, enter switch base MAC addresses and create the license file. It also has instructions on how to copy the license file onto each switch to unlock additional features associated with a license.

License file generation

After you purchase a license, you must generate the license file using the Avaya Electronic Licensing portal. The licensing portal works on the concept of a license bank—an electronic repository for all license entitlements and licenses. License entitlements are deposited into your license bank when you enter a License Authorization Code (LAC). The LAC is provided on the License Certificate when you purchase the license.

The software license file is based on authorized chassis base MAC addresses. You can generate an individual license file with one or multiple chassis base MAC addresses. You can add additional MAC addresses to the same license file at a later time, if required. A license file can support up to 100 unique MAC addresses.

Working with feature license files

After you obtain the license file to enable Advanced or Premier License features, you must install the license file on the switch to unlock the associated licensed features.

You can assign any filename and extension to a license file generated on Avaya’s Licensing portal for an Ethernet Routing Switch 8800/8600 switch. For an Ethernet Routing Switch 8800/8600, you can install a license file on to internal Flash, external memory card (PCMCIA or flash), or a TFTP

server. By default, an Ethernet Routing Switch 8800/8600 looks for the license file by the filename license.dat on internal Flash. However, if the license file is not named license.dat or is not located in the switch Flash directory, you must update the bootconfig file (CLI) or the boot choice (ACLI) with the exact license file name and path where the license file is located.

License transfer

For information about transferring a license and obtaining an updated license file for the Ethernet Routing Switch 8800/8600, see License transfer on page 92.

Chapter 8: Ethernet Routing Switch 8800/8600 licensing

Generate and install license files to enable advanced and premier features on your Avaya Ethernet Routing Switch 8800/8600.

Prerequisites to Ethernet Routing Switch 8800/8600 licensing

- You must purchase the appropriate license for the additional switch features. For more information, contact your Avaya sales representative.

Ethernet Routing Switch 8800/8600 licensing tasks

This work flows shows you the sequence of tasks you perform to configure licensed features.

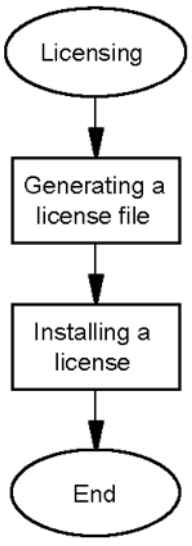


Figure 7: Licensing tasks

Chapter 9: License generation

Generate the license file you need to enable licensed features on the system. This task is independent of loading the license file on to the switch.

Generating a license

Generate a license to enable licensed features on the switch by performing this procedure.

Prerequisites

- You must have a purchased Ethernet Routing Switch 8800/8600 license kit containing a License Certificate with a License Authorization Code (LAC).
- Before you generate a license file, you need to obtain the Ethernet Routing Switch 8800/8600 base MAC address that you want to enable licensed features on. The base MAC address can be found by using the following CLI command:

  ```
  show sys info
  ```

  You can also find the base MAC address by using the Avaya command line interface (ACLI) command:

  ```
  show sys-info
  ```

  For sample output from these commands, see Job aid on page 90.

Procedure steps

1. Obtain the base MAC address for the chassis:`show sys-info`
2. Go to the Avaya Electronic Licensing portal at http://www.avayalicensing.com
3. Type your contact information in the required boxes.
4. Create a new license bank or provide details for an existing license bank to deposit licenses.
5. Select an E-mail notification option. The system sends newly generated licenses to the nominated E-mail address.

6. Enter the License Authorization Code provided on the License Certificate when you purchased the license.
7. Click **Submit**.

   A new screen appears while the portal activates and deposits the associated number of licenses in the license bank. Do not leave the page or close your Web browser. Upon successful completion, a confirmation message appears.
8. Click **Go to License Bank to Download license**.

   The License Bank screen appears and displays information about the License Authorization Code just activated.
9. Click **Generate License**.

   The Generate License screen appears.
10. Enter the required details for the license file.

    For additional information, see Variable definitions on page 89.
11. Click **Generate License File**.

    A confirmation message appears. The license file is immediately sent to the nominated E-mail address set up with the license bank. You can choose to return to the license bank or log out from the licensing portal.

    Important:

    The license file is a compressed binary file. It is important that while downloading or saving this file, the browser does not automatically decompress this file.

Variable definitions

Use the data in the following table to complete the Generate licensescreen.

Variable	Value
Switch MAC Address	Specifies the base MAC address of the switch for which the license file is being generated. Follow the example format displayed next to the entry box.
File Name of List of MAC Addresses	Specifies the file name containing multiple base MAC addresses of the switches for which the license file is being generated. The file must be an ASCII text file and adhere to the following rules: • Each line must contain one MAC address (use MS-DOS or UNIX line ending characters. • The MAC addresses can be in lower or upper case characters and must be in hexadecimal format with each pair (byte) separated by colons (XX:XX:XX:XX:XX:XX). • Do not use other characters or spaces.

Table continues…

Variable	Value
	• The file must contain the correct base MAC addresses. Incorrect addresses results in non-working licensed features. • The number of MAC addresses must not exceed the number of licenses allowed for the License Authorization Code.
Output License File Name	Specifies the name of the license file. The file name is limited to 63 alphanumeric, lowercase characters. The underscore (_) character is allowed. Do not use spaces or special characters. The filename must use a dot (.) with a three character file extension. For example, license.dat. **Important:** While a license file generated for an Avaya Ethernet Routing Switch 8800/8600 on the Avaya Licensing portal can be created using any filename or extension, an Avaya Ethernet Routing Switch 8800/8600 searches for a license filename with an extension of .dat in its flash directory. Therefore, you need to ensure the destination license file being copied to the Avaya Ethernet Routing Switch 8800/8600 has .dat as the file extension. Failure to do this results in Advanced or Premier features not being available.
User Comment 1	Provides a location for free-form, user-entered text related to the license file. For example, a location to assist in asset tracking.
User Comment 2	Provides a second location for free-form, user-entered text related to the license file. For example, a location to assist in asset tracking.

Job aid

The following shows sample output that is displayed when you use the CLI `show sys info` command. You can also use the ACLI `show sys-info` command to display the base MAC address.

```
ERS-8606:5# show sys info


General Info :

        SysDescr     : ERS-8610 (4.2.0.0)
        SysName      : ERS-8610
        SysUpTime    : 5 day(s), 02:53:56
        SysContact   : http://support.nortel.com/
        SysLocation  : 4655 Great America Parkway,Santa Clara,CA 95054

Chassis Info :

        Chassis     : 8010
        Serial#     : SSPN6C06YP
        HwRev       : 06
        H/W Config          : 02
        NumSlots            : 10
        NumPorts            : 47
        GlobalFilter        : enable
        VlanBySrcMac        : disable
        ForceTopologyIpFlag: false
        Ecn-Compatib        : enable
        WsmDirectMode       : disable
        max-vlan-resource-reservation : (disable) -> (disable)

        multicast-resource-reservation : (2048) -> (2048)
        BaseMacAddr         : 00:15:e8:9e:10:00
        MacAddrCapacity : 4096
        Temperature : 25 C
        MgmtMacAddr : 00:15:e8:9e:13:f4
        System MTU  : 1950
        clock_sync_time : 60

Power Supply Info :

--More-- (q = quit)
```

Chapter 10: License transfer

Transfer a license and obtain an updated license file for Avaya Ethernet Routing Switch 8800/8600. You need to transfer a license in the following scenarios:

- Due to a chassis failure, you replaced the switch with a replacement chassis that has a new base MAC address.
- You entered an incorrect base MAC address on the Avaya Electronic Licensing portal during the license file generation process.
- You need to transfer the license to a different switch.

Transferring a license

Transfer a license and obtain an updated license file for an Avaya Ethernet Routing Switch 8800/8600 by performing this procedure.

Prerequisites

- Before you transfer a license, you need to obtain the new replacement Ethernet Routing Switch 8800/8600 base MAC address. The base MAC address can be found by using the following command line interface (CLI) command:

  ```
  show sys info
  ```

  You can also find the base MAC address by using the Avaya command line interface (ACLI) command:

  ```
  show sys-info
  ```

Procedure steps

1. Find the base MAC address of the new chassis:`show sys-info`
2. Go to the Avaya Electronic Licensing portal at http://www.avayalicensing.com
3. Click **License Bank** on the left menu.
4. Login to the License Bank by entering the License Bank name and password.

5. Select the appropriate License Authorization Code (LAC) entry in the License Bank associated with the license type, and then click **View Details**.

   Note that a License Bank can contain many different License types for different products. Therefore, it is important that you select the correct LAC entry for the product and license type to access the license file containing the MAC address you want to replace. For example, if the Ethernet Routing Switch 8800/8600 base MAC address that is being replaced is running a Premier License, then select a Premier Licence LAC to view the transaction for the license file containing the base MAC.

   Important:

   MAC address replacements are allocated and limited on a per LAC basis. You can replace only one MAC address in a 1 or 10 license LAC entry. You can replace up to 5 or 10 MAC addresses for 50 or 100 license LAC deposits, respectively.

6. Within the View Details screen, select a transaction that has the license file name in use on the Ethernet Routing Switch 8800/8600 that is being replaced.

   The same license file name can appear in several transactions; choose any transaction that has the license file name that you need to replace. The license file always contains the latest full list of MAC addresses.

7. Click **Replace Switch**.

   The Replace Switch MAC screen appears displaying the name of the license file and the MAC addresses that it contains.

8. In the Enter Replacement Switch MAC Address box, type the new base MAC address.

9. In the Select the Switch MAC Address to replace list, select the MAC address that you want to replace.

   Before proceeding to the next step, ensure that you selected the correct MAC address to be replaced, and that the new base MAC address is correct.

10. Click **Replace Switch MAC**.

    A screen appears confirming the MAC address replacement. The license file is immediately updated, however it is not sent to the nominated License Bank E-mail address.

    If the MAC replacement limit reaches for the LAC, a message is displayed and the MAC replacement fails. If this occurs, you need to repeat this procedure with a different LAC entry in the License Bank. If there are no other LAC entries in the License Bank, contact Avaya Technical Support.

11. Click **Return to License Bank Details**.

12. Locate the transaction with the license file that is updated with the new MAC address, and then click **Download**.

    A File Download window appears.

13. When prompted, click **Save**.

You can save the license file on the PC being used to access the license portal. After downloading the license file, you need to install it on the new switch.

Chapter 11: NTP fundamentals

This chapter provides conceptual material on the Network Time Protocol (NTP). Review this content before you make changes to the NTP configuration

Overview

The Network Time Protocol (NTP) synchronizes the internal clocks of various network devices across large, diverse networks to universal standard time. NTP runs over the User Datagram Protocol (UDP), which in turn runs over IP. The NTP specification is documented in Request For Comments (RFC) 1305.

Every network device relies on an internal system clock to maintain accurate time. On local devices, the internal system clock is usually set by eye or by wristwatch to within a minute or two of the actual time and is rarely reset at regular intervals. Many local clocks are battery-backed devices that use room temperature clock oscillators that can drift as much as several seconds each day. NTP solves this problem by automatically adjusting the time of the devices so that they are synchronized within a millisecond (ms) on LANs and up to a few tens of milliseconds on WANs relative to Coordinated Universal Time (UTC).

The current implementation of NTP supports only unicast client mode. In this mode, the NTP client, which is tailored to the limitations of the Real Time Clock (RTC) on the SF/CPU board (Dallas Semiconductors DS1307 series), sends NTP time requests to other remote time servers in an asynchronous fashion. The NTP client collects four samples of time from each remote time server. A clock selection algorithm determines the best server among the selected samples based on stratum, delay, dispersion and the last updated time of the remote server. The RTC is adjusted to the selected sample from the chosen server.

NTP terms

A peer is a device that runs NTP software. However, this implementation of NTP refers to peers as remote time servers that provide time information to other time servers on the network and to the local NTP client. An NTP client refers to the local network device, an Ethernet Routing Switch 8800/8600, that accepts time information from other remote time servers.

NTP system implementation model

NTP is based on a hierarchical model that consists of a local NTP client that runs on the Ethernet Routing Switch 8800/8600 and on remote time servers. The NTP client requests and receives time information from one or more remote time servers. The local NTP client reviews the time information from all available time servers and synchronizes its internal clock to the time server whose time is most accurate. The NTP client does not forward time information to other devices running NTP.

Two types of time servers exist in the NTP model: primary time servers and secondary time servers. A primary time server is directly synchronized to a primary reference source, usually a wire or radio clock that is synchronized to a radio station providing a standard time service. The primary time server is the authoritative time source in the hierarchy, meaning that it is the one true time source to which the other NTP devices in the subnet synchronize their internal clocks.

A secondary time server uses a primary time server or one or more secondary time servers to synchronize its time, forming a synchronization subnet, see Figure 8: NTP time servers forming a synchronization subnet on page 96. A synchronization subnet is a self-organizing, hierarchical master-slave configuration with the primary servers at the root and secondary servers of decreasing accuracy at successive levels.

Figure 8: NTP time servers forming a synchronization subnet on page 96 shows NTP time servers forming a synchronization subnet.

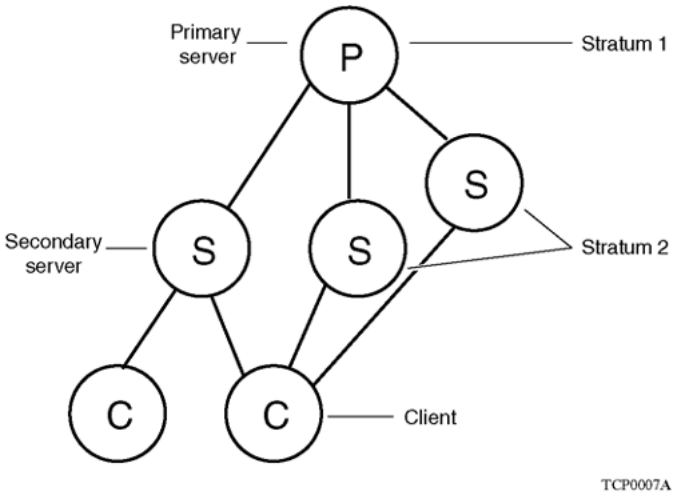


Figure 8: NTP time servers forming a synchronization subnet

In the NTP model, the synchronization subnet automatically reconfigures in a hierarchical primary-secondary (master-slave) configuration to produce accurate and reliable time, even if one or more primary time servers or the path between them fails. This feature applies in a case in which all the primary servers on a partitioned subnet fail, but one or more backup primary servers continue to operate. If all of the primary time servers in the subnet fail, the remaining secondary servers synchronize among themselves.

Time distribution within a subnet

NTP distributes time through a hierarchy of primary and secondary servers, with each server adopting a stratum, see Figure 8: NTP time servers forming a synchronization subnet on page 96. A stratum defines how many NTP hops away a particular secondary time server is from an authoritative time source (primary time server) in the synchronization subnet. A stratum 1 time server is located at the top of the hierarchy and is directly attached to an external time source, typically a wire or radio clock; a stratum 2 time server receives its time through NTP from a stratum 1 time server; a stratum 3 time server receives its time through NTP from a stratum 2 time server, and so forth.

Each NTP client in the synchronization subnet chooses as its time source the server with the lowest stratum number with which it is configured to communicate through NTP. This strategy effectively builds a self-organizing tree of NTP speakers. The number of strata is limited to 15 to avoid long synchronization loops.

NTP avoids synchronizing to a remote time server whose time is inaccurate. NTP never synchronizes to a remote time server that is not itself synchronized. NTP compares the times reported by several remote time servers.

Synchronization

Unlike other time synchronization protocols, NTP does not attempt to synchronize the internal clocks of the remote time servers to each other. Rather, NTP synchronizes the clocks to universal standard time, using the best available time source and transmission paths to that time source.

NTP uses the following criteria to determine the time server whose time is best:

- The time server with the lowest stratum.
- The time server closest in proximity to the primary time server (reduces network delays).
- The time server offering the highest claimed precision.

NTP accesses several (at least three) servers at the lower stratum level because it can apply an agreement algorithm to detect a problem on the time source.

NTP modes of operation

NTP uses unicast client mode to enable time servers and NTP clients to communicate in the synchronization subnet. The Ethernet Routing Switch 8800/8600 supports only unicast client mode.

After you configure a set of remote time servers (peers), NTP creates a list that includes each time server IP address. The NTP client uses this list to determine the remote time servers to query for time information.

After the NTP client queries the remote time servers, the servers respond with various timestamps, along with information about their clocks, such as stratum, precision, and time reference, see Figure 9: NTP time servers operating in unicast client mode on page 98. The NTP client reviews the list of responses from all available servers and chooses one as the best available time source from which to synchronize its internal clock.

Figure 9: NTP time servers operating in unicast client mode on page 98 shows how NTP time servers operate in unicast mode.

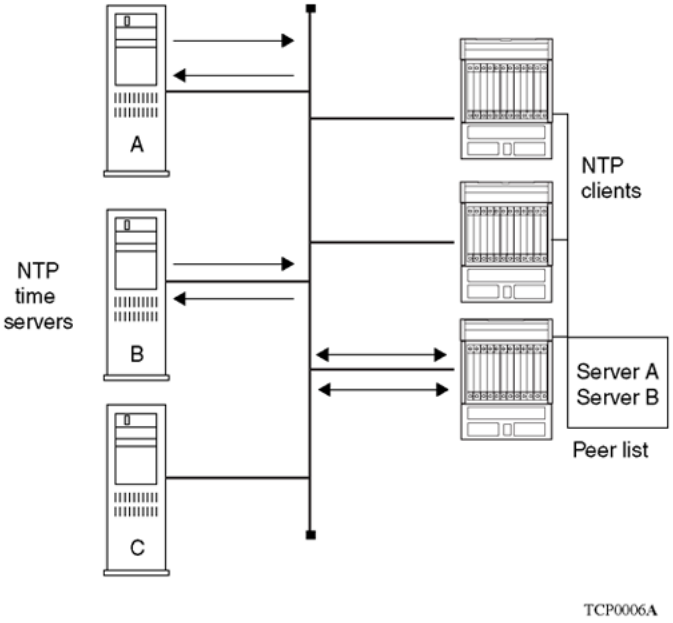


Figure 9: NTP time servers operating in unicast client mode

NTP authentication

You can authenticate time synchronization to ensure that the local time server obtains its time services only from known sources. NTP authentication adds a level of security to your NTP configuration. By default, network time synchronization is not authenticated.

If you select authentication, the Ethernet Routing Switch 8800/8600 uses the Message Digest 5 (MD5) algorithm to produce a message digest of the key. The message digest is created using the key and the message, but the key itself is not sent. The MD5 algorithm verifies the integrity of the communication, authenticates the origin, and checks for timeliness.

To authenticate the message, the client authentication key must match that of the time server. Therefore, the authentication key must be securely distributed in advance (the client administrator must obtain the key from the server administrator and configure it on the client).

While a server can know many keys (identified by many key IDs) it is possible to declare only a subset of these as trusted. The time server uses this feature to share keys with a client that requires authenticated time and that trusts the server, but that is not trusted by the time server.

NTP considerations and limitations

Keep the following information in mind when implementing NTP on the ERS 8800/8600:

- NTP does not support IPv6.
- NTP does not support VRFs; it supports global routers only.
- The NTP `ip-source-type` command is a global command for all associations, not just NTP associations.

Chapter 12: DNS fundamentals

This chapter provides conceptual material on the Domain Name Service (DNS) implementation for the Avaya Ethernet Routing Switch 8800/8600. Review this content before you make changes to the configurable DNS options.

DNS client

Every equipment interface connected to a Transmission Control Protocol over IP (TCP/IP) network is identified with a unique IP address. You can assign a name to every machine that uses an IP address. The TCP/IP does not require the usage of names, but these names make the task easier for network managers in the following ways:

- An IP client can contact a machine with its name, which is converted to an IP address, based on a mapping table. All applications that use this specific machine are not dependent on the addressing scheme.
- It is easier to remember a name than a full IP address.

To establish the mapping between an IP name and an IP address you use the Domain Name Service (DNS). DNS is a hierarchical database that you can distribute on several servers for backup and load sharing. After you add a new hostname, update this database. The information is sent to all the different hosts. An IP client that resolves the mapping between the hostname and the IP address sends a request to one of the database servers to resolve the name.

After you establish the mapping of IP name and IP address, the application is modified to use a hostname instead of an IP address. The switch converts the hostname to an IP address.

If the entry for translating the hostname to IP address is not found in the host file, the switch queries the configured DNS server for the mapping from hostname to IP address. You can configure connections for up to three different DNS servers—primary, secondary and tertiary. First the primary server is queried, and then the secondary, and finally the tertiary.

Ping, Telnet, and copy applications are modified. You can either enter a hostname or an IP address for invoking Ping, Telnet, and copy applications.

The DNS query to remote host is not performed if the application is invoked from the boot monitor. Only the /etc/hosts file lookup is performed for translating the hostname to IP address when invoked from the boot monitor.

In non-HA mode, you can configure a separate DNS server for master and slave SF/CPUs. In HA mode, you can configure a DNS server only from the master SF/CPU.

A log/debug report is generated for all the DNS requests sent to DNS servers and all successful DNS responses received from the DNS servers.

Avaya does not provide a default hosts file on the system. The format is similar to the one used in a Uniplexed Information and Computing Service (UNIX) workstation. Use the editor provided on the system to create, save, or modify such a file.

Chapter 13: Multicast group ID fundamentals

This chapter provides conceptual material on the expansion of the multicast group ID (MGID) for the Ethernet Routing Switch 8800/8600. Review this content before you make changes to the MGID reservation.

Introduction

The MGID is a hardware mechanism the switch uses to send data to several ports simultaneously. Instead of sending the data to a specific port number, the data is directed to an MGID. The switch maintains a table that maps MGIDs to their member ports. Both virtual LAN (VLAN) and IP multicast (IPMC) use MGIDs. The system also reserves a small number of MGIDs.

Generally, each VLAN requires one MGID, though more are required in certain situations, such as if IST is enabled on the system; or in certain chassis modes if the VLAN is associated with an MLT. Several IPMC streams can use a single MGID but performance begins to suffer after more than eight streams use one MGID.

Avaya Ethernet Routing Switch 8800/8600 Release 4.1 provides 2048 MGIDs split between system, VLAN, and IPMC use. Release 4.1 uses a fixed range of 64, from 64 to 127, of those MGIDs for IPMC.

Expansion

Release 7.0 expands the total number of MGIDs to 4096, still split between system, VLAN, and IPMC. MGID expansion provides support for more VLANs and higher performance for IPMC.

MGID expansion provides a maximum VLAN mode. If you configure maximum VLAN mode, every available MGID, except system-used MGIDs, is used for VLANs; no IPMC traffic occurs. The system supports a maximum of 4084 VLANs.

If you do not configure the maximum VLAN mode, you can reserve MGIDs for IPMC. You can reserve between 64 and 4084 MGIDs for IPMC. The default for IPMC is 2048.

MGID expansion requires an 8692 SF/CPU with a SuperMezz or an 8895 SF/CPU. The following figure illustrates MGID allocation in various modes and releases.

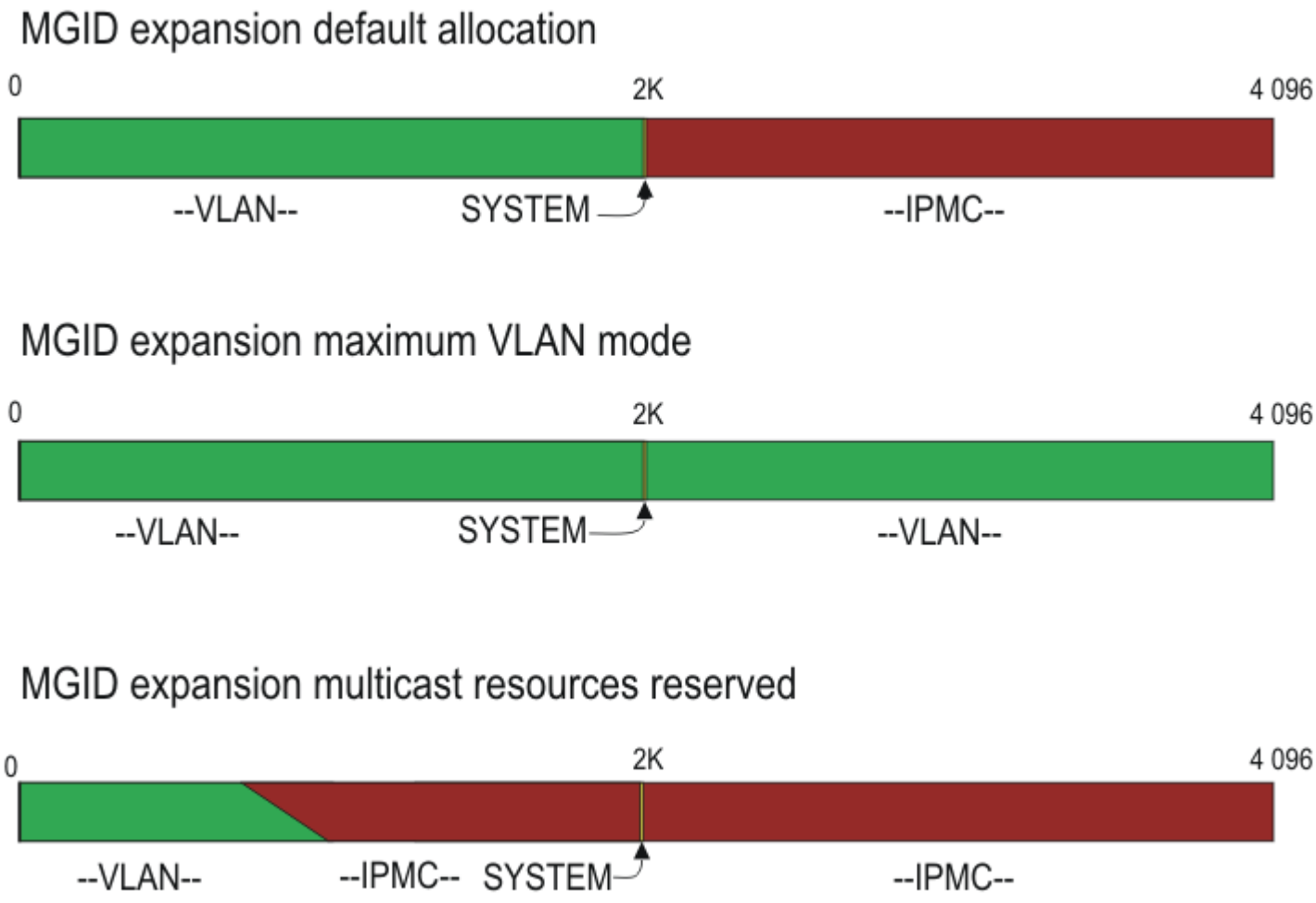


Figure 10: MGID allocation map

SPBM MGID usage

The multicast group ID (MGID) is a hardware mechanism the switch uses to send data to several ports simultaneously. Instead of sending the data to a specific port number, the data is directed to an MGID. The switch maintains a table that maps MGIDs to their member ports. Both virtual LAN (VLAN) and IP multicast (IPMC) use MGIDs. The system also reserves a small number of MGIDs.

SPBM also requires MGIDs for proper operation. When SPBM is enabled on the switch, the system reserves 519 MGIDs for SPBM operation. Therefore, the number of MGIDs on the system available

for VLANs and IP Multicast traffic is reduced by 519. To determine how many MGIDs are available, enter **show sys mgid-usage**.

```
ERS-8606:5# show sys mgid-usage
********************************************************************************
Command Execution Time: WED FEB 02 19:42:27 2011 UTC
********************************************************************************
Number of MGIDs used for VLANs : (3)
Number of MGIDs used for SPBM : (519)
Number of MGIDs used for multicast : (0)
Number of MGIDs remaining for VLANs : (1514)
Number of MGIDs remaining for multicast : (2048)
```

Before you enable SPBM on the switch, be sure that your network will not be adversely affected by this reduction in available MGIDs.

The Ethernet Routing Switch 8800/8600 supports a total of 4096 MGIDs, split between the system, VLAN, IPMC, and now SPBM. You can reserve MGIDs for IP Multicast (IPMC) traffic. You can reserve between 64 and 4084 MGIDs for IPMC. The default for IPMC is 2048. It is the responsibility of the network administrator to fully understand the network deployment strategy. Please ensure that MGIDs are planned appropriately. If assistance is required, please contact your Avaya technical representative.

For information about reserving MGIDs for IPMC, see *Avaya Ethernet Routing Switch 8800/8600 Administration* (NN46205–605).

Chapter 14: Boot parameter configuration using the CLI

Use the procedures in this chapter to configure and manage the boot parameters using the command line interface (CLI).

Prerequisites to boot parameter configuration

- You initiate a boot monitor session only through a direct serial-port connection to the switch. After the boot monitor is active, you can set the flags for Telnet and rlogin to allow remote access, but access to the boot monitor is still only available through a direct serial-port connection. Within the boot monitor, you can change the boot configuration, including boot choices and boot flags.

Job aid

The following table lists the commands and their parameters that you use to complete the procedures in this section.

Table 17: Job aid

Command	Parameter
config cli	defaultlogin <true|false>defaultpassword <true|false> info loginprompt <*string*> more <true|false> passwordprompt <*string*> prompt <*prompt*> rlogin-sessions <*nsessions*> screenlines <*nlines*> telnet-sessions <*nsessions*> timeout <*seconds*>
config bootconfig	info
	delay <*seconds*>
	loadconfigtime <*seconds*>
	logfile <*minsize*> <*maxsize*> <*maxoccupyPercentage*>

Table continues…

Command	Parameter
	master <*cpu-slot*>
	multicast <*value*>
config bootconfig choice <boot-choice>	info
	backup-config-file <*file*>
	config-file <*file*>
	image-file <*file*>
	license-file <*file*>
config bootconfig cli	info
	more <true|false>
	prompt <*value*>
	screenlines <*value*>
	timeout <*seconds*>
config bootconfig delay <seconds>	
config bootconfig flags	info
	alt-led-enable <true|false>
	autoboot <true|false>
	block-snmp <true|false>
	block-warmstandby-switchover <true|false>
	control-record-optimization <true|false>
	daylight-saving-time <true|false>
	debug-config <true|false>
	debugmode <true|false>
	factorydefaults <true|false>
	ftpd <true|false>
	ha-cpu <true|false>
	hsecure <true|false>
	logging <true|false>
	mezz <true|false>
	acli<true|false>
	reboot <true|false>
	rlogind <true|false>
	savetostandby <true|false>
	spanning-tree-mode <mstp|rstp|default>
	sshd <true|false>
	telnetd <true|false>

Table continues…

Command	Parameter
	tftpd <true|false>
	trace-logging <true|false>
	verify-config <true|false>
	wdt <true|false>
	cf-pc-compat <true|false>
config bootconfig host	info
	password <*value*>
	password <*value*>
	tftp-debug <true|false>
	tftp-hash <true|false>
	tftp-rexmit <*seconds*>
	tftp-timeout <*seconds*>
	user <*value*>
config bootconfig master <cpu-slot>	info
config bootconfig net <mgmt|cpu2cpu|pccard>	autonegotiate <true|false>
	bootp <true|false>
	chk-src-route <true|false>
	enable <true|false>
	fullduplex <true|false>
	ip <*ipaddr/mask*> [cpu-slot <*value*>]
	restart
	route [add|del] <*netaddr*> <*gateway*>
	speed <10|100>
	tftp <*ipaddr*>
	info
config bootconfig parity-errors	disable enable set <size> action-869xSF-disable <true|false> info
config bootconfig sio <cpu-sio-port>	8databits <true|false>
	baud <*rate*>
	enable <true|false>
	mode <ascii|slip|ppp>
	mtu <*bytes*>

Table continues…

Command	Parameter
	my-ip <*ipaddr*>
	peer-ip <*ipaddr*>
	pppfile <*file*>
	restart
	slip-compression <true|false>
	slip-rx-compression <true|false>
	info
config bootconfig slot <slots>	core-save <enable|disable> [<file>] info start-core
config bootconfig tz	dst-end <*Mm.n.d/hhmm|MMddhhmm*>
	dst-name <*dstname*>
	dst-offset <*minutes*>
	dst-start <*Mm.n.d/hhmm|MMddhhmm*>
	name <*tz*>
	offset-from-utc <*minutes*>
show bootconfig and config bootconfig show	choice
	cli
	config [verbose]
	flags
	host
	master
	mezz-image
	net
	show-all [file <*value*>]
	sio
	tz
	bootp
show bootconfig master	

Accessing the boot monitor

Access the boot monitor to configure and manage the boot process by performing this procedure.

Procedure steps

1. Restart the switch.
2. Interrupt the boot sequence by pressing the Enter key after the following prompt is displayed:

```
Press Enter to stop autoboot.
```

Configuring the boot monitor

Configure the boot monitor to configure connection settings for CLI sessions. Use the bootconfig command to configure the general boot monitor operations. The bootconfig command also provides several subcommands that are used in the procedures in this section.

Configure the boot monitor by performing this procedure.

Procedure steps

1. Configure the boot monitor connection settings by using the following command:

   ```
   config cli
   ```

2. Save the changed configuration file.
3. Configure the boot monitor operations by using the following command:

   ```
   config bootconfig
   ```

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

Variable definitions

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

Variable	Value
defaultlogin <true|false>	Specifies the current settings for the login prompt as true or false. The default value is true.
defaultpassword <true|false>	Specifies the current settings for the password prompt as true or false.

Table continues…

Variable	Value
	The default is true.
info	Specifies the current settings for the boot monitor CLI.
loginprompt<*string*>	Specifies the login prompt for the boot monitor as a string of 1–1513 characters.
more <true|false>	Configures scrolling for the output display. The default value is true. • true —configures output display scrolling to one page at a time. • false —configures the output display to continuous scrolling.
passwordprompt<*string*>	Specifies the password prompt for the boot monitor as a string of 1–1510 characters.
prompt <*prompt*>	Changes the boot monitor prompt to the defined string. • *prompt* is a string of 0–255 characters. The default prompt depends on the switch; for example, ERS-8606.
rlogin-sessions <*nsessions*>	Configures the allowable number of inbound remote boot monitor CLI logon sessions. • *nsessions* is the number of sessions from 0–8. The default value is 8.
screenlines <*nlines*>	Configures the number of lines in the output display. • *nlines* is the number of lines from 8–64. The default value is 23.
telnet-sessions <*nsessions*>	Configures the allowable number of inbound Telnet sessions. • *nsessions* is the number of sessions from 0–8. The default value is 8.
timeout <*seconds*>	Configures the idle timeout period before automatic logoff for CLI sessions. • *seconds* is the timeout period in seconds from 30–65535. The default is 900.

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

Variable	Value
delay <*seconds*>	Configures the number of seconds a standby SF/CPU waits (delays) before trying to become the master SF/CPU. This command applies only during a cold start and does not apply to a failover start. The default is 45 seconds delay.
info	Specifies the configured values.
loadconfigtime <*seconds*>	Configures the time-out value, in seconds, for loading a configuration file. *seconds* is a value from 0–300. The default is 60 seconds.
logfile <*minsize*> <*maxsize*> <*maxoccupyPercentage*>	Configures the parameters for the log file. • *minsize* is the minimum size of the log file from 64–500 kilobytes (KB). The default value is 100. • *maxsize* is the maximum size of the log file from 500–16384 KB. The default value is 1024. • *maxoccupyPercentage* is the percentage of free Personal Computer Memory Card International Association (PCMCIA) to use for a log file from 10–90. The default value is 90.
master <*cpu-slot*>	Indicates which SF/CPU becomes the master after the switch powers up. The master SF/CPU performs a loopback test to test the switch fabric. The default master is set for slot 5. • *cpu-slot* is the module position, either slot 5 or slot 6.
multicast <*value*>	Configures the system multicast scaling parameter from 0–2147483647. The default value is 0.

Modifying the boot sequence

Modify the boot sequence to prevent the switch from using the factory default settings or, conversely, to prevent loading a saved configuration file by performing this procedure.

Procedure steps

1. Bypass the loading of the switch configuration with the following command:

   ```
   flags factorydefault true
   ```

Important:

If the switch fails to read and load a saved configuration file after it starts, ensure this flag is set to *false* before investigating other options.

Enabling or disabling remote access services

Enable the remote access service to provide multiple methods of remote access by performing this procedure.

Prerequisites

- If you enable an rlogin flag, you must configure an access policy and specify the name of the user who can access the switch.

Procedure steps

1. While the switch is starting, press any key to interrupt the autoboot process.
2. Enable or disable the access service by using the following command:

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

3. 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. Enter one of the following: ftpd, rlogind, telnetd, tftpd, or sshd.
true|false	Specifies true to activate the service; false to disable the service.

Accessing the boot monitor CLI

Access the boot monitor CLI from the run-time CLI to configure and manage the boot process by performing this procedure.

Procedure steps

1. Configure the bootconfig autoboot flag by using the following command:

   ```
   config bootconfig flags autoboot false
   ```

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

   ```
   save bootconfig
   ```

3. Restart the switch.

Modifying the boot monitor CLI operation

Modify the boot monitor CLI operation to change the connection settings by performing this procedure.

Procedure steps

1. Modify the boot monitor CLI by using the following command:

   ```
   config bootconfig cli
   ```

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 cli` command.

Variable	Value
info	Specifies the current settings for the boot monitor CLI.
more <true|false>	Configures scrolling for the output display. The default value is true. • true configures output display scrolling to one page at a time. • false configures the output display to continuous scrolling.
prompt <*value*>	Changes the boot monitor prompt to the defined string. • *value* is a string from 1–32 characters.

Table continues…

Variable	Value
screenlines <*value*>	Configures the number of lines in the output display. The default is 23. • *value* is the number of lines from 8–64.
timeout <*seconds*>	Configures the idle timeout period before automatic logout for CLI sessions. The default value is 900. • *seconds* is the timeout period in seconds from 30–65535.

Modifying the boot sequence from the run-time CLI

Modify the boot sequence to prevent the switch from using the factory default settings or, conversely, to prevent loading a saved configuration file by performing this procedure.

Procedure steps

1. Bypass loading a saved configuration file with the following command:

   ```
   config bootconfig flags factorydefault true
   ```

   Important:

   If the switch fails to read and load a saved configuration file after it starts, ensure this flag is set to *false* before investigating other options.
2. Save the changed configuration to the boot.cfg and pcmboot.cfg files.
3. Restart the switch.

Changing the boot source order

Change the boot source order to display or change the order in which the boot sources (flash and Personal Computer Memory Card International Association, or PCMCIA, card) are accessed by performing this procedure.

Procedure steps

1. Change the boot order by using the following command:

   ```
   config bootconfig choice <boot-choice>
   ```
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 choice` command.

Variable	Value
backup-config-file <*file*>	Identifies the backup boot configuration file. • *file* is the device and file name, up to 256 characters including the path.
boot-choice	Lists the order in which the specified boot devices are accessed after you restart the switch. The options for boot-choice are primary, secondary, or tertiary. The primary source for files is the PCMCIA card, the secondary source is the onboard flash memory, and the tertiary source is the network server. The default order is to access the device specified in this command first, and then to access the onboard flash.
config-file <*file*>	Identifies the boot configuration file. • *file* is the device and file name, up to 255 characters including the path.
license-file <file>	Identifies the license file. • *file* is the device and file name, up to 256 characters including the path.
image-file <*file*>	Identifies the image file. • *file* is the device and file name, up to 255 characters including the path.
info	Specifies the current boot choices and associated files.

Example of changing the boot source order

1. Specify the configuration file in flash memory as the primary boot source:

   ```
   config bootconfig choice primary config-file /flash/config.cfg
   ```

Shutting down external compact flash cards

Use this shutdown procedure to avoid corrupting an external compact flash card by ensuring that the card is synchronized before it is safely removed. If you do not shutdown the system first, some situations such as power cycling and hard resets might cause flash corruption. There is no risk of flash corruption if you run the **`sys-shutdown`** command prior to a power cycle or hard reset.

System crashes might also corrupt flash cards so be sure to back up all configurations.

The command is called **sys-shutdown** in the CLI and **sys shutdown** in the ACLI. EDM does not support this command. In the CLI, the command is at the top level; in the ACLI, the command is in the EXEC Mode.

Procedure steps

1. Stop the compact flash card before you remove it by using the following command:

   ```
   dos-stop /pcmcia (on 8692 and 8895 SF/CPU)
   ```

   For backward compatibility, the **pcmcia-stop** command is still available with the 8692 SF/CPU. However, Avaya recommends using the **dos-stop /pcmcia**.

2. Dismount both internal and external file systems by shutting down the CPU.

   ```
   sys-shutdown
   ```

   The following message appears on the serial console:

   ```
   It is now safe to reset, remove, or power off this CP.
   ```

3. If you suspect that a card is corrupted, enter the following command to check and optionally try to repair the file system:

   ```
   dos-chkdsk <device> [repair]
   ```

4. If you cannot repair the file system, reformat the device.

   ```
   dos-format <device>
   ```

Configuring the standby-to-master delay

Configure the standby-to-master delay to set the number of seconds a standby SF/CPU waits before trying to become the master SF/CPU. The time delay you configure applies during a cold start; it does not apply to a failover start.

Configure the standby-to-master delay by performing this procedure.

Procedure steps

1. Configure the number of seconds by using the following command:

   ```
   config bootconfig delay <seconds>
   ```

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

Configuring system flags

Set the system flags to enable or disable flags for specific configuration settings by performing this procedure.

Important:

If you activate *auto-trace*, SF/CPU utilization increases by up to 30 percent.

Important:

After you change certain configuration parameters using the **`config bootconfig flags`** or the **`conf sys set flags`** command, you must save the changes to the configuration file and restart the switch before the changes take effect. For more information about which parameters require a switch reset, see the value descriptions in System flags on page 39.

Prerequisites

- After you enable the hsecure flag, you cannot enable the flags for the Web server or SSH password-authentication.

Procedure steps

1. Configure system flags by using the following command:

   ```
   config bootconfig flags
   ```

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 flags` command.

Variable	Value
alt-led-enable <true|false>	Activates or disables the alternate LED behavior. The default value is false (off). If you change this parameter, you must reset the switch. **Important:** Do not change this parameter unless directed by Avaya.
autoboot <true|false>	Enables or disables use of the automatic run-time image. • true—the switch automatically runs the run-time image after reset

Table continues…

Variable	Value
	• false—the boot process stops at the boot monitor prompt The default value is true. If you change this parameter, you must reset the switch. You can set autoboot <false> to facilitate debug tasks.
block-snmp <true|false>	Enables or disables Simple Network Management Protocol (SNMP) access. • true—disables SNMP access • false—enables SNMP access The default is value is false.
block-warmstandby-switchover <true|false>	Enables or disables use of the warm standby secondary SF/CPU as the primary SF/CPU if the primary SF/CPU is reset. • true—the system prevents the secondary SF/CPU in warm standby mode from becoming the primary SF/CPU if the primary SF/CPU is reset. • false—designates the secondary SF/CPU in warm standby mode as the primary SF/CPU if the primary SF/CPU is reset The default value is false. If you change the block-warmstandby-switchover variable, you must reset the switch.
control-record-optimization <true|false>	Enables or disables optimization of control records. The default setting is false (disabled). That is, the switch creates hardware records to route Layer 3 protocol destination multicast addresses even if the corresponding protocol is disabled. **Important:** This parameter must always be set to false (disabled).
daylight-saving-time <true|false>	Activates or disables Daylight Saving Time (DST) for the switch. The default value is false (disabled). If you set the daylight-saving-time variable to true (enabled), you must set the DST settings using the config bootconfig tz command.
debug-config <true|false>	Activates or disables run-time debugging of the configuration file. • true—the system displays the line by line configuration file processing on the console during SF/CPU initializing • false—disables run-time configuration file debug The default value for the debug-config variable is false. If you change the debug-config variable, you must reset the switch.

Table continues…

Variable	Value
debugmode <true|false>	Controls whether the switch stops in debug mode following a fatal error. Debug mode provides information equivalent to the trace commands. • true—the switch does not restart following a fatal error. • false—the switch automatically restarts following a fatal error. The default value is false. If you change this parameter, you must reset the switch. **Important:** Do not change this parameter unless directed by Avaya.
factorydefaults <true|false>	Specifies whether the switch uses the factory defaults at startup. The default value is false. • true—the switch uses the factory default configuration at startup • false—the switch uses the current configuration at startup If you change the factorydefaults variable, you must reset the switch. The system automatically resets the value to the default setting after the CPU restarts.
ftpd <true|false>	Activates or disables FTP service on the switch. The default value is false. To enable FTP, you must set the config bootconfig flags tftpd command variable to false.
ha-cpu <true|false>	Activates or disables High Availability (HA) mode. Switches with two SF/CPUs use HA mode to recover quickly if one SF/CPU fails. The default value is false. After you enable High Availability mode, the secondary SF/CPU resets to load settings from the saved boot configuration file. You must reset the primary SF/CPU after the secondary SF/CPU starting is complete. **Caution:** **Risk of service loss** Enabling HA mode can disable certain features. For more information about the HA supported features, see Table 5: Feature support for HA in specified software release versions on page 48.
hsecure <true|false>	Activates or disables High Secure mode in the switch. If you enable hsecure, the following password behaviors are available: • 10 characters enforcement

Table continues…

Variable	Value
	• aging time • limitation of failed login attempts • a protection mechanism to filter certain IP addresses After you enable High Secure mode, you must reset the switch to enforce secure passwords. In High Secure mode, a user with an invalid-length password is prompted to change their password. The default value is false.
logging <true|false>	If a PCMCIA is present, the logging command activates or disables system logging to a file on the PCMCIA. The default value is true. The system generates the log file name based on an 8.3 (xxxxxxxx.sss) format as described in the following list. • The first 6 characters of the file name contain the last three bytes of the chassis base MAC address. • The next two characters of the file name specify the slot number of the CPU that generated the logs. • The last three characters of the file name denote the sequence number of the log file. Under the following conditions, the system generates multiple sequence numbers for the same chassis and slot: • You replace or reinsert the CPU. • The log file reaches the maximum size.
mezz <true|false>	Permits or prevents the mezzanine card from starting when it is present on a SF/CPU card. On a dual CPU chassis the SuperMezz configuration must be identical on both CPUs: either both CPUs have a SuperMezz or both CPUs do not have a SuperMezz. The default value is true. If you change this value, you must reset the switch. Before you reset the switch with the mezz parameter enabled, you must ensure that the SuperMezz image resides on the switch.
acli <true|false>	Configures the switch to use ACLI or CLI mode. If you change the acli variable, you must restart the system. The default value is false.
reboot <true|false>	Activates or disables automatic reboot on a fatal error. The default value is true. If you change this parameter, you must reset the switch. The reboot command is equivalent to the debugmode command.

Table continues…

Variable	Value
	Important: Do not change this parameter unless directed by Avaya.
rlogind <true|false>	Activates or disables the rlogin and rsh server. The default value is false.
savetostandby <true|false>	Activates or disables the ability to save the configuration or boot configuration file automatically to the standby SF/CPU. The default value is true. If you have a dual SF/CPU system, for ease of operation Avaya recommends that you set the savetostandby variable to true.
spanning-tree-mode <mstp|rstp|default>	Selects the Multiple Spanning Tree Protocol (MSTP), Rapid Spanning Tree Protocol (RSTP), or default (legacy) spanning tree modes. If you do not specify a protocol, the switch uses the default spanning tree mode. If you change this parameter, you must save the current configuration and reset the switch. The default value is rstp.
sshd <true|false>	Activates or disables the SSH server service. The default value is true.
telnetd <true|false>	Activates or disables the Telnet server service. The default value is true. In a dual SF/CPU system, if you disable the Telnet server you prevent a Telnet connection from the other SF/CPU.
tftpd <true|false>	Activates or disables Trivial File Transfer Protocol (TFTP) server service. The default value is true. Even if you disable the TFTP server, you can copy files between the SF/CPUs.
trace-logging <true|false>	Activates or disables the creation of trace logs. The default value is false. **Important:** Do not change this parameter unless directed by Avaya.
verify-config <true|false>	Activates syntax checking of the configuration file. The default value is false. • true—when the system detects a syntax error, the system loads the factory default configuration • false—the system logs syntax errors and the SF/CPU continues to source the configuration file Avaya recommends that you use the default variable (false). If you change the verify-config variable, you must reset the switch.

Table continues…

Variable	Value
wdt <true|false>	Activates or disables the hardware watchdog timer that monitors a hardware circuit. Based on software errors, the watchdog timer restarts the switch. The default value for the wdt variable is true. • true—activates a hardware circuit watchdog timer • false—disables a hardware circuit watchdog timer If you change the wdt variable, you must reset the switch. **Important:** Do not change this parameter unless directed by Avaya.
cf-pc-compat <true|false>	Enables the compact flash interface to be formatted in either the Windows PC compatible format or its original format. • true—formats the compact flash interface in Windows PC compatible format. • false—ensures backward compatibility with the original format. The default value is false. If you change this parameter, you must reset the switch.

Configuring the remote host logon

Configure the remote host logon to modify parameters for FTP and TFTP access. The defaults allow TFTP transfers. If you want to use FTP as the transfer mechanism, you need to change the password to a non-null value.

Configure the remote host logon by performing this procedure

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>	Activates or disables debug mode on FTP. If you enable debug mode, debug messages display on the management console screen. The default value is false.
info	Specifies 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 this password is configured, only FTP is used for remote host logon. **Important:** This password must match the password set for the FTP server, or the FTP operation fails. Also, if the password is set to a nonnull value, all copying to and from the network uses FTP instead of TFTP. If the username or password is incorrect, copying over the network fails.
tftp-debug <true|false>	Activates or disables debug mode on TFTP/TFTPD. If you enable debug mode, debug messages display on the management console screen. The default value is false.
tftp-hash <true|false>	Activates or disables the TFTP hash bucket display. The default value is false.
tftp-rexmit <*seconds*>	Configures the TFTP retransmission timeout. The default value is 6 seconds. • *seconds* is the number of seconds from1–120.
tftp-timeout <*seconds*>	Configures the TFTP timeout value. The default value is 6 seconds. • *seconds* is the number of seconds from 1–120.
user <*value*>	Configures the remote user logon. • *value* is the user logon name, up to 16 characters long.

