Release Notes — Software Release 4.2.0.1 Avaya Ethernet Routing Switch 8300

4.2
NN46200-401, 05.11
May 2011

Notice

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

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

Licenses

Copyright

Third-party components

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

Trademarks

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

Avaya is a registered trademark of Avaya Inc.

All other trademarks are the property of their respective owners.

Downloading documents

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

Contact Avaya Support

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

Contents

Chapter 1: 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 (8300 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 (8300 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 55 022 Statements

This is to certify that the Avaya 8300 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 55 022 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 55 024 Statement

This is to certify that the Avaya 8300 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 55 024 (CISPR 24).

EN 300386 Statement

The Ethernet Routing Switch 8300 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 8300 Series chassis conforms to the provisions of the R&TTE Directive 1999/5/EC.

European Union and European Free Trade Association (EFTA) Notice

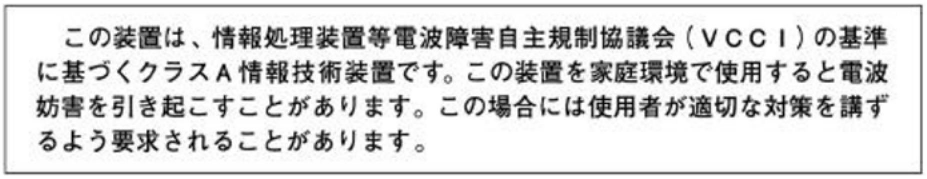
All products labeled with the CE marking comply with R&TTE Directive (1999/5/EEC) which includes the Electromagnetic Compliance (EMC) Directive (2004/108/EC) and the Low Voltage Directive (2006/95/EC) issued by the Commission of the European Community.

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

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。

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.

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. 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

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, S.A. de C.V.
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

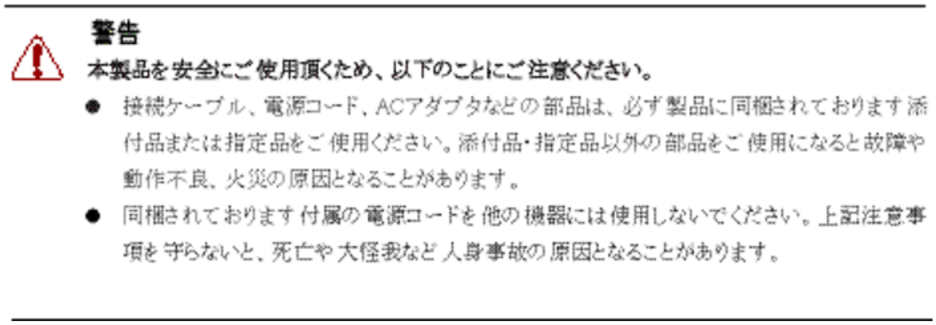
Model 8004DC:

-48 VCD, 29 A

Model 8005DC:

-48 VCD, 42 A

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。

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 8300.

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.

Chapter 2: New in this release

The following sections detail what's new in *Avaya Ethernet Routing Switch 8300 Release Notes — Software Release 4.2.0.1, NN46200-401*

Features

See the following sections for information about feature changes.

New software on page 19

New software

For Release 4.2.0.1, the Ethernet Routing Switch 8300 supports the following new features:

- IP spoof detection
- IGMPv3 snoopingand 3.0 Lite
- BGP Lite
- IP Source Guard
- BPDU Filtering
- DHCP Snooping
- Dynamic ARP inspection
- IPFIX
- Global VLACP MAC address

For more information about these new features, see New software features in Release 4.2.0.1 on page 23.

Other changes

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

- File names for upgrade on page 20
- Document changes on page 20

File names for upgrade

File names are updated; see File names for this release on page 28

Document changes

This document is reformatted to comply with the Avaya Customer Documentation Standards. For more information, see *Avaya Ethernet Routing Switch 8300 Documentation Roadmap, NN46200-101*.

Chapter 3: Introduction

This document describes new features, and known limitations, known issues, and resolved issues for Avaya Ethernet Routing Switch 8300 Software Release 4.2.0.1. Use this document to help you optimize the functionality of your Ethernet Routing Switch 8300.

For information about how to upgrade your version of Device Manager, see *Avaya Ethernet Routing Switch 8300 User Interface Fundamentals, NN46200-103*.

Navigation

Chapter 4: Important notices and new features

This section describes the supported and unsupported hardware and software features in the Ethernet Routing Switch 8300 Software Release 4.2.0.1, fixes to previously-known issues, and any remaining known issues.

Navigation

- New software features in Release 4.2.0.1 on page 23
- File names for this release on page 28
- Important information and restrictions on page 30
- Supported software and hardware capabilities on page 32

New software features in Release 4.2.0.1

The following sections introduce the new software features in Release 4.2.0.1.

New software features Navigation

- IPFIX on page 24
- BGP Lite on page 24
- IGMPv3 snooping on page 24
- DHCP Snooping on page 25
- Dynamic ARP inspection on page 25
- IP Source Guard on page 25
- IP spoof detection on page 25
- BPDU Filtering on page 25
- Global VLACP MAC address configuration (ER Q01660095/Q01958168) on page 26

- Premier trial license on page 26
- Enhanced local flow control for the 8248GTX module (ER Q01941996-02) on page 27
- TRUST-DSCP support (Q01971443-02) on page 27
- Static multicast ARP configuration (Q01958122) on page 27
- Silent CPU reset (Q01978449) on page 28

IPFIX

Release 4.2.0.1 introduces IPFIX. When enabled, this feature sample IP packets based on the IP source address, IP destination address, IP protocol, source protocol port, and destination protocol port of the packet, an IP flow is defined. IPFIX keeps statistics for each flow, provided there is still room in the hashing table.

- A CP card with 128M memory only supports 32K flows per system
- A CP card with 256M memory supports 128K flows per system

For more information, see *Avaya Ethernet Routing Switch 8300 Performance Management, NN46200-705*.

BGP Lite

Release 4.2.0.1 introduces BGP Lite. BGP lite is a subset of BGP