Specifying the master SF/CPU

Specify the master SF/CPU to determine which SF/CPU becomes the master after the switch performs a full power cycle. Specify the master SF/CPU by performing this procedure.

Procedure steps

1. View the current configuration for the master SF/CPU by using the following command:

   ```
   show bootconfig master
   ```

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

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

3. Save the changed 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, either 5 or 6, for the master SF/CPU. The default is slot 5.

Configuring SF/CPU network port devices

Configure the network port devices to define connection settings for the port. The three network ports are:

- management port (mgmt)
- SF/CPU port (cpu2cpu)
- PCMCIA card (pccard)

Configure the SF/CPU network port devices by performing this procedure.

Procedure steps

1. Configure the network port by using the following command:

   ```
   config bootconfig net <mgmt|cpu2cpu|pccard>
   ```

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

Variable definitions

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

Variable	Value
autonegotiate <true|false>	Activates or disables autonegotiation for the port. The default autonegotiation port values are as follows: • management port is true • SF/CPU port is false

Table continues…

Variable	Value
	• PCMCIA card is true
bootp <true|false>	Activates or disables the Bootstrap Protocol (BootP) for the port. The default bootp port values are as follows: • management port is true • SF/CPU port is true • PCMCIA card is true
chk-src-route <true|false>	Blocks traffic with no route back to source. The chk-src-route default port values are as follows: • management port is true • SF/CPU port is false • PCMCIA card is true
enable <true|false>	Activates or disables the specified port. The default enable port values are as follows: • management port is true • SF/CPU port is true • PCMCIA card is true
fullduplex <true|false>	Activates or disables full-duplex mode on the specified port. The default fullduplex port values are as follows: • management port is false • SF/CPU port is true • PCMCIA card is false
info	Specifies information about the current configuration of the specified port.
ip <*ipaddr/mask*> [cpu-slot <*value*>]	Assigns an IP address and mask for: • the management port • SF/CPU • PCMCIA Optional parameter: • cpu-slot *value* specifies the slot number to which the IP address applies. The valid options are 3, 5, or 6. If you do not specify a slot, the system assigns the IP address to the port in the currently active SF/CPU. **Important:** You cannot assign an address of 0.0.0.0/0.

Table continues…

Variable	Value
restart	Shuts down and re-initializes the port.
route [add|del] *<netaddr/subnet mask> <gateway>*	Configures a route for the port. • add adds a route. del deletes a route. • *netaddr* is the IP address of the network to be reached. • *gateway* is the gateway IP address.
speed <10|100>	Configures the connection speed for ports to 10 Mb/s, 100 Mb/s, or 1000 Mb/s. The default value for management port is 10Mb/s. The default value for SF/CPU port is 100Mb/s. The default value for PCMCIA card is 10Mb/s.
tftp *<ipaddr>*	Specifies a TFTP server for the port. • *ipaddr* is the IP address of the TFTP server. The default value is 0.0.0.0.

Checking the link state of the port

Check the link state of the management port of the CPU to ensure the standby CPU is properly connected.

Procedure steps

1. Check the link state of the management port by using the following command:

   ```
   config bootconfig net mgmt info
   ```

Job aid

See the following sample output for checking the link state of a management port.

Note:

To maintain backward-compatibility with pre-5.0 releases, if the management IP address network mask is equal to the natural network mask, then the mask is not displayed in response to the **`config bootconfig net mgmt info`**command. If the configured network mask is not equal, it will be shown. This is the correct behavior.

```
ERS-8606:5# config bootconfig net mgmt info
net mgmt autonegotiate false
net mgmt bootp true
net mgmt chk-src-route true
net mgmt enable true
net mgmt fullduplex false
net mgmt speed 100
net mgmt tftp 0.0.0.0
net mgmt ip 172.16.120.5/255.255.255.0 cpu-slot 5
net mgmt ip 192.168.168.169/255.255.255.0 cpu-slot 6
net mgmt route add 207.0.0.0/255.0.0.0 172.16.120.1
net mgmt route add 192.0.0.0/255.0.0.0 172.16.120.1
net mgmt route add 142.0.0.0/255.0.0.0 172.16.120.1
net mgmt route add 172.0.0.0/255.0.0.0 172.16.120.1
Current status: link: true speed: 100 duplex: half
ERS-8606:5# _
```

Figure 11: Checking the link state of a management port

Configuring SF/CPU serial port devices

Configure the serial port devices to define connection settings for serial ports such as the modem and console port or to disable the port. If you use American Standard Code for Information Interchange (ASCII) mode, configure the port if you need to use nondefault settings.

If you configure the mode for the modem port as either Serial Line IP (SLIP) or Point-to-Point Protocol (PPP), you must configure additional parameters.

Caution:

Risk of service interruption

Avaya recommends that you not configure the console port mode to SLIP or PPP. The switch can display log, trace, and error messages on the console port and these messages interfere with the SLIP or PPP operation.

Configure the SF/CPU serial port devices by performing this procedure.

Prerequisites

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

Procedure steps

1. Optionally, change the default generic port settings by using the following command:

   ```
   config bootconfig sio <console|modem|pccard> [8databits <true|
   false]> [baud <rate>] [mode <ascii|slip|ppp>]
   ```

2. If you use PPP mode, configure PPP options by using the following command:

   ```
   config bootconfig sio <console|modem|pccard> [mtu <bytes>] [my-ip
   <ipaddr>] [peer-ip <ipaddr>] pppfile <file>
   ```

3. If you use SLIP mode, optionally change the default SLIP settings by using the following command:

   ```
   config bootconfig sio <console|modem|pccard> [slip-compression
   <true|false>] [slip-rx-compression <true|false>]
   ```

4. Restart the port by using the following command:

   ```
   config bootconfig sio <console|modem|pccard> restart
   ```

5. Disable the port by using the following command:

   ```
   config bootconfig sio <console|modem|pccard> enable false
   ```

6. Save the changed configuration to the boot.cfg and pcmboot.cfg files.
7. 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 the software to interpret. The default value is 7 (false).
baud *<rate>*	Configures the baud rate for the port. The default value is 9600.
enable <true|false>	Activates or disables the port. The default value is true.
info	Specifies information about the specified port.
mode <ascii|slip|ppp>	Configures the communication mode for the serial port. The default communication mode is ASCII. If you are configuring the modem port, you can set the port to use either the SLIP or PPP communication mode.
mtu *<bytes>*	Configures the size of the maximum transmission unit for a PPP link from 0–2048. The default value is 0.
my-ip *<ipaddr>*	Configures the IP address for the server side, the Ethernet Routing Switch 8800/8600, of the point-to-point link. The default is value 0.0.0.0. Avaya recommends that you use the IP address for the management port.
peer-ip *<ipaddr>*	Configures the peer, the PC, IP address on the point-to-point link. The default value is 0.0.0.0. The switch assigns this value to a 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 Ethernet Routing Switch 8800/8600 accepts this address. If you use

Table continues…

Variable	Value
	the Password Authentication Protocol (PAP) authentication, you must ensure that the client uses the correct IP address.
pppfile <*file*>	Specifies the PPP configuration file to provide details for authentication, and other options, to include during the start procedure of the switch. If you set the port mode to PPP, you must specify a PPP file name. For more information about this file, see Job aid on page 129. 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>. **Important:** Do not specify a PPP file name with more than 64 characters.
restart	Shuts down and initializes the port.
slip-compression <true|false>	Activates or disables Transmission Control Protocol over IP (TCP/IP) header compression for SLIP mode. The default value is false.
slip-rx-compression <true|false>	Activates or disables TCP/IP header compression on the receive packet for SLIP mode. The default value 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 recognized options.

Table 18: Job aid

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 configuration 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

Table continues…

Option	Description
	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.
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.

Table continues…

Option	Description
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 configuration 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.
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.

Table continues…

Option	Description
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 19: Sample PPP file on page 132 shows example contents from a PPP file.

Table 19: 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"
```

Detecting a switch fabric failure

Use this feature to set a parity error threshold to determine if there is a switch fabric failure on the CPU. You can configure the sensitivity level of this threshold from most sensitive (8 errors) to least sensitive (50 errors). However, the detection mechanism requires at least one parity error per 500 ms on any I/O module TAP. For example, if you set 8 errors with **`config bootconfig parity-errors set 8`**, that means at least one error must be detected per 500ms in an interval of 4 seconds. When the number of parity errors exceeds this threshold, the switch fabric is considered failed.

For more information about this feature and its limitations, see Switch fabric failure detection on page 67.

Procedure steps

1. Enable the Switch Fabric Failure Detection feature by using the following command:

   ```
   config bootconfig parity-errors enable
   ```

2. Configure the threshold sensitivity level with the set value.

   ```
   config bootconfig parity-errors set <size>
   ```

3. Configure the switch fabric to recover, if possible.

   ```
   config bootconfig parity-errors action—869xSF—disable <true|false>
   ```

Variable definitions

Use the data in the following table to use the `config bootconfig parity-errors` command.

Variable	Value
disable	Disables parity error monitoring.
enable	Enables parity error monitoring for the switch fabric failure detection feature.
set <size>	Specifies the parity error threshold. When the number of parity errors exceeds this threshold per 500 ms in a 4 second interval, it reboots the CPU if **`action-869xSF-disable`** is set to true. The range is from 8 to 50.
action-869xSF-disable <true|false>	When set to true, this action reboots the CPU into boot-monitor mode when excess parity errors are detected. The default is false.
info	Displays the current parity error settings.

Configuring the time zone

Set the time zone to specify the time for your location and configure the settings for daylight saving by performing this procedure.

The format for the time zone command is derived with observation as hours:minutes when compared to minutes only in other Ethernet Routing Switches series for both DST offset and offset from GMT. The input value is positive for the west side of GMT as opposed to negative in every other commercial product.

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.

Variable	Value
dst-end <*Mm.n.d/hhmm*|*MMddhhmm*>	Configures the ending date of daylight saving time. You can specify the time in one of the following 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. **Important:** When you modify the DST end value, the configuration does not take effect until the next DST start is reached. If the DST start is already past when the you configure the DST end, the switch waits until the following year to use the new DST end date. In addition, for a valid configuration, the period between the DST start and the DST end must be greater than the configured offset time.
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 hours:minutes. The values range from -4:0 to 4:0 for hours:minutes and from -240 to 240 for minutes. The default value is 60.
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.

Table continues…

Variable	Value
info	Specifies 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 hours:minutes, to subtract from Universal Coordinated Time (UTC), where positive numbers mean west of Greenwich and negative numbers mean east of Greenwich. The values range from -14:0 to 14:0 for hours:minutes and from -840 to 840 for minutes. The default value is 0.

Enabling remote access services from the run-time CLI

Enable the remote access service to provide multiple methods of remote access by performing this procedure.

Prerequisites

- If you enable an rlogin flag, you must configure an access policy and specify the name of the user who can access the switch.

Procedure steps

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

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

2. Save the configuration.

Variable definitions

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

Variable	Value
access-service	Specify the type of remote access service. Enter one of the following: ftpd, rlogind, telnetd, tftpd, or sshd.
true|false	Enables or disables a remote access service. • true—activates a service • false—disables a service

Displaying the boot monitor configuration

Display the configuration to view current or changed settings for the boot monitor and boot monitor CLI by performing this procedure.

Caution:

Risk of equipment failure

Do not edit the boot.cfg file manually because the switch reads this file during the boot process. Errors generated while editing the file can render the switch inoperable.

Procedure steps

1. View the configuration using one of the following commands:

   ```
   show bootconfig
   ```

   or

   ```
   config bootconfig show
   ```

Variable definitions

Use the data in the following table to use the `show bootconfig` and `config bootconfig show` commands.

Variable	Value
choice	Specifies the current boot configuration choices.
cli	Specifies the current cli configuration.
config [verbose]	Specifies the current boot configuration. • verbose includes all possible information. If you omit verbose, only the values that were changed from their default settings are displayed.
flags	Specifies the current flag settings.
host	Specifies the current host configuration.
info	Specifies the current settings for the boot monitor.
master	Specifies the current SF/CPU slot set as master and the settings for the delay and multicast command.
mezz-image	Specifies the mezzanine image.
net	Specifies the current configuration of the SF/CPU network ports.

Table continues…

Variable	Value
show-all [file <*value*>]	Specifies all relevant information about boot configuration on the switch. • *value* is the filename to which the output is redirected.
sio	Specifies the current configuration of the SF/CPU serial ports.
slot	Specifies the slot number of the device.
tz	Specifies the current configuration of the switch time zone.
bootp	Specifies the BootP configuration.

Configuring core dumps

Enable or disable core dumps and configure the location where the core dump is saved. By default, core dumps are enabled and the file is saved to external flash card. To enable core dumps with FTP, you must configure the *host user* and *host password* bootconfig parameters.

Important:

If you configure the host user and password to nonnull values, all copying to and from the network (including image downloads) uses FTP instead of TFTP.

Because you can only configure one username and password combination for network copying and core dumps, be sure that the login for the remote system to which you are saving the core dumps is the same login used for the remote systems you are using for file copying.

Procedure steps

1. Configure the core dump by using the following command:

   ```
   config bootconfig slot <slots> core-save {enable|disable} [<file>]
   ```

Variable definitions

Use the data in the following table to use the `config bootconfig slot`<*slots*> command.

Variable	Value
core-save {enable|disable}*[<file>]*	Enables or disables the core image file. The default is enable.
info	Displays the core image file configuration information.
start-core	Saves the core image.

Chapter 15: Run-time process management using the CLI

Configure and manage the run-time process using the run-time command line interface (CLI). Access the run-time CLI after the boot process is complete by entering your username and password at the logon prompt.

Job aid

The following table lists the commands, with their parameters, that you use to complete the procedures in this section.

Table 20: Job aid

Command	Parameter
config cli	info
	defaultlogin <true|false>
	defaultpassword <true|false>
	loginprompt <*string*>
	more <true|false>
	passwordprompt <*string*>
	prompt <*prompt*>
	rlogin-sessions <*nsessions*>
	screenlines <*nlines*>
	telnet-sessions <*nsessions*>
	`timeout <seconds>`
config cli banner	info
	add <*string*>
	defaultbanner <true|false>
	delete
config cli clilog	enable <true|false>

Table continues…

Command	Parameter
	info
	maxfilesize <*integer*>
config cli monitor	info
	duration <*integer*>
	interval <*integer*>
config cli motd	info
	add <*string*>
	displaymotd <true|false>
	delete
config cli password	info
	access-level <*access-level*> <enable|disable>
	aging <*days*>
	min-password-len <*integer*>
	default-lockout-time <*secs*>
	lockout-time <*HostAddress*> <*secs*>
	l1<*username*> *[<password>]*
	l2 <*username*> *[<password>]*
	l3 <*username*> *[<password>]*
	l4oper <*username*>
	l4admin <*username*>
	oper <*username*>
	ro<*username*> *[<password>]*
	rw<*username*> *[<password>]*
	rwa<*username*> *[<password>]*
	password-history <*number*>
config slot <*slot*>	info
	state <*enable*|*disable*|*reset*>
config sys link-flap-detect	info
	auto-port-down <enable|disable>
	frequency <*frequency*>
	interval <*interval*>
	send-trap <enable|disable>
config sys set action	info

Table continues…

Command	Parameter
	cpuswitchover
	resetconsole
	resetcounters
	resetmodem
config sys set	clipId-topology-ip *<id>*
	clock-sync-time *<minutes>*
	contact *<contact>*
	ecn-compatibility <enable|disable>
	ecn-compatibility <enable|disable>
	force-topology-ip-flag <true|false>
	global-filter <enable|disable>
	max-vlan-resource-reservation <enable|disable>
	max-vlan-resource-reservation <enable|disable>
	max-vlan-resource-reservation <enable|disable>
	mgmt-virtual-ip *<ipaddr/mask>*
	mgmt-virtual-ipv6*<ipv6addr|prefix-len>*
	mroute-stream-limit <enable|disable>
	mtu *<bytes>*
	multicast-resource reservaton *<value>*
	name *<prompt>*
	portlock <on|off>
	sendAuthenticationTrap <true|false>
	topology <on|off>
	udp-checksum <enable|disable>
	udpsrc-by-vip <enable|disable>
	vlan-bysrcmac <enable|disable>
config sys set clock-sync-time *<minutes>*	
config sys set mgmt-virtual-ip *<ipaddr/mask>*	
config sys set msg-control	info
	action <suppress-msg | send-trap|both>
	control-interval *<minutes>*
	disable
	enable
	max-msg-num *<number>*

Table continues…

Command	Parameter
config sys set msg-control force-msg	info
	add <*string*>
	del <*string*>

Configuring the date

Configure the calendar time in the form of month, day, year, hour, minute, and second by performing this procedure.

Prerequisites

- You must log on as rwa to use this command.

Procedure steps

1. Configure the date by using the following command:

   ```
   config setdate <MMddyyyyhhmmss>
   ```

Configuring the run-time CLI

Configure the run-time CLI to define generic configuration settings for CLI sessions by performing this procedure.

Procedure steps

1. Configure the run-time CLI options by using the following command:

   ```
   config cli
   ```

Variable definitions

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

Variable	Value
defaultlogin <true|false>	Activates or disables use of the default logon string. • false disables the default logon banner and displays the new banner.
defaultpassword <true|false>	Activates or disables use of the default password string.
info	Specifies the current CLI parameter settings.
loginprompt <*string*>	Changes the CLI logon prompt. • *string* is an American Standard Code for Information Interchange (ASCII) string from 1–1513 characters.
more <true|false>	Configures scrolling for the output display. The default value is true. • true configures output display scrolling to one page at a time. • false configures the output display to continuous scrolling.
passwordprompt <*string*>	Changes the CLI password prompt. • *string* is an ASCII string from 1–1510 characters.
prompt <*prompt*>	Configures the root level prompt and sysName to a defined string. • *prompt* is a string from 0–255 characters.
rlogin-sessions <*nsessions*>	Configures the allowable number of inbound remote CLI logon sessions. The default value is 8. • *nsessions* is the number of sessions from 0–8.
screenlines <*nlines*>	Configures the number of lines in the output display. The default value is 23. • *nlines* is the number of lines from 8–64.
telnet-sessions <*nsessions*>	Configures the allowable number of inbound Telnet sessions. The default value is 8. • *nsessions* is the number of sessions from 0–8.
timeout <*seconds*>	Configures the idle timeout period before the system terminates CLI sessions. The default value is 900. • *seconds* is the timeout period, in seconds, from 30–65535.

Configuring the CLI logon banner

Configure the CLI logon banner to display a warning message to users before authentication by performing this procedure.

Procedure steps

1. Configure the CLI banner by using the following command:

   ```
   config cli banner add <string>
   ```

Variable definitions

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

Variable	Value
add <*string*>	Adds lines of text to the CLI logon banner. • *string* is an ASCII string from 1–80 characters.
defaultbanner <true|false>	Activates or disables using the default CLI logon banner.
delete	Deletes an existing customized logon banner.
info	Specifies the text added to the logon banner using the config cli add command.

Configuring the message-of-the-day

Configure a system login message-of-the-day in the form of a text banner that is displayed upon each successful logon by performing this procedure.

Procedure steps

1. Configure the message-of-the-day by using the following command:

   ```
   config cli motd add <string>
   ```

Variable definitions

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

Variable	Value
add <*string*>	Creates a message of the day to display with the logon banner. • *string* is an ASCII string from 1–1516 characters.

Table continues…

Variable	Value
delete	Deletes the message of the day.
displaymotd <true|false>	Specifies (true) or does not display (false) the message of the day.
info	Specifies information about the message of the day.

Configuring command logging

Configure logging of CLI commands to the file clilog.txt on the Personal Computer Memory Card International Association (PCMCIA). You can enable command logging to keep track of the commands a user enters during a login session.

Configure logging of CLI commands by performing this procedure.

Procedure steps

1. Configure CLI logging by using the following command:

   ```
   config cli clilog enable {true|false} [maxfilesize <integer>]
   ```

Variable definitions

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

Variable	Value
enable {true|false}	Enables or disables logging of CLI commands. • true—activates logging of CLI commands • false—disables CLI logging
info	Specifies information about the command log.
maxfilesize <*integer*>	Specifies the maximum size of the clilog.txt file, in kilobytes (KB), in a range from 64–256000. The default value is 256 KB.

Configuring individual system-level switch parameters

Configure individual system-level switch parameters to configure global options for the Avaya Ethernet Routing Switch 8800/8600 by performing this procedure.

Procedure steps

1. Configure system-level switch parameters by using the following command:

   ```
   config sys set
   ```

Variable definitions

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

Variable	Value
clipId-topology-ip <*id*>	Set the topology IP address from the available CLIP.
clock-sync-time <*minutes*>	Configures the RTC-to-system clock synchronization time. • *minutes* is 15–3600 minutes. The default value is 60.
contact <*contact*>	Configures the contact information for the switch. • *contact* is an ASCII string from 0–255 characters (for example a phone extension or email address). The default e-mail address is http://support.avaya.com/.
ecn-compatibility <enable|disable>	Activates or disables explicit congestion notification, as defined in Experimental Request For Comments (RFC) 2780. This feature is not currently supported on the Ethernet Routing Switch 8800/8600. The default value is enable.
force-topology-ip-flag <true|false>	Sets the flag to force the topology IP choice.
global-filter <enable|disable>	Activates or disables global filtering on the switch. After you activate this command, you must disable source MAC VLANs—use the config sys set vlan-bysrcmac disable command because you cannot enable global filtering and source MAC-based VLANs at the same time. The default value is enable.
`info`	Specifies current system settings.
location <*location*>	Configures the location information for the switch. • *location* is an ASCII string from 0–255 characters. The default location is 4655, Great America Parkway, Santa Clara, CA 95054.
max-vlan-resource-reservation <*enable*|*disable*>	Activates or disables the max-vlan feature. The default is false (disabled).
mroute-stream-limit <enable|disable>	Activates or disables multicast stream limiting.

Table continues…

Variable	Value
	The default value is disable.
mgmt-virtual-ip <*ipaddr/mask*>	Configures the virtual management port. • *ipaddr*|*mask* is the IP address and mask of the virtual management port. The default value is 0.0.0.0/0.0.0.0.
mgmt-virtual-ipv6 <ipv6addr|prefix-len>	Configures the management of virtual IPv6. • ipv6addr is the IPv6 address in the hexadecimal format. • prefix-len is the prefix length with a string length from 0–46. The default value is 0:0:0:0:0:0:0:0/0
multicast-resource-reservation <value>	Reserves MGIDs for IPMC.
mtu <*bytes*>	Activates Jumbo frame support for the data path. • *bytes* is the Ethernet frame size, either 1522, 1950 (default), or 9600 bytes. Settings of 1950 or 9600 activate Jumbo frame support. Jumbo frame support is activated by default.
name <*prompt*>	Configures the root level prompt name for the switch. • *prompt* is an ASCII string from 0–255 characters (for example, LabSC7 or Closet4).
portlock <on|off>	Turns port locking on or off. To specify the ports to be locked, use the config ethernet <*ports*> lock command. The default value is off.
sendAuthenticationTrap <true|false>	Configures whether to send authentication failure traps. The default value is false.
topology <on|off>	Turns the topology feature on or off. The topology feature generates topology packets used by Enterprise Network Management System (ENMS). If you disable this feature, the system does not generate the topology table. The default is on.
udp-checksum <enable|disable>	Activates or disables the UDP checksum calculation. The default value is enable.
udpsrc-by-vip <enable|disable>	Activates or disables virtual IP as the UDP source.
vlan-bysrcmac <enable|disable>	Activates or disables source MAC VLAN configuration on the switch. The default is disable. If you enable this command, you must disable the global filter command (config sys set global-filter disable) because you cannot enable global filtering and source MAC-based VLANs at the same time.

Example of configuring system-level switch parameters

1. Configure the contact parameter:

   ```
   ERS-8606:5# config sys set ERS-8606:5/config/sys/set# contact cbfw
   ```

2. Configure the location parameter:

   ```
   ERS-8606:5/config/sys/set# location Marketing
   ```

3. Configure the authentication trap parameter:

   ```
   ERS-8606:5/config/sys/set# sendAuthenticationTrap true
   ```

4. View the current system-level switch parameters:

   ```
   ERS-8606:5/config/sys/set# info Sub-Context: action flags msg-control
   record-reservation snmp ssh Current Context:

   mgmt-virtual-ip : 0.0.0.0/0.0.0.0
   mgmt-virtual-ipv6 : 0:0:0:0:0:0:0:0/0
   udp-checksum : enable
   udp-source : disable
   clock-sync-time : 60
   mroute-stream-limit : disable
   contact : cbfw
   location : Marketing
   name : ERS-8606
   portlock : off
   sendAuthenticationTrap : false
   topology : on
   globalFilter : enable
   vlanBySrcMac : disable
   ecn-compatibility : enable
   max-vlan-resource-reservation : (disable) -> (disable)
   multicast-resource-reservation : (2000) -> (2000)
   System MTU : 1950
   ERS-8606:5/config/sys/set#
   ```

Synchronizing the real-time and system clocks

Configure the regular interval to synchronize the real-time and system clocks. The switch generates log messages if the drift between the real-time clock and the system clock is more than 5 seconds.

Synchronize the real-time and system clocks by performing this procedure.

Procedure steps

1. Configure the synchronization interval by using the following command:

   config sys set clock-sync-time <*minutes*>

Variable definitions

Use the data in the following table to use the `config sys set clock-sync-time` command.

Variable	Value
minutes	Specifies the number of minutes between synchronization in a range from 15–3600 minutes. The default value is 60 minutes.

Creating a virtual management port

Create a virtual management port in addition to the physical management ports on the switch management modules.

After you assign an IP address to the virtual management port, the IP address provides access to both switch management modules. The master management module replies to all management requests sent to the virtual IP address, as well as to requests sent to its management port IP address. If the master management module fails and the standby management module takes over, the virtual management port IP address continues to provide management access to the switch.

Create a virtual management port by performing this procedure.

Procedure steps

1. Create a virtual management port by using the following command:

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

Example of creating a virtual management port

1. Create a virtual management port:

   ```
   ERS-8606:5# config sys set mgmt-virtual-ip
   47.140.54.40/255.255.255.0 Physical and Virtual IP must be in the
   same subnet
   ```

Configuring system message control

Configure system message control to enable or disable system messaging and define configuration settings by performing this procedure.

Procedure steps

1. Configure system message control action by using the following command:

   ```
   config sys set msg-control action <suppress-msg|send-trap|both>
   ```

2. Configure the maximum number of messages by using the following command:

   ```
   config sys set msg-control max-msg-num
   ```

3. Configure the interval by using the following command:

   ```
   config sys set msg-control control-interval <minutes>
   ```

Variable definitions

Use the data in the following table to use the `config sys set msg-control` command.

Variable	Value
action <suppress-msg|send-trap|both>	Configures the message control action.
control-interval <*minutes*>	Configures the message control interval in minutes. • *minutes* is a number from 1–30
disable	Disables system message control.
enable	Activates system message control. • enable suppresses duplicate error messages
info	Specifies the configuration of system message control.
max-msg-num <*number*>	Configures the number of occurrences of a message after which the control action occurs. • *number* is a value from 2–500

Forcing message control for system message control

Use the force message control option to extend the message control feature functionality to the software and hardware log messages.

To enable the message control feature, you must specify an action, control interval, and maximum message number. After enabling the feature, the log messages, which get repeated and cross the maximum message number in the control interval, trigger the force message feature. You can either suppress the message or send a trap notification, or both.

Use the force message control for system message control by performing this procedure.

Procedure steps

1. Configure the force message control option by using the following command:

   ```
   config sys set msg-control force-msg add <string>
   ```

Variable definitions

Use the data in the following table to use the `config sys set msg-control force-msg` command.

Variable	Value
add <*string*>	Adds a forced message control pattern • *string* is a string of 4 characters. You can add a four-byte pattern into the force-msg table. The software and the hardware log messages that use the first four bytes that match one of the patterns in the force-msg table undergo the configured message control action. You can specify up to 32 patterns in the force-msg table. The force-msg table can include a wild-card pattern (****). If you specify the wild-card pattern, all messages undergo message control.
del <*string*>	Deletes a forced message control pattern • *string* is a string of 4 characters.
info	Specifies the current configuration.

Enabling the administrative status of a module

Enable or disable the administrative status of the module by performing this procedure.

Procedure steps

1. View the current administrative status of the module by using the following command:

   `config slot` <*slots*> **`info`**

2. Change the administrative status of the module by using the following command:

   `config slot` <*slots*> **`state <enable|disable>`**

Chapter 16: Chassis operations configuration using the CLI

This chapter provides the details to configure operating modes and basic hardware and system settings.

Job aid

The following table lists the commands and their parameters that you use to complete the procedures in this section.

Table 21: Job aid

Command	Parameter
config ethernet <*slot/port*> cp-limit	<enable|disable>
	multicast-limit <*value*>
	broadcast-limit <*value*>
config ethernet <*ports*> ext-cp-limit	<None|SoftDown|HardDown>
	threshold-util-rate <*value*>
config ethernet <*port*> loop-detect	<enable|disable>
	action <*value*>
	arp-detect
	<enable|disable>
config ethernet <*port*> auto-recover-port	<enable|disable>
config auto-recover-delay <*5–3600 seconds*>	
config ethernet <*portlist*> slpp	info
	packet-rx <enable|disable>
	packet-rx-threshold <*integer*>
config mac-flap-time-limit <*10–5000 milliseconds*>	
config slpp	add <*vid*>
	etherType <*pid*>

Table continues…

Command	Parameter
	info
	operation enable
	remove <*vid*>
	tx-interval <*integer*>
config sys ext-cp-limit extcplimit	<enable|disable>
	info
	max-ports-to-check <*number of ports*>
	min-congestion-time <*time in msec*>
	port-congestion-time <*time in sec*>
	trap-level <Normal|Verbose|None>
config sys set flags	auto-reset-fabric <true|false>
	global-filter-ordering <true|false>
	info
	multicast-check-packet <true|false>
	regular-autoneg <true|false>
	take-iocard-offline <true|false>
config sys set power	fan-check-enable <true|false>
	info
	power-check-enable <true|false>
	slot-priority <*slot*> <criticial|high|low>
config sys set mtu	<*bytes*>
config sys set record-reservation	filter <*value*>
	info
	ipmc <*value*>
	local <*value*>
	mac <*value*>
	static-route <*value*>
	vrrp <*value*>

Enabling CPU High Availability mode

CPU high-availability (CPU-HA) mode enables switches with two CPUs to recover quickly from a failure of the master SF/CPU.

Use the procedure in this section to enable CPU-HA mode.

Procedure steps

1. To enable HA mode, enter the following boot flag command on the master SF/CPU:

   ```
   config bootconfig flags ha-cpu true
   ```

   After enabling HA mode on the master SF/CPU, the secondary SF/CPU automatically resets to load settings from its previously-saved boot configuration file. You must manually reset the primary SF/CPU while the secondary SF/CPU is booting.

   Important:

   Failure to manually boot the primary CPU before the secondary finishes booting can lead to system instability. Traffic is interrupted when the master is manually reset.

   Caution:

   Enabling the HA mode can cause certain features to become disabled. See the Release Notes for your software version for details on HA mode specific information.

Table 6: Release 3.5 and later synchronization capabilities in HA mode on page 49 shows which features are supported in each release.

Job aid

See the following sample output for the messages the switch returns when you enable HA mode using CLI:

```
ERS-8610:6# config bootconfig flags ha-cpu true Save bootconfig to file /flash/
boot.cfg successful.Boot configuration is being saved on secondary CPU You need
to reset the secondary CPU for the change to take effect !! Do you want to
restart the secondary CPU now (y/n) ? y
```

Important:

The preceding autosave of the boot configuration file occurs because the savetostandby flag is enabled. If this flag is not enabled, a manual save of the boot configuration file on the secondary SF/CPU is required.

Answering the user prompt with a "y" causes the secondary SF/CPU to reset itself automatically, and that secondary SF/CPU restarts with HA mode enabled. You must manually reset the master SF/CPU immediately (before the secondary CPU completes reset). Resetting the primary CPU causes an interruption to traffic. After the reset completes successfully, the CPUs reverse roles (the CPU that was the primary CPU before reset becomes the secondary CPU and the CPU that was secondary before reset becomes the primary CPU).

Disabling CPU High Availability mode

Use the procedure in this section to disable HA CPU mode.

Procedure steps

1. To disable HA mode, enter the following boot flag command on the master SF/CPU:

   config bootconfig flags ha-cpu false

   After disabling HA mode on the master SF/CPU, the secondary SF/CPU automatically resets to load settings from its previously-saved boot configuration file. You must manually reset the primary SF/CPU while the secondary SF/CPU is booting.

   Important:

   Failure to manually boot the primary CPU before the secondary finishes booting can lead to system instability. Traffic is interrupted when the master is manually reset.

Job aid

See the following sample output for the messages the switch returns when you disable HA mode using CLI:

```
ERS-8610:5(config)#config bootconfig flags ha-cpu false

Save bootconfig to file /flash/boot.cfg successful. Save to slave file /flash/
boot.cfg successful. CPU5 [02/12/09 15:14:44] SNMP INFO Save to slave file /
flash/boot.cfg successful. Boot configuration is being saved on both master and
slave. CPU5 [02/12/09 15:14:44] SNMP INFO Save boot successful.

You need to reset the master for the changes to take effect. Resetting Slave
CPU from Master CPU.
```

Removing a master CPU with CPU-HA mode activated

Properly remove the master SF/CPU to avoid loss of traffic if CPU-HA is activated by performing this procedure.

Procedure steps

1. Software reset the master SF/CPU, which becomes the standby.
2. Remove what is now the standby SF/CPU.

   The master is removed. Because CPU-HA is activated, no traffic data is lost during reset.

Important:

Reinserting an SF/CPU module before the HA-activated CPU becomes the master SF/CPU can cause the master SF/CPU to remain in a booting state.

Enabling jumbo frames

Enable jumbo frames to increase the size of Ethernet frames supported on the chassis by performing this procedure.

Note:

After changing the MTU size, you must reboot the switch for the change to take effect.

Procedure steps

1. Enable jumbo frames by using the following command:

   ```
   config sys set mtu <bytes>
   ```

Variable definitions

Use the data in the following table to configure the `config sys set mtu` command.

Variable	Value
<bytes>	The control plane (CPU, CPP) does not support Jumbo frames, but can learn properly when you use Jumbo frames. You can use **`mtu <bytes>`** to activate Jumbo frame support for the data path. • *bytes* is the Ethernet Frame size, either 1522, 1950 (default), or 9600 bytes. Settings of either 1950 or 9600 bytes activate Jumbo frame support. Jumbo frame support is activated by default.

Reserving records

Reserve records to change the number of hardware records available for each record type by performing this procedure.

Prerequisites

- You can reserve records only on modules E and M.
- You must use this command in the ACLI Global configuration command mode.

Procedure steps

1. At the prompt, enter `config sys set record-reservation [filter <value>| info|ipmc <value>|local <value>|mac <value>|static-route <value>| vrrp <value>]`

Variable definitions

Use the data in the following table to configure `config sys set record-reservation`.

Variable	Value
filter <*value*>	Configure reservation for filter record type expressed in a range from 1025–8192. The default value is 4096
info	Shows current level parameter settings and next level directories.
ipmc <*value*>	Configure reservation for ipmc record type expressed as an ipmc value in a range from 0–8000. The default value is 500.
local <*value*>	Configure reservation for local record type expressed as a local value in a range from 0–16000. The default value is 2000.
mac <*value*>	Configure reservation for mac record type expressed as a mac value in a range from 0–200000. The default value is 2000.
static-route <*value*>	Configure reservation for static-route record type expressed as a route value in a range from 0–1000. The default value is 200.
vrrp <*value*>	Configure reservation for vrrp record type expressed as a vrrp value from 0–510. The default value is 500.

Configuring SLPP

Enable the Simple Loop Prevention Protocol (SLPP) globally and on a VLAN to detect a loop and automatically stop it by performing this procedure.

Procedure steps

1. Enable SLPP by using the following command:

   ```
   config slpp operation enable
   ```

2. Specify the SLPP protocol ID by using the following command:

   ```
   config slpp etherType <pid>
   ```

3. Configure the transmission interval by using the following command:

   ```
   config slpp tx-interval <integer>
   ```

4. Add a VLAN to the transmission list by using the following command:

   ```
   config slpp add <vid>
   ```

Variable definitions

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

Variable	Value
add <*vid*>	Adds a VLAN to a SLPP transmission list. • <*vid*> is the VLAN ID.
etherType <*pid*>	Specifies the SLPP PDU Ethernet type. • <*pid*> is the SLPP protocol ID expressed as a decimal in the range from 1 to 65535 or in hexadecimal from 0x001 to 0xffff. The default value is 0x8102. To set this option to the default value, use the default operator with the command.
info	Shows current level parameter settings and next level directories.
operation <enable|disable>	Enables or disables the SLPP operation. **Important:** If the SLPP operation is disabled, the system sends no SLPP packets and discards received SLPP packets. The SLPP packets transmit and

Table continues…

Variable	Value
	receive process is active only if the SLPP operation is enabled.
remove <*vid*>	Removes a VLAN from a SLPP transmission list. • <*vid*> is the ID of the VLAN.
tx-interval <*integer*>	Configures the SLPP packet transmit interval, expressed in milliseconds in a range from 500–5000. • <*integer*> is the SLPP packet transmit interval. The default value is 500.

Configuring SLPP on a port

Enable SLPP on a port to detect, and automatically terminate, a loop by performing this procedure.

Important:

To provide protection against broadcast and multicast storms, Avaya recommends that you enable Rate Limiting for broadcast traffic and multicast traffic.

Procedure steps

1. Configure SLPP on a port by using the following command:

   ```
   config ethernet <portlist> slpp
   ```

Variable definitions

Use the data in the following table to use the `config ethernet <portlist> slpp` command.

Variable	Value
info	Shows current level parameter settings and next level directories.
packet-rx <enable|disable>	Activates or disables SLPP packet reception on the listed ports.
packet-rx-threshold <*integer*>	Specifies the threshold for packet reception. The SLPP packet receive threshold is set to a value (1-500) that represents the number of SLPP-PDUs that must be received to shut down the port. Note that this is a port-level parameter, therefore if the port is

Table continues…

Variable	Value
	tagged, SLPP-PDUs from the various VLANs increment this single threshold counter. See Table 14: SLPP recommended values on page 63 for recommended values in an SMLT environment.
<portlist>	Identifies the slot/port.

Viewing SLPP information

Use SLPP information to view simple loop information by performing this procedure.

Procedure steps

1. View SLPP information by using the following command:

   ```
   show slpp info
   ```

Viewing SLPP information for a port

Show SLPP information for a port so that you can view the loop information for a port by performing this procedure.

Procedure steps

1. Show the SLPP information for a port or all ports by using the following command.

   ```
   show ports info slpp [port <slot/port>]
   ```

Variable definitions

Use the data in the following table to help you view the `SLPP port` information.

Variable	Value
PORT NUM	Specifies the port number.
PKT-RX	Specifies whether SLPP is enabled or disabled.
PKT-RX THRESHOLD	Specifies the configured SLPP receive threshold configured on the port.
INCOMING VLAN ID VLAN	Specifies the ID of the classified packet on a port disabled by SLPP.
SLPP PDU ORIGINATOR	Specifies the originator of the SLPP PDU.

Table continues…

Variable	Value
PKT-RX COUNT	Specifies the SLPP RX PDU count.
TIME LEFT TO CLEAR RX COUNT	Specifies the time left to clear the SLPP RX PDU counter.

Clearing SLPP port counters

Clear SLPP port counters manually by performing this procedure.

Procedure steps

1. Clear the SLPP port counters manually:

   ```
   clear slpp stats <ports>
   ```

Variable definitions

Use the data in the following table to use the `clear slpp stats` command.

Variables	Value
ports	Specifies the slot and port number

Configuring Extended CP Limit on the chassis

CP Limit functionality protects the switch from becoming congested by an excess of data flowing through one or more ports. Currently the CP Limit functionality only protects the switch from broadcast and control traffic with a QoS value of 7. The Extended CP Limit functionality is configurable and you can use it to prevent overwhelming the switch.

Configure extended CP Limit on the chassis by performing this procedure.

Procedure steps

1. Enable Extended CP Limit by using the following command:

   ```
   config sys ext-cp-limit extcplimit enable
   ```

2. Configure additional optional parameters

Variable definitions

Use the data in the following table to use the `config sys ext-cp-limit` command.

Variable	Value
extcplimit <enable|disable>	Configures the extended CP limit. The default is disabled.
info	Specifies the current configuration.
max-ports-to-check <*number of ports*>	Configures the total number of ports to monitor. • *number of ports* is in the range of 0–512. The default is 0.
min-congestion-time <*time in msec*>	Configures the minimum time for which traffic keeps hitting the SF/CPU to trigger the congestion algorithm. • *time in msec* is the time in milliseconds in the range of 100–600000. The default value is 3000.
port-congestion-time <*time in sec*>	Configures the time duration for which, if the bandwidth utilization for a monitoring port remains more than the threshold, the port is disabled. • *time in sec* is the time in seconds in the range of 1–600. The default value is 5 seconds.
trap-level <Normal|Verbose|None>	Configures the trap level. The options are: • Normal–sends a single trap for all the ports which are disabled. • Verbose–sends a trap for each of the ports which is disabled. • None–no traps are sent. The default value is None.

Configuring Extended CP Limit on a port

CP Limit functionality protects the switch from becoming congested by an excess of data flowing through one or more ports. Currently the CP Limit functionality only protects the switch from broadcast and control traffic with a QoS value of 7. The Extended CP Limit functionality is configurable and you can use it to prevent overwhelming the switch.

Configure extended CP Limit on a port by performing this procedure.

Procedure steps

1. Configure Extended CP Limit on a port by using the following command:

```
config ethernet <ports> ext-cp-limit <None|SoftDown|HardDown>
[threshold-util-rate <value>]
```

Variable definitions

Use the data in the following table to use the `config ethernet ext-cp-limit` command.

Variable	Value
<None|SoftDown|HardDown>	Indicates the following: • None–the port does not need to be checked. • SoftDown–the port belongs to the may-go-down-port-list. • HardDown–the port belongs to the must-go-down-port-list.
<ports>	Specifies a port or list of ports.
threshold-util-rate	Specifies the threshold bandwidth utilization rate expressed in per cent in a range from 1–100. The default value is 50.

Configuring loop detect

Configure loop detect to determine if the same MAC address appears on different ports. Use the ARP-Detect feature to account for ARP packets on IP configured interfaces.

Configure loop detect by performing this procedure.

Procedure steps

1. Configure loop detect by using the following command:

   ```
   config ethernet <port> loop-detect <enable|disable> action <value>
   ```

2. Configure the interval at which MAC addresses are monitored:

   ```
   config mac-flap-time-limit <10..5000 milliseconds>
   ```

Variable definitions

Use the data in the following table to use the `config ethernet loop-detect` command.

Variable	Value
action <value>	Specifies the loop detect action to be taken. • port-down shuts down the port upon detecting a flapping MAC address • vlan-block shuts down the VLAN upon detecting a flapping MAC address • mac-discard. ARP-Detect does not support this action. The default is port-down.
arp-detect	Activates ARP-Detect. On routed interfaces, activate ARP-Detect with loop detect.
<enable|disable>	Activates or disables the loop detect feature for the port.

Configuring CP Limit

CP Limit functionality protects the switch from becoming congested by excess data flowing through one or more ports by performing this procedure.

Important:

Before CP Limit shuts down a port that exceeds the threshold, it captures the traffic statistics for that port. To see these logs, enter the following command: **`more /pcmcia/rxstats.txt`**.

Procedure steps

1. Configure CP Limit by using the following command:

```
config ethernet <slot/port> cp-limit <enable|disable> [multicast-limit <value>] [broadcast-limit <value>]
```

Variable definitions

Use the data in the following table to use the `config ethernet cp-limit` command.

Variable	Value
broadcast-limit <value>	Configures the broadcast control frame rate expressed as pps in a range from 1000–100000. The default value is 10000.

Table continues…

Variable	Value
	Note: If you are using the 8692 SF/CPU with a SuperMezz, change the default to 3000 pps
<enable|disable>	Activates or disables the CP Limit feature. The default is activated.
info	Specifies the configured parameters for CP Limit. The syntax for this command is: config ethernet slot/port info
multicast-limit <*value*>	Configures the multicast control frame rate expressed in pps in a range from 1000–100000. The default value is 15000. **Note:** If you are using the 8692 SF/CPU with a SuperMezz, change the default to 3000 pps

Configuring Auto Recovery

Configure Auto Recovery to reenable ports that were disabled because loops were detected. When enabled, this feature automatically recovers ports disabled by SLPP, CP Limit, link flap, or loop detect.

Procedure steps

1. Enable auto-recovery on a port by using the following command:

   ```
   config ethernet <ports> auto-recover-port enable
   ```

Variable definitions

The following table describes variables that you enter in the **`config ethernet <ports> auto-recover-port enable`** command.

Variable	Value
`<ports>`	Specifies the port or the list of ports in slot/port format.
`{enable|disable}`	`enable` activates Auto Recovery of the port from action taken by SLPP, CP Limit, link flap, or loop detect. The default value is `disable`.

Job aid: Loop detection warning messages

The following log message and trap is generated when a port, which has been disabled due to CP-Limit or link-flap, is auto-recovered:

```
port <port-num> re-enabled by auto recovery
```

The following log message and trap is generated when a port which has been disabled due to the loop detection feature is auto-recovered:

```
Loop detect action <action> cleared on port <port-num> by auto recovery
```

Setting the Auto Recovery timer

Set the Auto Recovery timer to the number of seconds you want to wait before reenabling ports that were disabled because loops were detected. This timer is a global setting that applies to all ports that have Auto Recovery enabled.

Procedure steps

1. Set the auto-recovery timer by using the following command:

   ```
   config auto-recover-delay <seconds>
   ```

Variable definitions

The following table describes variables that you enter in the **`config auto-recover-delay <seconds>`** command.

Variable	Value
`<seconds>`	Configures the delay in Auto Recovery. The value ranges from 5 to 3600 seconds. The default is 30.

Enabling power management

Enable power redundancy to create traps and events after power consumption exceeds redundancy capacity by performing this procedure.

Procedure steps

1. At the prompt, enter

   ```
   config sys set power
   ```

2. Configure power management by using the following command:

   ```
   power-check-enable true
   ```

   You must save the run-time configuration and reset the switch for this change to take effect.

Configuring slot priority

Configure slot priority to determine which slots shut down if not enough power is available in the chassis. The slot with the lowest priority shuts down first. Slots with the same priority shut down by highest slot number first.

Configure priority of slots by performing this procedure.

Procedure steps

1. Configure slot priority by using the following command:

   ```
   config sys set power slot-priority <slot> <critical|high|low>
   ```

Variable definitions

Use the data in the following table to use the `config sys set power slot-priority` command.

Variable	Value
<critical|high|low>	Configures the priority for the slot.
slot	Specifies the slot for which to set the priority value. You can configure priority for slots 1–4 and 7–10.

Enabling Fabric (FAB) Memory Full error handling

Use the procedure in this section to enable Fabric (FAB) Memory Full error handling to resolve the `Fab Memory Full` fault.

Procedure steps

To enable Fabric (FAB) Memory Full error handling, enter the following command:

```
config sys set flags
```

Important:

When enabled, Fabric (FAB) Memory Full error handling will cause the switch fabric to automatically reset when the Fabric (FAB) Memory Full error is detected. For redundant network designs, this will divert traffic around the affected switch and allow the network to recover with minimal interruption. If the network design does not support redundancy, then there will be network interruption while the switch is reset.

Variable definitions

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

Variable	Value
auto-reset-fabric <true|false>	Enable or disable fabric to be reset automatically on `Fab Memory Full` error. The default is `false`.
take-iocard-offline <true|false>	Enable or disable I/O card to go offline when there are excessive resets. The default is `true`.

Chapter 17: LLDP configuration using the CLI

Configure LLDP to use as part of fault management operations and to provide diagnostic information in troubleshooting procedures.

Related links

Job aid: roadmap of LLDP CLI commands

The following roadmap lists the CLI commands used to enable and configure LLDP.

Table 22: Job aid: roadmap of LLDP CLI commands

Command	Parameter
config lldp	info
	notification-interval <5-3600>]
	reinit-delay <1-10>
	tx-interval <1-32768>
	tx-hold-multiplier <2-10>

Table continues…

Command	Parameter
	tx-delay <1-8192>
config ethernet <portList> lldp	info
	config-notification
	[status {rx|txAndRx|tx|disabled}]
	port <portList> <config-notification | status>
config ethernet <portList> lldp tx-tlv	info
	port-desc <enable|disable>
	sys-name <enable|disable>
	sys-desc <enable|disable>
	sys-cap <enable|disable >
	local-mgmt-addr-tx <enable|disable>
config ethernet <portList> lldp tx-tlv dot1	info
	port-vlan-id <enable|disable>
	vlan-name <enable|disable> <vlanList>
	port-protocol-vlan-id <enable|disable> <vlanList>
	protocol-identity [EAP|LLDP|MSTP|RSTP] <enable|disable> <vlanList>
config ethernet <portList> lldp tx-tlv dot3	info
	mac-phy-config-status <enable|disable>
	link-aggregation <enable|disable>
	maximum-frame-size < enable|disable>
show lldp	[port <portList>] local-sys-data [capabilities | {[dot1] [dot3] [med]} | detail}
	mgmt-sys
	rx-stats <portList>
	tx-stats <portList>
	stats
	pdu-tlv-size
	neighbor <portList>
	neighbor-dot1 <vlan-names | protocol-id>
	neighbor-dot3
	neighbor-mgmt-addr <portList>
config lldp info	
config ethernet <portList> lldp info	
config ethernet < portList> lldp [tx-tlv {dot1|dot3}] info	

Related links

LLDP configuration using the CLI on page 168

Setting LLDP transmission parameters

Set the LLDP transmission parameters to configure LLDP on the Ethernet Routing Switch 8800/8600.

Procedure steps

1. To set the LLDP transmission parameters, use the following command:

   ```
   config lldp
   ```

Variable definitions

Use the data in the following table to configure the **`config lldp`** command.

Variable	Value
tx-interval <1-32768>	Sets the global interval (in seconds) between successive transmission cycles. The range is 1 to 32768 and the default is 30.
tx-hold-multiplier <2-10>	Sets the multiplier (in seconds) for the tx-interval used to compute the Time To Live value for the TTL TLV. The range is 2 to 10 and the default is 4.
reinit-delay <1-10>	Sets the delay (in seconds) for the reinitialization attempt if the adminStatus is disabled. The range is 1 to 10 and the default is 2.
tx-delay <1-8192>	Sets the minimum delay (in seconds) between successive LLDP frame transmissions. The range is 1 to 8192 and the default is 2.
notification-interval <5-3600>	Sets the interval (in seconds) for which only one remote table change notification is transmitted. The range is 5 to 3600 and the default is 5.

Related links

LLDP configuration using the CLI on page 168

Setting LLDP port parameters

Set the LLDP port parameters to configure LLDP on the Ethernet Routing Switch 8800/8600.

Procedure steps

1. Set the LLDP port parameters using the following command:

```
config ethernet <portlist> lldp
```

Variable definitions

Use the data in the following table to configure the **`config ethernet <portlist> lldp`** command.

Variable	Value
config-notification	Enables notifications from the agent. The default is enabled.
status <rxOnly|txAndRx|txOnly>	Sets the administrative status on the port. • `rxOnly`: enables LLDPU receive only. • `txAndrx`: enables LLDPU transmit and receive. • `txOnly`: enables LLDPU transmit only. The default is `txAndrx` (transmit and receive).
port <portList> <config-notification | status>	Sets either the `config-notification` state or the `status` (administrative state) of the indicated port(s). The default for `config-notification` is enabled; the default for `status` is txAndrx.

Related links

LLDP configuration using the CLI on page 168

Specifying the optional Management TLVs to transmit

Set the optional Management TLVs to transmit LLDP on the Ethernet Routing Switch 8800/8600.

Procedure steps

1. Set the optional Management TLVs to be included in the transmitted LLDPDUs using the following command:

   ```
   config ethernet <portlist> lldp tx-tlv
   ```

Variable definitions

Use the data in the following table to configure the **`config ethernet <portlist> lldp tx-tlv`** command.

Variable	Value
port-desc <enable|disable>	Enables or disables transmission of the port description TLV from this port. The default is disabled.

Table continues…

Variable	Value
sys-name <enable|disable>	Enables or disables transmission of the system name TLV from this port. The default is disabled.
sys-desc <enable|disable>	Enables or disables transmission of the system description TLV from this port. The default is disabled.
sys-cap <enable|disable>	Enables or disables transmission of the system capabilities TLV from this port. The default is disabled.
local-mgmt-addr-tx <enable|disable>	Enables or disables transmission of the local management address TLV from this port. The default is disabled.

Related links

LLDP configuration using the CLI on page 168

Specifying the optional IEEE 802.1 TLVs to transmit

Set the optional IEEE 802.1 TLVs to be included in the transmitted LLDPDUs.

Procedure steps

1. Set the optional IEEE 802.1 organizationally specific TLVs to transmit using the following command:

   ```
   config ethernet <portlist> lldp tx-tlv dot1
   ```

Variable definitions

Use the data in the following table to configure the **`config ethernet <portlist> lldp tx-tlv dot1`** command.

Variable	Value
port-vlan-id <enable|disable>	Enables or disables the transmission of port VLAN ID TLVs from this port(s). The default is disabled.
vlan-name <enable|disable> <vlanList>	Enables or disables the transmission of VLAN name TLVs from this port(s). The default is disabled.
port-protocol-vlan-id <enable|disable> <vlanList>	Enables or disables the transmission of protocol VLAN TLVs from this port(s). The default is disabled.
protocol-identity [EAP|LLDP|MSTP|RSTP} <enable|disable>	Enables or disables the transmission of the specified protocol identity TLVs from this port(s). The protocol can be EAP, LLDP, MSTP, or RSTP. The default is disabled.

Related links

LLDP configuration using the CLI on page 168

Specifying the optional IEEE 802.3 TLVs to transmit

Specify the optional IEEE 802.3 organizationally specific TLVs to be included in the transmitted LLDPDUs.

Procedure steps

1. Specify the optional IEEE 802.3 organizationally specific TLVs to transmit, using the following command:

   ```
   config ethernet <portlist> lldp tx-tlv dot3
   ```

Variable definitions

Use the data in the following table to configure the **`config ethernet <portlist> lldp tx-tlv dot3`** command.

Variable	Value
mac-phy-config-status <enable|disable>	Enables or disables the transmission of the MAC/Phy configuration/status TLVs from this port(s). The default is disabled.
link-aggregation <enable|disable>	Enables or disables the transmission of link aggregation TLVs from this port(s). The default is disabled.
maximum-frame-size <enable|disable>	Enables or disables the transmission of maximum frame size TLVs from this port(s). The default is disabled.

Related links

LLDP configuration using the CLI on page 168

Showing global LLDP information

Display the global LLDP parameters to view information about the LLDP settings on the switch.

Procedure steps

1. Display the global LLDP parameters with the following command:

   ```
   show lldp
   ```

Related links

LLDP configuration using the CLI on page 168

Showing local LLDP information

Display the LLDP information about the local LLDP settings

Procedure steps

1. Display the local LLDP parameters with the following command:

   ```
   show lldp
   ```

Variable definitions

Use the data in the following table to configure the **`show lldp`** command.

Variable	Value
[port <portList>] local-sys-data [capabilities | {[dot1] [dot3] [med]} | detail}	Displays the organizationally-specific TLV properties on the local switch: • `port <portList>`: displays LLDP information for the specified ports • `capabilities`: displays the LLDP capabilities information for the specified ports • `dot1`: displays the 802.1 TLV properties • `dot3`: displays the 802.3 TLV properties • `med`: displays the Media Endpoint Discovery (MED) properties • `detail`: displays all organizationally-specific TLV properties To display the properties of the optional management TLVs, include only the local-sys-data parameter in the command.
mgmt-sys-data	Displays the local management system data.
pdu-tlv-size	Displays the different TLV sizes and the number of TLVs in an LLDPDU.
rx-stats <portlist>	Displays the LLDP receive statistics for the local system.
stats	Displays the LLDP table statistics for the remote system.
tx-stats <portlist>	Displays the LLDP transmit statistics for the local system.
tx-tlv [dot1] [dot3]	Displays which TLVs are transmitted from the local switch in LLDPDUs: • `dot1`: displays status for 802.1 TLVs • `dot3`: displays status for 802.3 TLVs

Table continues…

Variable	Value
	To display the transmission status of the optional management TLVs for all ports, include only the tx-tlv parameter in the command.

Related links

LLDP configuration using the CLI on page 168

Showing LLDP neighbor information

Displays information about the LLDP neighbors.

Procedure steps

1. Display the LLDP neighbor parameters with the following command:

   ```
   show lldp neighbor <portlist>
   ```

Variable definitions

Use the data in the following table to configure the **`show lldp neighbor <portlist>`** command.

Variable	Value
detail	Displays detailed information about the LLDP neighbors.
neighbor-dot1 [vlan-names | protocol-id]	Displays the neighbor 802.1 TLVs: • `vlan-names`: VLAN Name TLV • `protocol-id`: Protocol Identity TLV
neighbor-dot3	Displays the neighbor 802.3 TLVs.
neighbor-mgmt-addr <portlist>	Displays the LLDP neighbor management address.

Related links

LLDP configuration using the CLI on page 168

Showing LLDP transmission parameters

Display the LLDP TLV transmission parameters to view TLV transmission information.

Procedure steps

1. Display the LLDP TLV transmission parameters with the following command:

   ```
   config lldp info
   ```

Related links

LLDP configuration using the CLI on page 168

Showing LLDP port parameters

Display the LLDP port parameters to view LLDP port information.

Procedure steps

1. Display the LLDP port parameters with the following command:

   ```
   config ethernet <portlist> lldp info
   ```

Related links

LLDP configuration using the CLI on page 168

Showing LLDP port TLV parameters

Display the LLDP port TLV parameters to view LLDP port TLV information.

Procedure steps

1. Display the LLDP port TLV parameters with the following command:

   ```
   config ethernet <portlist> lldp
   ```

Variable definitions

Use the data in the following table to configure the **`config ethernet <portlist> lldp`** command.

Variable	Value
[tx-tlv <dot1|dot3>] info	Displays which TLVs are transmitted from the local port in LLDPDUs: • `dot1`: displays status for 802.1 TLVs • `dot3`: displays status for 802.3 TLVs To display the transmission status of the optional management TLVs, include only the tx-tlv parameter in the command.

Related links

LLDP configuration using the CLI on page 168

Chapter 18: System access configuration using the CLI

The chapter provides procedures to manage system access through configurations such as usernames, passwords, and access policies.

Job aid

The following table lists the commands and their parameters that you use to complete the procedures in this section.

Table 23: Job aid

Command	Parameter
config cli password	access level <*access level*> <enable|disable>
	aging <*days*>
	default-lockout-time <*secs*>
	info
	l1 <*username*> [<*password*>]
	l2 <*username*> [<*password*>]
	l3 <*username*> [<*password*>]
	l4admin <*username*>
	l4oper <*username*>
	lockout-time <*HostAddress*> <*secs*>
	min-passwd-len <*integer*>
	oper <*username*>
	password-history <*number*>
	ro <*username*> [<*password*>]
	rw <*username*> [<*password*>]
	rwa <*username*> [<*password*>]
	slboper <*username*>

Table continues…

Command	Parameter
	slbadmin <*username*>
	ssladmin <*username*>
config cli password access-level	<*string length 2..8*>
	<enable|disable>
config cli password <access-level><username>	
config sys access-policy by-mac	add <*mac*> <*action*>
	del <*mac*>
	default-action <*default-action*>
	info
config sys access-policy enable <true|false>	
config sys access-policy policy <*pid*>	accesslevel <*level*>
	access-strict <true|false>
	create
	delete
	disable
	enable
	host <*ipaddr/IPv6addr*>
	info
	mode <allow|deny>
	name <*name*>
	network <*addr/mask*>
	precedence <*precedence*>
	snmp-group-add <*group-name*> <*model*>
	snmp-group-del <*group-name*> <*model*>
	snmp-group-info
	username <*string*>
config sys access-policy policy <*pid*> service	ftp <enable|disable>
	http <enable|disable>
	info
	rlogin <enable|disable>
	snmpv3 <enable|disable>
	ssh <enable|disable>
	telnet <enable|disable>
	tftp <enable|disable>
reset-passwd	

Enabling CLI access levels

Enable command line interface (CLI) access levels to control the configuration actions of system users by performing this procedure.

Important:

Only the RWA user can disable an access level on the switch. You cannot disable the RWA access level on the switch.

These configurations are preserved across restarts.

Procedure steps

1. Enable a CLI access level by using the following command:

```
config cli password access-level <access-level> <enable|disable>
```

Variable definitions

Use the data in the following table to use the `config cli password access-level` command.

Variable	Value
access level	Specifies the required access level with a string length of 2–8 characters.
enable|disable	Blocks or permits the access level. The default value is enable.

Changing passwords

Configure new passwords for each access level, or change the login or password for switch access levels.

The Ethernet Routing Switch 8800/8600 ships with default passwords set for access to the CLI. For security, passwords are saved to a hidden file. The optional parameter *password* is the password associated with the user name or login name.

If you use Simple Network Management Protocol version 3 (SNMPv3), you can change encrypted passwords. Change password by performing this procedure.

Prerequisites

- To change passwords, you must have read-write-all privileges.

Procedure steps

1. 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 an access level. • *access level* is expressed as an integer from 2–8. • enable|disable activates or disables the designated level.
aging <*days*>	Configures the age-out time for passwords. • *days* is expressed as an integer from 1–365.
default-lockout-time <*secs*>	Changes the default lockout time after three invalid attempts, expressed in seconds. . • *secs* is the lockout time in a range from 60–65000. The default value is 60.
info	Specifies the current level parameter settings and the next level directories.
l1 <*username*> [<*password*>]	Changes the Layer 1 read/write login and password. • *username* is the login name • *password* is the password associated with the login name.
l2 <*username*> [<*password*>]	Changes the Layer 2 read/write login and password. • *username* is the login name. • *password* is the password associated with the login name.
l3 <*username*> [<*password*>]	Changes the Layer 3 read/write login and password (applies only to the Ethernet Routing Switch 8800/8600). • *username* is the login name. • *password* is the password associated with the login name.

Table continues…

Variable	Value
lockout-time <*HostAddress*> <*secs*>	Configures the host lockout time. • *HostAddress* is the Host Internet Protocol (IP) address in the format a.b.c.d. • *secs* is the password lockout-out time, in seconds, expressed in a range from 60–65000. The default value is 60.
min-passwd-len <*integer*>	Configures the minimum length for passwords in high-secure mode. • *integer* is as an integer in a range from 10–20.
password-history <*number*>	Specifies the number of previous passwords to retain in system memory. • *number* is expressed as an integer in a range from 3–32. The default is 3.
ro <*username*> [<*password*>]	Changes the read-only login and password. • *username* is the login name. • *password* is the password associated with the login name.
rw <*username*> [<*password*>]	Changes the read/write login and password. • *username* is the login name. • *password* is the password associated with the login name.
rwa <*username*> [<*password*>]	Changes the read/write/all login and password. • *username* is the login name. • *password* is the password associated with the login name.

Enabling the access policy globally

Enable the access policy feature globally to control access across the switch. You can control access to the switch by creating an access policy. An access policy specifies the hosts or networks that can access the switch through various access services, such as Telnet, SNMP, Hypertext Transfer Protocol (HTTP), and remote login (rlogin). You must enable the feature globally before individual policies take effect. Enable access policy globally by performing this procedure.

Procedure steps

1. Enable the access policy feature globally with the following command:

   ```
   config sys access-policy enable <true|false>
   ```

Variable definitions

Use the data in the following table to use the `config sys access-policy` command.

Variables	Value
enable <true|false>	Activates the access policy on the switch. • true globally activates the access-policy feature. • false globally disables the access-policy feature.

Creating an access policy

Create an access policy to control access to the switch. You can define network stations that are explicitly allowed to access the switch or network stations that are explicitly forbidden to access the switch. For each service, you can also specify the level of access, such as read-only or read/write/all. Create an access policy by performing this procedure.

Procedure steps

1. Create an access policy by using the following command:

   config sys access-policy policy <*pid*> **create**

Variable definitions

Use the data in the following table to use the `config sys access-policy policy` command.

Variables	Value
create	Creates the specified access policy on the switch.
policy <*pid*>	Identifies a policy. • <*pid*> is a number that identifies a policy.

Example of creating an access policy

1. Enable access policies globally with the following command:

   ```
   ERS-8606:5# config sys access-policy enable true
   ```

2. Create the policy 2345 with the following command:

   ```
   ERS-8606:5# config sys access-policy policy 2345 create
   ```

Configuring an access policy

Configure an access policy to control access to the switch by performing this procedure.

Prerequisites

- You must enable the access policy feature globally before the individual policy can take effect.

Procedure steps

1. Configure optional parameters for an access policy by using the following command:

   `config sys access-policy policy` *<pid>*

2. Enable the access policy by using the following command:

   ```
   config sys access-policy policy <pid> enable
   ```

Variable definitions

Use the data in the following table to use the `config sys access-policy policy` command.

Variables	Value
accesslevel *<level>*	Specifies the level of access if you cofigure the policy to allow access. • *level* is the access level
access-strict <true|false>	Designates access associated with configured levels. • true—the system accepts only the currently configured access level

Table continues…

Variables	Value
	• false—the system accepts access up to the configured level
create	Creates the specified access policy on the switch.
delete	Removes the specified access policy from the switch.
disable	Disables the access policy on the switch.
enable	Activates the access policy on the switch.
host <*ipaddr/IPv6addr*>	For rlogin access, specifies the trusted host address as an IP address.
info	Shows the current status of an access policy.
mode <allow|deny>	Specifies whether a designated network address is allowed or denied access through the specified access service. The default setting is allow.
name <*name*>	Specifies the name of the policy. The default name is *policy_<ID>*
network <*addr/mask*>	Specifies whether the designated IP address and subnet mask are permitted or denied access through the specified access service.
precedence <*precedence*>	Specifies a precedence for a policy to determine which policy the system uses if multiple policies apply.. • *precedence* is expressed as a number from 1–128. Lower numbers take higher precedence. The default precedence value is 10.
snmp-group-add <*group-name*> <*model*>	Adds snmp-v3 group under the access policy. • *group-name* is the snmp-v3 group name expressed in a range from 1–32 characters. • *model* is the security model: either snmpv1, snmpv2c, or usm.
snmp-group-del <*group-name*> <*model*>	Removes an snmp-v3 group under the access policy. • *group name* is the snmp-v3 group name expressed in a range from 1–32 characters. • *model* is the security model: either snmpv1, snmpv2c, or usm.
snmp-group-info	Shows snmp-v3 groups under this access policy
username <*string*>	For rlogin access, specifies the trusted host user name.

Job aid

The following is an example of configuring an access policy.

Procedure steps

1. Enable access policies globally:

   ```
   ERS-8606:5# config sys access-policy enable true
   ```

2. Assuming no access policies exist, start with policy 2 and name the policy policy2 as follows:

   ```
   ERS-8606:5# config sys access-policy policy 2 create
   ERS-8606:5# config sys access-policy policy 2 name policy2
   ```

3. Add read/write/all access level to policy 2:

   ```
   ERS-8606:5# config sys access-policy policy 2 accesslevel rwa
   ```

4. Add the usm group group_example to policy 2:

   ```
   ERS-8610:5# config sys access-policy policy 2 snmp-group-add
   group_example usm
   ```

5. Enable access strict enable:

   ```
   ERS-8610:5# config sys access-policy policy 2 access-strict true
   ```

6. Enable policy 2:

   ```
   ERS-8610:5# config sys access-policy policy 2 enable
   ```

Specifying a name for an access policy

Assign a name to the access policy to uniquely identify the policy by performing this procedure.

Procedure steps

1. Assign a name to the access policy by using the following command:

   `config sys access-policy policy` *<pid>* `name` *<name>*

Variable definitions

Use the data in the following table to use the `config sys access-policy policy` command.

Variables	Value
name *<name>*	*name* is a string from 0–15 characters.
policy *<pid>*	Identifies the policy. • *<pid>* is a number that identifies the policy expressed in a range from 1—65535.

Specifying the host address and username for rlogin

Specify the address and username required to access the SF/CPU when using rlogin by performing this procedure.

Procedure steps

1. Specify the trusted host address with the following command:

   `config sys access-policy policy` ***<pid>*** `host` ***<ipaddr>***

2. Specify the trusted host user name with the following command:

   `config sys access-policy policy` ***<pid>*** `username` ***<string>***

Variable definitions

Use the data in the following table to use the `config sys access-policy` command.

Variables	Value
host *<ipaddr/IPv6addr>*	For rlogin access, specifies the trusted host address as an IP address.
username *<string>*	For rlogin access, specifies the trusted host user name.

Enabling an access service

Enable an access service for the specified policy. An access policy specifies the hosts or networks that can access the switch through various services, such as Telnet, SNMP, Hypertext Transfer Protocol (HTTP), Secure Shell (SSH), and remote login (Rlogin). Enable an access service by performing this procedure.

Procedure steps

1. Enable an access service for the specified policy by using the following command:

   ```
   config sys access-policy policy <pid> service
   ```

Variable definitions

Use the data in the following table to use the `config sys access-policy policy service` command.

Variables	Value
ftp <enable|disable>	Activates or disables FTP for the specified policy. Because FTP derives its access level and password from the CLI management filters, FTP works only for the following access levels: • read-write-only (rwo) • read-write (rw) FTP does not work for read-only (ro).
http <enable|disable>	Activates or disables HTTP for the specified policy.
info	Shows the status (disable or enable) of each service (for example, ftp, http, rlogin) .
rlogin <enable|disable>	Activates or disables rlogin for the specified policy.
snmpv3 <enable|disable>	Activates or disables SNMPv3 for the specified policy. For more information about SNMPv3, see *Avaya Ethernet Routing Switch 8800/8600 Security, NN46205-601*.
ssh <enable|disable>	Activates or disables SSH for the specified policy. For more information about SSH, see *Avaya Ethernet Routing Switch 8800/8600 Security, NN46205-601*.
telnet <enable|disable>	Activates or disables Telnet for the specified policy.
tftp <enable|disable>	Activates or disables Trivial File Transfer Protocol (TFTP) for the specified policy.

Job aid

The following is an example of enabling FTP, Rlogin, HTTP, SNMP, SSH, and Telnet access services.

Procedure steps

1. Enable access services:

```
ERS-8610:6/config/sys/access-policy/policy/2/service# ftp enable
ERS-8610:6/config/sys/access-policy/policy/2/service# rlogin enable
http enable
ERS-8610:6/config/sys/access-policy/policy/2/service# snmpv3 enable
ERS-8610:6/config/sys/access-policy/policy/2/service# ssh enable
telnet enable
```

Allowing a network access to the switch

Specify the network to which you want to allow access by performing this procedure.

Procedure steps

1. Specify the network with the following command:

   `config sys access-policy policy` <*pid*> **`network`** <*addr/prefix- length*>

Variable definitions

Use the data in the following table to use the `config sys access-policy policy` command.

Variables	Value
accesslevel <*level*>	Specifies an access level. • *level* is expressed as one of these access levels: ro, rw, rwa, or the equivalent community string designation (read-only, read/write, or read/write/all).
addr/prefix-length	Designates the IPv4 address/mask, or the IPv6 address/prefix-length that is permitted or denied access through the specified access service.
mode <*allow*|*deny*>	Specifies whether a designated network address is allowed or denied access through the specified access service. The default setting is allow.

Configuring access policies by MAC address

Configure access-policies by MAC address to permit or deny local MAC addresses on the network management port after you activate an access policy.

If the source MAC does not match a configured entry, then the default action is taken. The system generates a log message to record the denial of access.

For connections coming in from a different subnet, the source mac of the last hop is used in decision making.

Configure access-policies by MAC address does not perform MAC or forwarding database (FDB) filtering on data ports.

Access policies are changed from previous releases. Before you attempt to upgrade an access policy from a previous release, see *Avaya Ethernet Routing Switch 8800/8600 Upgrades — Software Release 7.0, NN46205-400*. Configure an access policy by MAC address by performing this procedure.

Procedure steps

1. Configure access-policies by MAC address by using the following command:

   ```
   config sys access-policy by-mac
   ```

Variable definitions

Use the data in the following table to use the `config sys access-policy by-mac` command.

Variables	Value
add <*mac*> <*action*>	Adds a MAC address for a designated action. • <*mac*> is the MAC address in the format 0x00:0x00:0x00:0x00:0x00:0x00:0x00. • <*action*> is allow or deny.
del <*mac*>	Deletes a designated MAC address.
default-action <*default-action*>	Specifies the default action to allow or deny a MAC address with no match. The default action is allow.
info	Specifies the current access level configured by MAC address.

Resetting and modifying passwords

Modify passwords to protect security if users forget passwords or you suspect they are compromised by performing this procedure.

Procedure steps

1. In the boot-monitor CLI, reset all passwords to the factory defaults by using the following command:

   ```
   reset-passwd
   ```

2. In the run-time CLI, change passwords by using the following command:

   ```
   config cli password <access-level><username>
   ```

   You are prompted to enter the old password, the new password, and to confirm the new password.

   Important:

   All passwords are case-sensitive.

Variable definitions

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

Variable	Value
access-level	Specifies the access level associated with the password to be changed.
username	Identifies the user account associated with the password to be changed.

Chapter 19: License installation using the CLI

Install and manage a license file for the Avaya Ethernet Routing Switch 8800/8600, using the command line interface (CLI).

Installing a license file using the CLI

Install a license file on an Avaya Ethernet Routing Switch 8800/8600 to enable licensed features by performing this procedure.

Prerequisites

- You must have the license file stored on a Trivial File Transfer Protocol (TFTP) server.
- Ensure that you have the correct license file with the base MAC address of the Ethernet Routing Switch 8800/8600 that you are installing the license on. Otherwise, system does not unblock the licensed features.
- If the Ethernet Routing Switch 8800/8600 chassis has two SF/CPU modules installed, you do not need to install the license file on the secondary SF/CPU. When you enable High Availability, the primary SF/CPU copies the license vectors to the secondary SF/CPU during table synchronization and the trial period counters stop. The system copies the license file to the secondary SF/CPU when you save the configuration on the primary SF/CPU.

  In warm-standby mode, license vectors are not synchronized with the secondary SF/CPU. However, the system copies the license file to the secondary SF/CPU when you save the configuration with the save to standby flag set to true.

Procedure steps

1. Install a license file by using the following command:

   ```
   copy <a.b.c.d>:<srcfile> /flash/<destfile>
   ```

   The following is an example of copying a license file from a TFTP server to the flash on an SF/CPU module of an Avaya Ethernet Routing Switch 8800/8600:

```
ERS-8610:5# copy 10.10.10.20:bld100_8610adv.lic /flash/
bld100_8610adv.dat
```

Important:

If the license filename is license.dat and it is located in the Flash directory, then no further configuration is required. You can continue with the next step. If you changed the license filename and location, you must specify the license file path. The license name must be in lower-case characters. For more information about specifying the license file path, see Specifying the license file path and name using the CLI on page 193.

2. Load the license file to unlock the licensed features.

   ```
   config load-license
   ```

   Important:

   If the loading fails, or if the switch restarts and cannot locate a license file in the specified location, the switch cannot unlock the licensed features and reverts to base functionality.

   The following shows sample output that is displayed on the console when issuing a load-license command:

   ```
   CPU5 [05/10/08 03:26:17] SW INFO Found serial number <00:19:69:7b:
   50:00> in file </flash/license.dat>

   CPU5 [05/10/08 03:26:17] SW INFO License Successfully Loaded From
   <license.dat> License Type -- PREMIER
   ```

3. Save the configuration.

   ```
   save config
   ```

Variable definitions

Use the data in the following table to help you install a license with the `copy` command.

Variable	Value
<a.b.c.d>	Specifies the IPv4 address of the TFTP server where the license file is to be copied from.
<destfile>	Specifies the name of the license file when copied to the flash. **Important:** By default, the switch searches for a license filename of license.dat on the on-board Flash on the SF/CPU module. A license file generated for an Ethernet Routing Switch 8800/8600 can use any filename and extension. If the license filename is not license.dat, or the file is not located in the switch Flash directory, you must update the bootconfig file with the license filename and the path to its location.

Table continues…

Variable	Value
<srcfile>	Specifies the name of the license file on the TFTP server. For example, bld100_8610adv.lic or license.dat.

Specifying the license file path and name using the CLI

If you changed the license name and location when you installed the license file, you must specify the license file path to identify the storage location of the license file.

Procedure steps

1. Specify the path for the license file using the following command:

   ```
   config bootconfig choice <boot-choice> license-file <file>
   ```

2. Reboot the switch for the configuration to take effect.

Variable definitions

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

Variable	Value
<bootchoice>	Specifies the order in which the boot path is accessed when the switch is booting up: primary, secondary, or tertiary.
<file>	The source can be internal Flash memory, external memory card (PCMCIA or Flash), or a remote TFTP server. • /flash/<file_name> • /pcmcia/<file_name> • <a.b.c.d>:<file_name> **Important:** By default, the switch searches for a license filename of license.dat on the on-board Flash on the SF/CPU module. A license file generated for an Ethernet Routing Switch 8800/8600 can use any filename and extension. If the license filename is not license.dat, or the file is not located in the switch Flash directory, you must update the bootconfig file with the license filename and the path to its location.

Showing a license file using the CLI

Display the existing software licenses on your switch by performing this procedure.

Procedure steps

1. To display the existing software licenses on your switch, use the following command:

   `show license`

   For samples of the output shown with this command, see Job aid on page 194.

Job aid

The following shows two sample outputs for different licenses with the `show license` command.

```
ERS-8610:5# show license

        License file name       :    /flash/bld100_8610adv.dat
        License Type            :    ADVANCED
        MD5 of Key              :    6d97e0c5 f74a9540 1ce8bd23 570b7512
        MD5 of File             :    703c5119 d1a6bbdb e39d5fca 8984e0b8
        Generation Time         :    2008/04/10 11:22:55
        Expiration Time         :
        Base Mac Addr           :    00:04:dc:7d:64:00
        flags                   :    0x00000022 SITE MEMO
        memo                    :
Advanced License


ERS-8610:5#
```

```
ERS-8610:5# show license

        License file name       :    /flash/bld100_8610prem.dat
        License Type            :    PREMIER
        MD5 of Key              :    6d97e0c5 f74a9540 1ce8bd23 570b7512
        MD5 of File             :    548cd140 ee6e20e1 cd53e169 c1fcda4a
        Generation Time         :    2008/04/10 11:24:15
        Expiration Time         :
        Base Mac Addr           :    00:04:dc:7d:64:00
        flags                   :    0x00000022 SITE MEMO
        memo                    :
Premier License


ERS-8610:5#
```

Chapter 20: NTP configuration using the CLI

This chapter describes how to configure the Network Time Protocol (NTP) using the command line interface (CLI).

Prerequisites to NTP configuration

- Before you configure NTP, you must perform the following tasks:
  - Configure an IP interface on the Ethernet Routing Switch 8800/8600 and ensure that the NTP server is reachable through this interface. For instructions, see *Avaya Ethernet Routing Switch 8800/8600 Configuration — IP Routing, NN46205-523*.
  - Ensure the Real Time Clock is present on the SF/CPU board.

Important:

NTP server MD5 authentication does not support passwords (keys) that start with a special character or that contain a space between characters.

NTP configuration procedures

This task flow shows you the sequence of procedures you perform to configure the NTP.

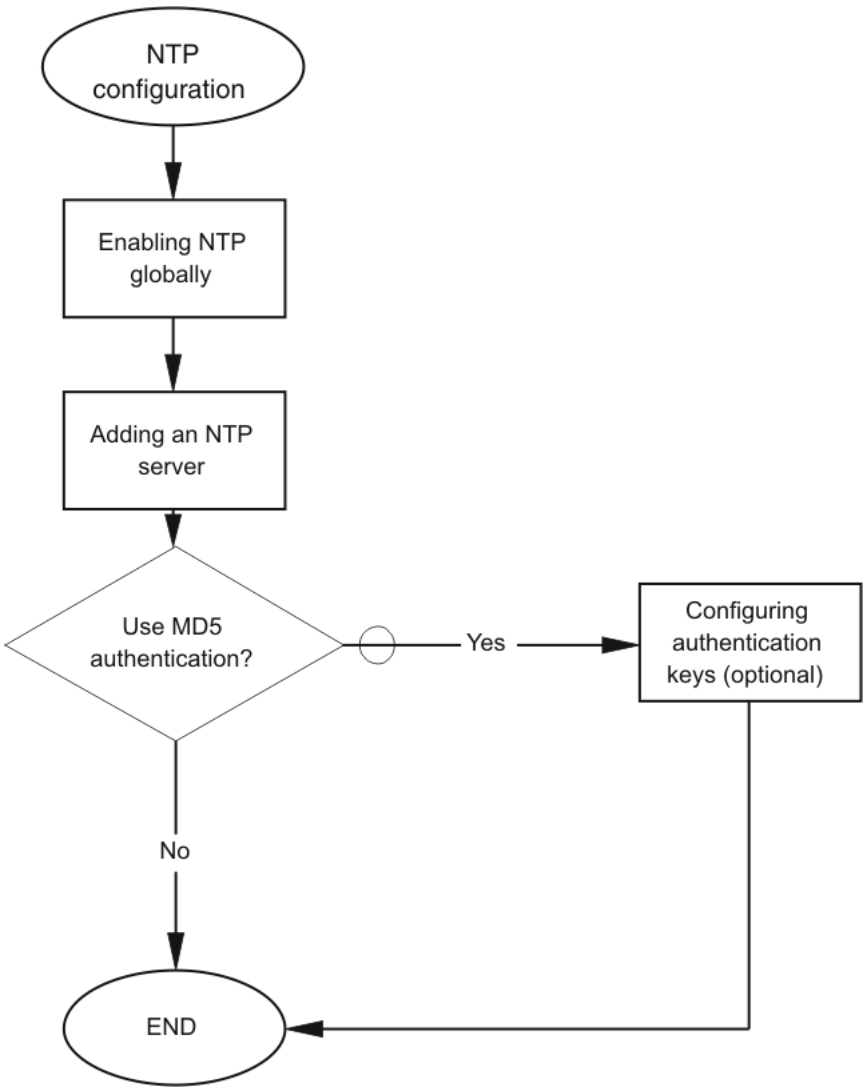


Figure 12: NTP configuration procedures

Job aid

The following table lists the commands and their parameters that you use to complete the procedures in this section.

Table 24: Job aid

Command	Parameter
config ntp	enable <true|false>

Table continues…

Command	Parameter
	info
	interval <*value*>
	ip-source-type <default | cicuitless-ip | management-virtual-ip>
config ntp key	create <*auth_key_value*> <*secret_key_value*>
	delete <*auth_key_value*>
	<*ID*>
	info
	<*IP address*>
	set <*auth_key_value*> <*secret_key_value*>
config ntp server	create <*ipaddr*> [enable <*value*>] [auth <*value*>] [key <*value*>]
	delete <*ipaddr*>
	info
	set <*ipaddr*> [enable <*value*>] [auth <*value*>] [key <*value*>]

Enabling NTP globally

Enable NTP globally. Default values are in effect for most parameters. You can customize NTP by modifying parameters. Enable NTP globally by performing this procedure.

Procedure steps

1. Enable NTP globally by using the following command:

   ```
   config ntp enable true interval <value>
   ```

Variable definitions

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

Variable	Value
enable <true|false>	Globally activates or disables NTP. The default is false.
info	Specifies current NTP settings on this NTP server.

Table continues…

Variable	Value
interval <*value*>	Specifies the time interval between successive NTP updates. *value* is the time interval expressed in minutes in a range from 10–1440. The default is 15. **Important:** If NTP is already activated, this configuration does not take effect until you disable NTP, and then reenable it.

Example of enabling NTP globally

1. Enable NTP :

```
ERS-8606:5# config ntp enable true
```

Adding an NTP server

Add an NTP server or modify existing NTP server parameters by performing this procedure.

You can configure a maximum of 10 NTP servers.

Procedure steps

1. Add an NTP server by using the following command:

```
config ntp server create <ipaddr> [enable <value>] [auth <value>]
[key <value>] [source—ip <value>]
```

Variable definitions

Use the data in the following table to use the `config ntp server create` command.

Variable	Value
ipaddr	Specifies the IP address of the NTP server.
enable <*value*>	The value *true* enables the server; the value *false* disables the NTP server. The default is true.
auth <*value*>	The value *true* enables authentication; the value *false* disables authentication. The default is false.

Table continues…

Variable	Value
key <*value*>	The authentication key *value* range is from 1–2147483647. The default value is 0, which indicates that authentication is disabled.
source-ip <*value*>	Sets the IP address as the NTP source IP address. The source IP address can be circuitless IP, management IP, management virtual IP, VLAN IP or brouter IP. To set the NTP source IP as an outgoing Interface IP, set 0.0.0.0 as the source-ip address.

Example of adding an NTP server

1. Add an NTP server:

   ```
   ERS-8606:5# config ntp server create 47.140.53.187 enable true
   ```

2. View the current configuration:

   ```
   ERS-8606:5# config ntp server
   ERS-8606:5/config/ntp/server# info

   Sub-Context:
   Current Context:
   create :
   Server Ip         Enabled     Auth      Key Id    Source IP
   47.140.53.187     true        false     1         0.0.0.0

                                       delete : N/A
                                          set : N/A
   ```

Configuring authentication keys

Configure NTP authentication keys to use MD5 authentication by performing this procedure.

Procedure steps

1. Create an authentication key by using the following command:

   ```
   config ntp key create <auth_key_value> <secret_key_value>
   ```

2. Enable MD5 authentication for the server by using the following command:

   ```
   config ntp server set <IP address> auth true
   ```

3. Assign an authentication key to the server by using the following command:

   ```
   config ntp server set <IP address> key <ID>
   ```

Variable definitions

Use the data in the following table to use the `config ntp key` command.

Variable	Value
create <*auth_key_value*> <*secret_key_value*>	Adds an MD5 authentication key entry to the list where: • *auth_key_value* is the key ID used to generate the MD5 digest. Specify a value between 1–2147483647. The default is 0. • *secret_key_value* is the MD5 key ID used to generate the MD5 digest. Specify an alphanumeric string between 0–8 characters.
delete <*auth_key_value*>	Delete an MD5 authentication key entry from the list. • *auth_key_value* is the key ID used to generate the MD5 digest.
<*ID*>	Specifies the entry ID of the authentication key to apply to the NTP server.
info	Display NTP authentication key configuration settings.
<*IP address*>	Specifies the IP address of the NTP server for which you are enabling MD5 authentication.
set <*auth_key_value*> <*secret_key_value*>	Modifies a MD5 authentication key value where: • *auth_key_value* is the key ID used to generate the MD5 digest. Specify a value between 1–2147483647. The default is 0. • *secret_key_value* is the MD5 key ID used to generate the MD5 digest. Specify an alphanumeric string between 0–8 characters.

Example of configuring an NTP authentication key

1. Create the authentication key:

   ```
   ERS-8606:5# config ntp key ERS-8606:5/config/ntp/key# create 5 18
   ```

2. Enable MD5 authentication for the NTP server:

   ```
   ERS-8606:5#
   config ntp server set 47.140.53.187 auth true
   ```

3. Assign an authentication key to the NTP server:

   ```
   ERS-8606:5/config/ntp/server#
   ```

```
set 47.140.53.187 key 5
```

Configuring the NTP source IP address

Use the following procedure to configure the NTP source IP address. You can specify a circuitless IP (CLIP) IP, a Management Virtual IP, or continue using the outgoing interface IP address (default).

Procedure steps

1. Configure the NTP source IP address by using the following command:

   ```
   config ntp server set <ipaddr> [source-ip <value>]
   ```

2. Verify your configuration:

   ```
   show ntp server config
   ```

Variable definitions

Use the data in the following table to use the `config ntp server set` command.

Variable	Value
ipaddr	Specifies the IP address of the NTP server.
source-ip <*value*>	Sets the IP address as the NTP source IP address. The source IP address can be circuitless IP, management IP, management virtual IP, VLAN IP or brouter IP. To set the NTP source IP as an outgoing Interface IP, set 0.0.0.0 as the source-ip address.

Chapter 21: DNS configuration using the CLI

This chapter describes how to configure the Domain Name Service (DNS) client using the command line interface (CLI).

Job aid

The following table lists the commands and their parameters that you use to complete the procedures in this section.

Table 25: Job aid

Command	Parameter
config sys dns	info
	delete <primary|secondary|tertiary>
	domain-name <*domain-name*>
	primary-create <*IPAddress*|*IPv6Address*>
	secondary-create <*IPAddress*|*IPv6Address*>
	tertiary-create <*IPAddress*|*IPv6Address*>
show host <*hostname*|*ipaddress*|*ipv6address*>	
show sys dns	

Configuring the DNS client

Configure the Domain Name Service to establish the mapping between an IP name and an IP address.

You can configure connection for up to three different DNS servers—primary, secondary and tertiary. First the primary server is queried, and then the secondary, and finally the tertiary. Configure DNS client by performing this procedure.

Procedure steps

1. Configure the DNS client by using the following command:

   ```
   config sys dns domain-name <domain-name> primary-create <IPAddress|
   IPv6Address>
   ```

2. Optionally, add addresses for additional DNS servers by using the following command:

   ```
   config sys dns domain-name <domain-name> secondary-create
   <IPAddress|IPv6Address> tertiary-create <IPAddress|IPv6Address>
   ```

3. View the DNS client system status by using the following command:

   ```
   show sys dns
   ```

Variable definitions

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

Variable	Value
delete <primary| secondary|tertiary>	Deletes the IP address of the specified primary, secondary, or tertiary DNS server.
domain-name <*domain-name*>	Configures the default domain name. • *domain-name* is a string 0–255 characters.
info	Specifies the list of DNS servers, with the status (active/inactive).
primary-create <*IPAddress*|*IPv6Address*>	Configures the primary DNS server address. • *IPAddress* in a.b.c.d format configures the IP address • *IPv6Address* in hexadecimal format (string length 0–46) configures the IPv6 address
secondary-create <*IPAddress*|*IPv6Address*>	Configures the secondary DNS server address. • *IPAddress* in a.b.c.d format configures the IP address • *IPv6Address* in hexadecimal format (string length 0–46) configures the IPv6 address
tertiary-create <*IPAddress*|*IPv6Address*>	Configures the tertiary DNS server address. • *IPAddress* in a.b.c.d format configures the IP address • *IPv6Address* in hexadecimal format (string length 0–46) configures the IPv6 address

Job aid

Figure 13: Job aid on page 204 shows sample output for the `show sys dns` command.

```
ERS-8606:5# show sys dns
    DNS Default Domain Name :
    Primary DNS server details:
    ===========================
         IP address : 10.10.10.0
         Status     : Inactive
         Total DNS Number of request made to this server : 0
         Number of Successful DNS : 0
    Secondary DNS server details:
    ===========================
         IP address : 20.20.20.0
         Status     : Inactive
         Total DNS Number of request made to this server : 0
         Number of Successful DNS : 0
    Tertiary DNS server details:
    ===========================
         IP address : 30.30.30.0
         Status     : Inactive
         Total DNS Number of request made to this server : 0
         Number of Successful DNS : 0
```

Figure 13: Job aid

Querying the DNS host

Query the DNS host for information about host addresses.

You can enter either a hostname or an IP address. If you enter the hostname, this command shows the IP address corresponding to the hostname and if you enter an IP address, this command shows the hostname for the IP address. Query the DNS host by performing this procedure.

Procedure steps

1. View the host information by using the following command:

   `show host` <*hostname*|*ipaddress*|*ipv6address*>

Variable definitions

Use the data in the following table to use the `show host` command.

Variable	Value
hostname	Specifies the name of the host DNS server as a string of 0–255 characters.
ipaddress	Specifies the IP address of the host DNS server in a.b.c.d format.
ipv6address	Specifies the IPv6 address of the host DNS server in hexadecimal format (string length 0–46).

Job aid

Figure 14: Job aid on page 205 shows sample output for the `show host` command.

```
ERS-8606:5# show host ipksun05
        Host Name        : ipksun05
        Host IP Address  : 198.202.188.174
ERS-8606:5#

ERS-8606:5# show host 196.1.196.79
        Host Name        : bgp.accelar.wall.com
        Host IP Address  : 196.1.196.79
```

Figure 14: Job aid

Chapter 22: Multicast group ID reservation using the CLI

This chapter provides procedures to create multicast group ID (MGID) reservations using the command line interface (CLI).

Job aid

The following table lists the commands and their parameters that you use to complete the procedures in this section.

Table 26: Job aid

Command	Parameter
config sys set max-vlan-resource-reservation	`<enable|config sys set multicast-resource-reservation <value>disable>`
`config sys setconfig sys set multicast-resource-reservation <value> multicast-resource-reservation` *<value>*	

Enabling maximum VLAN mode

Enable maximum VLAN mode to use all available MGIDs for VLANs. No IP multicast (IPMC) traffic transmits if you enable maximum VLAN mode. Enable maximum VLAN mode by performing this procedure.

Procedure steps

1. Enable maximum VLAN mode by using the following command:

   ```
   config sys set max-vlan-resource-reservation enable
   ```

Reserving MGIDs for IPMC

Reserve MGIDs for IPMC to increase the number of IPMC traffic streams supported on the system by performing this procedure.

Procedure steps

1. Reserve MGIDs for IPMC by using the following command:

   ```
   config sys set multicast-resource-reservation <value>
   ```

Variable definitions

Use the data in the following table to use the`config sys set multicast-resource-reservation` command.

Variable	Value
value	Specifies the number of MGIDs to reserve for IPMC traffic. Select from the range of 64–4083. The default value is 2048.

Chapter 23: Operational procedures using the CLI

This chapter describes common operational procedures that you use while configuring and monitoring the Avaya Ethernet Routing Switch 8800/8600 operations.

Job aid

The following table lists the commands and their parameters that you use to complete the procedures in this section.

Table 27: Job aid

Command	Parameter
boot	*<file>*
	config <*value*>
	-y
config sys set action	cpuswitchover
	info
	resetconsole
	resetcounters
	resetmodem
md5	wildcard (*)
	-f <*checksum-file-name*>
	-r
	-a
	-c
peer <*operation*>	
ping	count <*value*>

Table continues…

Command	Parameter
	-d
	datasize <*value*>
	<*HostName/ipv4address/ipv6address*>
	-l
	-s
	scopeid <*value*>
	-t
	vrf <*WORD 0–64*>
reset	
save <*savetype*>[file <*value*>*]*	verbose
	standby <*value*>
	backup <*value*>
source <*file*>	stop
	debug
	syntax

Saving the boot configuration to a file

Save a boot configuration to a file to retain the configuration settings by performing this procedure. You can configure the switch to load a specific configuration file.

Caution:

Risk of data loss

If a Personal Computer Memory Card International Association (PCMCIA) card is removed before a write operation is complete, the file can contain a corrupted end of file (EOF) marker. Before removing the PCMCIA card, execute the command line interface (CLI) command **`stop-pcmcia`**.

Prerequisites

- Some PCMCIA cards become file allocation table (FAT) corrupted after you insert them into the PC-card slot. If this situation occurs, format or repair the FAT on the card.
- The boot configuration file must be named boot.cfg for the system to boot using it.
- To save a file to the standby SF/CPU, you must enable Trivial File Transfer Protocol (TFTP) on the standby SF/CPU.

Procedure steps

1. Save the configuration by using the following command:

   ```
   save <savetype> [file <value>] [verbose] [standby <value>] [backup
   <value>]
   ```

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: • [a.b.c.d]:<file> • peer/<file> • /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.
savetype	Specifies what to save. Values for this parameter include: • config • bootconfig • log • trace • clilog
standby *<value>*	Saves the specified file name to the standby SF/CPU in the following format for *value*: • filename, /pcmcia/ <file>

Table continues…

Variable	Value
	• /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 changed.

Example of saving the boot configuration to a file

1. Save a boot configuration file as a backup file by using the following command:

   ```
   save bootconfig file boot.cfg backup2
   ```

Restarting the switch

Restart the switch to implement configuration changes or recover from a system failure. When you restart the system, you can specify the boot source (flash, PCMCIA card, or TFTP server) and file name. If you do not specify a device and file, the run-time CLI uses the software and configuration files on the primary boot device that is defined by the Boot Monitor **`choice`** command.

After the switch restarts normally, a cold trap is sent within 45 seconds after a restart. If a single strand fiber (SSF) switchover occurs, a warm-start management trap is sent within 45 seconds of a restart. Restart the switch by performing this procedure.

Procedure steps

1. Restart the switch by using the following command:

   ```
   boot [<file>] [config <value>] [-y]
   ```

   Important:

   Entering the **`boot`** command with no arguments causes the switch to start using the current boot choices defined by the **`choice`** command (next).

Variable definitions

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

Variable	Value
config <value>	Specifies the software configuration device and file name in the format: *[a.b.c.d:]<file>* /pcmcia/*<file>* / flash/*<file>*. The file name, including the directory structure, can include up to 99 characters.
file	Specifies the software image device and file name in the format: *[a.b.c.d:] <file>* /pcmcia/*<file>* /flash/ *<file>*. The file name, including the directory structure, can include up to 99 characters.
-y	Suppresses the confirmation message before the switch restarts. If you omit this parameter, you are asked to confirm the action before the switch restarts.

Resetting the switch

Reset the switch to reload system parameters from the most recently saved configuration file by performing this procedure.

Procedure steps

1. Reset the switch by using the following command:

   ```
   reset
   ```

Accessing the standby SF/CPU

Access the standby SF/CPU to make changes to the standby SF/CPU without reconnecting to the console port on that module by performing this procedure.

Prerequisites

- The Telnet daemon is activated.
- You must set an rlogin access policy on the standby SF/CPU before you can use the peer command to access it from the master SF/CPU using rlogin. To set an access policy on the standby SF/CPU, connect a terminal to the Console port on the standby SF/CPU. For more information about the access policy commands, see *Avaya Ethernet Routing Switch 8800/8600 Fundamentals — User Interfaces, NN46205-308*.

Procedure steps

1. Access the standby SF/CPU by using the following command:

   ```
   peer <operation>
   ```

Variable definitions

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

Variable	Value
operation	Specifies either Telnet or remote login (rlogin).

Pinging an IP device

Ping a device to test the connection between the Ethernet Routing Switch 8800/8600 and another network device. After you ping a device, an Internet Control Message Protocol (ICMP) packet is sent from the switch 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 that the specified IP address is alive. If no reply is received, the message indicates that the address is not responding. Ping an IP device by performing this procedure.

Procedure steps

1. 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).

Table continues…

Variable	Value
datasize value	Specifies the size of ping data sent, in bytes, as follows: • 16–4076 for IPv4 • 16–65487 for IPv6
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).
-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 time-out value in seconds (1–120) (for IPv4).
vrf <*WORD 0–64*>	Specifies the VRF name from 0–64 characters.

Calculating the MD5 digest

Calculate the MD5 digest to verify the MD5 checksum. The **`md5`** command calculates the MD5 digest for files on the switch flash or PCMCIA and either displays the output on screen or stores the output in a file that you specify. An MD5 command option compares the calculated MD5 digest with that in a checksum file on flash or PCMCIA, and the compared output appears on the screen. By verifying the MD5 checksum, you can verify that the file transferred properly to the switch. This command is available from both the boot monitor and runtime CLI.

The MD5 file, **`p80a5000.md5`**, is provided with the Release 5.0 software. This contains the MD5 checksums of all software Release 5.0 files. Calculate the MD5 digest by performing this procedure.

Important:

If the MD5 key file parameters change, you must remove the old file and create a new file.

Prerequisites

- Use the **`md5`** command with reserved files (for example, a password file) only if you possess sufficient permissions to access these files.
- A checksum file is provided with the images for download. Transfer your image files to the switch and use the **`md5`** command to ensure that the checksum of the images on the switch is the same as the checksum file.

Procedure steps

1. Calculate the MD5 digest by using the following command:

   ```
   md5 <filename>
   ```

Variable definitions

Use the data in the following table to use the `md5` command.

Variable	Value
wildcard *(*)*	Calculates the MD5 checksum of all files.

-f *<checksum-file-name>*	Stores the result of MD5 checksum to a file on flash or PCMCIA.
	If the output file specified with the -f option is one of the following:
	• reserved filenames on the switch, the command fails with the error message:
	`Error: Invalid operation.`
	• files for which MD5 checksum is to be computed, the command fails with the error message:
	`Ethernet Routing Switch-8610:5# md5 *.cfg -f config.cfg`
	`Error: Invalid operation on file <filename>`
	If the checksum filename specified by the -f option exists on the switch (and is not one of the reserved filenames), the following message appears on the switch:
	`File exists. Do you wish to overwrite? (y/n)`

-r	Reverses the output. Use with the **`-f`** option to store the output to a file. The -r option cannot be used with the -c option.
-a	Adds data to the output file instead of overwriting it. You cannot use the -a option with the -c option.
-c	Compares the checksum of the specified file by *<filename>* with the MD5 checksum present in the checksum file name. You can specify the checksum

Table continues…

Variable	Value
	file name using the -f option. If the checksum filename is not specified, the file /flash/checksum.md5 is used for comparison. If the supplied checksum filename and the default file are not available on flash, the following error message appears: Error: Checksum file <*filename*> not present. The -c option also: • calculates the checksum of files specified by *filename* • compares the checksum with all keys in the checksum file, even if filenames do not match • displays the output of comparison

Resetting system functions

Reset system functions to reset all statistics counters, the modem port, the console port, and the operation of the switchover function by performing this procedure.

Procedure steps

1. Reset system functions by using the following command:

   ```
   config sys set action
   ```

Variable definitions

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

Variable	Value
cpuswitchover	Resets the switch to change over to the backup SF/CPU.
info	Specifies the current settings for system actions.
resetconsole	Reinitializes the hardware universal asynchronous receiver transmitter (UART) drivers. Use this command only if the console or modem connection is hung.
resetcounters	Resets all the statistics counters in the switch to zero.
resetmodem	Resets the modem port.

Example of resetting system functions

1. Reset the switch to change over to the backup SF/CPU:

   ```
   ERS-8606:5# config sys set action cpuswitchover
   ```

2. Reset the statistics counters:

   ```
   ERS-8606:5# config sys set action resetcounters Are you sure you want
   to reset system counters (y/n)? y
   ```

3. Display information about the system function:

   ```
   Trusted 4:5# config sys set action info

   Sub-Context: clear config dump monitor mplsping mplstrace peer show
   switchover test trace Current Context: cpuswitchover : (N/A)
   resetconsole : (N/A) resetcounters : (N/A) resetmodem : (N/A)
   ERS-8606:5#
   ```

N/A displayed in a command output indicates that the information is Not Available or Not Applicable.

Sourcing a configuration

Source a configuration to merge a script file into the running configuration by performing this procedure.

Procedure steps

1. Source a configuration by using the following command:

   ```
   source <file> [stop] [debug] [syntax]
   ```

Variable definitions

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

Variable	Value
debug	Debugs the script output.
file	Specifies a filename and location from 1–99 characters. Use the format {a.b.c.d:|peer:|/pcmcia/|/flash/}<file>

Table continues…

Variable	Value
stop	Stops the merge after an error occurs.
syntax	Verifies the script syntax.

Chapter 24: CLI show command reference

This reference information provides show commands to view the operational status of the Avaya Ethernet Routing Switch 8800/8600.

Access, logon names, and passwords

Use the **show cli password** command to display the CLI access, logon name, and password combinations. The syntax for this command is as follows.

```
show cli password
```

The following figure shows output from the **show cli password** command.

```
aging     90

ACCESS    LOGIN           STATE
min-passwd-len 10

rwa       rwa             NA
rw        rw              ena
l3        l3              ena
l2        l2              ena
l1        l1              ena
ro        ro              ena

l4admin   l4admin         ena
slbadmin  slbadmin        ena
oper      oper            ena
l4oper    l4oper          ena
slboper   slboper         ena
ssladmin  ssladmin        ena
```

Figure 15: show cli password command output

All CLI configuration

Use the show command to display all relevant CLI information. The syntax for this command is as follows.

```
show cli show-all [file <value>]
```

The following table explains parameters for this command.

Table 28: Command parameters

Parameter	Description
file value	Specifies the filename to which output is redirected. Options include: • **/pcmcia/** *<file>* • **/flash/** *<file>* File is a string of 1 to 99 characters.

The following figure shows sample output.

```
================================================================================
                                  CLILog Info
================================================================================

        CLI Logging Enable    :  FALSE

        CLI Log Max File Size :  256

--------------------------------------------------------------------------------


# show cli info


cli configuration

more            : true
screen-lines    : 23

telnet-sessions : 8
rlogin-sessions : 8
timeout         : 900 seconds
monitor duration: 300 seconds
monitor interval: 5 seconds

use default login prompt    : true
default login prompt        : Login:
custom login prompt         : Login:
use default password prompt : true
default password prompt     : Password:
custom password prompt      : Password:


# show cli password


        aging     90

        ACCESS    LOGIN            STATE
        min-passwd-len 10

        rwa       rwa              NA

        rw        rw               ena
        l3        l3               ena
        l2        l2               ena
        l1        l1               ena
        ro        ro               ena

        l4admin   l4admin          ena
        slbadmin  slbadmin         ena
        oper      oper             ena
        l4oper    l4oper           ena
        slboper   slboper          ena
        ssladmin  ssladmin         ena


# show cli who

SESSION   USER               ACCESS    IP ADDRESS
Telnet0   rwa                rwa       207.179.154.61
Console                      none
Modem                        none
```

Figure 16: show cli show-all command output

Current switch configuration

Use the **show config** command to display the current switch configuration. The syntax for this command is as follows.

```
show config [verbose] [module <value>]
```

The following table explains parameters for this command.

Table 29: Command parameters

Parameter	Description
verbose	Specifies a complete list of all configuration information about the switch.
module <*value*>	**module** <*value*> specifies the command group for which you are requesting configuration settings. The options are: • cli • sys • web • rmon • vlan • port • qos • traffic-filter • mlt • stg • ip • diag • dvmrp • radius • ntp • lacp • cluster • bootp • filter • ipv6

If you make a change to the switch, it is displayed under that configuration heading. Figure 17: show config command (partial output) on page 222 shows a subset of the output of this command.

```
Preparing to Display Configuration...
#
# TUE NOV 06 02:30:52 2007 UTC
# box type             : ERS-8006
# software version     : REL4.2.0.0_B117
# monitor version      : 4.2.0.0/117
# cli mode             : 8600 CLI
#

#
# Asic Info :
# SlotNum|Name    |CardType  |MdaType    |Parts Description
#
# Slot  1   --     0x00000001 0x00000000
# Slot  2 8630GBR  0x2432511e 0x00000000  RSP=25 CLUE=2 F2I=1 F2E=1 FTMUX=17 CC=
3 FOQ=266 DPC=184 BMC=776 PIM=257 MAC=4
# Slot  3   --     0x00000001 0x00000000
# Slot  4   --     0x00000001 0x00000000
# Slot  5 8692SF   0x200e0100 0x00000000  CPU: CPLD=19 MEZZ=4  SFM: OP=3 TMUX=2
SWIP=23 FAD=16 CF=168
# Slot  6   --     0x00000001 0x00000000
#
#!flags m-mode false
#!flags enhanced-operational-mode false
#!flags vlan-optimization-mode false
#!flags global-filter-ordering false

#!flags r-mode true
#!resource-reservation max-vlan false
#!resource-reservation multicast 2000
#!flags multicast-check-packet true
#!flags system-monitor false
#!record-reservation filter 4096
#!record-reservation ipmc 500
#!record-reservation local 2000
#!record-reservation mac 2000
#!record-reservation static-route 200
#!record-reservation vrrp 500
#!system-monitor monitoring-enable true
#!system-monitor detection-time 30
#!power enable true
#!power slot-priority 1 high
#!power slot-priority 2 high
#!power slot-priority 3 high
#!power slot-priority 4 high
#!end
#
config

#

--More-- (q = quit)
```

Figure 17: show config command (partial output)

If you add **verbose** to the **show config** command, the output contains current switch configuration including software (versions), performance, VLANs (such as numbers, port members), ports (such as type, status), routes, OSPF (such as area, interface, neighbors), memory, interface, and log and trace files. With the verbose command, you can view the current configuration and default values.

Note:

The switch does not display all SNMPv3 target parameters when you enter the **show config** command. This is the expected behavior.

CLI settings

Use the **show cli info** command to display information about the CLI configuration. The syntax for this command is as follows.

```
show cli info
```

The following figure shows sample output from the **show cli info** command.

```
cli configuration

more            : true
screen-lines    : 23
telnet-sessions : 8
rlogin-sessions : 8
timeout         : 900 seconds
monitor duration: 300 seconds
monitor interval: 5 seconds

use default login prompt    : true
default login prompt        : Login:
custom login prompt         : Login:
use default password prompt : true
default password prompt     : Password:
custom password prompt      : Password:
```

Figure 18: show cli info command output

Hardware information

Use the **show sys info** command to display system status and technical information about the switch hardware components. The command displays several pages of information, including general information about the system (such as location), chassis (type, serial number, and base MAC address), temperature, power supplies, fans, cards, system errors, port locks, topology status, and message control information.

Important:

The user interfaces vary in how they identify and describe the system and chassis information. While the system description for your Ethernet Routing Switch 8800 correctly identifies the switch as an 8800 Series, the chassis information can identify the chassis as an 8010 or an 8006. The system description is correct. Use the **show tech** or **show sys info** command using CLI to find the system description for your Ethernet Routing Switch 8600 or 8800 Series switch.

The syntax for this command is as follows.

```
show sys info [card] [asic] [mda] [gbic]
```

The following table explains parameters for this command.

Table 30: Command parameters

Parameter	Description
info	Specifies the current settings.
card	Specifies information about all the installed modules.
asic	Specifies information about the application-specific integrated circuit (ASIC) installed on each module.

Table continues…

Parameter	Description
mda	Specifies information about installed media dependent adapters (MDA).
gbic	Specifies information about installed gigabit interface converters (GBIC).

The following figure shows partial output from the **show sys info** command.

```
General Info :

        SysDescr     : ERS-8606 (4.2.0.0)
        SysName      : ERS-8606
        SysUpTime    : 14 day(s), 21:48:39
        SysContact   : rick.dean@innovatia.net
        SysLocation  : Saint John, T3

Chassis Info :

        Chassis      : 8006
        Serial#      : SSNM0600Q2
        HwRev        : A
        H/W Config   :
        NumSlots     : 6
        NumPorts     : 30
        GlobalFilter: enable
        VlanBySrcMac: disable
        Ecn-Compatib: enable
        WsmDirectMode : disable
        max-vlan-resource-reservation : (disable) -> (disable)
        multicast-resource-reservation : (2000) -> (2000)
        BaseMacAddr : 00:80:2d:c1:34:00
        MacAddrCapacity : 1024
        Temperature : 23 C
        MgmtMacAddr : 00:80:2d:c1:37:f4
        System MTU  : 9600
        clock_sync_time : 60

Power Supply Info :

        Ps#1 Status       : up
        Ps#1 Type         : ac
        Ps#1 Description  : 8001 690W 110/220V AC Power Supply
        Ps#1 Serial Number: ARTS010313
        Ps#1 Version      : A
        Ps#1 Part Number  : 202067

        Ps#2 Status       : empty

        Ps#3 Status       : down
        Ps#3 Type         : Unknown
        Ps#3 Description  : UNKNOWN
        Ps#3 Serial Number:
        Ps#3 Version      :
        Ps#3 Part Number  :

Power Usage Info :
        Total Power Available : 690
        Total Power Usage     : 265

Fan Info :

        Fan#1: up, air temp: 22 C

Card Info :

        Slot#         FrontType  FrontHw    Oper   Admin  BackType   BackHw
                                 Version  Status  Status           Version
            2  30X1000BaseX-SFP       02      up      up      DPM3        03
            5               CPU       01      up      up      FSFM        02

MezzCard Info :

        Slot#5: MezzCard is running Admin status: enabled  Oper Status: up

System Error Info :
```

Figure 19: show sys info command (partial output)

Memory size for secondary CPU

Use the **show boot info** command to display the secondary CPU DRAM memory size, in hexadecimal format.

The syntax for the command is as follows: **show boot info**

Example of show boot info command output

Following is an example of the screen output for the **show boot info** command.

```
ERS-8606:5# show boot info
CPU Slot 5: PMC280-B-MV-B-MPC7447A (1.1)
Version: 5.1.0.0/022
Memory Size: 0x10000000
```

MTU for all ports

Use the **show port info** command to display the MTU values for all ports on the chassis. The syntax for this command is as follows.

```
show port info all
```

The following figure shows partial output for this command.

```
================================================================================
                              Port Interface
================================================================================

PORT                          LINK  PORT          PHYSICAL          STATUS
NUM   INDEX DESCRIPTION       TRAP  LOCK     MTU  ADDRESS           ADMIN  OPERATE
--------------------------------------------------------------------------------
2/1   128   GbicNone         true  false    9600 00:80:2d:c1:34:40 up     up
2/2   129   GbicNone         true  false    9600 00:80:2d:c1:34:41 up     up
2/3   130   GbicNone         true  false    9600 00:80:2d:c1:34:42 up     up
2/4   131   GbicNone         true  false    9600 00:80:2d:c1:34:43 up     up
2/5   132   GbicNone         true  false    9600 00:80:2d:c1:34:44 up     up
2/6   133   GbicNone         true  false    9600 00:80:2d:c1:34:45 up     up
2/7   134   GbicNone         true  false    9600 00:80:2d:c1:34:46 up     up
2/8   135   GbicNone         true  false    9600 00:80:2d:c1:34:47 up     up
2/9   136   GbicNone         true  false    9600 00:80:2d:c1:34:48 up     up
2/10  137   GbicNone         true  false    9600 00:80:2d:c1:34:49 up     up
2/11  138   GbicNone         true  false    9600 00:80:2d:c1:34:50 up     up
2/12  139   GbicNone         true  false    9600 00:80:2d:c1:34:51 up     up
2/13  140   GbicNone         true  false    9600 00:80:2d:c1:34:52 up     up
2/14  141   GbicNone         true  false    9600 00:80:2d:c1:34:53 up     up
2/15  142   GbicNone         true  false    9600 00:80:2d:c1:34:54 up     up
```

Figure 20: show port info all command (partial output)

NTP show commands

NTP global status

Use the `show ntp info` command to display the NTP administrative status, interval setting, and source IP address. The syntax for this command is as follows:

```
show ntp info
```

To display all the configured NTP information on the switch, use the `show ntp show-all` command.

NTP key status

Use the `show ntp key config` command to display the NTP key status. The syntax for this command is as follows:

```
show ntp key config
```

NTP server status

Use the `show ntp server` command to display the NTP server status. The syntax for this command is as follows:

```
show ntp server config
```

NTP statistics

Use the `show ntp server stat` command to view the following information:

- Stratum
- Version
- Sync Status
- Reachability
- Root Delay
- Precision
- Access Attempts — Number of NTP requests sent to this NTP server
- Server Synch — Number of times this NTP server updated the time
- Server Fail — Number of times this NTP server was rejected attempting to update the time

The syntax for this command is as follows.

```
show ntp server stat
```

The following figure shows sample command output.

```
                NTP Server : 134.177.216.230
-----------------------------------------
                  Stratum : 5
                  Version : 3
              Sync Status : synchronized
              Reachability: reachable
               Root Delay : 0.19053647
                Precision : 0.00003051
          Access Attempts : 1
             Server Synch : 1
              Server Fail : 0
```

Figure 21: show ntp server stat command output

Power summary

Use the **show sys power info** command to view a summary of the power information for the chassis.

The syntax for this command is as follows.

```
show sys power info
```

The following figure shows sample command output.

```
================================================================================
                          Chassis Power Information
================================================================================
Chass   TotalPS TotalPS TotalPS  TotalPS Consumed Consumed Consumed Consumed
Type    Max     Rail-3V Rail-12V Thermal Max      Rail-3V  Rail-12V Thermal
--------------------------------------------------------------------------------
8006    690     300     300      500     265      105      160      100
--------------------------------------------------------------------------------
```

Figure 22: show sys power info command output

Slot power details

Use the **show sys power slot-info** command to view detailed power information for each slot.

The syntax for this command is as follows.

```
show sys power slot-info
```

The following figure shows sample command output.

```
================================================================================
                          Slot Power Consumption
================================================================================
Slot CardType            Type  Priority    Power  Max   Rail-3V Rail-12V Thermal
No.                            (applicable Status Power Power   Power    Power
                               (only for
                               (R&RS Mod)
--------------------------------------------------------------------------------
2    8630GBR             RMod  high        ON     180   60      120      50
5    8692SF              CPU   critical    ON     85    45      40       50
--------------------------------------------------------------------------------
```

Figure 23: show sys power slot-info command output

System status (detailed)

Use the **show tech** command to display technical information about system status and information about the hardware, software, and operation of the switch.

The information available from the **show tech** command includes general information about the system (such as location), hardware (chassis, power supplies, fans, and modules), system errors, boot configuration, software versions, memory, port information (locking status, configurations, names, interface status), VLANs and STGs (numbers, port members), OSPF (area, interface, neighbors), VRRP, IPv6, RIP, PIM, PGM, and log and trace files. This command displays more information than the similar **show sys info** command.

Important:

The user interfaces vary in how they identify and describe the system and chassis information. While the system description for your Ethernet Routing Switch 8800 correctly identifies the switch as an 8800 Series, the chassis information can identify the chassis as an 8010 or an 8006. The system description is correct. Use the **show tech** or **show sys info** command using CLI to find the system description for your Ethernet Routing Switch 8600 or 8800 Series switch.

The syntax for this command is as follows.

```
show tech
```

The following figure shows representative output from the **show tech** command.

```
General Info :

        SysDescr     : ERS-8606 (4.2.0.0)
        SysName      : ERS-8606
        SysUpTime    : 14 day(s), 22:05:42
        SysContact   : rick.dean@innovatia.net
        SysLocation  : Saint John, T3

Chassis Info :

        Chassis     : 8006
        Serial#     : SSNM0600Q2
        HwRev       : A
        H/W Config  :
        NumSlots    : 6
        NumPorts    : 30
        GlobalFilter: enable
        VlanBySrcMac: disable

        Ecn-Compatib: enable
        WsmDirectMode : disable
        max-vlan-resource-reservation : (disable) -> (disable)
        multicast-resource-reservation : (2000) -> (2000)
        BaseMacAddr : 00:80:2d:c1:34:00
        MacAddrCapacity : 1024
        Temperature : 22 C
        MgmtMacAddr : 00:80:2d:c1:37:f4
        System MTU  : 9600
        clock_sync_time : 60

Power Supply Info :

        Ps#1 Status       : up
        Ps#1 Type         : ac
        Ps#1 Description  : 8001 690W 110/220V AC Power Supply
        Ps#1 Serial Number: ARTS010313
        Ps#1 Version      : A
        Ps#1 Part Number  : 202067

        Ps#2 Status       : empty

        Ps#3 Status       : down

        Ps#3 Type         : Unknown
        Ps#3 Description  : UNKNOWN
        Ps#3 Serial Number:
        Ps#3 Version      :
        Ps#3 Part Number  :

Power Usage Info :
        Total Power Available : 690
        Total Power Usage     : 265

Fan Info :

        Fan#1: up, air temp: 20 C

Card Info :

        Slot#         FrontType  FrontHw    Oper   Admin  BackType   BackHw
                                 Version  Status  Status           Version
            2  30X1000BaseX-SFP       02      up      up      DPM3        03
            5               CPU       01      up      up      FSFM        02

MezzCard Info :

        Slot#5: MezzCard is running Admin status: enabled  Oper Status: up
```

Figure 24: show tech command (partial output)

System status and parameter configuration

Use the **`show sys`** command to view current system status and parameter configuration. The syntax for this command is as follows.

```
show sys
```

The following table explains parameters for this command.

Table 31: Command parameters

Parameter	Description
`info [card] [asic] [mda] [gbic]`	Specifies system status and technical information about the switch hardware components. • **`card`** displays information about all the installed modules. • **`asic`** displays information about the ASICS installed on each module. • **`mda`** displays information about installed Media Dependent Adapters (MDA). • **`gbic`** displays information about installed Gigabit Interface Converters (GBIC).
`dns`	Specifies the DNS Default Domain Name, see Figure 25: show sys dns output on page 231.
`eapol`	Specifies the Extensible Authentication Protocol over LAN (EAPoL) settings, see Figure 26: show sys eapol output on page 231.
`ext-cp-limit`	Specifies the ext-cp-limit settings, see Figure 27: show sys ext-cp-limit output on page 232.
`force-msg`	Specifies the message control force message pattern settings, see Figure 28: show sys force-msg output on page 232.
`mcast-mlt-distribution`	Specifies the settings for multicast over MultiLink Trunking (MLT), see Figure 29: show sys mcast-mlt-distribution output on page 232.
`mcast-software-forwarding`	Specifies the settings for multicast software forwarding, see Figure 30: show sys mcast-software-forwarding output on page 232.
`msg-control`	Specifies the system message control function status (activated or disabled), see Figure 31: show sys msg-control output on page 232.
`perf`	Specifies system performance information, such as CPU utilization, switch fabric utilization, Non-Volatile Random Access Memory (NVRAM) size, and NVRAM used. The information is updated once a second, so it is no more than one second from real time, see Figure 32: show sys perf output on page 233.
`power`	Specifies chassis power summary, power supply information, and power information per slot basis. Options are: • **`info`**—chassis power summary

Table continues…

Parameter	Description
	• **power-supply-info**—power information for each power supply • **slot-info**—power information for each slot
record-reservation	Specifies the number of reserved records and usage information for each record type. Record types include filter, IP multicasting (IPMC), MAC, and static route, see Figure 33: show sys record-reservation output on page 233.
sw	Specifies the version of software running on the switch, the last update of that software, and the Boot Config Table. The Boot Config Table lists the current system settings and flags, see Figure 34: show sys sw output on page 233.
topology	Specifies the topology table. This table shows the information that is sent to Enterprise Network Management System for creating network displays, see Figure 35: show sys topology output on page 234.

The following figure shows output from the **show sys dns** command.

```
DNS Default Domain Name : ERS8600SJ
Primary DNS server details:
===========================
         IP address : 1111:0:0:0:0:0:0:1
         Status     : Inactive
         Total DNS Number of request made to this server : 0
         Number of Successful DNS : 0
Secondary DNS server details:
===========================
         IP address : 2222:0:0:0:0:0:0:1
         Status     : Inactive
         Total DNS Number of request made to this server : 0
         Number of Successful DNS : 0
Tertiary DNS server details:
===========================
         IP address : 3333:0:0:0:0:0:0:1
         Status     : Inactive
         Total DNS Number of request made to this server : 0
         Number of Successful DNS : 0
```

Figure 25: show sys dns output

The following figure shows output from the **show sys eapol** command.

```
        eap : disabled
sess-manage : false
```

Figure 26: show sys eapol output

The following figure shows output from the **show sys ext-cp-limit** command.

```
Sub-Context: clear config dump monitor mplsping mplstrace show switchover test t
race wsm asfm sam
Current Context:

        extcplimit           : disable
        max-ports-to-check   : 0
        min-congestion-time  : 3000
        port-congestion-time : 5
        trap-level           : None
```

Figure 27: show sys ext-cp-limit output

The following figure shows output from the **show sys force-msg** command.

```
================================================================================
                      Message Control Force Msg Patterns
================================================================================

                INDEX         PATTERN

--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
```

Figure 28: show sys force-msg output

The following figure shows output from the **show sys mcast-mlt-distribution** command.

```
================================================================================
                          Mcast over MLT Global Group
================================================================================
McastOverMLtStat              :disabled
GrpMask                       :255.255.255.255
SrcMask                       :255.255.255.255
Redistribution                :disabled
```

Figure 29: show sys mcast-mlt-distribution output

The following figure shows output from the **show sys mcast-software-forwarding** command.

```
================================================================================
                           Mcast Software Forwarding
================================================================================
McastSoftwareForwarding       :disabled
```

Figure 30: show sys mcast-software-forwarding output

The following figure shows output from the **show sys msg-control** command.

```
Message Control Info :
        action                : suppress-msg
        control-interval      : 5
        max-msg-num           : 5
        status                : disable
```

Figure 31: show sys msg-control output

The following figure shows output from the **show sys perf** command.

```
              CpuUtil: 12%
     SwitchFabricUtil: 0%
OtherSwitchFabricUtil: 0%
           BufferUtil: 0%
              DramSize: 512 M
              DramUsed: 28 %
              DramFree: 373873 K
```

Figure 32: show sys perf output

The following figure shows output from the **show sys record-reservation** command.

```
================================================================================
                              HW Record Reservation
================================================================================

Record Type       Used Reserved New-Reserved Def-Reserved
--------------------------------------------------------------------------------
filter               2     4096         4096         4096
ipmc                 0      500          500          500
local                6     2000         2000         2000
mac                 65     2000         2000         2000
static-route         0      200          200          200
vrrp                 0      500          500          500
--------------------------------------------------------------------------------
TOTAL               73     9296         9296         9296
```

Figure 33: show sys record-reservation output

The following figure shows output from the **show sys sw** command.

```
System Software Info :

Default Runtime Config File : /flash/config.cfg
Default Boot Config File : /flash/boot.cfg
Config File :
Last Runtime Config Save : MON NOV 05 22:24:07 2007
Last Runtime Config Save to Slave : 0
Last Boot Config Save : 0
Last Boot Config Save on Slave : 0

Boot Config Table
Slot# : 5
Version : Build REL4.2.0.0_B117 on Thu Oct 11 19:39:45 EDT 2007
LastBootConfigSource : /flash/boot.cfg
LastRuntimeImageSource : /flash/p80a4200b117.img
LastRuntimeConfigSource : /flash/config.cfg
PrimaryImageSource : /flash/p80a4200b117.img
PrimaryConfigSource : /flash/config.cfg
SecondaryImageSource : /flash/p80a4200.img
SecondaryConfigSource : /flash/config.cfg
TertiaryImageSource : 0.0.0.0:
TertiaryConfigSource : /flash/config.cfg

LastRunTimeMezzSource: /flash/mezz.img
EnableAutoBoot : true
EnableFactoryDefaults : false
EnableDebugMode : false
EnableHwWatchDogTimer : true
EnableRebootOnError : true
EnableTelnetServer : true
EnableRloginServer : false
EnableFtpServer : true
EnableTftpServer : true
EnableMezz : true

DLD software:
Slot#  2: file /flash/p80j4200.dld version 4.2.0.0/117
```

Figure 34: show sys sw output

The following figure shows output from the **show sys topology** command.

```
================================================================================
                                Topology Table
================================================================================
Local                                                                      Rem
Port  IpAddress       SegmentId MacAddress   ChassisType      BT LS  CS   Port
--------------------------------------------------------------------------------
0/0   2.2.2.2         0x000000  00802dc13400 ERS8606          12 Yes HtBt  0/0
```

Figure 35: show sys topology output

Job aid

Field	Description
Local Port	Specifies the local port number.
IP Address	Specifies the IP address.
Segment Id	
MACAddress	Specifies the MAC address of the system.
ChassisType	Specifies the type of chassis.
BT	Back Lane Type
LS	Specifies the local segment as yes or no.
CS	Specifies the current state as one of the following: • HtBt (Heartbeat)—topology has not changed. • New— the sending agent is in a new state.
Rem Port	

Users logged on

Use the **show cli who** command to display a list of users who are logged on to the switch. The syntax for this command is as follows.

```
show cli who
```

The following figure shows output from the **show cli who** command.

```
SESSION   USER              ACCESS    IP ADDRESS
Telnet1   rwa               rwa       207.179.154.87
Console                     none
Modem                       none
```

Figure 36: show cli who command output

Chapter 25: Boot parameter configuration using the ACLI

Use the procedures in this section to configure and manage the boot monitor using the Avaya command line interface (ACLI).

Prerequisites to boot parameter configuration

- You initiate a boot monitor session only through a direct serial-port connection to the switch. After the boot monitor is active, you can set the flags for Telnet and rlogin to allow remote access, but access to the boot monitor is still only available through a direct serial-port connection. Within the boot monitor, you can change the boot configuration, including boot choices and boot flags.
- To perform the procedures in this section, you must log on to the Global Configuration mode in the ACLI. For more information about using ACLI, see *Avaya Ethernet Routing Switch 8800/8600 User Interface Fundamentals, NN46205-308*.

Job aid

The following table lists the commands and their parameters that you use to complete the procedures in this section.

Table 32: Job aid

Command	Parameter
Privileged EXEC mode	
show boot config	bootp
	choice
	cli
	flags
	general

Table continues…

Command	Parameter
	host
	master
	mezz-image
	parity-errors
	running-config
	sio
	tz
Global Configuration mode	
boot config choice	<primary|secondary|tertiary>
	backup-config-file <*file*>
	config-file <*file*>
	image-file <*file*>
	license-file <*file*>
boot config cli	more
	prompt <*value*>
	screenlines <*value*>
	timeout <*seconds*>
boot config flags	alt-led
	autoboot
	block-snmp
	block-warmstandby-switchover
	control-record-optimization
	daylight-saving-time
	debug-config
	debugmode
	factorydefaults
	ftpd
	ha-cpu
	hsecure
	logging
	mezz
	acli
	reboot
	rlogind
	savetostandby

Table continues…

Command	Parameter
	spanning-tree-mode
	sshd
	telnetd
	tftpd
	trace-logging
	verify-config
	wdt
	cf-pc-compat
boot config host	ftp-debug
	password
	tftp-debug
	tftp-hash
	tftp-rexmit
	tftp-timeout
	user
boot config master <*cpu-slot*>	
boot config net <*cpu-network-port*>	mgmt
	cpu2cpu
	pccard
boot config parity-errors	enable set <size> action-869XSF-disable <true|false>
boot config sio <console|modem|pccard>	8databits
	baud
	mode
	mtu
	my-ip
	peer-ip
	pppfile
	restart
	slip-compression
	slip-rx-compression
boot config slot <*slots*>	slotlist
boot config tz	dst-end
	dst-name

Table continues…

Command	Parameter
	dst-offset
	dst-start
	name
	offset-from-utc

Accessing the boot monitor

Access the boot monitor to configure and manage the boot process by performing this procedure.

Procedure steps

1. Restart the switch.
2. Interrupt the boot sequence by pressing the Enter key after the following prompt is displayed:

```
Press Enter to stop autoboot.
```

Accessing the boot monitor from the run-time environment

Access the boot monitor from the run-time environment to configure and manage the boot process by performing this procedure.

Prerequisites

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

Procedure steps

1. Configure the autoboot flag by using the following command:

   ```
   no boot config flags autoboot
   ```

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

   ```
   save bootconfig
   ```

3. Restart the switch.

Configuring the boot monitor

Configure the boot monitor to configure connection settings for ACLI sessions by performing this procedure.

Prerequisites

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

Procedure steps

1. Configure the boot monitor CLI by using the following command:

   ```
   boot config cli [more] [prompt <value>] [screenlines <value>]
   [timeout <seconds>]
   ```

2. Save the changed configuration file.
3. Restart the switch.

Variable definitions

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

Variable	Value
more	Configures scrolling for the output display. The default is true. Use the no operator to remove this configuration. To set this option to the default value, use the default operator with the command.
prompt <*value*>	Changes the boot monitor prompt to the defined string. • *value* is a string from 1–32 characters. To set this option to the default value, use the default operator with the command.
screenlines <*value*>	Configures the number of lines in the output display. • *value* is the number of lines from 1–64. To set this option to the default value, use the default operator with the command. The default is value 23.

Table continues…

Variable	Value
timeout <*seconds*>	Configures the idle timeout period before automatic logoff for ACLI sessions. • *seconds* is the timeout period, in seconds, from 0–65536. To set this option to the default value, use the default operator with the command. The default value is 900.

Modifying the boot sequence

Modify the boot sequence to prevent the switch from using the factory default settings or, conversely, to prevent loading a saved configuration file by performing this procedure.

Prerequisites

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

Procedure steps

1. Bypass the loading of the switch configuration with the following command:

   ```
   boot config flags factorydefaults
   ```

   Important:

   If the switch fails to read and load a saved configuration file after it starts, ensure you use the no operator with this command, *no boot config flags factorydefaults*, before investigating other options.

Enabling remote access services

Enable the remote access service to provide multiple methods of remote access by performing this procedure.

Prerequisites

- If you enable an rlogin flag, you must configure an access policy to specify the name of the user who can access the switch.
- 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 the type of remote access service to enable. Select from the following list: • ftpd • rlogind • sshd • telnetd • tftpd Use the no operator to remove this configuration. To set this option to the default value, use the default operator with the command.

Changing the boot source order

Change the boot source order to display or change the order in which the system accesses the boot sources (flash and PCMCIA card) by performing this procedure.

Prerequisites

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

Procedure steps

1. Change the boot order by using the following command:

   ```
   boot config choice <primary|secondary|tertiary> backup-config-file
   <file> config-file <file> image-file <file> license-file <file>
   ```

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 choice` command.

Variable	Value
backup-config-file <*file*>	Identifies the backup boot configuration file. • *file* is the device and file name, up to 255 characters including the path. To set this option to the default value, use the default operator with the command.
config-file <*file*>	Identifies the boot configuration file. • *file* is the device and file name, up to 255 characters including the path. To set this option to the default value, use the default operator with the command.
license-file <file>	Identifies the license file. • *file* is the device and file name, up to 255 characters including the path.
image-file <*file*>	Identifies the image file. • *file* is the device and file name, up to 255 characters including the path. To set this option to the default value, use the default operator with the command.
<primary|secondary|tertiary>	Lists the order in which the specified boot devices are accessed after you restart the switch. The primary source for files is the PCMCIA card, the secondary source is the onboard flash memory, and the tertiary source is the network server. The default order is to access the device specified in this command first, and then to access the onboard flash.

Example of changing the boot source order

1. Specify the configuration file in flash memory as the primary boot source:

   ```
   boot config choice primary config-file /flash/config.cfg
   ```

Shutting down external compact flash cards

Use this shutdown procedure to avoid corrupting an external compact flash card by ensuring that the card is synchronized before it is safely removed. If you do not shutdown the system first, some situations such as power cycling and hard resets might cause flash corruption. There is no risk of flash corruption if you run the **sys shutdown** command prior to a power cycle or hard reset.

System crashes might also corrupt flash cards so be sure to back up all configurations.

The command is called **sys shutdown** in the ACLI and **sys-shutdown** in the CLI. EDM does not support this command. In the ACLI, the command is in the EXEC Mode; in the CLI, the command is at the top level.

Procedure steps

1. Stop the compact flash card before you remove it by using the following command:

   ```
   dos-stop /pcmcia (on 8692 and 8895 SF/CPU)
   ```

   For backward compatibility, the **pcmcia-stop** command is still available with the 8692 SF/CPU. However, Avaya recommends using the **dos-stop /pcmcia**.

2. Dismount both internal and external file systems by shutting down the CPU.

   ```
   sys shutdown
   ```

   The following message appears on the serial console:

   ```
   It is now safe to reset, remove, or power off this CP.
   ```

3. If you suspect that a card is corrupted, enter the following command to check and optionally try to repair the file system:

   ```
   dos-chkdsk <device> [repair]
   ```

4. If you cannot repair the file system, reformat the device.

   ```
   dos-format <device>
   ```

Configuring the standby-to-master delay

Configure the standby-to-master delay to set the number of seconds a standby SF/CPU waits before trying to become the master SF/CPU. The time delay you configure applies during a cold start; it does not apply to a failover start.

Configure the standby-to-master delay by performing this procedure.

Prerequisites

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

Procedure steps

1. Configure the number of seconds by using the following command:

   ```
   boot config cli delay <seconds>
   ```

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

Configuring system flags

Set the system flags to enable flags for specific configuration settings by performing this procedure.

Important:

If *auto-trace* is activated, SF/CPU utilization increases by up to 30 percent.

Important:

After you change certain configuration parameters using the **`boot config flags`** command, you must save the changes to the configuration file and restart the switch before the changes take effect. For more information about which parameters require a switch reset, see the variable definitions table following the procedure.

Prerequisites

- If you enable the hsecure flag, you cannot enable the flags for the Web server or SSH password-authentication.
- You must log on to the Global Configuration mode in the ACLI.

Procedure steps

1. Enable system flags by using the following command:

   ```
   boot config flags <flag>
   ```

To disable a flag use the **no** operator before the flag command: **no boot config flags <flag>**.

To set a flag to the default value, use the **default** operator with the command.

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 flags` command.

Variable	Value
alt-led	Activates the alternate LED behavior. The default is false (disabled). If you change this parameter, you must reset the switch. **Important:** Do not change this parameter unless directed by Avaya.
autoboot	Enables or disables automatic use of the run-time image by the switch after reset. The default value is true (enabled). If you disable autoboot, the boot process stops at the boot monitor prompt. Disabling autoboot can facilitate debug tasks. If you change this parameter, you must reset the switch.
block-snmp	Enables or disables Simple Network Management Protocol (SNMP) management. The default value is disabled.
block-warmstandby-switchover	Enables or disables use of the secondary SF/CPU (in warm standby mode) as the primary SF/CPU if you reset the switch. • enabled—prevents use of the secondary SF/CPU (in warm standby mode) from as the primary SF/CPU if you reset the primary SF/CPU/ • disabled—designates the secondary SF/CPU in warm standby mode as the primary SF/CPU if you reset the primary SF/CPU. The default setting is disabled. If you change the block-warmstandby-switchover setting, you must reset the switch.
control-record-optimization	Enables or disables optimization of control records.

Table continues…

Variable	Value
	The default setting is false (disabled). That is, the switch creates hardware records to route Layer 3 protocol destination multicast addresses even if the corresponding protocol is disabled. **Important:** This parameter must always be set to false (disabled).
daylight-saving-time	Activates or disables Daylight Saving Time (DST) for the switch. If you enable DST you must configure the DST settings using the config bootconfig tz command. The default value is disabled.
debug-config	Activates or disables run-time debugging of the configuration file. Use one of the following variables to configure the command. • true—line by line configuration file processing displays on the console during SF/CPU initialization • false—disables run-time configuration file debug The default value is false (disabled). If you change the debug-config variable value, you must reset the switch.
debugmode	Controls whether the switch stops in debug mode following a fatal error. Debug mode provides information equivalent to the trace commands. • true (enabled)—the switch does not restart following a fatal error • false (disabled)—the switch restarts automatically following a fatal error The default value is disabled. If you change this parameter, you must reset the switch. **Important:** Do not change this parameter unless directed by Avaya.
factorydefaults	Specifies whether the switch uses the factory default settings at startup. The default value is disabled. This flag is automatically set back to the default setting after the CPU restarts. If you change this parameter, you must reset the switch.
ftpd	Activates or disables theFTP server on the switch. The default value is disabled. To enable FTP, ensure that the **`tftpd`** flag is disabled.
ha-cpu	Activates or disables High Availability (HA) mode. Switches with two SF/CPUs use HA mode to recover quickly from a failure of one of the SF/CPUs.

Table continues…

Variable	Value
	If you enable High Availability mode, the secondary SF/CPU resets to load settings from the saved boot configuration file. You must reset the primary SF/CPU after the secondary SF/CPU starting is complete. **Caution:** **Risk of service loss** Enabling HA mode can disable certain features. For more information about what features are supported with HA, see Table 5: Feature support for HA in specified software release versions on page 48.
hsecure	Activates or disables High Secure mode in the switch. The hsecure command provides the following password behavior: • 10 character enforcement • aging time • failed login attempt limitation • designated IP address filtration The default value is false (disabled). If you enable High Secure mode, you must reset the switch to enforce secure passwords. If you operate the switch in High Secure mode, the switch prompts a password change if you enter invalid-length passwords.
logging	If a PCMCIA exists in the system, you can use the logging command to activate or disable system logging to a file on the PCMCIA. The default value is true (enabled). The system names log files according to the following: • File names appear in 8.3 (xxxxxxxx.sss) format. • The first 6 characters of the file name contain the last three bytes of the chassis base MAC address. • The next two characters in the file name specify the slot number of the CPU that generated the logs. • The last three characters in the file name are the sequence number of the log file.

Table continues…

Variable	Value
	The system generates multiple sequence numbers for the same chassis and same slot if • you replace the CPU • you reinsert the CPU • the system reaches the maximum log file size
mezz	Permits or prevents the mezzanine card from starting if it is present on a SF/CPU card. If you enable mezz on a dual CPU chassis, ensure that both CPUs contain a SuperMezz card. The mezz default value is enabled. If you change this parameter, you must reset the switch. If you reset the switch with mezz enabled, ensure that the SuperMezz image resides on the switch prior to the reset.
acli	Configures the switch to use ACLI or CLI mode. After you change this parameter, you must restart the system for the change to take effect. The default value is true.
reboot	Activates or disables automatic reboot on a fatal error. The default value is activated. The reboot command is equivalent to the debugmode command. If you change the reboot variable value, you must reset the switch. **Important:** Do not change this parameter unless directed by Avaya.
rlogind	Activates or disables the rlogin and rsh server. The default value is disabled.
savetostandby	Activates or disables automatic save of the configuration or boot configuration file to the standby SF/CPU. The default value is disabled. If you operate a dual SF/CPU system, Avaya recommends that you enable this flag for ease of operation.
spanning-tree-mode <mstp|rstp|default>	Specifies the Multiple Spanning Tree Protocol (MSTP), Rapid Spanning Tree Protocol (RSTP), or default (legacy) spanning tree mode. If you do not specify a protocol, the switch uses the default mode. The default mode is rstp. If you change the spanning tree mode, you must save the current configuration and reset the switch.
sshd	Activates or disables the SSH server service. The default value is true (enabled).
telnetd	Activates or disables the Telnet server service. The default is disabled.

Table continues…

Variable	Value
	If you disable the Telnet server service in a dual SF/CPU system, the Telnet server prevents a Telnet connection initiated from the other SF/CPU.
tftpd	Activates or disables Trivial File Transfer Protocol (TFTP) server service. The default value is disabled. If you disable the TFTP server you can still copy files between the SF/CPUs.
trace-logging	Activates or disables the creation of trace logs. The default value is disabled. **Important:** Do not change this parameter unless directed by Avaya.
verify-config	Activates syntax checking of the configuration file. The default value is true (enabled). If the system finds a syntax error, it loads the factory default configuration. If you set the variable to false, the system logs syntax errors and the SF/CPU continues to source the configuration file. Avaya recommends that you set the verify-config variable to false. If you change this parameter, you must reset the switch.
wdt	Activates or disables the hardware watchdog timer monitoring a hardware circuit. The default value is activated. The watchdog timer restarts the switch based on software errors. If you change the wtd variable, you must reset the switch. **Important:** Do not change this parameter unless directed by Avaya.
cf-pc-compat	Enables the compact flash interface to be formatted in either the Windows PC compatible format or its original format. • true—formats the compact flash interface in Windows PC compatible format. • false—ensures backward compatibility with the original format. The default value is false. If you change this parameter, you must reset the switch.

Configuring the remote host logon

Configure the remote host logon to modify parameters for FTP and TFTP access. The defaults allow TFTP transfers. If you want to use FTP as the transfer mechanism, you need to change the password to a non-null value.

Configure the remote host logon by performing this procedure.

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	Activates or disables debug mode on FTP. If you enable debug mode, debug messages display on the management console screen. The default value is disabled. Use the no operator to remove this configuration. To set this option to the default value, use the default operator with the command.
password <*value*>	Configures the password to enable FTP transfers. • *value* is the password, up to 16 characters long. If you configure this password, you can use only FTP for remote host logon. **Important:** This password must match the password set for the FTP server, or the FTP operation fails. If you set the password to a non-null value, all copy operations to and from the network use FTP instead of TFTP. If the user name or password is incorrect, copy operations over the network fail.
tftp-debug	Activates or disables debug mode on TFTP/TFTPD. If you enable debug mode, debug messages display on the management console screen. The

Table continues…

Variable	Value
	default value is disabled. Use the no operator to remove this configuration. To set this option to the default value, use the default operator with the command.
tftp-hash	Activates or disables the TFTP hash bucket display. The default value is disabled. Use the no operator to remove this configuration. To set 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 from 1–120. To set this option to the default value, use the default operator with the command.
tftp-timeout <*seconds*>	Configures the TFTP timeout. The default value is 10 seconds. • *seconds* is the number of seconds from 1–120. To set 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 long. To set this option to the default value, use the default operator with the command.

Specifying the master SF/CPU

Specify the master SF/CPU to designate which SF/CPU becomes the master after the switch performs a full power cycle. Specify the master SF/CPU by performing this procedure.

Prerequisites

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

Procedure steps

1. View the current configuration for the master SF/CPU by using the following command:

   ```
   show boot config master
   ```

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

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

3. Save the changed 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, either 5 or 6, for the master SF/CPU. The default value is slot 5.

Configuring SF/CPU network port devices

Configure the network port devices to define connection settings for the port. The three network ports are:

- management port (mgmt)
- SF/CPU port (cpu2cpu)
- PCMCIA card (pccard)

Prerequisites

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

Procedure steps

1. Configure the network port by using the following command:

   ```
   boot config net <cpu-network-port>
   ```

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

Variable definitions

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

Variable	Value
<cpu-network-port>	Identifies the port using one of the following: • mgmt

Table continues…

Variable	Value
	• cpu2cpu • pccard
autonegotiate	Activates or disables autonegotiation for the port. The default value is disabled. Use the no operator to remove this configuration. To set this option to the default value, use the default operator with the command.
bootp	Activates or disables the Bootstrap Protocol (BootP) for the port. The default value is activated. Use the no operator to remove this configuration. To set this option to the default value, use the default operator with the command.
chk-src-route	Blocks traffic with no route back to the source. The default value is activated. Use the no operator to remove this configuration. To set this option to the default value, use the default operator with the command.
fullduplex	Activates or disables full-duplex mode on the specified port. The default value is activated. Use the no operator to remove this configuration. To set this option to the default value, use the default operator with the command.
ip <*ipaddr/mask*> [cpu-slot <*value*>]	Assigns an IP address/mask for the management port, SF/CPU, or PCMCIA card. Optional parameter: • cpu-slot *value* specifies the slot number to which the IP address applies. The valid options are 3, 5, or 6. If you do not specify a slot, the system assigns the IP address to the port in the currently active SF/CPU. In an 8003-R chassis, only SF/CPU slot 3 is available. **Important:** You cannot assign an address of 0.0.0.0/0.
restart	Restarts the port.
route <*netaddr*>	Configures a route for the port. *netaddr* is the IP address and mask of the network you want to reach. Use the no operator to remove this configuration.
speed <10|100>	Configures the connection speed for ports to 10 Mb/s, 100 Mb/s, or 1000 Mb/s. The default is 10 Mb/s. To set this option to the default value, use the default operator with the command.
tftp <*ipaddr*>	Specifies a TFTP server for the port. *ipaddr* is the IP address of the TFTP server.

Configuring SF/CPU serial port devices

Configure the serial port devices to define connection settings for serial ports; for example, the modem and console port .

If you configure the modem port mode as either Serial Line IP (SLIP) or Point-to-Point Protocol (PPP), you must configure additional parameters.

Caution:

Risk of service interruption

Avaya recommends that you not configure the console port mode to SLIP or PPP. The switch can display log, trace, and error messages on the console port and these messages interfere with the SLIP or PPP operation.

Prerequisites

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

Procedure steps

1. Optionally, change the default generic port settings by using the following command:

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

2. If you use PPP mode, configure PPP options by using the following command:

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

3. If you use SLIP mode, optionally change the default SLIP settings by using the following command:

   ```
   boot config sio <console|modem|pccard> [slip-compression <true|
   false>] [slip-rx-compression <true|false>]
   ```

4. Restart the port by using the following command:

   ```
   boot config sio <console|modem|pccard> restart
   ```

5. Disable the port by using the following command:

   ```
   no boot config sio <console|modem|pccard>
   ```

6. Save the changed configuration to the boot.cfg and pcmboot.cfg files.
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 (activated) or 7 (disabled) data bits for each byte for the software to interpret. The default value is 7 (disabled). Use the no operator to remove this configuration. To set this option to the default value, use the default operator with the command.
baud <*rate*>	Configures the baud rate for the port. The default value is 9600. To set 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 ASCII (American Standard Code for Information Interchange). If you are configuring the modem port, you can set the port to use either the SLIP or PPP communication mode. To set 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, from 0–2048. The default value is 0. To set 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 Ethernet Routing Switch 8800/8600, of the point-to-point link. The default value is 0.0.0.0. Avaya recommends that you use the current IP address for the management port. To set this option to the default value, use the default operator with the command.
peer-ip <*ipaddr*>	Configures the peer (the PC) IP address on the point-to-point link. The default is 0.0.0.0. The switch assigns the peer IP address to a PC that connects through the modem port if the TCP/IP properties for the PC are configured to obtain an IP address automatically. If the client uses a static IP address, the 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 set this option to the default value, use the default operator with the command.
pppfile <*file*>	Specifies the PPP configuration file that provides authentication details and options to include during the switch boot procedure. 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>. **Important:** Do not specify a PPP file name with more than 64 characters.

Table continues…

Variable	Value
	To set this option to the default value, use the default operator with the command.
restart	Shuts down and initializes the port.
slip-compression <true|false>	Activates or disables Transmission Control Protocol over IP (TCP/IP) header compression for SLIP mode. The default value is false. Use the no operator to remove this configuration. To set this option to the default value, use the default operator with the command.
slip-rx-compression <true|false>	Activates or disables TCP/IP header compression on the receive packet for SLIP mode. The default value is false. Use the no operator to remove this configuration. To set 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.

Table 33: Job aid

Option	Description
asyncmap <*value*>	Configures the async map. • *value* is the value you sprcify
chap_file <*file*>	Obtains Challenge-Handshake Authentication Protocol (CHAP) secrets from the specified file. If either peer requires CHAP authentication, you must specify a file name. If users must use the same IP address • the PAP and CHAP secret files must specify the same IP address for all users • the IP address must match the peer-ip configuration on the modem port
chap_interval <*value*>	Configures the interval for the CHAP rechallenge. • *value*, expressed in seconds, is the interval that you specify.
chap_restart <*value*>	Configures the timeout for CHAP negotiation. • *value*, expressed in seconds, is the interval that 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

Table continues…

Option	Description
	PPP connection ends, the system removes the default routing table entry.
driver_debug	Activates PPP driver debug mode.
escape_chars <*value*>	Configures the characters to escape on transmission. • *value* is the number of characters you specify.
ipcp_accept_local	Accepts the remote peer target local IP address as the target local IP address, whether the local IP address is specified or not.
ipcp_accept_remote	Accepts the remote peer IP address, whether the remote IP address is specified or not.
ipcp_max_configure <*value*>	Configures the maximum number of transmissions for IPCP configuration requests. • *value* is the number you specify
ipcp_max_failure <*value*>	Configures the maximum number of IPCP configuration negative acknowledgements (NAK). • *value* is the number you specify
ipcp_max_terminate <*value*>	Configures the maximum number of transmissions for IPCP termination requests. • *value* is the number you specify
ipcp_restart <*value*>	Configures the timeout interval for IPCP negotiation. • *value* is the interval, in seconds, that you specify
lcp_echo_failure<*value*>	Configures the maximum consecutive Link Control Protocol (LCP) echo failures. • *value* is the number that you specify
lcp_echo_interval <*value*>	Configures the interval between LCP echo requests. • *value* is the interval, in seconds, that you specify.
lcp_max_configure <*value*>	Configures the maximum number of transmissions for LCP configuration requests. • *value* is a number that you specify
lcp_max_failure <*value*>	Configures the maximum number of LCP configuration NAKs • *value* is a number that you specify
lcp_max_terminate <*value*>	Configures the maximum number of transmissions for LCP termination requests • *value* is a number that you specify
lcp_restart <*value*>	Configures the timeout for the LCP negotiation. • *value* is the interval, in seconds, that you specify

Table continues…

Option	Description
local_auth_name <*name*>	Configures the local name for authentication. • *name* is the name that you specify
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 • *value* is the number you specify
mru <*value*>	Configures the maximum receive unit (MRU) size for negotiation. • *value* is the MRU size for negotiation that you specify
mtu <*value*>	Configures the maximum transmission unit (MTU) size for negotiation. • *value* is the MTU size for negotiation that you specify
netmask <*value*>	Configures the netmask value for negotiation. • *value* is the netmask that you specify
no_acc	Disables address control compression.
no_all	Does not request or allow options.
no_asyncmap	Disables asynchronous 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. Use this option if either peer requires PAP authentication. If users must use the same IP address, you must specify the same IP address for all users in the PAP and CHAP secret files and the IP address must match the peer-ip configuration on the modem port.
pap_max_authreq <*value*>	Configures the maximum number of transmissions for PAP authentication requests. • *value* is the number you specify

Table continues…

Option	Description
pap_passwd <*password*>	Configures the password for PAP authentication with the peer. • *password* is the password you specify
pap_restart <*value*>	Configures the timeout for PAP negotiation. • *value* is the interval, in seconds, that you specify
pap_user_name <*name*>	Configures the user name for PAP authentication with the peer. • *name* is the name you specify
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. • *name* is the name you specify
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. • *value* is the number you specify

Table 34: Sample PPP file on page 259 shows example contents from a PPP file.

Table 34: 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"
```

Detecting a switch fabric failure

Use this feature to set a parity error threshold to determine if there is a switch fabric failure on the CPU. You can configure the sensitivity level of this threshold from most sensitive (8 errors) to least sensitive (50 errors). However, the detection mechanism requires at least one parity error per 500 ms on any I/O module TAP. For example, if you set 8 errors with **`boot config parity-errors set 8`**, that means at least one error must be detected per 500ms in an interval of 4 seconds. When the number of parity errors exceeds this threshold, the switch fabric is considered failed.

For more information about this feature and its limitations, see Switch fabric failure detection on page 67.

Procedure steps

1. Enable the Switch Fabric Failure Detection feature by using the following command:

   ```
   boot config parity-errors enable
   ```

2. Configure the threshold sensitivity level with the set value.

   ```
   boot config parity-errors set <size>
   ```

3. Configure the switch fabric to recover, if possible.

   ```
   boot config parity-errors action—869XSF—disable <true|false>
   ```

Variable definitions

Use the data in the following table to use the `boot config parity-errors` command.

Variable	Value
enable	Enables parity error monitoring for the switch fabric failure detection feature. **`no boot config parity-errors`** disables parity error monitoring.
set <size>	Specifies the parity error threshold. When the number of parity errors exceeds this threshold per 500 ms in a 4 second interval, it reboots the CPU if **`action-869XSF-disable`** is set to true. The range is from 8 to 50.
action-869XSF-disable <true|false>	When set to true, this action reboots the CPU into boot-monitor mode when excess parity errors are detected. The default is false.

Configuring the time zone

Set the time zone to specify the time for your location and configure settings for daylight saving.

The format for the time zone command is hours:minutes for both Daylight Savings Time (DST) offset and offset from Greenwich Mean Time (GMT); the format is minutes only in other Ethernet Routing Switch products. The input value is positive for the west side of GMT; it is negative in other commercial products.

Configure the time zone by performing this procedure.

Prerequisites

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

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 daylight saving time. You can specify the time in one of the 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. **Important:** When you modify the DST end value, the configuration does not take effect until the next DST start is reached. If the DST start is already past when the you configure the DST end, the switch waits until the following year to use the new DST end date.

Table continues…

Variable	Value
	In addition, for a valid configuration, the period between the DST start and the DST end must be greater than the configured offset time.
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). To set this option to the default value, use the default operator with the command.
dst-offset <*minutes*|*hh:mm*>	Configures the daylight saving adjustment in minutes or hours:minutes. The values range from -4:0 to 4:0 for hours:minutes and from -240 to 240 for minutes. The default, in minutes, is 60. To set this option to the default value, use the default operator with the command.
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.
name <*tz*>	Configures an abbreviated name for the local time zone name. • *tz* is the name (for example "pst" is Pacific Standard Time). To set this option to the default value, use the default operator with the command.
offset-from-utc <*minutes*| *hh:mm*>	Configures the time zone offset in minutes or hours:minutes to subtract from Universal Coordinated Time (UTC), where positive numbers mean west of Greenwich and negative numbers mean east of Greenwich. The values range from -14:0 to 14:0 for hours:minutes and from -840 to 840 for minutes. The default value is 0. To set this option to the default value, use the default operator with the command.

Displaying the boot monitor configuration

Display the configuration to view current or changed settings for the boot monitor and boot monitor by performing this procedure.

Caution:

Risk of system failure

Do not edit the boot.cfg file manually because the switch reads this file during the boot process. Errors generated while editing the file can render the switch inoperable.

Prerequisites

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

Procedure steps

1. View the configuration by using the following command:

   ```
   show boot config
   ```

Variable definitions

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

Variable	Value
bootp	Specifies the bootp configuration.
choice	Specifies the current boot configuration choices.
cli	Specifies the current cli configuration.
flags	Specifies the current flag settings.
general	Specifies system information.
host	Specifies the current host configuration.
master	Specifies the current SF/CPU slot set as master and the settings for the delay and multicast command.
mezz-image	Specifies the mezzanine image.
net	Specifies the current configuration of the SF/CPU network ports.
running-config [verbose]	Specifies the current boot configuration. • verbose includes all possible information. If you omit verbose, the system displays only the values that you changed from their default settings.
sio	Specifies the current configuration of the SF/CPU serial ports.
slot	Specifies the slot number of the device.
tz	Specifies the current configuration of the switch time zone.

Configuring core dumps

Enable or disable core dumps and configure the location where the core dump is saved. By default, core dumps are enabled and the file is saved to PCMCIA. To enable core dumps with FTP, you must configure the *host user* and *host password* bootconfig parameters.

Important:

If you configure the host user and password to nonnull values, all copying to and from the network (including image downloads) uses FTP instead of TFTP.

Because you can only configure one username and password combination for network copying and core dumps, be sure that the login for the remote system to which you are saving the core dumps is the same login used for the remote systems you are using for file copying.

Prerequisites

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

Procedure steps

1. Configure the core dump by using the following command:

   ```
   [no] boot config slot <slots> core-save [<file>]
   ```

Variable definitions

Use the data in the following table to use the `boot config slot <slots>` command.

Variable	Value
core-save*[<file>]*	Enables or disables the core image file. The default is enable.
start-core	Saves the core image.

Chapter 26: Run-time process management using the ACLI

Configure and manage the run-time process using the Avaya command line interface (ACLI).

Prerequisites to run-time process management

- To perform the procedures in this section, you must log on to the Global Configuration mode in the ACLI. For more information about using ACLI, see *Avaya Ethernet Routing Switch 8800/8600 User Interface Fundamentals, NN46205-308*.

Job aid

The following table lists the commands and parameters that you use to complete the procedures in this section.

Table 35: Job aid

Command	Parameter
Privileged EXEC mode	
clock set <*MMddyyyyhhmmss*>	
Global Configuration mode	
banner	custom
	displaymotd
	motd <*string*>
	static
	word<1-80>
clilog	`enable`
	maxfilesize <*integer*>
clock sync-time <*minutes*>	*minutes <15-3600>*

Table continues…

Command	Parameter
link-flap-detect	auto-port-down
	frequency
	interval
	send-trap
login-message <*string*>	*WORD <1-1513>*
max-logins <*nsessions*>	*nsessions <0-8>*
passwordprompt <*string*>	*WORD <1-1510>*
sys ecn-compatibility	
sys force-msg <*string*>	*WORD <4-4>*
sys global-filter	
sys mgmt-virtual-ip <*ipaddr/mask*>	
sys mtu <*bytes*>	*bytes <1522-9600>*
sys msg-control	action <suppress-msg|send-trap|both>
	control-interval <*minutes*>
	max-msg-num
sys name <*string*>	*WORD <0-255>*
telnet-access	login-timeout <*seconds*>
	sessions <*nsessions*>
udp-checksum enable	
udpsrc-by-vip	

Configuring the date

Configure the calendar time in the form of month, day, year, hour, minute, and second by performing this procedure.

Prerequisites

- You must log on as rwa to use this command.
- You must log on to the Privileged EXEC mode in the ACLI.

Procedure steps

1. Configure the date by using the following command:

   ```
   clock set <MMddyyyyhhmmss>
   ```

Configuring the run-time environment

Configure the run-time environment to define generic configuration settings for ACLI sessions by performing this procedure.

Prerequisites

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

Procedure steps

1. Change the login prompt by using the following command:

   ```
   login-message WORD <1-1513>
   ```

2. Change the password prompt by using the following command:

   ```
   passwordprompt word <1-1510>
   ```

3. Configure the number of supported rlogin sessions by using the following command:

   ```
   max-logins <0-8>
   ```

4. Configure the number of supported Telnet sessions by using the following command:

   ```
   telnet-access sessions <0-8>
   ```

5. Configure the Telnet login timeout by using the following command:

   ```
   telnet-access login-timeout <30-65535>
   ```

Variable definitions

Use the data in the following table to use the run-time environment commands.

Variable	Value
login-message <*string*>	Changes the ACLI logon prompt. • *string* is an American Standard Code for Information Interchange (ASCII) string from 1–1513 characters. • Use the default option before this parameter, default loginmessage, to enable use of the default logon string. • Use the no operator before this parameter, no loginmessage, to disable the default logon banner and display the new banner.

Table continues…

Variable	Value
passwordprompt <*string*>	Changes the ACLI password prompt. • *string* is an ASCII string from 1–1510 characters. • Use the default option before this parameter, default passwordprompt, to enable using the default password string. • Use the no operator before this parameter, no passwordprompt, to disable the default password string.
max-logins <*nsessions*>	Configures the allowable number of inbound remote ACLI logon sessions. The default value is 8. • *nsessions* is the number of sessions from 0–8.
telnet-access login-timeout <seconds>	Configures the time, in seconds, to wait for a Telnet login before terminating the connection. • *seconds* is a number from 30–65535
telnet-access sessions <*nsessions*>	Configures the allowable number of inbound Telnet sessions. The default value is 8. • *nsessions* is a number from 0–8.

Configuring the ACLI logon banner

Configure the ACLI logon banner to display a warning message to users before authentication by performing this procedure.

Prerequisites

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

Procedure steps

1. Configure the switch to use a custom banner or use the default banner by using the following command:

   ```
   banner <custom|static>
   ```

2. Create a custom banner by using the following command:

   ```
   banner <string>
   ```

Variable definitions

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

Variable	Value
string	Adds lines of text to the ACLI logon banner. • *string* is an ASCII string from 1–80 characters
custom|static	Activates or disables use of the default banner.

Configuring the message-of-the-day

Configure a system login message-of-the-day in the form of a text banner that is displayed upon each successful logon by performing this procedure.

Prerequisites

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

Procedure steps

1. Create the message-of-the-day by using the following command:

   ```
   banner motd <string>
   ```

2. Enable the custom message-of-the-day by using the following command:

   ```
   banner displaymotd
   ```

Variable definitions

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

Variable	Value
<*string*>	Creates a message of the day to display with the logon banner. To provide a string with spaces, include the text in quotation marks ("). To set this option to the default value, use the default operator with the command. • *string* is an ASCII string from 1–1516 characters

Table continues…

Variable	Value
displaymotd	Specifies the message of the day. To set this option to the default value, use the default operator with the command.

Configuring command logging

Configure logging of ACLI commands to the file clilog.txt on the Personal Computer Memory Card International Association (PCMCIA). You can enable command logging to keep track of the commands a user enters during a login session.

Configure logging of CLI commands by performing this procedure.

Prerequisites

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

Procedure steps

1. Configure ACLI logging by using the following command:

   ```
   clilog enable [maxfilesize <integer>]
   ```

Variable definitions

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

Variable	Value
enable	Activates ACLI logging to the file clilog.txt on the PCMCIA, To disable ACLI logging, use the no form of the command, no clilog enable.
maxfilesize <*integer*>	Specify the maximum size of the file clilog.txt in a range from 64–256000. The file size is expressed in kilobytes (KB). The default value is 256.

Configuring system-level switch parameters

Configure individual system-level switch parameters to configure global options for the Ethernet Routing Switch 8800/8600 by performing this procedure.

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 <string>
   ```

2. Enable explicit congestion notification by using the following command:

   ```
   sys ecn-compatibility
   ```

3. Enable global filtering by using the following command:

   ```
   sys global-filter
   ```

4. Enable support for Jumbo frames by using the following command: (where <bytes> is either 1950 or 9600)

   ```
   sys mtu <bytes>
   ```

5. Enable the UDP checksum calculation by using the following command:

   ```
   udp-checksum enable
   ```

6. Enable virtual IP as the UDP source by using the following command:

   ```
   udpsrc-by-vip
   ```

Variable definitions

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

Variable	Value
ecn-compatibility	Activates explicit congestion notification, as defined in Experimental Request For Comments (RFC) 2780. This feature is not currently supported on the Ethernet Routing Switch 8800/8600.
sys global-filter	Activates global filtering on the switch. If you activate global filtering, you must disable source MAC VLANs because you cannot enable global filtering and source MAC-based VLANs at the same time.
mtu <*bytes*>	Activates Jumbo frame support for the data path. • *bytes* is the Ethernet frame size, either 1522, 1950 (default), or 9600 bytes. Settings of 1950 or 9600 bytes

Table continues…

Variable	Value
	activate Jumbo frame support. Jumbo frame support is activated by default.
name <*string*>	Configures the system, or root level, prompt name for the switch. • *string* is an ASCII string from 0–255 characters (for example, LabSC7 or Closet4).

Synchronizing the real-time and system clocks

Configure the regular interval to synchronize the real-time and system clocks. The switch generates log messages if the drift between the real-time clock and the system clock is more than 5 seconds.

Synchronize the real-time and system clocks by performing this procedure.

Prerequisites

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

Procedure steps

1. Configure the synchronization interval by using the following command:

   ```
   clock sync-time <minutes>
   ```

Variable definitions

Use the data in the following table to use the`clock sync-time` command.

Variable	Value
<*minutes*>	Specifies the number of minutes between synchronization in a range from 15–3600. The default value is 60. To set this option to the default value, use the default operator with the command.

Creating a virtual management port

Create a virtual management port in addition to the physical management ports on the switch management modules.

After you assign an IP address to the virtual management port, the IP address provides access to both switch management modules. The master management module replies to all management requests sent to the virtual IP address, as well as to requests sent to its management port IP address. If the master management module fails and the standby management module takes over, the virtual management port IP address continues to provide management access to the switch.

Create a virtual management port by performing this procedure.

Prerequisites

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

Procedure steps

1. Create a virtual management port by using the following command:

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

Example of creating a virtual management port

1. Create a virtual management port:

   ```
   ERS-8606:5(config)# sys mgmt-virtual-ip 47.140.54.40/255.255.255.0
   Physical and Virtual IP must be in the same subnet
   ```

Configuring system message control

Configure system message control to enable or disable system messaging and define configuration settings by performing this procedure.

Prerequisites

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

Procedure steps

1. Configure system message control action by using the following command:

   ```
   sys msg-control action <suppress-msg|send-trap|both>
   ```

2. Configure the maximum number of messages by using the following command:

   ```
   sys msg-control max-msg-num <number>
   ```

3. Configure the interval by using the following command:

   ```
   sys msg-control control-interval <minutes>
   ```

Variable definitions

Use the data in the following table to use the `sys msg-control` command.

Variable	Value
action <suppress-msg|send-trap|both>	Configures the message control action. The default value is *supress-msg*. To set this option to the default value, use the default operator with the command.
control-interval <*minutes*>	Configures the message control interval, in minutes. The default value is 5. • *minutes* is a value from 1–30 To set this option to the default value, use the default operator with the command.
max-msg-num <*number*>	Configures the number of occurrences of a message after which the control action occurs. The default value is 5. • *number* is a value from 2–500 To set this option to the default value, use the default operator with the command.

Forcing message control for system message control

Use the force message control option to extend the message control feature functionality to the software and hardware log messages.

To enable the message control feature, you must specify an action, control interval, and maximum message number. After enabling the feature, the log messages, which get repeated and cross the maximum message number in the control interval, trigger the force message feature. You can either suppress the message or send a trap notification, or both.

Use the force message control for system message control by performing this procedure.

Prerequisites

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

Procedure steps

1. Configure the force message control option by using the following command:

   ```
   sys force-msg <string>
   ```

Variable definitions

Use the data in the following table to use the `sys force-msg` command.

Variable	Value
<*string*>	Adds a forced message control pattern • *string* is a string of 4 characters. You can add a four-byte pattern into the force-msg table. The software and the hardware log messages that use the first four bytes that match one of the patterns in the force-msg table undergo the configured message control action. You can specify up to 32 different patterns in the force-msg table including a wild-card pattern (****) . If you specify the wild-card pattern, all messages undergo message control.

Chapter 27: Chassis operations configuration using the ACLI

This chapter provides the details to configure operating modes and basic hardware and system settings.

Job aid

The following table lists the commands and their parameters that you use to complete the procedures in this section.

Table 36: Job aid

Command	Parameter
Global Configuration mode	
boot config flags	ha-cpu
auto-recover-delay *<5–3600 seconds>*	
mac-flap-time-limit *<10–5000 milliseconds>*	
slpp	enable
	ethertype
	operation
	tx-interval
	vid
sys ext-cp-limit	max-ports-to-check <value>
	min-congestion-time <time>
	port-congestion-time <time>
	trap-level <dummy|None|Normal|Verbose>
sys flags	auto-reset-fabric
	global-filter-ordering
	multicast-check-packet
	take-iocard-offline

Table continues…

Command	Parameter
sys mtu <*bytes*>	
sys power	
sys power slot-priority <1–10>	critical|high|low
sys record-reservation	filter <value>
	ipmc <value>
	local <value>
	mac <value>
	static-route <value>
	vrrp <value>
Interface Configuration mode	
auto-recover-port	<enable|disable>
cp-limit port	broadcast-limit <value>
	multicast-limit <value>
ext-cp-limit port <*PortList*>	<None|SoftDown|HardDown>
	threshold-util-rate <value>
loop-detect	action <mac-discard|port-down|vlan-block>
	arp-detect
slpp port <*portlist*>	packet-rx
	packet-rx-threshold <1-500>
	port <portlist>
Privileged EXEC mode	
show slpp interface	
	GigabitEthernet <slot/port>
	Fastethernet <slot/port>

Enabling the CPU High Availability mode

CPU high-availability (HA) mode enables switches with two CPUs to recover quickly from a failure of the master SF/CPU.

Use the procedure in this section to enable HA CPU mode.

Prerequisites

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

Procedure steps

1. To enable HA mode, enter the following boot flag command on the master SF/CPU:

   boot config flags ha-cpu

   After enabling HA mode on the master SF/CPU, the secondary SF/CPU automatically resets to load settings from its previously-saved boot configuration file. You must manually reset the primary SF/CPU while the secondary SF/CPU is booting.

   Important:

   Failure to manually boot the primary CPU before the secondary finishes booting can lead to system instability. Traffic is interrupted when the master is manually reset.

   Caution:

   Enabling the HA mode can cause certain features to become disabled. See the Release Notes for your software version for details on HA mode specific information.

Table 6: Release 3.5 and later synchronization capabilities in HA mode on page 49 shows which features are supported in each release.

Job aid

See the following sample output for the messages while enabling the HA mode using ACLI:

```
ERS-8610:6(config)#boot config flags ha-cpu

The config files on the Master and Slave will be overwritten with the current
active configuration. Note: -Layer 2/3 features except IPX will be enabled in
L2/L3 redundancy mode.

Do you want to continue (y/n) ? y Save bootconfig to file /flash/boot.cfg
successful. Save to slave file /flash/boot.cfg successful. CPU6 [02/02/09
12:41:33] SNMP INFO Save to slave file /flash/boot.cfg successful. CPU6
[02/02/09 12:41:33] SNMP INFO Save boot successful.

Boot configuration is being saved on both master and slave. Save config to
file /flash/config.cfg successful. Save to slave file /flash/config.cfg
successful. CPU6 [02/02/09 12:41:37] SNMP INFO Save config successful.

Runtime configuration is being saved on master and slave.

You need to reset the master for the changes to take effect. Resetting Slave
CPU from Master CPU.
```

Important:

The preceding autosave of the boot configuration file occurs because the savetostandby flag is enabled. If this flag is not enabled, a manual save of the boot configuration file on the secondary SF/CPU is required.

Answering the user prompt with a "y" causes the secondary SF/CPU to reset itself automatically, and that secondary SF/CPU restarts with HA mode enabled. You must manually reset the master SF/CPU immediately (before the secondary CPU completes reset). Resetting the primary CPU causes an interruption to traffic. After the reset completes successfully, the CPUs reverse roles (the CPU that was the primary CPU before reset becomes the secondary CPU and the CPU that was secondary before reset becomes the primary CPU).

Disabling CPU High Availability mode

Use the procedure in this section to disable HA CPU mode.

Prerequisites

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

Procedure steps

1. To disable HA mode, enter the following boot flag command on the master SF/CPU:

   `no boot config flags ha-cpu`

   After disabling HA mode on the master SF/CPU, the secondary SF/CPU automatically resets to load settings from its previously-saved boot configuration file. You must manually reset the primary SF/CPU while the secondary SF/CPU is booting.

   Important:

   Failure to manually boot the primary CPU before the secondary finishes booting can lead to system instability. Traffic is interrupted when the master is manually reset.

Job aid

See the following sample output for the messages the switch returns when you disable HA mode using ACLI:

```
ERS-8610:5(config)#no boot config flags ha-cpu

Note: -savetostandby flag is TRUE. Modify the same if required.

Save bootconfig to file /flash/boot.cfg successful. Save to slave file /flash/
boot.cfg successful.

Boot configuration is being saved on both master and slave. CPU5 [02/02/09
12:30:19] SNMP INFO Save to slave file /flash/boot.cfg successful. CPU5
[02/02/09 12:30:19] SNMP INFO Save boot successful. You need to reset the
master for the changes to take effect. Resetting Slave CPU from Master CPU.
```

Removing a master SF/CPU with CPU-HA mode activated

Properly remove the master SF/CPU to avoid loss of traffic if CPU-HA is activated by performing this procedure.

Prerequisites

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

Procedure steps

1. Software reset the master SF/CPU to becomes the standby.
2. Remove the standby SF/CPU.

   The master is removed. Because CPU-HA is activated, no traffic data is lost during reset.

   Important:

   Reinserting a SF/CPU module before the HA-activated SF/CPU becomes the master SF/CPU can cause the master SF/CPU to remain in a booting state.

Enabling jumbo frames

Enable jumbo frames to increase the size of Ethernet frames supported on the chassis by performing this procedure.

Note:

After changing the MTU size, you must reboot the switch for the change to take effect.

Prerequisites

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

Procedure steps

1. Enable jumbo frames by using the following command:

   `sys mtu` <*bytes*>

Variable definitions

Use the data in the following table to configure the `sys mtu` command.

Variable	Value
<*bytes*>	The control plane (CPU, CPP) does not support Jumbo frames, but can learn properly when you use Jumbo frames. You can use mtu <bytes> to activate Jumbo frames support for the data path. • *bytes* is the Ethernet Frame size, either 1522, 1950 (default), or 9600 bytes. Settings of either 1950 or 9600 bytes activate Jumbo frame support. Jumbo frame support is activated by default.

Reserving records

Reserve records to change the number of hardware records available for each record type by performing this procedure.

Prerequisites

- You must use this command in the ACLI Global configuration command mode.

Procedure steps

1. At the Global configuration prompt, enter

```
sys record-reservation [filter <value>|ipmc <value>|local <value>|
mac <value>|static-route <value>|vrrp <value>]
```

Variable definitions

Use the data in the following table to configure `sys record-reservation`.

Variable	Value
filter <*value*>	Configure reservation for filter record type expressed in a range from 1025–8192. The default value is 4096

Table continues…

Variable	Value
ipmc <*value*>	Configure reservation for ipmc record type expressed as an ipmc value in a range from 0–8000. The default value is 500.
local <*value*>	Configure reservation for local record type expressed as a local value in a range from 0–16000. The default value is 2000.
mac <*value*>	Configure reservation for mac record type expressed as a mac value in a range from 0–200000. The default value is 2000.
static-route <*value*>	Configure reservation for static-route record type expressed as a route value in a range from 0–1000. The default value is 200.
vrrp <*value*>	Configure reservation for vrrp record type expressed as a vrrp value from 0–510. The default value is 500.

Job aid

After you enter the `show sys record-reservation` command, the system displays the HW Record Reservation table. The following table explains the column headings in the HW Record Reservation table.

Column heading	Description
Record Type	Identifies the record type as follows: • filter • ipmc • local • mac • static-route • vrrp
Reserved	Specifies the number of hardware records reserved for the record type.
Used	Specifies the number of hardware records actually used by the record type.
New-Reserved	Specifies the number of hardware records reserved for this record type after a switch reset if you save the current configuration.
Def-Reserved	Specifies the number of hardware records reserved for this record type after a switch reset if you use the factory default configuration.

Configuring SLPP

Enable the Simple Loop Prevention Protocol (SLPP) globally and on a VLAN to detect a loop and automatically stop it by performing this procedure.

Prerequisites

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

Procedure steps

1. Enable SLPP by using the following command:

   ```
   slpp operation
   ```

2. Specify the PDU Ether type by using the following command:

   ```
   slpp ethertype <pid>
   ```

3. Configure the transmission interval by using the following command:

   ```
   slpp tx-interval <integer>
   ```

4. Add a VLAN to the transmission list by using the following command:

   ```
   slpp <vid>
   ```

Variable definitions

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

Variable	Value
ethertype *<pid>*	Specifies the SLPP PDU Ethernet type. • *<pid>* is the SLPP protocol ID expressed as a decimal in the range from 1 to 65535 or in hexadecimal from 0x001 to 0xffff. The default value is 0x8102. To set this option to the default value, use the default operator with the command.
operation	Enables or disables the SLPP operation. You must enable the SLPP operation to enable the SLPP packet transmit and receive process.

Table continues…

Variable	Value
	If you disable the SLPP operation, the system sends no SLPP packets and discards received SLPP packets. To set this option to the default value, use the default operator with the command.
tx-interval *<integer>*	Configures the SLPP packet transmit interval. • *<integer>* is the SLPP packet transmit interval expressed in milliseconds in a range from 500–5000. The default value is 500. To set this option to the default value, use the default operator with the command.
<vid>	Adds a VLAN to a SLPP transmission list. • *<vid>* is the VLAN ID expressed in a range from 1–4095. Use the no operator to remove this configuration.

Configuring SLPP on a port

Enable SLPP by port to detect a loop and automatically stop it by performing this procedure.

Important:

To provide protection against broadcast and multicast storms, Avaya recommends that you enable Rate Limiting for broadcast traffic and multicast traffic.

Prerequisites

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

Procedure steps

1. Configure SLPP on a port by using the following command:

```
slpp port <portlist> [packet-rx] [packet-rx-threshold <1-500>]
```

Variable definitions

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

Variable	Value
packet-rx	Activates SLPP packet reception on the listed ports. To set this option to the default value, use the default operator with the command.
packet-rx-threshold *<1-500>*	Specifies the threshold for packet reception. The SLPP packet receive threshold is set to a value (1-500) that represents the number of SLPP-PDUs that must be received to shut down the port. Note that this is a port-level parameter, therefore if the port is tagged, SLPP-PDUs from the various VLANs increment this single threshold counter. See Table 14: SLPP recommended values on page 63 for recommended values in an SMLT environment. To set this option to the default value, use the default operator with the command.
<portlist>	Identifies the slot/port.

Viewing SLPP information

Use SLPP information to view loop information by performing this procedure.

Prerequisites

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

Procedure steps

1. View SLPP information by using the following command:

```
show slpp
```

Viewing SLPP information for a port

Show SLPP information for a port so that you can view the loop information for a port by performing this procedure.

Prerequisites

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

Procedure steps

1. View SLPP information for a port by using the following command:

   ```
   show slpp interface
   ```

Variable definitions

Use the data in the following table to help you view the `SLPP interface` information.

Variable	Value
PORT NUM	Specifies the port number.
PKT-RX	Specifies whether SLPP is enabled or disabled.
PKT-RX THRESHOLD	Specifies the configured SLPP receive threshold configured on the port.
INCOMING VLAN ID VLAN	Specifies the ID of the classified packet on a port disabled by SLPP.
SLPP PDU ORIGINATOR	Specifies the originator of the SLPP PDU.
PKT-RX COUNT	Specifies the SLPP RX PDU count.
TIME LEFT TO CLEAR RX COUNT	Specifies the time left to clear the SLPP RX PDU counter.

Clearing SLPP port counters

Clear SLPP port counters manually by performing this procedure.

Prerequisites

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

Procedure steps

1. Clear the SLPP port counters manually:

```
clear slpp stats <ports>
```

Variable definitions

Use the data in the following table to help you view the `clear slpp stats` information.

Variable	Value
ports	Specifies the slot and port number

Configuring Extended CP Limit on the chassis

CP Limit functionality protects the switch from becoming congested by excess data flowing through one or more ports. You can configure the Extended CP Limit functionality to prevent the switch from being overwhelmed.

Currently the CP Limit functionality only protects the switch from broadcast and control traffic with a QoS value of 7.

Configure extended CP Limit on the chassis by performing this procedure.

Prerequisites

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

Procedure steps

1. Configure Extended CP Limit by using the following command:

   ```
   sys ext-cp-limit [max-ports-to-check <value>] [min-congestion-time
   <time>] [port-congestion-time <time>] [trap-level <dummy|None|
   Normal|Verbose>]
   ```

Variable definitions

Use the data in the following table to use the `sys ext-cp-limit` command.

Variable	Value
max-ports-to-check <*number of ports*>	Configures the total number of ports to monitor. • *number of ports* is expressed in a range from 0–512. The default value is 0. To set this option to the default value, use the default operator with the command.
min-congestion-time <*time in msec*>	Configures the minimum time required to trigger the congestion algorithm (while traffic continues to hit the SF/CPU). • *time in msec* is expressed milliseconds in a range from 100–600000. The default value is 300. To set this option to the default value, use the default operator with the command.
port-congestion-time <*time in sec*>	Specifies the duration that the monitoring port bandwidth utilization can exceed threshold before the system disables the port. • *time in sec* is expressed in a range from 1–600. The default value is 5. To set this option to the default value, use the default operator with the command.
trap-level <dummy|None|Normal|Verbose>	Configures the trap level. Trap levels are: • dummy • None–no traps are sent • Normal–sends a single trap for all disabled ports • Verbose–sends a trap for each disabled port The default value is None. To set this option to the default value, use the default operator with the command.

Configuring Extended CP Limit on a port

CP Limit functionality protects the switch from becoming congested by excess data flowing through one or more ports. You can configure Extended CP Limit functionality to prevent excess data from overwhelming the switch.

Important:

Each user interface has unique terminology and naming conventions for parameters and values. For example, a parameter in EDM can appear in ACLI with different spelling or syntax.

The following interface comparisons show examples of differences in terminology and syntax between identical parameters and values when you configure and verify CP Limit and Extended CP Limit functionality:

- EDM: displays the ExtCplimitUtilRate parameter
- ACLI: displays the UTIL-RATE parameter

  and

- EDM: displays the CpMulticastLimit and CpBroadcastLimit parameters
- ACLI: displays MULTICAST-LIMIT and BROADCAST-LIMIT parameters

  and

- EDM: displays the ExtCplimitConf parameter
- ACLI: displays the EXT-CP-LIMIT parameter

Configure extended CP Limit on a port by performing this procedure.

Prerequisites

- You must log on to the ACLI FastEthernet or GigabitEthernet Interface configuration mode.

Procedure steps

1. Configure Extended CP Limit on a port by using the following command:

   ```
   ext-cp-limit port <PortList> <None|SoftDown|HardDown> [threshold-util-rate <value>]
   ```

Variable definitions

Use the data in the following table to use the `ext-cp-limit` command.

Variable	Value
<None|SoftDown|HardDown>	Specifies port status as follows: • None–the port does not need to be checked. • SoftDown–the port belongs to the may-go-down-port-list. • HardDown–the port belongs to the must-go-down-port-list.
port *<PortList>*	Specifies a port or list of ports.

Table continues…

Variable	Value
threshold-util-rate	Specifies the threshold bandwidth utilization expressed as per cent in a range from 1–100. The default value is 50. To set this option to the default value, use the **default** operator with the command.

Configuring loop detect

Configure loop detect to determine if the same MAC address appears on different ports. Use the ARP-Detect feature to account for ARP packets on IP configured interfaces.

Configure loop detect by performing this procedure.

Prerequisites

- To use the loop-detect command, you must log on to the FastEthernet or GigabitEthernet Interface Configuration mode.
- Complete the remainder of the procedure in Global Configuration mode.
- On routed interfaces you must activate ARP-Detect with loop detect.

Procedure steps

1. Configure loop detect by using the following command:

   ```
   loop-detect action <mac-discard|port-down|vlan-block> arp-detect
   ```

2. Exit to Global Configuration mode:

   ```
   exit
   ```

3. Configure the interval at which MAC addresses are monitored:

   ```
   mac-flap-time-limit <10-5000 milliseconds>
   ```

Variable definitions

Use the data in the following table to use the `loop-detect` command.

Variable	Value
action <mac-discard|port-down|vlan-block>	Specifies the loop detect action to be taken. • port-down shuts down the port if the system detects a flapping MAC address • vlan-block shuts down the VLAN if the system detects a flapping MAC address • mac-discard—ARP-Detect does not support this action. The default is port-down.
arp-detect	Activates ARP-Detect.

Configuring CP Limit

CP Limit functionality protects the switch from becoming congested by excess data flowing through one or more ports by performing this procedure.

Important:

Before CP Limit shuts down a port that exceeds the threshold, it captures the traffic statistics for that port. To see these logs, enter the following command: **`more /pcmcia/rxstats.txt`**.

Prerequisites

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

Procedure steps

1. Configure CP Limit by using the following command:

   ```
   cp-limit port [multicast-limit <value>] [broadcast-limit <value>]
   ```

Important:

Each user interface has unique terminology and naming conventions for parameters and values. For example, a parameter in EDM can appear in ACLI with different spelling or syntax.

The following interface comparisons show examples of differences in terminology and syntax between identical parameters and values when you configure and verify CP Limit and Extended CP Limit functionality:

- EDM: displays the ExtCplimitUtilRate parameter
- ACLI: displays the UTIL-RATE parameter

and

- EDM: displays the CpMulticastLimit and CpBroadcastLimit parameters
- ACLI: displays MULTICAST-LIMIT and BROADCAST-LIMIT parameters

and

- EDM: displays the ExtCplimitConf parameter
- ACLI: displays the EXT-CP-LIMIT parameter

Variable definitions

Use the data in the following table to use the `cp-limit` command.

Variable	Value
broadcast-limit <*value*>	Configures the broadcast control frame rate expressed as pps in a range from 1000–100000. The default value is 10000. To set this option to the default value, use the default operator with the command. **Note:** If you are using the 8692 SF/CPU with a SuperMezz, change the default to 3000 pps
multicast-limit <*value*>	Configures the multicast control frame rate expressed as pps in a range from 1000–100000. The default is 15000. To set this option to the default value, use the default operator with the command. **Note:** If you are using the 8692 SF/CPU with a SuperMezz, change the default to 3000 pps
port	Specifies a port or list of ports. To set this option to the default value, use the default operator with the command.

Configuring Auto Recovery

Configure Auto Recovery to reenable ports that were disabled because loops were detected. When enabled, this feature automatically recovers ports disabled by SLPP, CP Limit, link flap, or loop detect.

Prerequisites

- Select a port and log on to the Interface Configuration mode.

Procedure steps

1. Enable auto-recovery on a port by using the following command:

   ```
   auto-recover-port enable
   ```

Variable definitions

The following table describes variables that you enter in the **`interface gigabitEthernet <slot/port> auto-recover-port {enable|disable}`** command.

Variable	Value
`<slot/port>`	Specifies the port or the list of ports in slot/port format.
`{enable|disable}`	`enable` activates Auto Recovery of the port from action taken by SLPP, CP Limit, link flap, or loop detect. The default value is `disable`.

Job aid: Loop detection warning messages

The following log message and trap is generated when a port, which has been disabled due to CP-Limit or link-flap, is auto-recovered:

```
port <port-num> re-enabled by auto recovery
```

The following log message and trap is generated when a port which has been disabled due to the loop detection feature is auto-recovered:

```
Loop detect action <action> cleared on port <port-num> by auto recovery
```

Setting the Auto Recovery timer

Set the Auto Recovery timer to the number of seconds you want to wait before reenabling ports that were disabled because loops were detected. This timer is a global setting that applies to all ports that have Auto Recovery enabled.

Prerequisites

- Log on to the Global Configuration mode.

Procedure steps

1. Set the auto-recovery timer by using the following command:

   ```
   auto-recover-delay <seconds>
   ```

Variable definitions

The following table describes variables that you enter in the **`auto-recover-delay <seconds>`** command.

Variable	Value
<seconds>	Configures the delay in Auto Recovery. The value ranges from 5 to 3600 seconds. The default is 30.

Enabling power management

Enable power redundancy to create traps and events after power consumption exceeds redundancy capacity by performing this procedure.

Prerequisites

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

Procedure steps

1. Enable power management by using the following command:

   ```
   sys power
   ```

Configuring slot priority

Configure slot priority to determine which slots shut down if insufficient power is available in the chassis. The slot with the lowest priority shuts down first. Slots with the same priority shut down in descending order (highest slot number first).

Configure priority of a slot by performing this procedure.

Prerequisites

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

Procedure steps

1. Configure slot priority by using the following command:

   ```
   sys power slot-priority <1-10> {critical|high|low}
   ```

Variable definitions

Use the data in the following table to use the `sys power slot-priority` command.

Variable	Value
critical|high|low	Specifies slot priority.
1–10	Designates the slot for priority setting. You can configure priority for slots 1–4 and 7–10. To set this option to the default value, use the default operator with the command.

Enabling Fabric (FAB) Memory Full error handling

Use the procedure in this section to enable Fabric (FAB) Memory Full error handling to resolve the `Fab Memory Full` fault.

Procedure steps

From the Global Configuration mode, enable Fabric (FAB) Memory Full error handling by entering the following command:

```
sys flags
```

Important:

When enabled, Fabric (FAB) Memory Full error handling will cause the switch fabric to automatically reset when the Fabric (FAB) Memory Full error is detected. For redundant network designs, this will divert traffic around the affected switch and allow the network to recover with minimal interruption. If the network design does not support redundancy, then there will be network interruption while the switch is reset.

Variable definitions

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

Variable	Value
auto-reset-fabric	Enable or disable fabric to be reset automatically on fab mem full error. The default is `disable`.

Table continues…

Variable	Value
take-iocard-offline	Enable or disable I/O-card to go offline when there are excessive resets. The default is `enable`.

Chapter 28: LLDP configuration using the ACLI

Configure LLDP to use as part of fault management operations and to provide diagnostic information in troubleshooting procedures.

Related links

Job aid: roadmap of LLDP ACLI commands on page 297
Setting LLDP transmission parameters on page 298
Setting LLDP port parameters on page 299
Specifying the optional Management TLVs to transmit on page 300
Specifying the optional IEEE 802.1 TLVs to transmit on page 301
Specifying the optional IEEE 802.3 TLVs to transmit on page 302
Showing global LLDP information on page 303
Showing local LLDP information on page 303
Showing LLDP neighbor information on page 304

Job aid: roadmap of LLDP ACLI commands

The following roadmap lists the ACLI commands used to enable and configure LLDP.

Command	Parameter
Global configuration mode	
lldp	tx-interval <1-32768>
	tx-hold-multiplier <2-10>
	reinit-delay <1-10>
	tx-delay <1-8192>
	notification-interval <5–3600>
Interface configuration mode	
lldp	config-notification
	status {rxOnly|txAndrx|txOnly }
	port <portList> <config-notification | status>

Table continues…

Command	Parameter
lldp tx-tlv	port-desc
	sys-name
	sys-desc
	sys-cap
	local-mgmt-addr
lldp tx-tlv dot1	port-vlan-id
	vlan-name <vlanList>
	port-protocol-vlan-id <vlanList>
	protocol-identity {EAP|LLDP|MSTP|RSTP}
lldp tx-tlv dot3	mac-phy-config-status
	link-aggregation
	maximum-frame-size

Related links

LLDP configuration using the ACLI on page 297

Setting LLDP transmission parameters

Set the LLDP transmission parameters to configure LLDP on the Ethernet Routing Switch 8800/8600.

Procedure steps

1. Log on to the Global Configuration mode in the ACLI.
2. Set the LLDP transmission parameters with the following command:

   ```
   lldp
   ```

Variable definitions

Use the data in the following table to configure the **lldp** command.

Variable	Value
tx-interval <1-32768>	Sets the global interval (in seconds) between successive transmission cycles. The range is 1 to 32768 and the default is 30.
tx-hold-multiplier <2-10>	Sets the multiplier (in seconds) for the tx-interval used to compute the Time To Live value for the TTL TLV. The range is 2 to 10 and the default is 4.

Table continues…

Variable	Value
reinit-delay <1-10>	Sets the delay (in seconds) for the reinitialization attempt if the adminStatus is disabled. The range is 1 to 10 and the default is 2.
tx-delay <1-8192>	Sets the minimum delay (in seconds) between successive LLDP frame transmissions. The range is 1 to 8192 and the default is 2.
notification-interval <5-3600>	Sets the interval (in seconds) for which only one remote table change notification is transmitted. The range is 5 to 3600 and the default is 5.

To set the LLDP transmission parameters to their default values, use the following command from the Global configuration mode:

```
default lldp [tx-interval ] [tx-hold-multiplier ] [reinit-delay] [tx-delay] [notification-interval]
```

If you do not specify any parameters, the `default lldp` command sets all parameters to their default values.

Related links

LLDP configuration using the ACLI on page 297

Setting LLDP port parameters

Set the LLDP port parameters to configure LLDP on the Ethernet Routing Switch 8800/8600.

Procedure steps

1. Log on to the Interface Configuration mode in the ACLI.
2. Set the LLDP port parameters using the following command:

   ```
   lldp
   ```

Variable definitions

Use the data in the following table to configure the **`lldp`** command.

Variable	Value
config-notification	Enables notifications from the agent. The default is enabled.
status <rxOnly|txAndRx|txOnly>	Sets the administrative status on the port. • `rxOnly`: enables LLDPU receive only. • `txAndrx`: enables LLDPU transmit and receive. • `txOnly`: enables LLDPU transmit only.

Table continues…

Variable	Value
	The default is `txAndrx` (transmit and receive).
port <portList> <config-notification | status>	Sets either the `config-notification` state or the `status` (administrative state) of the indicated port(s). The default for `config-notification` is enabled; the default for `status` is txAndrx.

To disable LLDP features on the port, use the following command from the Interface configuration mode:

```
no lldp port <portList> <config-notification | status>
```

To set the LLDP port parameters to their default values, use the following command from the Interface configuration mode:

```
default lldp port <portList>
```

Related links

LLDP configuration using the ACLI on page 297

Specifying the optional Management TLVs to transmit

Set the optional Management TLVs to transmit to configure LLDP on the Ethernet Routing Switch 8800/8600.

Procedure steps

1. Log on to the Interface Configuration mode in the ACLI.
2. Set the optional Management TLVs to be included in the transmitted LLDPDUs using the following command:

   ```
   lldp tx-tlv
   ```

Variable definitions

Use the data in the following table to configure the **`lldp tx-tlv`** command.

Variable	Value
port-desc	Enables transmission of the port description TLV from this port. The default is disabled.
sys-name	Enables transmission of the system name TLV from this port. The default is disabled.
sys-desc	Enables transmission of the system description TLV from this port. The default is disabled.
sys-cap	Enables transmission of the system capabilities TLV from this port. The default is disabled.

Table continues…

Variable	Value
local-mgmt-addr	Enables transmission of the local management address TLV from this port. The default is disabled.

To specify the optional Management TLVs not to be included in the transmitted LLDPDUs, use the following command from the Interface configuration mode:

```
no lldp tx-tlv [port-desc] [sys-name] [sys-desc] [sys-cap] [local-mgmt-addr]
```

To set the LLDP Management TLVs to their default values, use the following command from the Interface configuration mode:

```
default lldp tx-tlv [port-desc] [sys-name] [sys-desc] [sys-cap] [local-mgmt-addr]
```

Related links

LLDP configuration using the ACLI on page 297

Specifying the optional IEEE 802.1 TLVs to transmit

Set the optional IEEE 802.1 TLVs to be included in the transmitted LLDPDUs,

Procedure steps

1. Log on to the Interface Configuration mode in the ACLI.
2. Set the optional IEEE 802.1 organizationally specific TLVs to transmit using the following command:

   ```
   lldp tx-tlv dot1
   ```

Variable definitions

Use the data in the following table to configure the **`lldp tx-tlv dot1`** command.

Variable	Value
port-vlan-id	Enables transmission of port VLAN ID TLVs from this port. The default is disabled.
vlan-name <vlanList>	Enables transmission of VLAN name TLVs from this port. The default is disabled.
port-protocol-vlan-id	Enables transmission of protocol VLAN TLVs from this port. The default is disabled.
protocol-identity [EAP|LLDP|MSTP|RSTP}	Enables transmission of the specified protocol identity TLVs from this port. The protocol can be EAP, LLDP, MSTP, or RSTP. The default is disabled.

To specify the optional IEEE 802.1 TLVs not to be included in the transmitted LLDPDUs, use the following command from the Interface configuration mode:

```
no lldp tx-tlv dot1 [port-vlan-id] [vlan-name] [port-protocol-vlan-id]
[protocol-identity {EAP|LLDP|MSTP|RSTP}]
```

To reset the optional IEEE 802.1 organizationally specific TLVs to their default values, use the following command from the Interface configuration mode:

```
default lldp tx-tlv dot1 [vlan-name] [port-protocol-vlan-id] [protocol-
identity {EAP|LLDP|MSTP|RSTP}]
```

Related links

LLDP configuration using the ACLI on page 297

Specifying the optional IEEE 802.3 TLVs to transmit

Specify the optional IEEE 802.3 organizationally-specific TLVs to be included in the transmitted LLDPDUs.

Procedure steps

1. Log on to the Interface Configuration mode in the ACLI.
2. Specify the optional IEEE 802.3 organizationally specific TLVs to transmit, using the following command:

   ```
   lldp tx-tlv dot3
   ```

Variable definitions

Use the data in the following table to configure the **`lldp tx-tlv dot3`** command.

Variable	Value
mac-phy-config-status	Enables the transmission of the MAC/Phy configuration/status TLVs from this port. The default is disabled.
link-aggregation	Enables the transmission of link aggregation TLVs from this port. The default is disabled.
maximum-frame-size	Enables the transmission of maximum frame size TLVs from this port. The default is disabled.

To specify the optional IEEE 802.3 TLVs not to be included in the transmitted LLDPDUs, use the following command from the Interface configuration mode:

```
no lldp tx-tlv dot3 [mac-phy-config-status] [link-aggregation] [maximum-
frame-size]
```

To set the optional IEEE 802.3 organizationally specific TLVs to their default values, use the following command from the Interface configuration mode:

```
default lldp tx-tlv dot3 [mac-phy-config-status] [link-aggregation]
[maximum-frame-size]
```

Related links

LLDP configuration using the ACLI on page 297

Showing global LLDP information

Display the global LLDP parameters to view information about the LLDP settings on the switch.

Procedure steps

1. Log on to the Privileged EXEC command mode in the ACLI.
2. Display the global LLDP parameters with the following command:

   ```
   show lldp
   ```

Related links

LLDP configuration using the ACLI on page 297

Showing local LLDP information

Display the LLDP information about the local LLDP settings

Procedure steps

1. Log on to the Privileged EXEC command mode in the ACLI.
2. Display the local LLDP parameters, using the following command:

   ```
   show lldp
   ```

Variable definitions

Use the data in the following table to configure the **`show lldp`** command.

Variable	Value
[port <portList>] local-sys-data [capabilities | {[dot1] [dot3] [med]} | detail}	Displays the organizationally-specific TLV properties on the local switch: • `port <portList>`: displays LLDP information for the specified ports • `capabilities`: displays the LLDP capabilities information for the specified ports • `dot1`: displays the 802.1 TLV properties • `dot3`: displays the 802.3 TLV properties • `med`: displays the Media Endpoint Discovery (MED) properties • `detail`: displays all organizationally-specific TLV properties To display the properties of the optional management TLVs, include only the local-sys-data parameter in the command.

Table continues…

Variable	Value
mgmt-sys-data	Displays the local management system data.
pdu-tlv-size	Displays the different TLV sizes and the number of TLVs in an LLDPDU.
port {GigabitEthernet | <portList> [local-sys-data [detail] | [dot1] [dot3]] [neighbor [detail | [dot1 [protocol-id] [vlan-names]] [dot3]] [neighbor-mgmt-addr] [pdu-tlv-size] [rx-stats] [tx-stats] [tx-tlv [dot1] [dot3]}	Displays LLDP port parameters.
rx-stats	Displays the LLDP receive statistics for the local system.
stats	Displays the LLDP table statistics for the remote system.
tx-stats	Displays the LLDP transmit statistics for the local system.
tx-tlv [dot1] [dot3]	Displays which TLVs are transmitted from the local switch in LLDPDUs: • `dot1`: displays status for 802.1 TLVs • `dot3`: displays status for 802.3 TLVs To display the transmission status of the optional management TLVs for all ports, include only the tx-tlv parameter in the command.

Related links

LLDP configuration using the ACLI on page 297

Showing LLDP neighbor information

Displays information about the LLDP neighbors.

Procedure steps

1. Log on to the User EXEC command mode in the ACLI.
2. Display the LLDP neighbor parameters, using the following command:

   ```
   show lldp neighbor [detail | [dot1[protocol-id][vlan-names]][dot3]]
   ```

3. Display the LLDP neighbor's management address:

   ```
   show lldp neighbor—mgmt—addr
   ```

Variable definitions

Use the data in the following table to configure the **`show lldp neighbor`** command.

Variable	Value
detail	Displays detailed information about the LLDP neighbors.
dot1 [vlan-names | protocol-id]	Displays the neighbor 802.1 TLVs: • `vlan-names`: VLAN Name TLV • `protocol-id`: Protocol Identity TLV
dot3	Displays 802.3 TLVs
neighbor-mgmt-addr	Displays the LLDP neighbor management address.

Related links

LLDP configuration using the ACLI on page 297

Chapter 29: System access configuration using the ACLI

The chapter provides procedures to manage system access through configurations such as usernames, passwords, and access policies.

Prerequisites

- To perform the procedures in this section, you must log on to the Global Configuration mode in the ACLI. For more information about using ACLI, see *Avaya Ethernet Routing Switch 8800/8600 User Interface Fundamentals, NN46205-308*.

Job aid

The following table lists the commands and their parameters that you use to complete the procedures in this section.

Table 37: Job aid

Command	Parameter
Global Configuration mode	
access-policy <1-65535>	access-strict
	accesslevel <ro|rwa|rw>
	enable
	ftp
	host <*word*>
	http
	mode <allow|deny>
	name <*word*>
	network <*A.B.C.D*>

Table continues…

Command	Parameter
	precedence <1-128>
	rlogin
	snmp-group <*word*> <snmpv1|snmpv2c|usm>
	snmpv3
	ssh
	telnet
	tftp
	username <*word*>
access-policy by-mac	*<0x00:0x00:0x00:0x00:0x00:0x00:0x00:0x00>*
	action <allow|deny>
cli password <*word*> <*access-level*>	l4admin
	l4 oper
	layer 1
	layer 2
	layer 3
	oper
	read-only
	read-write
	read-write-all
	slbadmin
	slboper
	ssladmin
password	access-level <*word*>
	aging-time day <1-365>
	default-lockout-time <60-65000>
	lockout <*word*> <*time*>
	min-passwd-len <10-20>
	password-history <0-32>

Enabling CLI access levels

Enable CLI access levels to control the configuration actions of various users by performing this procedure.

Important:

Only the RWA user can disable an access level on the switch. The RWA access level cannot be disabled on the switch.

These configurations are preserved across restarts.

Prerequisites

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

Procedure steps

1. Enable an access level by using the following command:

   ```
   password access-level <word>
   ```

Variable definitions

Use the data in the following table to use the `password access-level` command.

Variable	Value
word	Specifies the name of the required access level, expressed as a string length from 2–8 characters. To set this option to the default value, use the default operator with the command.

Changing passwords

Configure new passwords for each access level, or change the login or password for the access levels of the switch.

The Ethernet Routing Switch 8800/8600 ships with default passwords set for access to the CLI. For security, the system saves passwords to a hidden file.

If you use Simple Network Management Protocol version 3 (SNMPv3), you can change encrypted passwords. Change passwords by performing this procedure.

Prerequisites

- You must have read-write-all privileges to change passwords.
- You must log on to the ACLI Global Configuration mode.

Procedure steps

1. Change a password by using the following command:

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

2. Configure password options by using the following command:

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

Variable definitions

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

Variable	Value
access level	Permits or blocks a designated access level from the following list: • l4admin • l4oper • layer1 <word> • layer2 • layer3 <word> • oper • read-only <word> • read-write <word> • read-write-all <word>
aging-time day *<1-365>*	Configures the age-out time for passwords, in days.
default-lockout-time *<60-65000>*	Changes the default lockout time after three invalid attempts. Configures the lockout time in seconds and is in the range of 60–65000. The default is 60 seconds. To set this option to the default value, use the default operator with the command.
lockout *<word>* *<time>*	Configures the host lockout time. • *word* is the Host Internet Protocol (IP) address in the format a.b.c.d.

Table continues…

Variable	Value
	• *time* is the lockout-out time in seconds for passwords lockout in the range of 60–65000. The default is 60 seconds.
min-passwd-len <*10-20*>	Configures the minimum length for passwords in high-secure mode. To set this option to the default value, use the default operator with the command.
password-history <*3-32*>	Specifies the number of previous passwords to remember. The default is 3. To set this option to the default value, use the default operator with the command.
<*word*>	Represents the new password containing 0–20 characters.

Creating an access policy

Create an access policy to control access to the switch by performing this procedure.

Prerequisites

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

Procedure steps

1. Create an access policy by assigning it a number

   ```
   access-policy <1-65535>
   ```

Configuring an access policy

Configure an access policy to control access to the switch.

You can define network stations that are explicitly allowed to access the switch or network stations that are explicitly forbidden to access the switch.

For each service, you can also specify the level of access; for example, read-only or read/write/all. Configure an access policy by performing this procedure.

Prerequisites

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

Procedure steps

1. Configure access for an access policy by using the following command:

   ```
   access-policy <1-65535> [access-strict] [accesslevel <ro|rwa|rw>]
   ```

2. Configure the access policy mode, network and precedence by using the following command:

   ```
   access-policy <1-65535> [mode <allow|deny>] [network <A.B.C.D>]
   [precedence <1-128>]
   ```

3. Configure optional access protocols for an access policy by using the following command:

   ```
   access-policy <1-65535> [ftp] [http] [ssh] [telnet] [tftp]
   ```

4. Configure optional rlogin access for an access policy by using the following command:

   ```
   access-policy <1-65535> host <word> rlogin username <word>
   ```

5. Configure optional SNMP parameters for an access policy by using the following command:

   ```
   access-policy <1-65535> [snmp-group <word> <snmpv1|snmpv2c|usm>]
   [snmpv3]
   ```

Variable definitions

Use the data in the following table to use the `access-policy` command.

Variables	Value
accesslevel <ro|rwa|rw>	Specifies the level of access if you configure the policy to allow access.
access-strict	Restrains access to criteria specified in the access policy. • true—the system accepts only the currently configured access level • false—the system accepts access up to the configured level Use the no operator to remove this configuration. To set this option to the default value, use the default operator with the command.

Table continues…

Variables	Value
ftp	Activates or disables FTP for the specified policy. Because FTP derives its login/password from the CLI management filters, FTP works for read-write-only (rwo) and read-write (rw) access but not for the read-only (ro) access. Use the no operator to remove this configuration. To set this option to the default value, use the default operator with the command.
host <*word*>	For rlogin access, specifies the trusted host address as an IP address.
http	Activates the HTTP for this access policy. Use the no operator to remove this configuration. To set this option to the default value, use the default operator with the command.
mode <allow|deny>	Specifies whether the designated network address is allowed access to the system through the specified access service. The default setting is allow.
network <*A.B.C.D*>	Specifies the IP address and subnet mask that can access the system through the specified access service.
precedence <*1-128*>	Specifies a precedence value for a policy, expressed as a number from 1–128. The precedence value determines which policy the system uses if multiple policies apply. Lower numbers take higher precedence. The default value is 10.
rlogin	Activates remote login for the access policy. Use the no operator to remove this configuration. To set this option to the default value, use the default operator with the command.
snmp-group <*word*> <*snmpv1*|*snmpv2c*|*usm*>	Adds an snmp-v3 group under the access policy. • *word* is the snmp-v3 group name consisting of 1–32 characters. • <snmpv1|snmpv2c|usm> is the security model; either snmpv1, snmpv2c, or usm. Use the no operator to remove this configuration.
snmpv3	Activates SNMP version 3 for the access policy. For more information about SNMPv3, see *Avaya Ethernet Routing Switch 8800/8600 Security, NN46205-601*. Use the no operator to remove this configuration. To set this option to the default value, use the default operator with the command.

Table continues…

Variables	Value
ssh	Activates SSH for the access policy. For more information about SSH, see *Avaya Ethernet Routing Switch 8800/8600 Security, NN46205-601*. Use the no operator to remove this configuration. To set this option to the default value, use the default operator with the command.
telnet	Activates Telnet for the access policy. Use the no operator to remove this configuration. To set this option to the default value, use the default operator with the command.
tftp	Activates the Trivial File Transfer Protocol (TFTP) for this access policy. Use the no operator to remove this configuration. To set this option to the default value, use the default operator with the command.
username <*word*>	Specifies the trusted host user name for remote login access.

Example of configuring an access policy

1. Assuming no access policies exist, start with policy 3 and name the policy policy3 as follows:

   ```
   ERS-8606:5(config)# access-policy 3 name policy3
   ```

2. Add read/write/all access level to policy 3:

   ```
   ERS-8606:5(config)# access-policy 3 accesslevel rwa
   ```

3. Add the usm group group_example to policy 3:

   ```
   ERS-8606:5(config)# access-policy 3 snmp-group group_example usm
   ```

4. Enable access strict:

   ```
   ERS-8606:5(config)# access-policy 3 access-strict
   ```

5. Enable policy 3:

   ```
   ERS-8606:5(config)# access-policy 3 enable
   ```

Enabling the access policy globally

Enable the access policy globally to control access across the switch. You can control access to the switch by creating an access policy. An access policy specifies the hosts or networks that can access the switch through various access services, such as Telnet, SNMP, Hypertext Transfer Protocol (HTTP), and remote login (rlogin). Enable an access policy globally by performing this procedure.

Prerequisites

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

Procedure steps

1. Enable the access policy globally with the following command:

   ```
   access-policy <1-65535> enable
   ```

Specifying a name for an access policy

Assign a name to the access policy to uniquely identify the policy by performing this procedure.

Prerequisites

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

Procedure steps

1. Assign a name to the access policy by using the following command:

   ```
   access-policy <1-65535> name <word>
   ```

Variable definitions

Use the data in the following table to use the `access-policy` command.

Variables	Value
name<*word*>	Specifies a name expressed as a string from 0–15 characters.

Allowing a network access to the switch

Specify the network to which you want to allow access by performing this procedure.

Prerequisites

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

Procedure steps

1. Specify the network with the following command:

   ```
   access-policy <1-65535> [accesslevel <ro|rwa|rw>] [mode <allow|
   deny>] [network <A.B.C.D>]
   ```

Variable definitions

Use the data in the following table to use the `access-policy` command.

Variables	Value
accesslevel *<ro|rwa|rw>*	Configures the access level (ro, rw, rwa) or equivalent community string designation (read-only, read/write, or read/write/all).
mode *<allow|deny>*	Specifies whether a designated network address is allowed or denied access through the specified access service. The default setting is allow.
network*<A.B.C.D>*	The IPv4 address/mask, or the IPv6 address/prefix-length permitted, or denied, access through the specified access service.

Configuring access policies by MAC address

Configure access-policies by MAC address to allow or deny local MAC addresses on the network management port after an access policy is activated. If the source MAC does not match a configured entry, then the default action is taken. A log message is generated to record the denial of access. For connections coming in from a different subnet, the source mac of the last hop is used in decision making. Configure access-policies by MAC address does not perform MAC or Forwarding Database (FDB) filtering on data ports.

Access policies are changed from previous releases. Before you attempt to upgrade an access policy from a previous release, see *Avaya Ethernet Routing Switch 8800/8600 Upgrades — Software Release 7.0, NN46205-400*. Configure access policy by MAC address by performing this procedure.

Prerequisites

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

Procedure steps

1. Add the MAC address and configure the action for the policy by using the following command:

   ```
   access-policy by-mac <0x00:0x00:0x00:0x00:0x00:0x00> action <allow|deny>
   ```

Variable definitions

Use the data in the following table to use the `access-policy by-mac` command.

Variables	Value
<0x00:0x00:0x00:0x00: 0x00:0x00>	Adds a MAC address to the policy. Enter the MAC address in hexadecimal format.
<allow|deny>	Specifies the action to take for the designated MAC address.

Chapter 30: License installation using the ACLI

Install and manage a license file for the Avaya Ethernet Routing Switch 8800/8600, using the Avaya command line interface (ACLI).

Installing a license file using the ACLI

Install a license file on an Ethernet Routing Switch 8800/8600 to enable licensed features.

Prerequisites

- You must log on to the Global Configuration mode in the ACLI.
- You must have the license file stored on a Trivial File Transfer Protocol (TFTP) server.
- Ensure that you have the correct license file with the base MAC address of the Ethernet Routing Switch 8800/8600 that you are installing the license on. Otherwise, system does not unblock the licensed features.
- If the Ethernet Routing Switch 8800/8600 chassis has two SF/CPU modules installed, you do not need to install the license file on the secondary SF/CPU. When you enable High Availability, the primary SF/CPU copies the license vectors to the secondary SF/CPU during table sync and the trial period countdown is stopped. This ensures that the run time vectors of the primary and secondary SF/CPU are the same. When you save the configuration on the primary SF/CPU, the system copies the license file to the secondary SF/CPU.

  In warm-standby mode, license vectors are not synchronized with the secondary SF/CPU. However, the system copies the license file to the secondary SF/CPU when you save the configuration with the save to standby flag set to true.

Procedure steps

1. Install a license file by using the following command:

   ```
   copy <a.b.c.d>:<srcfile> /flash/<destfile>
   ```

The following is an example of copying a license file from a TFTP server to the flash on an SF/CPU module of an Avaya Ethernet Routing Switch 8800/8600:

```
ERS-8610:5# copy 10.10.10.20:bld100_8610adv.lic /flash/
bld100_8610adv.dat
```

Important:

If the license filename is license.dat and it is located in the Flash directory, then no further configuration is required. You can continue with the next step. If you changed the license filename and location, you must specify the license file path. The license name must be in lower-case characters. For more information about specifying the license file path, see Specifying the license file path and name using the ACLI on page 319.

2. Load the license file to unlock the licensed features.

   ```
   load-license
   ```

   Important:

   If the loading fails, or if the switch restarts and cannot locate a license file in the specified location, the switch cannot unlock the licensed features and reverts to base functionality.

   The following shows sample output that is displayed on the console when issuing a load-license command:

   ```
   CPU5 [05/10/08 03:26:17] SW INFO Found serial number <00:19:69:7b:
   50:00> in file </flash/license.dat>

   CPU5 [05/10/08 03:26:17] SW INFO License Successfully Loaded From
   <license.dat> License Type -- PREMIER
   ```

3. Save the configuration.

   ```
   save config
   ```

Variable definitions

Use the data in the following table to help you install a license with the `copy` command.

Variable	Value
<a.b.c.d>	Specifies the IPv4 address of the TFTP server where the license file is to be copied from.
<destfile>	Specifies the name of the license file when copied to the flash. **Important:** By default, the switch searches for a license filename of license.dat on the on-board Flash on the SF/CPU module. A license file generated for an Ethernet Routing Switch 8800/8600 can use any filename and extension. If the license filename is not

Table continues…

Variable	Value
	license.dat, or the file is not located in the switch Flash directory, you must update the bootconfig file with the license filename and the path to its location.
<*srcfile*>	Specifies the name of the license file on the TFTP server. For example, bld100_8610adv.lic or license.dat.

Specifying the license file path and name using the ACLI

If you changed the license name and location when you installed the license file, you must specify the license file path to identify the storage location of the license file.

Prerequisites

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

Procedure steps

1. Specify the path for the license file using the following command:

   ```
   boot config choice <bootchoice> license-file <license-file-name>
   ```

2. Reboot the switch for the configuration to take effect.

Variable definitions

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

Variable	Value
<*bootchoice*>	Specifies the order in which the boot path is accessed when the switch is booting up: primary, secondary, or tertiary.
<*license-file-name*>	The source can be internal Flash memory, external memory card (PCMCIA or Flash), or a remote TFTP server. • /flash/<file_name> • /pcmcia/<file_name> • <a.b.c.d>:<file_name>

Table continues…

Variable	Value
	Important: By default, the switch searches for a license filename of license.dat on the on-board Flash on the SF/CPU module. A license file generated for an Ethernet Routing Switch 8800/8600 can use any filename and extension. If the license filename is not license.dat, or the file is not located in the switch Flash directory, you must update the bootconfig file with the license filename and the path to its location.

Showing a license file using the ACLI

Display the existing software licenses on your switch.

Procedure steps

1. To display the existing software licenses on your switch, use the following command:

   `show license`

   For samples of the output displayed with this command, see Job aid on page 320.

Job aid

The following shows two sample outputs for different licenses with the `show license` command.

```
ERS-8610:5# show license

        License file name       :    /flash/bld100_8610adv.dat
        License Type            :    ADVANCED
        MD5 of Key              :    6d97e0c5 f74a9540 1ce8bd23 570b7512
        MD5 of File             :    703c5119 d1a6bbdb e39d5fca 8984e0b8
        Generation Time         :    2008/04/10 11:22:55
        Expiration Time         :
        Base Mac Addr           :    00:04:dc:7d:64:00
        flags                   :    0x00000022 SITE MEMO
        memo                    :
Advanced License


ERS-8610:5#
```

```
ERS-8610:5# show license

        License file name       :    /flash/bld100_8610prem.dat
        License Type            :    PREMIER
        MD5 of Key              :    6d97e0c5 f74a9540 1ce8bd23 570b7512
        MD5 of File             :    548cd140 ee6e20e1 cd53e169 c1fcda4a
        Generation Time         :    2008/04/10 11:24:15
        Expiration Time         :
        Base Mac Addr           :    00:04:dc:7d:64:00
        flags                   :    0x00000022 SITE MEMO
        memo                    :
Premier License

ERS-8610:5#
```

Chapter 31: NTP configuration using the ACLI

This chapter describes how to configure the Network Time Protocol (NTP) using the Avaya command line interface (ACLI).

Prerequisites to NTP configuration

- Unless otherwise stated, to perform the procedures in this section, you must log on to the Global Configuration mode in the ACLI. For more information about using ACLI, see *Avaya Ethernet Routing Switch 8800/8600 User Interface Fundamentals, NN46205-308*.
- Before you configure NTP, you must perform the following tasks:
  - Configure an IP interface on the Ethernet Routing Switch 8800/8600 and ensure that the NTP server is reachable through this interface. For instructions, see *Avaya Ethernet Routing Switch 8800/8600 Configuration — IP Routing, NN46205-523*.
  - Ensure the Real Time Clock is present on the SF/CPU board.

Important:

NTP server MD5 authentication does not support passwords (keys) that start with a special character or that contain a space between characters.

NTP configuration procedures

This task flow shows you the sequence of procedures you perform to configure NTP.

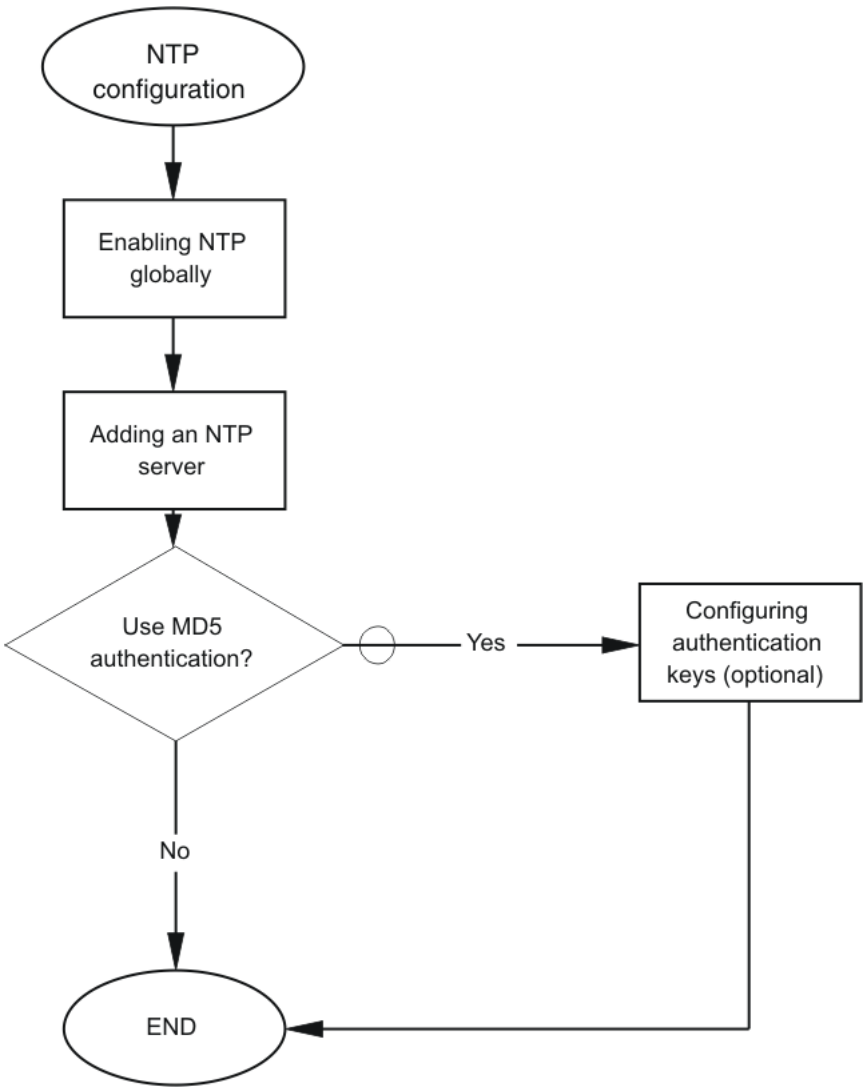


Figure 37: NTP configuration procedures

Job aid

The following table lists the commands and their parameters that you use to complete the procedures in this section.

Table 38: Job aid

Command	Parameter
Global Configuration mode	

Table continues…

Command	Parameter
ntp	authentication-key <1-2147483647> <*word*>
	interval <10-1440>
	ip-source-type {[loopback] [management-virtual-ip]}
ntp server <*A.B.C.D*>	auth-enable
	authentication-key <0-2147483647>
	enable

Enabling NTP globally

Enable NTP globally. Default values are in effect for most parameters. You can customize NTP by modifying parameters. Enable NTP globally by performing this procedure.

Prerequisites

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

Procedure steps

1. Enable NTP globally by using the following command:

   ```
   ntp interval <10-1440>
   ```

2. Create an authentication key by using the following command:

   ```
   ntp authentication-key <1-2147483647> <word>
   ```

Variable definitions

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

Variable	Value
authentication-key <*1-2147483647*> <*word*>	Creates an authentication key for MD5 authentication. To set this option to the default value, use the default operator with the command.

Table continues…

Variable	Value
interval *<10-1440>*	Specifies the time interval, in minutes, between successive NTP updates. • *interval* is expressed as an integer in a range from 10–1440 The default value is 15. To set this option to the default value, use the default operator with the command. **Important:** If NTP is already activated, this configuration does not take effect until you disable NTP, and then re-enable it.

Adding an NTP server

Add an NTP server or modify existing NTP server parameters by performing this procedure.

You can configure a maximum of 10 NTP servers.

Prerequisites

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

Procedure steps

1. Add an NTP server by using the following command:

   ```
   ntp server <A.B.C.D>
   ```

2. Configure additional options for the NTP server by using the following command:

   ```
   ntp server <A.B.C.D> [auth-enable] [authentication-key
   <0-2147483647>] [enable] [source—ip <value>]
   ```

Variable definitions

Use the data in the following table to use the `ntp server` command.

Variable	Value
auth-enable	Activates MD5 authentication on this NTP server. The default is no MD5 authentication. To set this option to the default value, use the default operator with the command.

Table continues…

Variable	Value
authentication-key <*0-2147483647*>	Specifies the key ID value used to generate the MD5 digest for the NTP server. The value range is an integer from 1–2147483647. The default value is 0, which indicates disabled authentication. To set this option to the default value, use the default operator with the command.
enable	Activates the NTP server. To set this option to the default value, use the default operator with the command.
source-ip <*value*>	Sets the IP address as the NTP source IP address. The source IP address can be circuitless IP, management IP, management virtual IP, VLAN IP or brouter IP. To set the NTP source IP as an outgoing Interface IP, set 0.0.0.0 as the source-ip address.

Example of adding an NTP server

1. Add an NTP server:

   ```
   ERS-8606:5(config)# ntp server 47.140.53.187
   ```

Configuring authentication keys

Configure NTP authentication keys to use MD5 authentication by performing this procedure.

Prerequisites

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

Procedure steps

1. Create an authentication key by using the following command:

   ```
   ntp authentication-key <1-2147483647> <word>
   ```

2. Enable MD5 authentication for the server by using the following command:

   ```
   ntp server <A.B.C.D> auth-enable
   ```

3. Assign an authentication key to the server by using the following command:

   ```
   ntp server <A.B.C.D> authentication-key <0-2147483647>
   ```

Example of configuring an NTP authentication key

1. Create the authentication key:

   ```
   ERS-8606:5(config)# ntp authentication-key 5 test
   ```

2. Enable MD5 authentication for the NTP server:

   ```
   ERS-8606:5(config)# ntp server 47.140.53.187 auth-enable
   ```

3. Assign an authentication key to the NTP server:

   ```
   ERS-8606:5(config)# ntp server 47.140.53.187 authentication-key 5
   ```

Configuring the NTP source IP address

Use the following procedure to configure the NTP source IP address. You can specify a circuitless IP (CLIP) IP, a Management Virtual IP, or continue using the outgoing interface IP address (default).

Procedure steps

1. Log on to the Global Configuration mode.
2. Configure the NTP source IP address by using the following command:

   ```
   ntp server <ipaddr> [source-ip <value>]
   ```

   `default ntp server` sets the outgoing interface IP address as the NTP source IP address.
3. Verify your configuration:

   ```
   show ntp server config
   ```

Variable definitions

Use the data in the following table to use the `ntp server` command.

Variable	Value
ipaddr	Specifies the IP address of the NTP server.
source-ip <*value*>	Sets the IP address as the NTP source IP address. The source IP address can be circuitless IP, management IP, management virtual IP, VLAN IP or brouter IP. To set the NTP source IP as an outgoing Interface IP, set 0.0.0.0 as the source-ip address.

Chapter 32: DNS configuration using the ACLI

This chapter describes how to configure the Domain Name Service (DNS) client using the Avaya command line interface (ACLI).

Prerequisites to DNS configuration

- Unless otherwise stated, to perform the procedures in this section, you must log on to the Global Configuration mode in the ACLI. For more information about using ACLI, see *Avaya Ethernet Routing Switch 8800/8600 User Interface Fundamentals, NN46205-308*.

Job aid

The following table lists the commands and their parameters that you use to complete the procedures in this section.

Table 39: Job aid

Command	Parameter
Privileged EXEC mode	
show hosts <word>	
show ip dns	
Global Configuration mode	
ip domain-name <word>	
ip name-server	primatertiary <word>ry <word>
	setertiary <word>condary <word>
	tetertiary <word>rtiary <word>

Configuring the DNS client

Configure the Domain Name Service to establish the mapping between an IP name and an IP address.

You can configure connection for up to three different DNS servers—primary, secondary and tertiary. First the primary server is queried, and then the secondary, and finally the tertiary. Configure DNS client by performing this procedure.

Prerequisites

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

Procedure steps

1. Configure the DNS client by using the following command:

   ```
   ip domain-name <word>
   ```

2. Optionally, add addresses for additional DNS servers by using the following command:

   ```
   ip name-server primary <word> [secondary <word>] [tertiary <word>]
   ```

3. View the DNS client system status by using the following command:

   ```
   show ip dns
   ```

Variable definitions

Use the data in the following table to use the `ip domain-name` and `ip name-server` commands.

Variable	Value
domain-name <*word*>	Configures the default domain name. • *word* is a string 0–255 characters.
primary <*word*>	Configures the primary DNS server address. Enter the IP address in a.b.c.d format for IPv4 or hexadecimal format (string length 0–46) for IPv6.
secondary <*word*>	Configures the secondary DNS server address. Enter the IP address in a.b.c.d format for IPv4 or hexadecimal format (string length 0–46) for IPv6.
tertiary <*word*>	Configures the tertiary DNS server address. Enter the IP address in a.b.c.d format for IPv4 or hexadecimal format (string length 0–46) for IPv6.

Querying the DNS host

Query the DNS host for information about host addresses.

You can enter either a hostname or an IP address. If you enter the hostname, this command shows the IP address corresponding to the hostname and if you enter an IP address, this command shows the hostname for the IP address. Query the DNS host by performing this procedure.

Prerequisites

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

Procedure steps

1. View the host information by using the following command:

   `show hosts` <*word*>

Variable definitions

Use the data in the following table to use the `show hosts` command.

Variable	Value
word	Specifies one of the following: • the name of the host DNS server as a string of 0–255 characters. • the IP address of the host DNS server in a.b.c.d format. • the IPv6 address of the host DNS server in hexadecimal format (string length 0–46).

Chapter 33: Operational procedures using the ACLI

This chapter describes common operational procedures that you use while configuring and monitoring the Avaya Ethernet Routing Switch 8800/8600 operations.

Prerequisites to common procedures

- Unless otherwise stated, to perform the procedures in this section, you must log on to the Privileged EXEC mode in the Avaya command line interface (ACLI). For more information about using ACLI, see *Avaya Ethernet Routing Switch 8800/8600 User Interface Fundamentals, NN46205-308*.

Job aid

The following table lists the commands and their parameters that you use to complete the procedures in this section.

Table 40: Job aid

Command	Parameter
Privileged EXEC mode	
boot *[<file>]*	config <*value*>
	-y
peer <telnet|rlogin>	
md5 <*filename*>	-a
	-c
	-f
	-r
ping <*HostName/ipv4address/ipv6address*>	scopeid <*value*>

Table continues…

Command	Parameter
	datasize <*value*>
	count <*value*>
	-s
	-l <*value*>
	-t <*value*>
	-d
	vrf <*word*>
reset	-y
save bootconfig [file <*word*>]	verbose
	standby <*value*>
	backup <*word*>
	mode (cli|acli)
save config [file <*word*>*]*	verbose
	standby <*value*>
	backup <*word*>
	mode (cli|acli)
source <*file*>	debug
	stop
	syntax
Global Configuration mode	
sys action	cpu-switch-over
	reset {console|counters|modem]

Saving the boot configuration to a file

Save a boot configuration to a file to retain the configuration settings by performing this procedure. You can configure the switch to load a specific configuration file.

Caution:

Risk of data loss

If a Personal Computer Memory Card International Association (PCMCIA) card is removed before a write operation is complete, the file can contain a corrupted end of file (EOF) marker. Before removing the PCMCIA card, execute the command **`pcmcia-stop`**.

Prerequisites

- Some PCMCIA cards become file allocation table (FAT) corrupted after you insert them into the PC-card slot. If this situation occurs, format or repair the FAT on the card.
- The boot configuration file must be named boot.cfg for the system to boot using it.
- To save a file to the standby SF/CPU, you must enable Trivial File Transfer Protocol (TFTP) on the standby SF/CPU.
- You must log on to the Privileged EXEC mode in the ACLI.

Procedure steps

1. Save the configuration by using the following command:

   ```
   save bootconfig [file <word>] [verbose] [standby <value>] [backup
   <word>] [mode (cli|acli)]
   ```

Variable definitions

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

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 *value*: • [a.b.c.d]: <file> • peer/<file> • /pcmcia/ <file> • /flash/ <file> `File`

Table continues…

Variable	Value
	is a string of 1–99 characters.
mode (cli|acli)	Saves the boot configuration in either CLI or ACLI format.
standby *<word>*	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 changed.

Example of saving the boot configuration to a file

1. Save a boot configuration file as a backup file by using the following command:

```
ERS-8606:5# save bootconfig file boot.cfg mode acli File [boot.cfg]
already existing, overwrite (y/n) ?
```

Saving the current configuration to a file

Save the current configuration to a file to retain the configuration settings by performing this procedure.

Caution:

Risk of data loss

If a PCMCIA card is removed before a write operation is complete, the file can contain a corrupted end of file (EOF) marker. Before removing the PCMCIA card, execute the command **`pcmcia-stop`**.

Prerequisites

- Some PCMCIA cards become file allocation table (FAT) corrupted after you insert them into the PC-card slot. If this situation occurs, format or repair the FAT on the card.
- The boot configuration file must be named boot.cfg for the system to boot using it.
- To save a file to the standby SF/CPU, you must enable TFTP on the standby SF/CPU.
- You must log on to the Privileged EXEC mode in the ACLI.

Procedure steps

1. Save the configuration by using the following command:

```
save config [file <word>] [verbose] [standby <value>] [backup
<word>] [mode (cli|acli)]
```

Variable definitions

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

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 *value*: • [a.b.c.d]: <file> • peer/<file> • /pcmcia/ <file> • /flash/ <file> *file* is a string of 1–99 characters.
mode (cli|acli)	Saves the boot configuration in either CLI or ACLI format.
standby *<word>*	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.

Table continues…

Variable	Value
verbose	Saves the default and current configuration. If you omit this parameter, the command saves only parameters you changed.

Example of saving the boot configuration to a file

1. Save a boot configuration file as a backup file by using the following command:

```
ERS-8606:5# save bootconfig file boot.cfg mode acli File [boot.cfg]
already existing, overwrite (y/n) ?
```

Restarting the switch

Restart the switch to implement configuration changes or recover from a system failure. When you restart the system, you can specify the boot source (flash, PCMCIA card, or TFTP server) and file name. If you do not specify a device and file, the run-time ACLI uses the software and configuration files on the primary boot device that is defined by the Boot Monitor **choice** command.

After the switch rerestarts normally, a cold trap is sent within 45 seconds after a restart. If a single strand fiber (SSF) switchover occurs, a warm-start management trap is sent within 45 seconds of a restart. Restart the switch by performing this procedure.

Prerequisites

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

Procedure steps

1. Restart the switch by using the following command:

```
boot [<file>] [config <value>] [-y]
```

Important:

Entering the **boot** command with no arguments causes the switch to start using the current boot choices defined by the **choice** command (next).

Variable definitions

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

Variable	Value
file	Specifies the software image device and file name in the format: *[a.b.c.d:]<file>* /pcmcia/*<file>* /flash/*<file>*. The file name, including the directory structure, can include up to 99 characters.
config<*value*>	Specifies the software configuration device and file name in the format: *[a.b.c.d:]<file>* /pcmcia/*<file>*/ flash/*<file>*. The file name, including the directory structure, can include up to 99 characters.
-y	Suppresses the confirmation message before the switch restarts. If you omit this parameter, you are asked to confirm the action before the switch restarts.

Resetting the switch

Reset the switch to reload system parameters from the most recently saved configuration file by performing this procedure.

Prerequisites

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

Procedure steps

1. Reset the switch by using the following command:

   ```
   reset [-y]
   ```

Variable definitions

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

Variable	Value
-y	Suppresses the confirmation message before the switch resets. If you omit this parameter, you are asked to confirm the action before the switch resets.

Accessing the standby SF/CPU

Access the standby SF/CPU to make changes to the standby SF/CPU without reconnecting to the console port on that module by performing this procedure.

Prerequisites

- The Telnet daemon is activated.
- You must set an rlogin access policy on the standby SF/CPU before you can use the peer command to access it from the master SF/CPU using rlogin. To set an access policy on the standby SF/CPU, connect a terminal to the console port on the standby SF/CPU. For more information about the access policy commands, see *Avaya Ethernet Routing Switch 8800/8600 Fundamentals — User Interfaces, NN46205-308*.
- You must log on to the Privileged EXEC mode in the ACLI.

Procedure steps

1. Access the standby SF/CPU by using the following command:

   ```
   peer <telnet|rlogin>
   ```

Variable definitions

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

Variable	Value
(telnet|rlogin)	Specifies either Telnet or rlogin to use to access the standby SF/CPU.

Pinging an IP device

Ping a device to test the connection between the Ethernet Routing Switch 8800/8600 and another network device. After you ping a device, an Internet Control Message Protocol (ICMP) packet is sent from the switch 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 that the specified IP address is alive. If no reply is received, the message indicates that the address is not responding. Ping an IP device by performing this procedure.

Prerequisites

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

Procedure steps

1. 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).
-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 time-out value in seconds (1–120)(for IPv4).
vrf <WORD 0–64>	Specifies the VRF name from 1–64 characters.

Calculating the MD5 digest

Calculate the MD5 digest to verify the MD5 checksum. The **`md5`** command calculates the MD5 digest for files on the switch flash or PCMCIA and either displays the output on screen or stores the output in a file that you specify. An **`md5`** command option compares the calculated MD5 digest with that in a checksum file on flash or PCMCIA, and displays the compared output on the screen. By

verifying the MD5 checksum, you can verify that the file transferred properly to the switch. This command is available from both the boot monitor and runtime ACLI.

The MD5 file, **p80a5000.md5**, is provided with the Release 5.0 software. This contains the MD5 checksums of all software Release 5.0 files. Calculate the MD5 digest by performing this procedure.

Important:

If the MD5 key file parameters change, you must remove the old file and create a new file.

Prerequisites

- Use the **md5** command with reserved files (for example, a password file) only if you possess sufficient permissions to access these files.
- A checksum file is provided with the images for download. Transfer your image files to the switch and use the **md5** command to ensure that the checksum of the images on the switch is the same as the checksum file.
- You must log on to the Privileged EXEC mode in the ACLI.

Procedure steps

1. Calculate the MD5 digest by using the following command:

   ```
   md5 <filename> [-a] [-c] [-f] [-r]
   ```

Variable definitions

Use the data in the following table to use the `md5` command.

Variable	Value
-a	Adds data to the output file instead of overwriting it. You cannot use the -a option with the -c option.
-c	Compares the checksum of the specified file by <*filename*> with the MD5 checksum present in the checksum file name. You can specify the checksum file name using the -f option. If the checksum filename is not specified, the file /flash/checksum.md5 is used for comparison. If the supplied checksum filename and the default file are not available on flash, the following error message appears: Error: Checksum file <*filename*> not present.

Table continues…

Variable	Value
	The -c option also: • calculates the checksum of files specified by *filename* • compares the checksum with all keys in the checksum file, even if filenames do not match • displays the output of comparison

-f <*checksum-file-name*>	Stores the result of MD5 checksum to a file on flash or PCMCIA.
	If the output file specified with the **-f** option is one of the:
	• reserved filenames on the switch, the command fails with the error message:
	`Error: Invalid operation.`
	• files for which MD5 checksum is to be computed, the command fails with the error message:
	`Ethernet Routing Switch-8610:5# md5 *.cfg -f config.cfg`
	`Error: Invalid operation on file <filename>`
	If the checksum filename specified by the **-f** option exists on the switch (and is not one of the reserved filenames), the following message appears on the switch:
	`File exists. Do you wish to overwrite? (y/n)`

-r	Reverses the output. Use with the **-f** option to store the output to a file. The -r option cannot be used with the -c option.

Resetting system functions

Reset system functions to reset all statistics counters, the modem port, the console port, and the operation of the switchover function by performing this procedure.

Prerequisites

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

Procedure steps

1. Change to the backup SF/CPU by using the following command:

   ```
   sys action cpu-switch-over
   ```

2. Reset system functions by using the following command:

   ```
   sys action reset {console|counters|modem}
   ```

Variable definitions

Use the data in the following table to use the `sys action` command.

Variable	Value
cpuswitchover	Resets the switch to change over to the backup SF/CPU.
reset {console|counters|modem}	Reinitializes the hardware universal asynchronous receiver transmitter (UART) drivers. Use this command only if the console or modem connection is hung. Resets all the statistics counters in the switch to zero. Resets the modem port.

Example of resetting system functions

1. Reset the switch to change over to the backup SF/CPU:

   ```
   ERS-8606:5(config)# sys action cpuswitchover
   ```

2. Reset the statistics counters:

   ```
   ERS-8606:5(config)# sys action reset counters Are you sure you want
   to reset system counters (y/n)? y
   ```

Sourcing a configuration

Source a configuration to merge a script file into the running configuration by performing this procedure.

Prerequisites

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

Procedure steps

1. Source a configuration by using the following command:

   ```
   source <file> [stop] [debug] [syntax]
   ```

Variable definitions

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

Variable	Value
debug	Debugs the script output.
file	Specifies a filename and location from 1–99 characters. Use the format {a.b.c.d:|peer:|/pcmcia/|/flash/}<file>
stop	Stops the merge after an error occurs.
syntax	Verifies the script syntax.

Chapter 34: Multicast group ID reservation using the ACLI

This chapter provides procedures to create multicast group ID (MGID) reservations using the Avaya command line interface (ACLI).

Prerequisites to multicast group ID reservation

- To perform the procedures in this section, you must log on to the Global Configuration mode in the ACLI. For more information about using ACLI, see *Avaya Ethernet Routing Switch 8800/8600 User Interface Fundamentals, NN46205-308*.

Job aid

The following table lists the commands and their parameters that you use to complete the procedures in this section.

Table 41: Job aid

Command
Global Configuration mode
sys max-vlan-resource-reservation
sys multicast-resource-reservation <*value*>

Enabling maximum VLAN mode

Enable maximum VLAN mode to use all available MGIDs for VLANs. No IP multicast (IPMC) traffic transmits if you enable maximum VLAN mode. Enable maximum VLAN mode by performing this procedure.

Prerequisites

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

Procedure steps

1. Enable maximum VLAN mode by using the following command:

   ```
   sys max-vlan-resource-reservation
   ```

Reserving MGIDs for IPMC

Reserve MGIDs for IPMC to increase the number of IPMC traffic streams supported on the system by performing this procedure.

Prerequisites

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

Procedure steps

1. Reserve MGIDs for IPMC by using the following command:

   ```
   sys multicast-resource-reservation <value>
   ```

Variable definitions

Use the data in the following table to use the `sys multicast-resource-reservation` command.

Variable	Value
value	Specifies the number of MGIDs to reserve for IPMC traffic. Select from the range of 64–4083. The default value is 2048. To set this option to the default value, use the default operator with the command.

Chapter 35: ACLI show command reference

This reference information provides show commands to view the operational status of the Avaya Ethernet Routing Switch 8800/ 8600.

Access, logon names, and passwords

Use the **show cli password** command to display the access, logon name, and password combinations. The syntax for this command is as follows.

```
show cli password
```

The following figure shows output from the **show cli password** command.

```
access-level
aging     90

min-passwd-len 10
password-history 3

ACCESS    LOGIN            STATE
rwa       rwa              NA
rw        rw               ena
l3        l3               ena
l2        l2               ena
l1        l1               ena
ro        ro               ena

l4admin   l4admin          ena
slbadmin  slbadmin         ena
oper      oper             ena
l4oper    l4oper           ena
slboper   slboper          ena
ssladmin  ssladmin         ena
Default Lockout Time       60
Lockout-Time:
            IP                    Time
```

Figure 38: show cli password command output

Basic switch configuration

Use the **show basic config** command to display the basic switch configuration. The syntax for this command is as follows.

```
show basic config
```

The following figure shows the output of this command.

```
            setdate : N/A
mac-flap-time-limit : 500
 auto-recover-delay : 30
```

Figure 39: show basic config command output

Current switch configuration

Use the **show running-config** command to display the current switch configuration. The syntax for this command is as follows.

```
show running-config [mode (cli|acli)][module <value>][verbose]
```

The following table explains parameters for this command.

Table 42: Command parameters

Parameter	Description
mode (cli|acli)	Selects the mode between CLI and ACLI.
module *<value>*	**module** *<value>* specifies the command group for which you are requesting configuration settings. The options are: • cli • sys • web • rmon • vlan • port • qos • traffic-filter • mlt • stg • ip • diag • dvmrp • radius • ntp • lacp • cluster

Table continues…

Parameter	Description
	• bootp • filter • ipv6
`verbose`	Specifies a complete list of all configuration information about the switch.

If you make a change to the switch, it is displayed under that configuration heading. shows a subset of the output of this command.

```
Preparing to Display Configuration...
#
# TUE NOV 06 18:38:57 2007 UTC
# box type             : ERS-8010
# software version     : REL4.2.0.0_B118
# monitor version      : 4.2.0.0/118
# cli mode             : NNCLI
#

#
# Asic Info :
# SlotNum|Name    |CardType  |MdaType    |Parts Description
#
# Slot  1 ERS SDM 8660 0x70e20108 0x00000000  BFM: OP=3 TMUX=2 RARU=4 CPLD=9
# Slot  2 8683XLR  0x24334103 0x00000000  RSP=25 CLUE=2 F2I=1 F2E=1 FTMUX=17 CC=
3 FOQ=267 DPC=184 BMC=776 PIM=0 MAC=0
# Slot  3 8672ATM  0x20550108 0x20541204  0x20551201  BFM: OP=2 TMUX=2 RARU=2 CP
LD=4
# Slot  4 8648GTR  0x24220130 0x00000000  RSP=25 CLUE=2 F2I=1 F2E=1 FTMUX=17 CC=
3 FOQ=266 DPC=184 BMC=776 PIM=3 MAC=2
# Slot  5 8692SF   0x200e0100 0x00000000  CPU: CPLD=19 MEZZ=4  SFM: OP=3 TMUX=2
SWIP=23 FAD=16 CF=104
# Slot  6   --     0x00000001 0x00000000
# Slot  7   --     0x00000001 0x00000000
# Slot  8   --     0x00000001 0x00000000
# Slot  9   --     0x00000001 0x00000000
# Slot 10 8683POSE 0x20452106 00000001  0x20450201  00000001  BFM: OP=3 TMUX=2 R
ARU=4 CPLD=5
#

#!flags m-mode false
#!flags enhanced-operational-mode false
#!flags vlan-optimization-mode false
#!flags global-filter-ordering false
#!flags r-mode false
#!resource-reservation max-vlan false
#!resource-reservation multicast 2048
#!flags multicast-check-packet true
#!flags system-monitor true
#!record-reservation filter 4096
#!record-reservation ipmc 500
#!record-reservation local 2000
#!record-reservation mac 2000
#!record-reservation static-route 200
#!record-reservation vrrp 500
#!system-monitor monitoring-enable true
#!system-monitor detection-time 30
#!power enable true
#!power slot-priority 1 high
#!power slot-priority 2 high
#!power slot-priority 3 high
#!power slot-priority 4 high
#!power slot-priority 7 high
#!power slot-priority 8 high
#!power slot-priority 9 high
#!power slot-priority 10 high
#!end
#
config terminal

--More-- (q = quit)
```

Figure 40: show running-config partial output

If you add **`verbose`** to the **`show running-config`** command, the output contains current switch configuration including software (versions), performance, VLANs (such as numbers, port members), ports (such as type, status), routes, OSPF (such as area, interface, neighbors), memory, interface,

and log and trace files. With the verbose command, you can view the current configuration and default values.

Note:

The switch does not display all SNMPv3 target parameters when you enter the **show running-config** command. This is the expected behavior.

CLI settings

Use the **show cli info** command to display information about the ACLI configuration. The syntax for this command is as follows.

```
show cli info
```

The following figure shows sample output from the **show cli info** command.

```
cli configuration

more            : true
screen-lines    : 23
telnet-sessions : 8
rlogin-sessions : 8
timeout         : 900 seconds
monitor duration: 300 seconds
monitor interval: 5 seconds

use default login prompt    : true
default login prompt        : Login:
custom login prompt         : Login:
use default password prompt : true
default password prompt     : Password:
custom password prompt      : Password:
prompt : ERS-8610
```

Figure 41: show cli info command output

Hardware information

Use the **show sys info** command to display system status and technical information about the switch hardware components. The command displays several pages of information, including general information about the system (such as location), chassis (type, serial number, and base MAC address), temperature, power supplies, fans, cards, system errors, port locks, topology status, and message control information.

Important:

The user interfaces vary in how they identify and describe the system and chassis information. While the system description for your Ethernet Routing Switch 8800 correctly identifies the switch as an 8800 Series, the chassis information can identify the chassis as an 8010 or an 8006. The system description is correct. Use the **show tech** or **show sys info** command

using CLI to find the system description for your Ethernet Routing Switch 8600 or 8800 Series switch.

The syntax for this command is as follows.

```
show sys info [card] [asic] [mda] [gbic]
```

The following table explains parameters for this command.

Table 43: Command parameters

Parameter	Description
`info`	Specifies the current settings.
`card`	Specifies information about all the installed modules.
`asic`	Specifies information about the application-specific integrated circuit (ASIC) installed on each module.
`mda`	Specifies information about installed media dependent adapters (MDA).
`gbic`	Specifies information about installed gigabit interface converters (GBIC).

The following figure shows partial output from the **`show sys info`** command.

```
General Info :

        SysDescr     : ERS-8606 (4.2.0.0)
        SysName      : ERS-8606
        SysUpTime    : 14 day(s), 21:48:39
        SysContact   : rick.dean@innovatia.net
        SysLocation  : Saint John, T3

Chassis Info :

        Chassis      : 8006
        Serial#      : SSNM0600Q2
        HwRev        : A
        H/W Config   :
        NumSlots     : 6
        NumPorts     : 30
        GlobalFilter: enable
        VlanBySrcMac: disable
        Ecn-Compatib: enable
        WsmDirectMode : disable
        max-vlan-resource-reservation : (disable) -> (disable)
        multicast-resource-reservation : (2000) -> (2000)
        BaseMacAddr : 00:80:2d:c1:34:00
        MacAddrCapacity : 1024
        Temperature : 23 C
        MgmtMacAddr : 00:80:2d:c1:37:f4
        System MTU  : 9600
        clock_sync_time : 60

Power Supply Info :

        Ps#1 Status       : up
        Ps#1 Type         : ac
        Ps#1 Description  : 8001 690W 110/220V AC Power Supply
        Ps#1 Serial Number: ARTS010313
        Ps#1 Version      : A
        Ps#1 Part Number  : 202067

        Ps#2 Status       : empty

        Ps#3 Status       : down
        Ps#3 Type         : Unknown
        Ps#3 Description  : UNKNOWN
        Ps#3 Serial Number:
        Ps#3 Version      :
        Ps#3 Part Number  :

Power Usage Info :
        Total Power Available : 690
        Total Power Usage     : 265

Fan Info :

        Fan#1: up, air temp: 22 C

Card Info :

        Slot#         FrontType  FrontHw    Oper   Admin  BackType   BackHw
                                 Version  Status  Status           Version
            2  30X1000BaseX-SFP       02      up      up      DPM3        03
            5               CPU       01      up      up      FSFM        02

MezzCard Info :

        Slot#5: MezzCard is running Admin status: enabled  Oper Status: up

System Error Info :
```

Figure 42: show sys info command (partial output)

Memory size for secondary CPU

Use the **show boot config** command to display the secondary CPU DRAM memory size, in hexadecimal format.

From the Privileged Executive command prompt, the syntax for this command is as follows: **show boot config general**

Example of show boot config general command output

The following is an example of the screen output for the **show boot config general** command.

```
ERS-8610:5#show boot config general

CPU Slot 5:    PMC280-B-MV-B-MPC7447A (1.1)

Version:       5.1.0.0/022

Memory Size:   0x10000000

ERS-8610:5#
```

NTP show commands

NTP global status

Use the `show ntp` command to display the NTP administrative status, interval setting, and source IP address. The syntax for this command is as follows:

```
show ntp
```

NTP key status

Use the `show ntp key` command to display the NTP key status. The syntax for this command is as follows:

```
show ntp key
```

NTP server status

Use the `show ntp server` command to display the NTP server status. The syntax for this command is as follows:

```
show ntp server
```

NTP statistics

Use the `show ntp statistics` command to view the following information:

- Stratum

- Version
- Sync Status
- Reachability
- Root Delay
- Precision
- Access Attempts — Number of NTP requests sent to this NTP server
- Server Synch — Number of times this NTP server updated the time
- Server Fail — Number of times this NTP server was rejected attempting to update the time

The syntax for this command is as follows.

```
show ntp statistics
```

The following figure shows sample command output.

```
              NTP Server : 134.177.216.230
-----------------------------------------
                 Stratum : 5
                 Version : 3
             Sync Status : synchronized
             Reachability: reachable
              Root Delay : 0.19053647
               Precision : 0.00003051
         Access Attempts : 1
            Server Synch : 1
             Server Fail : 0
```

Figure 43: show ntp statistics command output

Power summary

Use the **show sys power** command to view a summary of the power information for the chassis.

The syntax for this command is as follows.

```
show sys power
```

The following figure shows sample command output.

```
================================================================================
                          Chassis Power Information
================================================================================
Chass   TotalPS TotalPS TotalPS  TotalPS Consumed Consumed Consumed Consumed
Type    Max     Rail-3V Rail-12V Thermal Max      Rail-3V  Rail-12V Thermal
--------------------------------------------------------------------------------
8006    690     300     300      500     265      105      160      100
--------------------------------------------------------------------------------
```

Figure 44: show sys power command sample output

Power management information

Use the **show sys power global** command to view a summary of the power redundancy settings.

The syntax for this command is as follows.

```
show sys power global
```

The following figure shows sample command output.

```
ERS-8610:5>show sys power global
                                power-check-enable : (true) -> true
                                fan-check-enable : (true) -> true
                                slot 1 : (high) -> high
                                slot 2 : (high) -> high
                                slot 3 : (high) -> high
                                slot 4 : (high) -> high
                                slot 5 : critical
                                slot 6 : critical
                                slot 7 : (high) -> high
                                slot 8 : (high) -> high
                                slot 9 : (high) -> high
                                slot 10 : (high) -> high
```

Figure 45: show sys power global command sample output

Power information for power supplies

Use the **show sys power power-supply** command to view detailed power information for each power supply.

The syntax for this command is as follows.

```
show sys power power-supply
```

The following figure shows sample command output.

```
ERS-8610:5>show sys power power-supply

================================================================================
                          Power Supply Information
================================================================================
Power Type Serial          Part            Input     Oper        Max   Rail3 Rail12
Slot       Num             Num             Line      Status      Power Power Power
                                                     (Line V)
--------------------------------------------------------------------------------
PS# 1  Unknown                                 110V      dwn(110V) 410   406   390
PS# 2  ac    ARTSAT008319     314463          110V      up (110V) 1050  507   864
--------------------------------------------------------------------------------
ERS-8610:5>_
```

Figure 46: show sys power power-supply command sample output

Slot power details

Use the **show sys power slot** command to view detailed power information for each slot.

The syntax for this command is as follows.

```
show sys power slot
```

The following figure shows sample command output.

```
================================================================================
                          Slot Power Consumption
================================================================================
Slot CardType            Type  Priority    Power  Max   Rail-3V Rail-12V Thermal
No.                            (applicable Status Power Power   Power    Power
                               (only for
                               (R&RS Mod)
--------------------------------------------------------------------------------
2    8630GBR             RMod  high        ON     180   60      120      50
5    8692SF              CPU   critical    ON     85    45      40       50
--------------------------------------------------------------------------------
```

Figure 47: show sys power slot command sample output

System information

Use the **show sys** command to display system status and technical information about the switch hardware components and software configuration. The command displays several pages of information, including general information about the system (such as location), chassis (type, serial number, and base MAC address), temperature, power supplies, fans, cards, system errors, port locks, topology status, and message control information. The syntax for this command is as follows.

```
show sys
```

The following table explains parameters for this command.

Parameter	Description
8648gtr	Specifies technical information about the 8648gtr settings, see Figure 48: show sys 8648gtr command output on page 357.
action	Specifies the configuration for the system action parameter, see Figure 49: show sys action command output on page 357.
dns	Specifies the DNS default domain name, see Figure 50: show sys dns command output on page 357.
ecn-compatibility	Specifies the status of Explicit Congestion Notification (ECN) compatibility, either enabled or disabled.
ext-cp-limit	Specifies the ext-cp-limit settings, see Figure 51: show sys ext-cp-limit command output on page 357.
flags	Specifies the configuration of system flags, see Figure 52: show sys flags command output on page 357.
force-msg	Specifies the message control force message pattern settings.
global-filter	Specifies the status of system global filter settings, either enabled or disabled.

Table continues…

Parameter	Description
mcast-smlt	Specifies the settings for multicast over Split MultiLink Trunking (MLT).
mgid-usage	Specifies the multicast group ID (MGID) usage for VLANs and multicast traffic, see Figure 53: show sys mgid-usage command output on page 357.
msg-control	Specifies the system message control function status (activated or disabled), see Figure 54: show sys msg-control command output on page 358.
mtu	Specifies system maximum transmission unit (MTU) information.
performance	Specifies system performance information, such as CPU utilization, switch fabric utilization, Non-Volatile Random Access Memory (NVRAM) size, and NVRAM used. The information is updated once a second, see Figure 55: show sys performance command output on page 358.
power	Specifies power information for the chassis. Command options are: • **group**—power management settings • **power-supply**—power information for each power supply • **slot**—power information for each slot
setting	Display system settings, see Figure 57: show sys setting command output on page 358.
smlt-on-single-cp	Specifies whether smlt-on-single-cp is enabled or disabled and what the timer value is set to.
software	Specifies the version of software running on the switch, the last update of that software, and the Boot Config Table. The Boot Config Table lists the current system settings and flags, see Figure 58: show sys software command output on page 359.
stats	Specifies system statistics. For more information about statistics, see *Avaya Ethernet Routing Switch 8800/8600 Performance Management, NN46205-704*.
topology-ip	Specifies the topology IP address from the available CLIP.
vlan-bysrcmac	Specifies the status of VLANs created by source MAC address, either enabled or disabled.

The following figure shows output from the **show sys 8648gtr** command.

```
high-control-priority-mac    0    01:80:c2:00:00:00
high-control-priority-mac    1    01:00:5e:00:00:05
high-control-priority-mac    2    01:00:5e:00:00:06
high-control-priority-mac    3    01:00:5e:00:00:09
high-control-priority-mac    4    01:00:5e:00:00:04
high-control-priority-mac    5    01:00:5e:00:00:12
```

Figure 48: show sys 8648gtr command output

The following figure shows output from the **show sys action** command.

```
cpuswitchover : (N/A)
 resetconsole : (N/A)
resetcounters : (N/A)
   resetmodem : (N/A)
```

Figure 49: show sys action command output

The following figure shows output from the **show sys dns** command.

```
DNS Default Domain Name : ERS8600SJ
Primary DNS server details:
===========================
         IP address : 1111:0:0:0:0:0:0:1
         Status     : Inactive
         Total DNS Number of request made to this server : 0
         Number of Successful DNS : 0
```

Figure 50: show sys dns command output

The following figure shows output from the **show sys ext-cp-limit** command.

```
extcplimit           : disable
max-ports-to-check   : 0
min-congestion-time  : 3000
port-congestion-time : 5
trap-level           : None
```

Figure 51: show sys ext-cp-limit command output

The following figure shows output from the **show sys flags** command.

```
global-filter-ordering: (false) -> false
multicast-check-packet: (true) -> true
regular-Autoneg: (false) -> false
take-iocard-offline: (false) -> false
auto-reset-fabric: (false) -> false
```

Figure 52: show sys flags command output

The following figure shows output from the **show sys mgid-usage** command.

```
Number of MGIDs used for VLANs : (1709)
Number of MGIDs used for SPBM : (519)
Number of MGIDs used for multicast : (1024)
Number of MGIDs remaining for VLANs : (832)
Number of MGIDs remaining for multicast : (0)
```

Figure 53: show sys mgid-usage command output

The following figure shows output from the **show sys msg-control** command.

```
Message Control Info :
        action                  : suppress-msg
        control-interval        : 5
        max-msg-num             : 5
        status                  : disable
```

Figure 54: show sys msg-control command output

The following figure shows output from the **show sys performance** command.

```
              CpuUtil: 12%
     SwitchFabricUtil: 0%
OtherSwitchFabricUtil: 0%
           BufferUtil: 0%
             DramSize: 512 M
             DramUsed: 28 %
             DramFree: 373873 K
```

Figure 55: show sys performance command output

The following figure shows output from the **show sys record-reservation** command.

```
================================================================================
                            HW Record Reservation
================================================================================

Record Type       Used Reserved New-Reserved Def-Reserved
--------------------------------------------------------------------------------
filter               2     4096         4096         4096
ipmc                 0      500          500          500
local                6     2000         2000         2000
mac                 65     2000         2000         2000
static-route         0      200          200          200
vrrp                 0      500          500          500
--------------------------------------------------------------------------------
TOTAL               73     9296         9296         9296
```

Figure 56: show sys record-reservation command output

The following figure shows output from the **show sys setting** command.

```
        mgmt-virtual-ip : 0.0.0.0/0.0.0.0
      mgmt-virtual-ipv6 : 0:0:0:0:0:0:0:0/0
          udp-checksum : enable
            udp-source : disable
        clock-sync-time : 60
    mroute-stream-limit : disable
               contact : http://support.nortel.com/
              location : 4655 Great America Parkway,Santa Clara,CA 95054
                  name : ERS-8610
              portlock : off
  sendAuthenticationTrap : false
              topology : on
         globalFilter : enable
         vlanBySrcMac : disable
      ecn-compatibility : enable
        wsm-direct-mode : disable
     smlt-on-single-cp : disable timer 3
  max-vlan-resource-reservation : (disable) -> (disable)
  multicast-resource-reservation : (2048) -> (2048)
           System MTU : 1950
```

Figure 57: show sys setting command output

The following figure shows output from the **show sys software** command.

```
System Software Info :

Default Runtime Config File : /flash/config.cfg
Default Boot Config File : /flash/boot.cfg
Config File :
Last Runtime Config Save : MON NOV 05 22:24:07 2007
Last Runtime Config Save to Slave : 0
Last Boot Config Save : 0
Last Boot Config Save on Slave : 0

Boot Config Table
Slot# : 5
Version : Build REL4.2.0.0_B117 on Thu Oct 11 19:39:45 EDT 2007
LastBootConfigSource : /flash/boot.cfg
LastRuntimeImageSource : /flash/p80a4200b117.img
LastRuntimeConfigSource : /flash/config.cfg
PrimaryImageSource : /flash/p80a4200b117.img
PrimaryConfigSource : /flash/config.cfg
SecondaryImageSource : /flash/p80a4200.img
SecondaryConfigSource : /flash/config.cfg
TertiaryImageSource : 0.0.0.0:
TertiaryConfigSource : /flash/config.cfg

LastRunTimeMezzSource: /flash/mezz.img
EnableAutoBoot : true
EnableFactoryDefaults : false
EnableDebugMode : false
EnableHwWatchDogTimer : true
EnableRebootOnError : true
EnableTelnetServer : true
EnableRloginServer : false
EnableFtpServer : true
EnableTftpServer : true
EnableMezz : true

DLD software:
Slot#  2: file /flash/p80j4200.dld version 4.2.0.0/117
```

Figure 58: show sys software command output

System status (detailed)

Use the **show tech** command to display technical information about system status and information about the hardware, software, and operation of the switch.

The information available from the **show tech** command includes general information about the system (such as location), hardware (chassis, power supplies, fans, and modules), system errors, boot configuration, software versions, memory, port information (locking status, configurations, names, interface status), VLANs and STGs (numbers, port members), OSPF (area, interface, neighbors), VRRP, IPv6, RIP, PIM, PGM, and log and trace files. This command displays more information than the similar **show sys-info** command. The syntax for this command is as follows.

```
show tech
```

The following figure shows representative output from the **show tech** command.

```
ERS-8606:5#show tech

Sys Info:
---------------


General Info :

        SysDescr     : ERS-8606 (4.2.0.0)
        SysName      : ERS-8606
        SysUpTime    : 0 day(s), 05:37:14
        SysContact   : support@nortelnetworks.com
        SysLocation  : 4655 Great America Parkway,Santa Clara,CA 95054

Chassis Info :

        Chassis     : 8006
        Serial#     : SSNM0600Q2
        HwRev       : A
        H/W Config  :
        NumSlots    : 6
        NumPorts    : 3
        GlobalFilter: enable
        VlanBySrcMac: disable

        Ecn-Compatib: enable
        WsmDirectMode : disable
        max-vlan-resource-reservation : (disable) -> (disable)
        multicast-resource-reservation : (2048) -> (2048)
        BaseMacAddr : 00:80:2d:c1:34:00
        MacAddrCapacity : 1024
        Temperature : 24 C
        MgmtMacAddr : 00:80:2d:c1:37:f4
        System MTU  : 1950
        clock_sync_time : 60
```

Figure 59: show tech command partial output

Users logged on

Use the **show users** command to display a list of users who are logged on to the switch. The syntax for this command is as follows.

```
show users
```

The following figure shows output from the **show users** command.

```
SESSION   USER              ACCESS    IP ADDRESS
Telnet1   rwa               rwa       207.179.154.87
Console                     none
Modem                       none
```

Figure 60: show users command output

Chapter 36: Chassis operations configuration using Enterprise Device Manager

This chapter provides the details to configure operating modes and basic hardware and system settings.

Editing system information

You can edit system information such as the contact person, the name of the device, and its location. Other information cannot be edited, but is very useful, such as the software version running on the device.

Edit system information by performing this procedure.

Procedure steps

1. In the navigation tree, open the following folders: **Configuration** > **Edit** .
2. Click **Chassis**. The **System** tab is displayed.
3. Edit the required options.
4. Click **Apply**.
5. Click **Close**.

Variable definitions

Use the data in the following table to configure the Chassis, Systemtab.

Variable	Value
sysDescr	Shows the system assigned name and the current, running software version.

Table continues…

Variable	Value
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 device name.
sysLocation	Configures the physical location of the device. The default location is 4655, Great America Parkway, Santa Clara, CA - 95054.
VirtualIpAddr	Configures the virtual IP address advertised by the master SF/CPU. Unlike the management port IP address, the virtual IP address is stored in the switch configuration file, not the boot configuration file. The default IP address is 0.0.0.0.
VirtualNetMask	Configures the net mask of the virtual management IP address. The default net mask is 0.0.0.0.
VirtualIpv6Address	Configures the virtual IPv6 address advertised by the master SF/CPU. Unlike the management port IPv6 address, this address is stored in the switch configuration file, not the boot configuration file. The default address is 0:0:0:0:0:0:0:0.
VirtualIPv6PrefixLength	Configures the length of the virtual IPv6 prefix entry. The default is 0.
DnsDomainName	Configures the default domain for querying the DNS server.
LastChange	Specifies the time since the last configuration change.
LastVlanChange	Specifies the time since the last VLAN change.
LastStatisticsReset	Specifies the time since the statistics counters were last reset.
LastRunTimeConfigSave	Specifies the last run-time configuration saved.
LastRunTimeConfigSaveToSlave	Specifies the last run-time configuration saved to the standby device.
LastBootConfigSave	Specifies the last boot configuration saved.
LastBootConfigSaveOnSlave	Specifies the last boot configuration saved on the standby device.
DefaultRuntimeConfigFileName	Specifies the default Runtime Configuration File directory name.
DefaultBootConfigFileName	Specifies the default Boot Configuration File directory name. The default name is /flash/boot.cfg.
ConfigFileName	Specifies the name of a new boot or runtime configuration file. For more information, see saveBootConfig and saveRuntimeConfig in ActionGroup1. The default name is /flash/config.cfg.
ConfigMode	This is used in conjunction with the Action field in order to decide the mode in which the config file is going to be saved.

Table continues…

Variable	Value
ActionGroup1	Specifies one of the following actions: • `resetCounters` —resets all statistic counters. • `saveRuntimeConfig`—saves the current run-time configuration to the file specified in ConfigFileName. If the configFileName field is blank, the switch saves the run-time configuration to the current run-time configuration file. • `saveRuntimeConfigToSlave`—saves the current run-time configuration to the secondary SF/CPU. • `saveBootConfig`—saves the current boot configuration to the file specified in ConfigFileName. If the configFileName field is blank, the switch saves the boot configuration to the current boot configuration file. • `saveSlaveBootConfig`—saves the current boot configuration to the secondary SF/CPU. • `loadLicense`—loads a software license file to enable features.
ActionGroup2	Specifies one of the following actions: • `resetIstStatCounters`—resets the IST statistic counters. • `resetLspStats`—resets the LSP statistics
ActionGroup3	`flushIpRouteTbl`—flushes IP routes from the routing table.
ActionGroup4	Specifies one of the following actions: • `hardReset`—resets the device and runs power-on tests. • `softReset` —resets the device without running power-on tests. • `cpuSwitchOver`—swaps control from one SF/CPU to another. • `resetConsole`—reinitializes the hardware UART drivers. Reset the console only if the console or modem connection is hanging. • `resetModem`—reinitializes the UART drivers on the modem port. Reset the modem only if the console or modem connection is hunging.
Result	Specifies a message after you click Apply.

Editing chassis information

Edit the chassis information to make changes to chassis-wide settings by performing this procedure.

Important:

The user interfaces vary in how they identify and describe the system and chassis information. While the system description for your Ethernet Routing Switch 8800 correctly identifies the switch as an 8800 Series, the chassis information can identify the chassis as an 8010 or an 8006. The system description is correct. Use the **`show tech`** or **`show sys info`** command using CLI to find the system description for your Ethernet Routing Switch 8600 or 8800 Series switch.

Procedure steps

1. On the Device Physical View, select the chassis.
2. In the navigation tree, open the following folders: **Configuration** > **Edit** .
3. Click **Chassis**. The Chassis screen appears with the **System** tab displayed.

   Edit the necessary options.
4. Click **Apply**.

Variable definitions

Use the data in the following table to configure the Chassistab.

Variable	Value
Type	Specifies the Ethernet Routing Switch 8800/8600 module type.
SerialNumber	Specifies a unique chassis serial number.
HardwareRevision	Specifies the current hardware revision of the device chassis.
NumSlots	Specifies the number of slots (or cards) this device can contain.
NumPorts	Specifies the number of ports currently on this device.
BaseMacAddr	Specifies the starting point of the block of MAC addresses used by the switch for logical and physical interfaces.
MacAddrCapacity	Specifies the MAC address capacity. The default value is 4096.
MacFlapLimitTime	Configures the time limit for the loop-detect feature, in milliseconds, for MAC flapping. The value ranges from 10 to 5000. The default value is 500.
AutoRecoverDelay	Configures the delay in autorecovery. The value ranges from 5 to 3600. The default is 30 seconds.
MTUSize	Configures the maximum transmission unit size. The default is 1950.
Temperature	Specifies the current temperature of the chassis in degrees Celsius.

Table continues…

Variable	Value
PrimaryCPUType	Specifies the primary SF/CPU type; for example, the 8692SuperMezz SF/CPU.
PrimaryCPUMemory	Specifies the primary SF/CPU memory size; for example, 256 MB.
SecondaryCPUType	Specifies the secondary SF/CPU type; for example, the 8692SuperMezz SF/CPU.
SecondaryCPUMemory	Specifies the secondary SF/CPU memory size; for example, 256 MB.
PowerUsage	Specifies the amount of power the SF/CPU uses. The default value is 665.
PowerAvailable	Specifies the amount of power available to the SF/CPU. The default is 1050.

Configuring system flags

Configure the system flags to enable or disable flags for specific configuration settings by performing this procedure.

Procedure steps

1. On the Device Physical View, select chassis.
2. In the navigation tree, open the following folders: **Configuration** > **Edit** .
3. Click **Chassis**.
4. Click the **System Flags** tab.
5. Select the system flags you want to set.
6. You can assign a specific mode by selecting it in the mode section of the dialog box.
7. Click **Apply**.

Important:

After you change certain configuration parameters, you must save the changes to the configuration file and restart the switch before the changes take effect. For more information about which parameters require a switch reset, see the value descriptions in Variables definitions.

Variable definitions

Use the data in the following table to configure the Chassis, System Flags tab.

Variable	Value
AuthenticationTraps	Activates Authentication traps. If you change this parameter, you must restart the system for the change to take effect.
EnableAccessPolicy	Activates access policies. If you change this parameter, you must restart the system for the change to take effect.
MrouteStreamLimit	Enables or disables Mroute Stream Limit. If you change this parameter, you must restart the system for the change to take effect.
ForceTrapSender	Configures CLIP (Circuit Less IP) as a trap originator. If you change this parameter, you must restart the system for the change to take effect.
ForceIpHdrSender	If you enable Force IP Header Senter, the system matches the IP header source address with SNMP header sender networks. If you change this parameter, you must restart the system for the change to take effect.
GlobalFilterEnable	Enables or disables the ordering of global filters by their ID in the system. If you change this parameter, you must restart the system for the change to take effect.
VlanBySrcMacEnable	Enables or disables source MAC based VLANs. If you change this parameter, you must restart the system for the change to take effect.
DiffServEcnCompatibilityEnable	Enables or disables the Explicit Congestion Notification (ECN) compatibility feature. If you select false, the system masks the ECN bits in the DS field while re-marking DSCP and does not match on ECN capable flows if the filter is set on DSmatch. If you select true, the system preserves the ECN bits in the DS field while re-marking and makes matches based on the full 8-bit DS field. If you change this parameter, you must restart the system for the change to take effect.
TakeIOCardOfflineEnable	Takes the I/O module offline when there are excessive resets during egress processing.
AutoResetFabricEnable	Enables or disables fabric to be reset on fabric memory full error.
ForceTopologyIpFlagEnable	Enables or disables the flag that sets the CLIP ID as the topology IP. Values are true or false. The default value is false (disabled).
CircuitlessIpId	Sets the CLIP ID to be used as the topology IP. Enter a value from 1 to 256.
SystemMonitorEnable	Activates or disables system monitoring in the switch. If you change this parameter, you must restart the system for the change to take effect.
MonitoringEnable	Starts or ends a monitoring session.
MonitorDetectionTime	Configures the interval, in seconds, for system monitoring, in a range from 10 to 600 seconds. The default value is 30.

Table continues…

Variable	Value
HaCpu	Activates or disables the High Availability CPU feature. If you change this parameter, you must restart the system for the change to take effect. The default value is disabled.
HaCpuState	Indicates the High Availability CPU state. • `initialization`—indicates the SF/CPU is in this state • `oneWayActive`—modules that need to be synchronized register with the framework (either locally or a message received from a remote SF/CPU) • `twoWayActive`—modules that need to be synchronized register with the framework (either locally or a message received from a remote SF/CPU) • `synchronized`—table-based synchronization is complete on the current SF/CPU • `remoteIncompatible`—SF/CPU framework version is incompatible with the remote SF/CPU • `error`—if an invalid event is generated in a specific state the SF/CPU enters Error state • `disabled`—High Availability is not activated • `peerNotConnected`—no established peer connection • `peerConnected`—established peer connection is established • `lostPeerConnection`—lost connection to peer or standby SF/CPU • `notSynchronized`—table-based synchronization is not complete The default is disabled.
HaEvent	Indicates the High Availability event status. • `restart`—causes the state machine to restart. • `systemRegistrationDone`—causes the SF/CPU to transfer to One Way or Two Way Active state. • `tableSynchronizationDone`—causes the SF/CPU to transfer to synchronized state. • `versionIncompatible`—causes the SF/CPU to go to remote incompatible state • `noEvent`—means no event occurred to date.
StandbyCpu	Indicates the state of the standby SF/CPU.

Enabling Fabric (FAB) Memory Full error handling

Use the procedure in this section to enable Fabric (FAB) Memory Full error handling to resolve the `Fab Memory Full` fault.

Procedure steps

1. On the Device Physical View, select chassis.
2. In the navigation tree, open the following folders: **Configuration** > **Edit** .
3. Click **Chassis**.
4. Click the **System Flags** tab.
5. Choose **TakeIOCardOfflineEnable.**
6. Choose **AutoResetFabricEnable.**
7. Click **Apply**.
8. Click **Yes** to confirm and reboot the chassis.

   Important:

   When enabled, **AutoResetFabricEnable** will cause the switch fabric to automatically reset when the Fabric (FAB) Memory Full error is detected. For redundant network designs, this will divert traffic around the affected switch and allow the network to recover with minimal interruption. If the network design does not support redundancy, then there will be network interruption while the switch is reset.

Enabling CPU High Availability

CPU high-availability (HA) mode enables switches with two CPUs to recover quickly from a failure of the master SF/CPU. Use the procedure in this section to enable HA CPU mode.

Procedure steps

1. On the Device Physical View, select chassis.
2. In the navigation tree, open the following folders: **Configuration** > **Edit** .
3. Click **Chassis**.
4. Click the **System Flags** tab.
5. In **HaCpu** section, select **Enable**.
6. Click **Apply**.

7. Click **Yes** to confirm.

   After enabling HA mode on the master SF/CPU, the secondary SF/CPU automatically resets to load settings from its previously-saved boot configuration file. You must manually reset the primary SF/CPU while the secondary SF/CPU is booting.

   Important:

   Failure to manually boot the primary CPU before the secondary finishes booting can lead to system instability. Traffic is interrupted when the master is manually reset.

Configuring a basic configuration

You can set options for a basic port configuration through the Interface tab in the Port dialog box. Additional tabs and screen entries for module-specific functions appear when applicable. For example, on the Interface dialog box for a port, tabs for Layer 3 (routing) functions appear if Device Manager accesses an Ethernet Routing Switch 8800/8600.

Configure the basic port configuration by performing this procedure.

Procedure steps

1. On the Device Physical View, select a port.
2. In the navigation tree, open the following folders: **Configuration** > **Edit** > **Port**.
3. Click **General** . The Port General screen appears with the **Interface** tab displayed.
4. Configure the fields as required.

   The 10/100Base-TX ports do not consistently autonegotiate with older 10/100Base-TX equipment. You can sometimes upgrade the older devices with new firmware or driver revisions. If an upgrade does not allow autonegotiation to correctly identify the link speed and duplex settings, you can manually configure the settings for the link in question. Check the Avaya Web site for the latest compatibility information.

5. Click **Apply**.

Variable definitions

Use the data in the following table to use theInterface tab.

Variable	Value
Index	A unique value, in a range from 64–511, assigned to each interface.

Table continues…

Variable	Value
Name	The name assigned to the port.
Descr	The port type of this interface.
Type	The media type of this interface.
Mtu	The size of the largest packet, in octets, the switch can send or receive on the interface (maximum transmission unit). The default is 1950.
PhysAddress	The MAC address assigned to a particular interface.
VendorDescr	The name of the interface chipset. (This does not apply to all port types.)
AdminStatus	AdminStatus is expressed as one of the following states: • up • down • testing After a managed system initializes, all interfaces start with AdminStatus in the up state. AdminStatus changes to either the down or the testing state (or remains in the down state) if you make explicit management action or if the managed system retains configuration information. The testing state indicates that the switch does not pass operational packets. The default state is up.
OperStatus	The current operational state of the interface expressed as one of the following states: • up • down • testing The testing state indicates that the switch does not pass operational packets. If AdminStatus is down, OperStatus is down. If AdminStatus changes to up, OperStatus changes to up if the interface is ready to transmit and receive network traffic. AdminStatus remains in the down state if, and only if, a fault exists that prevents it from going to the up state. The default operating status is down.
LastChange	The value of sysUpTime at the time the interface entered its current operational state. If the interface entered the current state prior to the last reinitialization of the local network management subsystem, the value is zero.
LinkTrap	Indicates whether the system generates link Up or link Down traps for this interface. The default setting is enabled.
AutoNegotiate	Indicates whether this port is activated for autonegotiations (only 10/100Base ports). Avaya recommends that you use

Table continues…

Variable	Value
	autonegotiation whenever it is supported by the devices on both ends of a Gigabit fiber link. If the Ethernet Routing Switch 8800/8600 is connected to a device that does not support it, disable autonegotiation and enable SFFD. The default setting is true. For more information, see *Avaya Ethernet Routing Switch 8800/8600 Planning and Engineering -- Network Design* (NN46205-200).
AdminDuplex	Indicates the current duplex value of the port as one of the following modes: • `half-duplex` • `full-duplex` The default is half-duplex.
OperDuplex	The current operational duplex mode of the port (half or full). The default is Full-duplex.
AdminSpeed	Indicates the port data rate (10 Mb/s or 100 Mb/s).
OperSpeed	The current operating data rate of the port.
AutoNegAd	The port speed to advertise.
QosLevel	Quality of Service level. The default is level 1.
DiffServ	Activates Differentiated Services on this port.
Layer3Trust	Configures the type of Differentiated Service to one of the following: • `none` • `access` • `core` The default is core.
MltId	The MultiLink Trunk to which the port is assigned. The default is 0.
Locked	Indicates whether or not the port is locked. If the port is locked, you cannot change the port configuration. To lock or unlock a port, select Edit, Security, Port Lock. The default is false.
UnknownMacDiscard	If you enable UnknownMacDiscard on a port, the system drops a packet with an unknown source MAC address on that port, and other ports discard packets that contain the unknown MAC address in the destination field. For example, if 11:22:33:44:55:66 is an unknown source MAC, packets tagged with a source MAC of 11:22:33:44:55 coming from this port are discarded; packets tagged with a destination MAC of 11:22:33:44:55:66 coming from other ports are also discarded, unless the address is learned on another port or the restriction ages out.

Table continues…

Variable	Value
	You must enable autolearn before you can set the unknown-mac-discard lock-autolearn-mac disable parameter.
DirectBroadcastEnable	Indicates whether this interface forwards direct broadcast traffic.
EgressRateLimitState	Enables or disables the administrative state of egress rate limit.
EgressRateLimit	Indicates the rate at which packets are egressing from this port. The range is from 1000 to 10 000 000 Kb per second.
AdminRouting	Indicates whether the port is routable.
OperRouting	The status of the port; whether it is routable.
HighSecureEnable	Activates or disables the high secure feature.
Layer 2 Override 8021p	Activates or disables IEEE 802.1p override. If activated, the 802.1p value from a tagged frame is not used.
Action	One of the following port-related actions: • `none` • `flushMacFdb`—flush MAC forwarding table for port • `flushArp`—flush ARP table for port • `flushIp`—flush IP route table for port • `flushAll`—flush all tables for port • `triggerRipUpdate`—manually update the RIP table • `clearLoopDetectAlarm`—manually enable the port on all the disabled vlans
Result	The result of port-related actions.

Editing ports

If you edit multiple ports, some options are not available, and other options appear to be available even though the dialog box or tab is not applicable. If a dialog box or tab does not apply for a port, you receive a NoSuchObject message.

If you edit a single port, dialog boxes and tabs that are not applicable are not available for the selection.

Edit multiple ports by performing this procedure.

Important:

If a port is modified while an alarm is active on the port, and the port sends faults to a Multiservice Data Manager (MDM) server. It is possible that duplicate alarms appear in the MDM Active Alarm browser due to a component name change. To clear these alarms, use the

procedure called Clearing Local Alarms in *Avaya Multiservice Data Manager (MDM) Fault Management — Tools, NN10470-011*.

Procedure steps

1. On the Device Physical View, select a port.
2. In the navigation tree, open the following folders: **Configuration** > **Edit** > **Port**.
3. A list appears with **General**, **IP**, and **IPv6** options displayed under **Port**.
4. Click on the required option to edit the ports.

Viewing the boot configuration

View the boot source, as well as view the source from which the switch started last by performing this procedure.

Procedure steps

1. On the Device Physical View, select chassis.
2. In the navigation tree, open the following folders: **Configuration** > **Edit**.
3. Click **Chassis**.
4. Click **Boot Config** tab.

Variable definitions

Use the data in the following table to use the Boot Configtab.

Variable	Value
Slot	Specifies the slot number of the device
SwVersion	Specifies the software version that is currently running
LastBootConfigSource	Specifies the last source from which the switch started
LastRuntimeImageSource	Specifies the last source for the run-time image
LastRuntimeConfigSource	Specifies the last source for the run-time configuration

Enabling jumbo frames

Enable Jumbo frames to increase the size of Ethernet frames supported on the chassis by performing this procedure.

Note:

After changing the MTU size, you must reboot the switch for the change to take effect.

Procedure steps

1. In the navigation tree, open the following folders: **Configuration** > **Edit**.
2. Click **Chassis**.
3. Click the **Chassis** tab.
4. Click **MTU size: 1522, 1950, or 9600**.
5. Click **Apply**.

Viewing the trap sender table

Use the trap sender table to view source and receiving addresses by performing this procedure.

Procedure steps

1. On the Device Physical View, select chassis.
2. In the navigation tree, open the following folders: **Configuration** > **Edit**.
3. Click **Chassis**.
4. Click the **Trap Sender Table** tab.

Variable definitions

Use the data in the following table to use the Chassis, Trap Sender Tabletab.

Variable	Value
RecvAddress	Specifies the IP address for the trap receiver. This variable is a read-only variable containing the IP address configured in the TAddress field in the TargetTable.
SrcAddress	Identifies the IP address for the trap sender.

Configuring the time

Set the date and time on the switch with the User Set Time tab by performing this procedure.

Procedure steps

1. On the Device Physical View, select chassis.
2. In the navigation tree, open the following folders: **Configuration** > **Edit**.
3. Click **,Chassis**.
4. Click the **User Set Time** tab.
5. Enter the correct details.
6. Click **Apply**.

Variable definitions

Use the data in the following table to configure the User Set Timetab.

Variable	Value
Year	Configures the year (integer from 1998–2097).
Month	Configures the month (integer from 1–12).
Date	Configures the day (integer from 1–31).
Hour	Configures the hour (integer from 0–23).
Minute	Configures the minute (integer from 0–59).
Second	Configures the second (integer from 0–59).

Configuring SLPP globally

Enable the Simple Loop Prevention Protocol (SLPP) to detect a loop and automatically stop it by performing this procedure.

Procedure steps

1. In the navigation tree, open the following folders: **Configuration** > **VLAN**.
2. Click **SLPP**.
3. In the Global tab, Select **GlobalEnable** check box.
4. In the **TransmissionInterval** box, enter a value for the time interval for loop detection.

5. In the **EtherType** box, enter the SLPP protocol value as a hexadecimal number.
6. Click **Apply**.

Variable definitions

Use the data in the following table to configure theSlpp dialog box.

Variable	Value
GlobalEnable	Enables or disables SLPP globally.
TransmissionInterval	Sets the interval for which loop detection occurs. The interval is expressed in milliseconds in a range from 500–5000. The default value is 500.
EtherType	Specifies the SLPP protocol identification. This value is expressed as a decimal in the range from 1 to 65535 or in hexadecimal from 0x001 to 0xffff. The default value is 0x8102.

Configuring the SLPP by VLAN

Activates SLPP on a VLAN to enable forwarding of the SLPP packet over the VLAN by performing this procedure.

Prerequisites

- Enable the SLPP globally before configuring it on a VLAN.

Procedure steps

1. In the navigation tree, open the following folders: **Configuration** > **VLAN**.
2. Click **SLPP**.
3. Click the **VLANS** tab.
4. Click **Insert**.
5. Click the **[...,]** button.
6. Select the desired VLAN ID.
7. Click **Ok**.
8. To enable SLPP, select the **SlppEnable** check box.
9. Click **Insert**.

The ID and status of the selected VLAN appears in the Insert VLANS dialog box.

Variable definitions

Use the data in the following table to configure the SLPP, Insert VLANS dialog box.

Variable	Value
VlanId	Specifies the VLAN. Click the ellipsis button to select from a list of VLANs.
SlppEnable	Enables SLPP on the selected VLAN. The SLPP packet transmission and reception process is active only if you enable the SLPP operation. When you disable the SLPP operation, the following occurs: • the system sends no SLPP packets • the system discards received SLPP packets

Configuring the SLPP by port

Use SLPP on a port to avoid traffic loops on the port by performing this procedure.

Important:

To provide protection against broadcast and multicast storms, Avaya recommends that you enable Rate Limiting for broadcast traffic and multicast traffic.

Procedure steps

1. In the navigation tree, open the following folders: **Configuration** > **VLAN**.
2. Click **SLPP**.
3. Click the **Ports** tab.
4. In the **PktRxThreshold** box for the desired port, specify the threshold value for packet reception.
5. Click the **SlppEnable** box for the desired port.
6. Select **true** to enable SLPP.
7. Click **Apply**.

Variable definitions

Use the data in the following table to configure the Slpp, Ports tab.

Variable	Value
IfIndex	Specifies the interface index number for a port.
PktRxThreshold	Specifies the threshold for packet reception. The SLPP packet receive threshold is set to a value (1-500) that represents the number of SLPP-PDUs that must be received to shut down the port. Note that this is a port-level parameter, therefore if the port is tagged, SLPP-PDUs from the various VLANs increment this single threshold counter.
SlppEnable	Enables SLPP on the selected interface.
IncomingVlanId	VLAN ID of the classified packet on a port disabled by SLPP.
SrcNodeType	Specifies the source node type of the received SLPP packet.
PktRxCount	Specifies the SLPP count.
TimeToClrPkRxCount	Specifies the time left to clear the SLPP RX PDU count.
RemainingTimeToClrPktRxCount	Specifies the remaining time left to clear the SLPP RX PDU counter.

Clearing the SLPP port counters

Clear SLPP port counters manually by performing this procedure.

Procedure steps

1. In the navigation tree, open the following folders: **Configuration** > **VLAN**.
2. Click **SLPP**.
3. Click the **Ports** tab.
4. Highlight the port you wish to clear.
5. Click the **ClearStats** button to clear the SLPP port counters.

Configuring Extended CP Limit globally

Extended CP Limit protects the switch from congestion caused by excess data flowing through one or more ports. Configure the Extended CP Limit to prevent the switch from being overwhelmed by performing this procedure.

Prerequisites

- You must enable and configure Extended CP Limit at the chassis level.

Procedure steps

1. In the navigation tree, open the following folders: **Configuration** > **Edit**.
2. Click **Chassis**. The Chassis screen appears with the **System** tab displayed.
3. Click **EXT. CP Limit** tab.

   Enter appropriate information in the fields provided.
4. Click **Apply**.

Variable definitions

Use the data in the following table to configure the Ext. CP Limit tab.

Variable	Value
Enable	Select this check box to enable the Extended CP Limit functionality. Clear the checkbox to disable Extended CP Limit functionality.
MinCongTime	Configures the minimum time the system octapid remains in a congested state before triggering the congestion algorithm. The default interval is 3000 milliseconds.
MaxPorts	Configures the total number of ports that need to be analyzed from the may-go-down port list. The range is from 0 to 512. The default is 0.
PortCongTime	Configures the interval a port can remain at the congestion threshold until the system disables it. The value ranges from 1 to 600 seconds. The default value is 5.
TrapLevel	Indicates the trap level for extended CP Limit as: • none • normal • verbose

Table continues…

Variable	Value
	The default is none.
SysOctapidCongested	Indicates whether system octapid congestion is detected for extended CP Limit.
PortsMonitored	Indicates ports monitored by extended CP Limit.
PortsShutDown	Indicates whether ports are shut down due to extended CP Limit.

Configuring extended CP Limit for a port

CP Limit functionality protects the switch from becoming congested by an excess of data flowing through one or more ports. Currently the CP Limit functionality only protects the switch from broadcast and control traffic with a QoS value of 7. The Extended CP Limit functionality is configurable and you can use it to prevent overwhelming the switch.

Configure extended CP limit for a port by performing this procedure.

Prerequisites

- You must enable extended CP Limit at the chassis level before you enable it for a port.

Procedure steps

1. On the Device Physical View, select a port.
2. In the navigation tree, open the following folders: **Configuration** > **Edit** > **Port**.
3. Click **General**.
4. Click the **CP Limit** tab.
5. Select a value for **ExtCplimitConf**.
6. Configure the threshold for **ExtCplimitUtilRate**.
7. Click **Apply**.

Variable definitions

Use the data in the following table to configure the CP Limit tab.

Variable	Value
CpLimitEnable	Activates or disables the CP Limit feature. The default is activated.

Table continues…

Variable	Value
CpMulticastLimit	Configures the multicast control frame rate in a range from 1000–100000 packets per second (pps). The default value is 10000. **Note:** If you are using the 8692 SF/CPU with a SuperMezz, change the default to 3000 pps
CpBroadcastLimit	Configures the broadcast control frame rate in a range from 1000–100000 pps. The default value is 10000. **Note:** If you are using the 8692 SF/CPU with a SuperMezz, change the default to 3000 pps
AutoRecoverPort	Activates or disables auto recovery of the port from action taken by CP Limit, link flap, or loop detect features. The default value is disabled.
ExtCplimitConf	Configures the manner in which the individual port participates in the Extended CP limit functionality. Select one of the following values for the port: • `None`- port is not monitored. • `SoftDown`- port belongs to may-go-down port list. • `HardDown`- port belongs to must-go-down port list. The default setting is none.
ExtCplimitUtilRate	Configures the threshold percentage, from 1–100, at which bandwidth utilization triggers the monitoring algorithm. The default value is 50.

Important:

Each user interface has unique terminology and naming conventions for parameters and values. For example, a parameter in EDM can appear in ACLI with different spelling or syntax.

The following interface comparisons show examples of differences in terminology and syntax between identical parameters and values when you configure and verify CP Limit and Extended CP Limit functionality:

- EDM: displays the ExtCplimitUtilRate parameter
- ACLI: displays the UTIL-RATE parameter

  and

- EDM: displays the CpMulticastLimit and CpBroadcastLimit parameters
- ACLI: displays MULTICAST-LIMIT and BROADCAST-LIMIT parameters

  and

- EDM: displays the ExtCplimitConf parameter
- ACLI: displays the EXT-CP-LIMIT parameter

Configuring loop detect

Configure loop detect to determine if the same MAC address appears on different ports. Use the optional ARP-Detect feature to account for ARP packets on IP configured interfaces.

Configure loop detect by performing this procedure.

Procedure steps

1. On the Device Physical View, select a port.
2. In the navigation tree, open the following folders: **Configuration** > **Edit** > **Port**.
3. Click **General**.
4. Click the **VLAN** tab.
5. Select the **LoopDetect** check box to enable loop detection.
6. If required, select the **ArpDetect** check box.
7. Select the appropriate action.
8. Click **Apply**.

Variable definitions

Use the data in the following table to configure the Loop Detect options on the VLANtab.

Variable	Value
LoopDetect	Activates or disables the loop detect feature for the port.
ArpDetect	Activates ARP-Detect. Activate ARP-Detect and loop detect on routed interfaces.
LoopDetectAction	Specifies the loop detect action to be taken. • portDown shuts down the port when the system detects a flapping MAC address • vlanBlock shuts down the VLAN when the system detects flapping MAC address • macDiscard. ARP-Detect does not support macDiscard.

Configuring CP Limit

CP Limit functionality protects the switch from becoming congested by an excess of data flowing through one or more ports. Currently the CP Limit functionality only protects the switch from broadcast and control traffic with a QoS value of 7.

Configure CP limit by performing this procedure.

Important:

Before CP Limit shuts down a port that exceeds the threshold, it captures the traffic statistics for that port. To see these logs, enter the following command: `more /pcmcia/rxstats.txt`.

Procedure steps

1. In the navigation tree, open the following folders: **Configuration** > **Edit** > **Port**.
2. Click **General**.
3. Click the **CP Limit** tab.
4. Select **Enable** or **Disable** for the CP Limit option.
5. Enter the multicast control frame rate.
6. Enter the broadcast control frame rate.
7. Click **Apply**.

Variable definitions

Use the data in the following table to configure the CP Limit tab.

Variable	Value
CpLimitEnable	Activates or disables the CP Limit feature. The default is activated.
CpMulticastLimit	Configures the multicast control frame rate in a range from 1000–100000 pps. The default is 15000. **Note:** If you are using the 8692 SF/CPU with a SuperMezz, change the default to 3000 pps
CpBroadcastLimit	Configures the broadcast control frame rate in a range from 1000–100000 pps. The default is 10000. **Note:** If you are using the 8692 SF/CPU with a SuperMezz, change the default to 3000 pps

Table continues…

Variable	Value
AutoRecoverPort	Activates or disables auto recovery of the port from action taken by CP Limit, link flap, or loop detect features. The default value is disabled.
ExtCplimitConf	Configures the way a port participates in the Extended CP limit functionality. Select one of the following values for the port: • `None`- port is not monitored. • `SoftDown`- port belongs to may-go-down port list. • `HardDown`- port belongs to must-go-down port list.
ExtCplimitUtilRate	Configures the threshold percentage, from 1–100, at which bandwidth utilization triggers the monitoring algorithm. The default value is 50.

Configuring Auto Recovery

Configure Auto Recovery to reenable ports that were disabled because loops were detected. When enabled, this feature automatically recovers ports disabled by SLPP, CP Limit, link flap, or loop detect.

Procedure steps

1. On the Device Physical View, select the port you want to enable for auto recovery.
2. In the navigation tree, open **Edit** > **Port** > **General** > **CP Limit**.
3. Check **AutoRecoverPort**.

Job aid: Loop detection warning messages

The following log message and trap is generated when a port, which has been disabled due to CP-Limit or link-flap, is auto-recovered:

```
port <port-num> re-enabled by auto recovery
```

The following log message and trap is generated when a port which has been disabled due to the loop detection feature is auto-recovered:

```
Loop detect action <action> cleared on port <port-num> by auto recovery
```

Setting the Auto Recovery timer

Set the Auto Recovery timer to the number of seconds you want to wait before reenabling ports that were disabled because loops were detected. This timer is a global setting that applies to all ports that have Auto Recovery enabled.

Procedure steps

1. On the Device Physical View, select the chassis.
2. In the navigation tree, open **Edit** > **Chassis** > **Chassis**.
3. In the **AutoRecoverDelay** box, enter the number of seconds set the auto-recovery timer.

Variable definitions

Use the data in the following table to configure the Auto Recovery timer.

Variable	Value
<seconds>	Configures the delay in Auto Recovery. The value ranges from 5 to 3600 seconds. The default is 30.

Editing the boot file

Edit the boot file to specify configuration settings such as the boot source and order for your switch by performing this procedure.

Procedure steps

1. Select an SF/CPU card.
2. In the navigation tree, open the following folders: **Configuration** > **Edit**.
3. Click **Card**.
4. Click the **Boot** tab.
5. Change the appropriate settings.
6. Click **Apply**.

Variable definitions

Use the data in the following table to configure the Card, Boot tab.

Variable	Value
SwVersion	Specifies the currently running software version
LastBootConfigSource	Specifies the boot configuration file used most recently
LastRuntimeImageSource	Specifies the run-time image loaded most recently
LastRuntimeConfigSource	Specifies the run-time configuration loaded most recently

Table continues…

Variable	Value
PrimaryImageSource	Specifies the primary image source file
PrimaryConfigSource	Specifies the primary configuration source file
PrimaryLicenceSource	Specifies the primary license file name.
SecondaryImageSource	Specifies the secondary image source file
SecondaryConfigSource	Specifies the secondary configuration source file
SecondaryLicenseSource	Specifies the secondary license file name.
TertiaryImageSource	Specifies the tertiary image source file
TertiaryConfigSource	Specifies the tertiary configuration source file
TertiaryLicenseSource	Specifies the tertiary license file name.
MezzImageSource	Specifies the SuperMezz configuration source file
EnableAutoBoot	Activates the autoboot option. After you power up the switch, the switch waits 5 seconds and then starts. If you set this option to false, the boot process stops at the Boot Monitor.
EnableFactoryDefaults	Activates the factory defaults option
EnableDebugMode	Activates the debug mode option
EnableHwWatchDogTimer	Activates the hardware watchdog timer option
EnableRebootOnError	Activates the reboot on error option
EnableTelnetServer	Activates the Telnet server option
EnableRloginServer	Activates the rlogin server option
EnableFtpServer	Activates the FTP server option
EnableTftpServer	Activates the Trivial File Transfer Protocol (TFTP) server option
EnableSshServer	Activates the SSH server option
EnableMezz	Activates the SuperMezz option

Editing the management port parameters

The management port on the switch fabric/CPU module is a 10/100 Mb/s Ethernet port that you can use for an out-of-band management connection to the switch.

You can use the Mgmt Port dialog box to specify, among other things, management information for the device and to set device configuration.

If you use Enterprise Device Manager to configure the static routes of the management port, you do not receive a warning if you set a non-natural mask. After you save the changes to the boot.cfg file, those static routes are deleted upon the next restart, possibly causing the loss of IP connectivity to the management port.

If you are uncertain whether the mask you set is non-natural, use the CLI or ACLI to configure static routes.

Edit the management port parameter by performing this procedure.

Procedure steps

1. Select the management port object.
2. In the navigation tree, open the following folders: **Configuration** > **Edit**.
3. Click **Mgmt Port**.
4. Modify the appropriate settings.
5. Click **Apply**.

Variable definitions

Use the data in the following table to configure the Mgmt Port-IP tab.

Variable	Value
IfIndex	Specifies the slot and port number of the management port.
Descr	Specifies the description of the management port.
AdminStatus	Configures the administrative status of the device.
OperStatus	Specifies the operational status of the device.
MgmtMacAddr	Specifies the MAC address of the management device.
Addr	Configures the IP address of the device.
Mask	Configures the subnet IP mask.
AutoNegotiate	Enables or disables autonegotiate.
AdminDuplex	Specifies the administrative duplex mode for the management port. If you change the duplex mode for the management port, from full to half duplex on a 8649GTR port, there is a 30 second loss of bidirectional traffic while the software resets.
OperDuplex	Specifies the operational duplex configuration for this port.
AdminSpeed	Specifies the administrative speed for this port.
OperSpeed	Indicates the operational duplex mode for this port.
EnableBootp	Activates or disables BootP.

Editing the management port CPU route table

Edit the management port CPU route table to specify network and gateway IP addresses used to remotely manage the device.

Open the Mgmt Port Route Table dialog box by performing this procedure.

Procedure steps

1. Select the management port object.
2. In the navigation tree, open the following folders: **Configuration** > **Edit**.
3. Click **Mgmt Port**.
4. On the **Mgmt Port** dialog box, click the **CPU Route Table** tab.
5. On the CPU Route Table dialog box, 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 Mgmt Port, Insert CPU Route Table tab.

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

Configuring the management port IPv6 interface parameters

Configure IPv6 management port parameters to use IPv6 routing on the port by performing this procedure.

Procedure steps

1. Select the management port object.
2. In the navigation tree, open the following folders: **Configuration** > **Edit**.
3. Click **Mgmt Port**.
4. On the Mgmt Port dialog box, click the **Mgmt Port-IPv6 Interface** tab.
5. Click **Insert**.

   The Insert Mgmt Port IPv6 Interface dialog box appears.
6. Edit the fields as required.
7. Click **Insert**.

8. Click **Apply**.

Variable definitions

Use the data in the following table to configure the Mgmt Port-IPv6 Interface dialog box.

Variable	Value
IfIndex	Specifies the interface index number for this port.
Identifier	Configures the IPv6 address interface identifiers. Identifier is a binary string of up to 8 octets in network byte-order.
IdentifierLength	Specifies the length of the Interface Identifier in bits.
Descr	Specifies a textual string containing information about the interface. Descr string is also set by the network management system.
Type	Specifies the Ethernet Routing Switch 8800/8600 module type.
ReasmMaxSize	Configures the MTU for this IPv6 interface. This value must be same for all the IP addresses defined on this interface. The default value is 1500. IPv6 does not support Jumbo Frames in Release 4.1.
PhysicalAddress	Specifies the MAC address for this port.
AdminStatus	Configures the indication of whether IPv6 is activated (up) or disabled (down) on this interface. This object does not affect the state of the interface, only the interface connection to an IPv6 stack. The default is false.
ReachableTime	Configures the time a neighbor is considered reachable after receiving a reachability confirmation. The value is expressed in milliseconds in a range from 0–3600000. The default value is 30000.
RetransmitTime	Configures the time between retransmissions of neighbor solicitation messages to a neighbor; during address resolution or neighbor reachability discovery. The value is expressed in milliseconds in a range from 0–3600000. The default value is 1000.
MulticastAdminStatus	Configures the status indication for IPv6 multicasting on this interface. The default is false.

Configuring management port IPv6 addresses

Configure management port IPv6 addresses to add or remove IPv6 addresses from the port by performing this procedure.

Avaya supports IPv6 addressing with HTTP, SSH, TELNET, SNMPv3, FTP, RLOGIN, and TFTP access to the switch.

Procedure steps

1. On the Device Physical View, select a management port.
2. In the navigation tree, open the following folders: **Configuration** > **Edit**.
3. Click **Mgmt Port**.
4. Click the **Mgmt Port-IPv6 Addresses** tab.
5. Click **Insert**.
6. In the **Addr** box, enter the required IPv6 address for the management port.
7. In the **AddrLen** box, enter the number of bits from the IPv6 address you want to advertise.
8. Click **Insert**.
9. Click **Apply**.

Variable definitions

Use the data in the following table to configure the Mgmt Port, Insert Mgmt Port-IPv6 Addresses dialog box.

Variable	Value
Addr	Specifies the IPv6 address to which this entry addressing information pertains. If the IPv6 address exceeds 116 octets, the object identifiers (OIDS) of instances of columns in this row is more than 128 sub identifiers and you cannot use SNMPv1, SNMPv2c, or SNMPv3 to access them.
AddrLen	Specifies the prefix length value for this address. You cannot change the address length after creation. You must provide this field to create an entry in this table.
Type	Specifies Unicast, the only supported type.

Configuring the CPU IPv6 route table

Use the management port for switch connectivity and management. As with other ports, you can configure the management port to route IPv6 and configure a number of IP addresses on an interface. The switch does not advertise the management port address to the other ports.

Configure the CPU IPv6 route table by performing this procedure.

Procedure steps

1. On 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 IPv6 Route Table** tab.
5. Click **Insert**.
6. Edit the fields as required.
7. Click **Insert**.
8. Click **Apply**.

Variable definitions

Use the data in the following table to configure the Mgmt Port, Insert CPU IPv6 Route Table dialog box.

Variable	Value
Network	Specifies the IPv6 destination address.
Gateway	Configures the gateway as the IPv6 address of the management port.
PrefixLength	Specifies the length of the prefix in bits. The value ranges from 0 to 128 bits.

Editing serial port parameters

The serial ports on the switch fabric/CPU module include the modem port and the console port.

Use the Serial Port dialog box to specify serial port communication settings by performing this procedure.

Procedure steps

1. On the Device Physical View, select the serial port.
2. Perform one of the following actions:
3. Right-click the serial port and click **Edit**.
4. Edit the port parameters as required.
5. Click **Apply**.

OR

6. In the Device Physical View, select a serial port.
7. In the navigation tree, open the following folders: **Configuration** > **Edit**.
8. Click **Serial Port**.
9. Edit the port parameters as required.
10. Click **Apply**.

Variable definitions

Use the data in the following table to configure the Serial Port dialog box.

Variable	Value
IfIndex	Specifies the slot and port number of the serial port.
Descr	Specifies the description of the serial port.
Mode	Specifies the mode in which this port operates. The default is **cli**.
BaudRate	Specifies the baud rate of this port. The default is **9600**.
DataBits	Specifies the number of data bits, for each byte of data, this port sends and receives. The default is **seven**.
MyAddr	Specifies this IP address of the port. Use the IP address for both SLIP and PPP modes.
PeerAddr	Specifies the peer IP address. Use the peer IP address for both SLIP and PPP modes.
SlipMtu	Specifies the MTU for this port in a range from 0–224.
SlipTxRxCompress	Activates or disables compression of TCP/IP packet headers on this port for SLIP mode only.
SlipRxCompress	Activates or disables compression for receiving packets on this port for SLIP mode only.
PppConfigFile	Specifies the configuration file to use PPP.

Enabling port lock

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

Enable port lock by performing this procedure.

Procedure steps

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

Variable definitions

Use the data in the following table to configure the Port Lock tab.

Variable	Value
Enable	Activates the port lock feature.
LockedPorts	Lists the locked ports. Click the ellipsis (...) button to select the ports you want to lock or unlock.

Locking a port

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

Lock a port by performing this procedure.

Prerequisites

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

Procedure steps

1. In the navigation tree, open the following folders: **Configuration** > **Security** > **Control Path**.
2. Click **General**.
3. In the Port Lock tab, click the **[...]** button.
4. Select the port or ports that you want to lock in the **Port Editor: undefined** dialog box.
5. Click **Ok**.
6. Click **Apply**.

Variable definitions

Use the data in the following table to configure the Port Lock tab.

Variable	Value
Enable	Activates the port lock feature.
LockedPorts	Lists the locked ports. Click the ellipsis (...) button to select the ports you want to lock or unlock.

Enabling power management

Enable power redundancy to create traps and events after power consumption exceeds redundancy capacity by performing this procedure.

Procedure steps

1. In the navigation tree, open the following folders: **Configuration** > **Edit**.
2. Click **Chassis**.
3. Click the **Power Management** tab.
4. Select **PowerManagementEnable** check box.
5. Select **PowerManagementFanCheckEnable** check box.
6. Click **Apply**.

Variable definitions

Use the data in the following table to configure the Power Management tab.

Variable	Value
PowerManagementEnable	Activates power redundancy to create traps and events if power consumption exceeds redundancy capacity.
PowerManagementFanCheckEnable	Enables the fan check.

Configuring slot priority

Configure slot priority to determine which slots shut down when not enough power is available in the chassis. The slot with the lowest priority shuts down first. Slots with the same priority shut down by highest slot number first.

Configure priority of slots by performing this procedure.

Procedure steps

1. On the Device Physical View, select a card.
2. In the navigation tree, open the following folders: **Configuration** > **Edit**.
3. Click **Card**.
4. In the **PowerManagementPriority** box, select the priority level.
5. Click **Apply**.

Chapter 37: Hardware status using Enterprise Device Manager

This chapter provides methods to check the status of basic hardware installed in the chassis.

Configuring polling intervals

About this task

Enable and configure polling intervals to determine how frequently EDM polls for port and LED status changes or detects the hot swap of installed modules.

Procedure

1. In the navigation pane, expand the following folders: **Configuration** > **Device**.
2. Click **Preference Setting**.
3. Enable polling or hot swap detection.
4. Configure the frequency to poll the device.
5. Click **Apply**.

Viewing card information

View the administrative status for all input/output (I/O) cards except the SF/CPU card.

Procedure steps

1. In the Device Physical View, select a module.
2. Do one of the following:

   Click the module.

   OR
3. Right-click the module. On the shortcut menu, choose **Edit**.

OR

4. In the navigation tree, open the following folders: **Configuration** > **Edit**.

   Click **Card**.

5. The card tab appears with the administrative status of the card.

Variable definitions

Use the data in the following table to use the Card, Card tab.

Variable	Value
FrontType	Indicates card types in the Ethernet Routing Switch 8800/8600. Front refers to the I/O portion of the module, the I/O card.
FrontDescription	Specifies the model number of the module.
FrontAdminStatus	Indicates the administrative status of the card.
FrontOperStatus	Indicates the operational status of the designated module.
FrontSerialNum	Specifies the serial number of the I/O card.
FrontHwVersion	Specifies the hardware version of the I/O card.
FrontPartNumber	Specifies the part number of the I/O card.
FrontDateCode	Specifies the manufacturing date code for the I/O card.
FrontDeviations	Shows deviations.
BackType	Indicates card type in the Ethernet Routing Switch 8800/8600.
BackDescription	Specifies the model number of the module.
BackSerialNum	Specifies the serial number of the I/O card.
BackHwVersion	Specifies the hardware version of the I/O card.
BackPartNumber	Specifies the part number of the I/O card.
BackDateCode	Specifies the manufacturing date code for the I/O card.
BackDeviations	Shows deviations.
ModuleSerialNum	Specifies the serial number of the I/O card.
ModulePartNumber	Specifies the part number of the I/O card.
ModuleAssemblyDate	Specifies the date when this I/O card was assembled.
PowerManagementPriority	Configures the priority level for the slot. Configure slot priority to determine which slots shut down if insufficient power is available in the chassis. The slot with the lowest priority shuts down first. Slots with the same priority shut down in descending order (highest slot number first).
PowerManagementPriorityStatus	Shows the status of the power management priority: critical, high, or low.

Viewing fan details

The Fan dialog box provides read-only information about the operating status of the switch fans.

Procedure steps

1. Select the fan object.
2. Perform one of the following steps:
3. Click the fan object.

   OR
4. Right-click the fan object and click **Edit**.

   OR
5. In the navigation tree, open the following folders: **Configuration** > **Edit**.
6. Click **Fan**.
7. The Fan tab appears with the operating status information of the switch fans.

Variable definitions

Use the data in the following table to use the Fan, Details tab.

Variable	Value
Id	Specifies the fan ID.
OperStatus	Specifies the status of the fan as follows: • unknown—status cannot be determined. • up—present and supplying power. • down—present, but failure indicated.
Type	Indicates the fan type. Fan types are the following: • unknown—type cannot be determined. • regularSpeed—a regular speed fan is present. • highSpeed—a high speed fan is present.
AmbientTemperature	Indicates the temperature of the air entering the fan.

Viewing power supply parameters

The Power Supply dialog box provides read-only information about the operating status of the switch power supplies.

Procedure steps

1. Select the power supply object.
2. Perform one of the following steps:
3. Click the power supply object.

   OR

4. Right-click the power supply object and click **Edit**.

   OR

5. In the navigation tree, open the following folders: **Configuration** > **Edit**.
6. Click **Power Supply**.
7. The Power Supply tab appears with the operating status information of the selected power supply.

Variable definitions

Use the information in the following table to understand the Power Supply, Detail tab.

Variable	Value
Type	Describes the type of power used—AC or DC.
Description	Provides a description of the power supply.
SerialNumber	Specifies the power supply serial number.
HardwareRevision	Specifies the hardware revision number.
PartNumber	Specifies the power supply part number.
PowerSupplyOperStatus	Specifies the status of the power supply as one of the following:. • on (up) • off (down)
InputLineVoltage	Specifies the input line voltage. There are two possible states: • low 110v—power supply connected to a 110 Volt source • high 220v—power supply connected to a 220 Volt source

Table continues…

Variable	Value
	If the power supplies in a chassis are not of identical input line voltage values, the operating line voltage displays the low 110v value.
OperLineVoltage	Specifies the operating line voltage. There are two possible states: • low 110v—output power equivalent to power supply operating with a 110 Volt input • high 220v—output power equivalent to power supply operating with a 220 Volt input If the power supplies in a chassis are not of identical input line voltage values, the operating line voltage displays the low 110v value.

Chapter 38: System access configuration using Enterprise Device Manager

The chapter provides procedures you can use to manage system access. Procedures include configurations for usernames, passwords, and access policies.

Enabling access levels

Enable access levels to control the configuration actions of various users by performing this procedure.

Important:

Only the RWA user can disable an access level on the switch. The RWA access level cannot be disabled on the switch.

These configurations are preserved across restarts.

Procedure steps

1. In the navigation tree, open the following folders: **Configuration** > **Security** > **Control Path**.
2. Click **General**.
3. Click the **CLI** tab.
4. Select the **Enable** check box for the required access level.
5. Click **Apply**.

Variable definitions

Use the data in the following table to configure the Control Path Security 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.
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.
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.
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.
RWL1UserName	Specifies the user name for the Layer 1 read/write CLI account.
RWL1Password	Specifies the password for the Layer 1 read/write CLI account.
ROEnable	Activates the read-only CLI account.
ROUserName	Specifies the user name for the read-only CLI account.
ROPassword	Specifies the password for the read-only CLI account.
MaxTelnetSessions	Specifies the maximum number of concurrent Telnet sessions that are allowed expressed in a range from 0–8.
MaxRloginSessions	Specifies the maximum number of concurrent Rlogin sessions that are allowed in a range from 0–8 .
Timeout	Specifies the number of seconds of inactivity for a Telnet or Rlogin session before the system initiates automatic timeout and disconnect, expressed in a range from 30–65535.
NumAccessViolations	Indicates the number of CLI access violations detected by the system. This variable is a read-only field.

Changing passwords

Use this procedure to

- configure new passwords for each access level
- change the login for different access levels
- change the password for different access levels

The Ethernet Routing Switch 8800/8600 ships with default passwords set for access to the CLI. If you use Simple Network Management Protocol version 3 (SNMPv3), you can change encrypted passwords.

Procedure steps

1. In the navigation tree, open the following folders: **Configuration** > **Security** > **Control Path**.
2. Click **General**.
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 Control Path Security 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.
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.
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.
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.
RWL1UserName	Specifies the user name for the Layer 1 read/write CLI account.
RWL1Password	Specifies the password for the Layer 1 read/write CLI account.
ROEnable	Activates the read-only CLI account.
ROUserName	Specifies the user name for the read-only CLI account.
ROPassword	Specifies the password for the read-only CLI account.
MaxTelnetSessions	Specifies the maximum number of concurrent Telnet sessions that are allowed expressed in a range from 0–8.
MaxRloginSessions	Specifies the maximum number of concurrent Rlogin sessions that are allowed expressed in a range from 0–8.

Table continues…

Variable	Value
Timeout	Specifies the number of seconds of inactivity for a Telnet or Rlogin session before the switch initiates automatic timeout and disconnect expressed in a range from 30– 65535.
NumAccessViolations	Indicates the number of CLI access violations detected by the system. This is a read-only field.

Creating an access policy

You can control access to the switch by creating an access policy. An access policy specifies the hosts or networks that can access the switch through various services, such as Telnet, SNMP, HTTP, rsh, and rlogin.

You can define network stations that are explicitly allowed to access the switch or network stations that are explicitly forbidden to access the switch. For each service, you can also specify the level of access, such as read-only or read/write/all. Create an access policy by performing this procedure.

Important:

Enterprise Device Manager does not provide SNMPv3 support for an access policy. If you modify an access policy with Device Manager, SNMPV3 is disabled.

Procedure steps

1. In the navigation tree, open the following folders: **Configuration** > **Security** > **Control Path**.
2. Click **Access Policies**.
3. In the Access Policies tab, click **Insert**.
4. In the **ID** box, type the policy ID.
5. In the **Name** box, type the policy name.
6. Select the **PolicyEnable** check box.
7. Select the **Mode** option to allow or deny a service.
8. From the **Service** options, select a service.
9. In the **Precedence** box, type a precedence number for the service (lower numbers mean higher precedence).
10. Select the **NetInetAddrType**.
11. In the **NetInetAddress** box, type an IP address.
12. In the **NetInetAddrPrefixLen** box, type the prefix length.
13. In the **TrustedHostInet Address** box, type an IP address for the trusted host.
14. In the **TrustedHostUserName** box, type a user name for the trusted host.

15. Select an **AccessLevel** for the service.
16. Select the **AccessStrict** check box, if desired.

    Important:

    If you select the **AccessStrict** check box, you specify that a user must use an access level identical to the one you selected in the dialog box to use this service.
17. Click **Insert**.
18. Click **Apply**.

Variable definitions

Use the data in the following table to configure the Insert access policies tab.

Variable	Value
Id	Specifies the policy ID.
Name	Specifies the name of the policy.
PolicyEnable	Activates the access policy.
Mode	Indicates whether a packet with a source IP address matching this entry is permitted to enter the device or is denied access.
Service	Indicates the protocol to which this entry applies.
Precedence	Indicates the precedence of the policy expressed in a range from 1–128. The lower the number, the higher the precedence.
NetInetAddrType	Indicates the source network Internet address type as one of the following. • `any` • `IPv4` • `IPv6` IPv4 is expressed in the format a.b.c.d. IPv6 is expressed in the format a:b:c:d:e:f:g:h.
NetInetAddress	Indicates the source network Inet address (prefix/network). If the address type is IPv4, you must enter an IPv4 address and its mask length. If the type is IPv6, you must enter an IPv6 address.
NetInetAddrPrefixLen	Indicates the source network Inet address prefix-length/mask. If the type is IPv4, you must enter an IPv4 address and mask length; If the type is IPv6, you must enter an IPv6 address and prefix length.
TrustedHostInetAddr	Indicates the trusted Inet address of a host performing a remote login to the device. TrustedHostInetAddr applies only to rlogin and rsh.

Table continues…

Variable	Value
	Important: You cannot use wildcard entries in the TrustedHostInetAddr field.
TrustedHostUserName	Specifies the user name assigned to the trusted host. The trusted host name applies only to rlogin and rsh. Ensure that the trusted host user name is the same as your network logon user name; do not use the switch user name, for example, rwa. **Important:** You cannot use wildcard entries. The user must already be logged in with the user name to be assigned to the trusted host. For example, using "rlogin -l newusername xx.xx.xx.xx" does not work from a UNIX workstation.
AccessLevel	Specifies the access level of the trusted host as one of the following: • `readOnly` • `readWrite` • `readWriteAll`
Usage	Shows the number of access policies currently in use.
AccessStrict	Enables or disables strict access criteria for remote users. If unchecked, a user must use an access level identical to the one you selected in the dialog box to use this service. • true: remote login users can use only the currently configured access level • false: remote users can use any access level **Important:** If you do not select true or false, user access is governed by criteria specified in the policy table. For example, a user with an rw access level specified for a policy ID in the policy table is allowed rw and rw access, and ro is denied access.

Enabling an access policy

Enable the access policy feature globally to control access across the switch.

You can create an access policy to control access to the switch. An access policy specifies the hosts or networks that can access the switch through access services; for example Telnet, SNMP, Hypertext Transfer Protocol (HTTP), and remote login (rlogin). Enable an access policy by performing this procedure.

Procedure steps

1. In the navigation tree, open the following folders: **Configuration** > **Edit**.
2. Click **Chassis**.
3. Click the **System Flags** tab.
4. Select the **EnableAccessPolicy** check box.
5. Click **Apply**.
6. Click **Close**.

Chapter 39: License installation using Enterprise Device Manager

Install and manage a license file for the Avaya Ethernet Routing Switch 8800/8600 by using the Enterprise Device Manager.

Installing a license file

Install a license file on an Avaya Ethernet Routing Switch 8800/8600 to enable licensed features by performing this procedure.

Prerequisites

- You must have the license file stored on a Trivial File Transfer Protocol (TFTP) server.
- Ensure that you have the correct license file with the base MAC address of the Avaya Ethernet Routing Switch 8800/8600 that you are installing the license on. Otherwise, system does not unblock the licensed features.
- If the Avaya Ethernet Routing Switch 8800/8600 chassis has two SF/CPU modules installed, you do not need to install the license file on the secondary SF/CPU. When you enable High Availability, the primary SF/CPU copies the license vectors to the secondary SF/CPU during table synchronization and the trial period counters stop. The system copies the license file to the secondary SF/CPU when you save the configuration on the primary SF/CPU.

  In warm-standby mode, license vectors are not synchronized with the secondary SF/CPU. However, the system copies the license file to the secondary SF/CPU when you save the configuration using the saveRuntimeConfigtoSlave option.

Procedure steps

1. In the navigation tree, open the following folders: **Configuration** > **Edit**.
2. Click **File System**.
3. In the Source field, enter the IP address of the TFTP server where the license file is located and the name of the license file.

4. In the Destination field, enter the flash device and the name of the license file.

   The license file name must be lower case.

   Important:

   If the license filename is license.dat and it is located in the Flash directory, then no further configuration is required. You can continue with the next step. If you changed the license filename and location, you must specify the license file path. The license name must be in lower-case characters. For more information about specifying the license file path, see Specifying the license file path and name on page 410.

5. In the Action field, select **start**.
6. Click **Apply**.

   The license file is copied to the flash of the primary SF/CPU module. The status of the file copy is provided in the Result field.

7. In the navigation tree, open the following folders: **Configuration** > **Edit**.
8. Click **Chassis**.
9. In **ActionGroup1**, select **loadLicense**.
10. Click **Apply**.

    Important:

    If the loading fails, the switch cannot unlock the licensed features and reverts to base functionality.

11. If you have two SF/CPU modules installed, you need to save the configuration so that the license file is copied to the secondary SF/CPU. From the Enterprise Device Manager navigation tree, open the following folders: **Edit** > **Chassis**.
12. On the System tab, select **saveRuntimeConfig** from **ActionGroup1**.
13. Click **Apply**.

Variable definitions

Use the data in the following table when copying a license file with the Copy Filetab.

Variable	Value
Source	Identifies the IPv4 address of the TFTP server and the name of the license file that you are copying.
Destination	Specifies the location and the name of the license file when copied to the SF/CPU.

Table continues…

Variable	Value
	Important: By default, the switch searches for a license filename of license.dat on the on-board Flash on the SF/CPU module. A license file generated for an Ethernet Routing Switch 8800/8600 can use any filename and extension. If the license filename is not license.dat, or the file is not located in the switch Flash directory, you must update the bootconfig file with the license filename and the path to its location.
Action	Starts the copy process or cancels the copy process.
Result	Specifies the result of the copy process: • none • inProgress • success • fail • invalidSource • invalidDestination • outOfMemory • outOfSpace • fileNotFound

Specifying the license file path and name

If you changed the license name and location when you installed the license file, you must specify the license file path to identify the storage location of the license file.

Procedure steps

1. Select the master SF/CPU module.
2. In the navigation tree, open the following folders: **Configuration** > **Edit**.
3. Click **Card**.
4. Select the **Boot** tab.
5. In the **PrimaryLicenseSource** field, enter the path and name of the license file.
6. Click **Apply**.

Variable definitions

Use the data in the following when copying a license file with the Boottab.

Variable	Value
PrimaryLicenseSource	The source can be internal Flash memory, external memory card (PCMCIA or Flash), or a remote TFTP server. • /flash/<file_name> • /pcmcia/<file_name> • <a.b.c.d>:<file_name> **Important:** By default, the switch searches for a license filename of license.dat on the on-board Flash on the SF/CPU module. A license file generated for an Ethernet Routing Switch 8800/8600 can use any filename and extension. If the license filename is not license.dat, or the file is not located in the switch Flash directory, you must update the bootconfig file with the license filename and the path to its location.

Chapter 40: NTP configuration using Enterprise Device Manager

This chapter describes how to configure the Network Time Protocol (NTP) using Enterprise Device Manager.

Prerequisites to NTP configuration

- Before you configure NTP, you must perform the following tasks:
  - Configure an IP interface on the Ethernet Routing Switch 8800/8600 and ensure that the NTP server is reachable through this interface. For instructions, see *Avaya Ethernet Routing Switch 8800/8600 Configuration — IP Routing, NN46205-523*.
  - Ensure the Real Time Clock is present on the SF/CPU board.

Important:

NTP server MD5 authentication does not support passwords (keys) that start with a special character or that contain a space between characters.

Enabling NTP globally

Enable NTP globally on the Ethernet Routing Switch 8800/8600 by performing this procedure. Default values are in effect for most NTP parameters.

Procedure steps

1. In the navigation tree, open the following folders: **Configuration** > **Edit**.
2. Click **NTP**.
3. Select the **Enable** check box.
4. Click **Apply**.

Variable definitions

Use the data in the following table to configure the Globalstab.

Variable	Value
Enable	Activates (true) or disables (false) NTP. By default, NTP is disabled.
Interval	Specifies the time interval (10–1440 minutes) between successive NTP updates. The default interval is 15 minutes. **Important:** If NTP is already activated, this configuration does not take effect until you disable NTP, and then re-enable it.

Adding an NTP server

Add a remote NTP server to the configuration by specifying its IP address. NTP adds this IP address to a list of servers, which the local NTP client uses when it queries remote time servers for time information. The list of qualified servers called to as a peer list.

You can configure a maximum of 10 time servers. Add an NTP server by performing this procedure.

Procedure steps

1. In the navigation tree, open the following folders: **Configuration** > **Edit**.
2. Click **NTP**.
3. Click the **Server** tab.
4. Click **Insert**.
5. Specify the IP address of the NTP server.
6. Click **Insert**.

   The IP address of the NTP server that you configured is displayed in the ServerAddress tab of the NTP dialog box.

Variable definitions

Use the data in the following table to configure the Servertab.

Variable	Value
ServerAddress	Specifies the IP address of the remote NTP server.
Enable	Activates or disables the remote NTP server.
Authentication	Activates or disables MD5 authentication on this NTP server. MD5 produces a message digest of the key. MD5 verifies the integrity of the communication, authenticates the origin, and checks for timeliness. The default is no MD5 authentication.
KeyId	Specifies the key ID used to generate the MD5 digest for this NTP server. You must specify a number between 1–214743647. The default is 0, which indicates that authentication is disabled.
AccessAttempts	Specifies the number of NTP requests sent to this NTP server.
AccessSuccess	Specifies the number of times this NTP server updated the time.
AccessFailure	Specifies the number of times this NTP server was rejected while attempting to update the time.
Stratum	This variable is the stratum of the server.
Version	This variable is the NTP version of the server.
RootDelay	This variable is the root delay of the server.
Precision	This variable is the NTP precision of the server in seconds.
Reachable	This variable is the NTP reach ability of the server.
Synchronized	This variable is the status of synchronization with the server.

Configuring authentication keys

Assign an NTP key to use MD5 authentication on the server by performing this procedure.

Procedure steps

1. In the navigation tree, open the following folders: **Configuration** > **Edit**.
2. Click **NTP**.
3. Click the **Key** tab.
4. Click **Insert**.
5. Insert the key ID and the MD5 key ID in the Insert Key dialog box.
6. Click **Insert**.

   The values that you specified for the key ID and the MD5 key ID are displayed in the Key tab of the NTP dialog box.

Variable definitions

Use the data in the following table to configure the Keytab.

Variable	Value
KeyId	This field is the key id used to generate the MD5 digest. You must specify a value between 1–214743647. The default value is 1, which indicates that authentication is disabled.
KeySecret	This field is the MD5 key used to generate the MD5 Digest. You must specify an alphanumeric string between 0–8 **Important:** You cannot specify the number sign (#) as a value in the KeySecret field. The NTP server interprets the # as the beginning of a comment and truncates all text entered after the #. This limitation applies to xntpd, the NTP daemon, version 3 or lower.

Chapter 41: DNS configuration using Enterprise Device Manager

This section describes how to configure the Domain Name Service (DNS) using Enterprise Device Manager.

Configuring the DNS client

Use the DNS client to establish the mapping between an IP name and an IP address.

You can configure connections for up to three different DNS servers—primary, secondary and tertiary. First the primary server is queried, and then the secondary, and finally the tertiary. Configure DNS client by performing this procedure.

Procedure steps

1. In the navigation tree, open the following folders: **Configuration** > **Edit** > **Diagnostics**.
2. Click **DNS**.
3. Click the **DNS Servers** tab.
4. In the DNS Servers tab, click **Insert**.
5. In the DnsServerListType box, select the DNs server type.
6. In the DnsServerListAddressType box, select the IP version.
7. In the DnsServerListAddress box, enter the DNS server IP address.
8. Click **Insert**.

Variable definitions

Use the data in the following table to configure the DNS Serverstab.

Variable	Value
DnsServerListType	Configures the DNS server as primary, secondary, or tertiary.
DnsServerListAddressType	Configures the DNS server address type as IPv4 or IPv6.
DnsServerListAddress	Specifies the DNS server address. • *ipaddress* in a.b.c.d format configures the IPv4 address. • *ipv6address* in hexadecimal format (string length 0–46) configures the IPv6 address.
DnsServerListStatus	Specifies the status of the DNS server.
DnsServerListRequestCount	Specifies the number of requests sent to the DNS server.
DnsServerListSuccessCount	Specifies the number of successful requests sent to the DNS server.

Querying the DNS host

Query the DNS host for information about host addresses.

You can enter either a hostname or an IP address. If you enter the hostname, this command shows the IP address corresponding to the hostname and if you enter an IP address, this command shows the hostname for the IP address. Query the DNS host by performing this procedure.

Procedure steps

1. In the navigation tree, open the following folders: **Configuration** > **Edit** > **Diagnostics**.
2. Click **DNS**.
3. In the **HostData** field, enter the DNS host name or IP address.
4. Click the **Query** button.

Variable definitions

Use the data in the following table to use the DNS Hosttab.

Variable	Value
HostData	Identifies the host name or host IP address. This variable is a read-only field.
HostName	Identifies the host name. This variable is a read-only field.
HostAddressType	Identifies the address type of the host.
HostAddress	Identifies the host IP address. This variable is a read-only field.

Table continues…

Variable	Value
HostSource	Identifies the DNS server IP or host file. This variable is a read-only field.

Chapter 42: Multicast group ID reservation using Enterprise Device Manager

This chapter provides procedures to create multicast group ID (MGID) reservations using Enterprise Device Manager.

Enabling maximum VLAN mode

Enable maximum VLAN mode to use all available MGIDs for VLANs. No IP multicast (IPMC) traffic transmits if you enable maximum VLAN mode. Enable maximum VLAN mode by performing this procedure.

Procedure steps

1. In the navigation tree, open the following folders: **Configuration** > **Edit**.
2. Click **Chassis**.
3. Click the **MGID Expansion** tab.
4. For **NewMaxVlanResourceReservation**, select **Enable**.
5. Click **Apply**.

Variable definitions

Use the data in the following tab to configure the Chassis, MGID Expansiontab.

Variable	Value
NewMulticastResourceReservation	Specifies the number of MGIDs to reserve for IPMC traffic. Select from the range of 64–4083. The default value is 2048. You cannot configure this option if maximum VLAN mode is activated.

Table continues…

Variable	Value
MulticastResourceReservation	Specifies the current IPMC MGID reservation. The default value is 2048.
NewMaxVlanResourceReservation	Activates or disables the maximum VLAN mode for MGID use. The default is disabled.
MaxVlanResourceReservation	Specifies the current configuration status of maximum VLAN mode. The default is disabled.
UsageVlanCurrent	Specifies the number of MGIDs currently in use by VLANs. The default value is 11.
UsageVlanRemaining	Specifies the number of VLAN reserved MGIDs still available. The default value is 2025.
UsageMulticastCurrent	Specifies the number of MGIDs currently in use by IPMC. The default value is 0.
UsageMulticastRemaining	Specifies the number of IPMC reserved MGIDs still available. The default value is 2048.

Reserving MGIDs for IPMC

Reserve MGIDs for IPMC to increase the number of IPMC traffic streams supported on the system by performing this procedure.

Procedure steps

1. In the navigation tree, open the following folders: **Configuration** > **Edit**.
2. Click **Chassis**.
3. Click the **MGID Expansion** tab.
4. In **NewMulticastResourceReservation**, type the number of MGIDs to reserve for IPMC.
5. Click **Apply**.

Chapter 43: Operational procedures using Enterprise Device Manager

This chapter describes common operational procedures that you use while configuring and monitoring the Ethernet Routing Switch 8800/8600 operations.

Showing the MTU for the system

Show the MTU configured for the entire system by performing this procedure.

Procedure steps

1. In the navigation tree, open the following folders: **Configuration** > **Edit**.
2. Click **Chassis**.
3. Click on the **Chassis** tab.
4. Ensure that 9600 is selected for MTU size.

Showing the MTU for each port

Show the MTU for each port by performing this procedure.

Procedure steps

1. On the Device Physical View, click the port for which you want to display information.
2. In the navigation tree, open the following folders: **Configuration** > **Edit** > **Port**.
3. Click **General**.
4. Examine the MTU box to verify the MTU size for each port.

Viewing topology status information

View topology status information (which includes Avaya Management MIB status information) by performing this procedure.

Procedure steps

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

   The Topology dialog box appears with the Topology tab visible.

Variable definitions

The following table describes the Topologytab fields.

Variable	Value
IpAddr	Specifies the IP address of the device.
Status	Indicates whether Avaya topology is on or off for the device.
NmmLstChg	Specifies the value of sysUpTime, the last time an entry in the network management MIB (NMM) topology table was added, deleted, or modified, if the table did not change since the last cold or warm start of the agent.
NmmMaxNum	Specifies the maximum number of entries in the NMM topology table.
NmmCurNum	Specifies the current number of entries in the NMM topology table.

Viewing the MIB status

View MIB status (which includes topology message status) by performing this procedure.

Procedure steps

1. In the navigation tree, open the following folders: **Configuration** > **Edit** > **Diagnostics**.
2. Click **Topology**.
3. Click the **Topology Table** tab.

   The Topology Table tab appears.

Variable definitions

The following table describes the Topology Tablefields.

Variable	Value
Slot	Specifies the slot number in the chassis that received the topology message.
Port	Specifies the port that received the topology message.
IpAddr	Specifies the IP address of the sender of the topology message.
SegId	Specifies the segment identifier of the segment from which the remote agent sent the topology message. This value is extracted from the message.
MacAddr	Specifies the MAC address of the sender of the topology message.
ChassisType	Specifies the chassis type of the device that sent the topology message.
BkplType	Specifies the backplane type of the device that sent the topology message.
LocalSeg	Indicates if the sender of the topology message is on the same Ethernet segment as the reporting agent.
CurState	Specifies the current state of the sender of the topology message. The choices are: • `topChanged`—Topology information recently changed. • `heartbeat`—Topology information is unchanged. • `new`—The sending agent is in a new state.

Displaying flash memory and PCMCIA information for the system

Display the amount of memory used and available for both onboard flash memory and an installed Personal Computer Memory Card International Association (PCMCIA) card, as well as the number of files in each location. Display flash memory and PCMCIA information for the system by performing this procedure.

Procedure steps

1. In the navigation tree, open the following folders: **Configuration** > **Edit**.
2. Click **File System**.
3. Click the **Device Info** tab.

Variable definitions

Use the data in the following table to use the Device Infotab.

Variable	Value
Slot	Specifies the slot number of the SF/CPU module.
FlashBytesUsed	Specifies the number of bytes used in flash memory.
FlashBytesFree	Specifies the number of bytes available for use in flash memory.
FlashNumFiles	Specifies the number of files in flash memory.
PcmciaBytesUsed	Specifies the number of bytes used on the PCMCIA card.
PcmciaBytesFree	Specifies the number of bytes available for use on the PCMCIA card.
PcmciaNumFiles	Specifies the number of files on the PCMCIA card.
PcmciaAction	Used to reset the PCMCIA card.
Result	Specifies the result of the PCMCIA action.

Displaying flash file information for a specific SF/CPU

Display information about the files in flash memory for a specific SF/CPU module to view general file information by performing this procedure.

Procedure steps

1. On the Device Physical View, select an SF/CPU module.
2. In the navigation tree, open the following folders: **Configuration** > **Edit**.
3. Click **Card**.
4. Click the **Flash Files** tab.

Variable definitions

Use the data in the following table to use the Card, Flash Filestab.

Variable	Value
Name	Specifies the directory name of the flash file.
Date	Specifies the creation or modification date of the flash file.
Size	Specifies the size of the flash file.
Slot	Specifies the slot number of the SF/CPU module.

Displaying flash file information for the system

Display information about the files in flash memory for all SF/CPU modules to view general file information by performing this procedure.

Procedure steps

1. In the navigation tree, open the following folders: **Configuration** > **Edit**.
2. Click **File System**.
3. Click the **Flash Files** tab.

Variable definitions

Use the data in the following table to use the Flash Filestab.

Variable	Value
Slot	Specifies the slot number of the SF/CPU module.
Name	Specifies the name of the flash file.
Date	Specifies the creation or modification date and time of the Flash file.
Size	Specifies the size of the flash file in bytes.

Displaying PCMCIA file information for a specific SF/CPU

Display information about the files stores in the PCMCIA card for a specific SF/CPU module to view general file information by performing this procedure.

Procedure steps

1. On the Device Physical View, select an SF/CPU card.
2. In the navigation tree, open the following folders: **Configuration** > **Edit**.
3. Click **Card**.
4. Click the **PCMCIA Files** tab.

Variable definitions

Use the data in the following table to use the Card, PCMCIA Filestab.

Variable	Value
Name	Specifies the directory name of the PCMCIA file.
Date	Specifies the creation or modification date of the PCMCIA file.
Size	Specifies the size of the PCMCIA file.

Displaying PCMCIA file information for the system

Display information about the files stored in the PCMCIA card for all SF/CPU modules to view general file information by performing this procedure.

Procedure steps

1. In the navigation tree, open the following folders: **Configuration** > **Edit**.
2. Click **File System**.
3. Click the **PCMCIA Files** tab.

Variable definitions

Use the data in the following table to use the PCMCIA Filestab.

Variable	Value
Slot	Specifies the slot number of the SF/CPU module.
Name	Specifies the name of the PCMCIA file.
Date	Specifies the creation or modification date and time of the PCMCIA file.
Size	Specifies the size of the PCMCIA file in bytes.

Copying a PCMCIA or flash file

Copy files between the flash and the PCMCIA. File copying and file information are all related to files on the switch SF/CPU module. Copy a PCMCIA or flash file by performing this procedure.

Procedure steps

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

3. Edit the fields as required.
4. Click **Apply**.

Variable definitions

Use the data in the following table to configure the Copy Filetab.

Variable	Value
Source	Identifies the source file to copy from the flash/PCMCIA or the config file on the NVRAM or trace file.
Destination	Identifies the device and the file name (optional) to which the source file is to be copied. The destination options are • `flash` • `PCMCIA` • `NVRAM` Trace files are not a valid destination.
Action	Starts the copy process or cancels the copy process.
Result	Specifies the result of the copy process: • `none` • `inProgress` • `success` • `fail` • `invalidSource` • `invalidDestination` • `outOfMemory` • `outOfSpace` • `fileNotFound`

Chapter 44: Port numbering and MAC address assignment reference

This chapter provides information about the port numbering and Media Access Control (MAC) address assignment used on the Avaya Ethernet Routing Switch 8800/8600.

Port numbering

A port number includes the slot location of the module in the chassis, as well as the port position in the input/output (I/O) module. In the Ethernet Routing Switch 8800/8600, slots are numbered from top to bottom. Figure 61: 8010 chassis slots on page 428 shows slot numbering for an 8010 chassis.

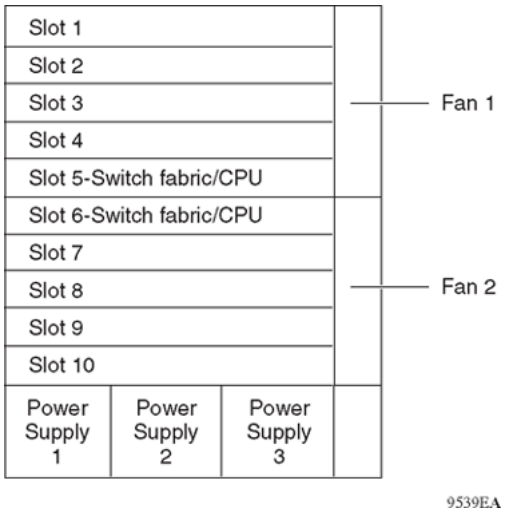


Figure 61: 8010 chassis slots

Ports are numbered from left to right beginning with 1 for the far left port. On high-density modules with two rows of ports, ports in the top row are assigned sequential odd numbers, and ports in the bottom row are assigned sequential even numbers, seeFigure 62: Port numbers on high-density modules on page 429.

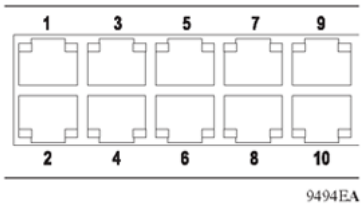


Figure 62: Port numbers on high-density modules

Interface indexes

The Simple Network Management Protocol (SNMP) uses interface indexes to identify ports, Virtual Local Area Networks (VLAN), and multilink trunks (MLT).

Port interface index

The interface index of a port is computed using the following formula:

ifIndex = (64 x slot number) + (port number – 1)

- Slot number is a value between 1–10, inclusive.
- Port number is a value between 1–48, inclusive.

For example, the interface index of port 1/1 is 64, and the interface index of port 10/48 is 687.

VLAN interface index

The interface index of a VLAN is computed using the following formula:

ifIndex = 2048 + VLAN multicast group ID (MGID)

Because the default VLAN always uses an MGID value of 1, its interface index is always 2049.

MLT interface index

The interface index of a multilink trunk (MLT) for Release 5.0 is computed using the following formula:

ifIndex = 6143 + MLT ID number

For releases earlier than 5.0, use the following formula:

ifIndex = 4095 + MLT ID number

MAC address assignment

It is important to understand how MAC addresses are assigned if you perform one of the following actions:

- define static Address Resolution Protocol (ARP) entries for IP addresses in the switch
- use a network analyzer to decode network traffic

System assigns each chassis a base of 4096 MAC addresses. Within the switch, system assigns these MAC addresses as follows:

- 512 addresses for ports in the switch (physical MAC addresses)
- 3584 addresses for VLANs in the switch (virtual MAC addresses).
  - If you have the maximum VLAN resource reservation (max-vlan-resource-reservation) enabled, you can create only 2000 VLANs with an IP address.
  - The last 12 addresses are reserved for the SF/CPU.

A MAC address uses the format shown in the following figure.

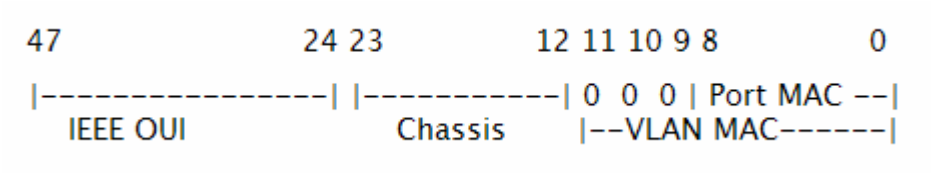


Figure 63: Parts of a MAC address

The MAC address is divided into the following parts:

- Bits 47–24: Institute of Electrical and Electronics Engineers (IEEE) Organization Unique Identity (OUI) (for example, 00-80-2d)
- Bits 23–12: Chassis ID
- Bit 11-9: Type of MAC address in the switch

  If all zeroes (000), it is a port address (physical MAC address); otherwise it is a VLAN address (virtual MAC address)
- Bits 8-0: 512 port MAC addresses
- Bits 11–0: 3584 VLAN MAC addresses

Physical MAC addresses

Physical MAC addresses are addresses assigned to the physical interfaces or ports visible on the device. The physical MAC addresses are used in the following types of frames:

- Spanning Tree Protocol Bridge Packet Data Units (BPDU) sent by the switch
- Frames to or from the physical interface an isolated routing port

BPDUs are sent using the physical MAC address as the source because the Spanning Tree Protocol must identify the physical port that sent the BPDU.

The ports on the SF/CPU module use the following last bytes:

- Management port in slot 5: 0xf4
- SF/CPU port (an internal port) in slot 5: 0xf5
- Management port in slot 6: 0xf6
- SF/CPU port in slot 6: 0xf7

Virtual MAC addresses

Virtual MAC addresses are the addresses assigned to VLANs. System assigns a virtual MAC address to a VLAN when the VLAN is created. The MAC address for a VLAN IP address is the virtual MAC address assigned to the VLAN.

Address Resolution Protocol (ARP)

Maps an IP address to a physical machine address, for example, maps an IP address to an Ethernet media access control (MAC) address.

Avaya command line interface (ACLI)

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

Border Gateway Protocol (BGP)

An inter-domain routing protocol that provides loop-free inter-domain routing between Autonomous Systems (AS) or within an AS.

Bridge Protocol Data Unit (BPDU)

A data frame used to exchange information among the bridges in local or wide area networks for network topology maintenance.

Challenge Handshake Authentication Protocol (CHAP)

An access protocol that exchanges a random value between the server and the client and is encrypted with a challenge password.

Domain Name System (DNS)

A system that maps and converts domain and host names to IP addresses.

Link Aggregation Control Protocol (LACP)

A protocol that exists between two endpoints to bundle links into an aggregated link group for bandwidth increase and link redundancy.

Media Access Control (MAC)

Arbitrates access to and from a shared medium.

Multiple Spanning Tree Protocol (MSTP)

Configures multiple instances of the Rapid Spanning Tree Protocol (RSTP) on the switch.

Open Shortest Path First (OSPF)

A link-state routing protocol used as an Interior Gateway Protocol (IGP).

out of band (OOB)

Network dedicated for management access to chassis.

Point-to-Point Protocol (PPP)

A network protocol used to dial into an Internet Service Provider (ISP). Serial Line Interface Protocol (SLIP) and PPP provide full Transmission Control Protocol/Internet Protocol (TCP/IP) capabilities to the casual dial-up user.

Protocol Independent Multicast, Source Specific (PIM-SSM)

Uses only shortest-path trees to provide multicast services based on subscription to a particular (source, group) channel.

Protocol Independent Multicast, Sparse Mode (PIM-SM)

Adds a Rendezvous Point router to avoid multicast-data flooding. Use PIM-SM when receivers for multicast data are sparsely distributed throughout the network.

Rapid Spanning Tree Protocol (RSTP)

Reduces the recovery time after a network breakdown. RSTP enhances switch-generated Topology Change Notification (TCN) packets to reduce network flooding.

Remote Authentication Dial-in User Service (RADIUS)

A protocol that authenticates, authorizes, and accounts for remote access connections that use dial-up networking and Virtual Private Network (VPN) functionality.

Routed Split MultiLink Trunking (RSMLT)

Provides full router redundancy and rapid failover in routed core SMLT networks and as RSMLT-edge in routed SMLT edge applications; eliminating routing protocol timer dependencies when network failures occur.

Routing Information Protocol (RIP)

A distance vector protocol in the IP suite, used by IP network-layer protocol, that enables routers in the same AS to exchange routing information by means of periodic updates. The RIP is most often used as a very simple IGP within small networks.

Secure Copy (SCP)

Securely transfers files between the switch and a remote station.

Secure Shell (SSH)

Used for secure remote logons and data transfer over the Internet. SSH uses encryption to provide security.

Simple Loop Prevention Protocol (SLPP)

Simple Hello Protocol that prevents loops in a Layer 2 network (VLAN).

Simple Network Management Protocol (SNMP)

Administratively monitors network performance through agents and management stations.

spanning tree

A simple, fully-connected active topology formed from the arbitrary physical topology of connected bridged Local Area Network components by relaying frames through selected bridge ports. The protocol parameters and states that are used and exchanged to facilitate the calculation of the active topology and to control the bridge relay function.

Spanning Tree Group (STG)

A collection of ports in one spanning tree instance.

Split MultiLink Trunking (SMLT)

An Avaya extension to IEEE 802.1AX (link aggregation), provides nodal and link failure protection and flexible bandwidth scaling to improve on the level of Layer 2 resiliency.

Trivial File Transfer Protocol (TFTP)

A protocol that governs transferring files between nodes without protection against packet loss.

Virtual Link Aggregation Control Protocol (VLACP)

A Layer 2 handshaking protocol that can detect end-to-end failure between two physical Ethernet interfaces.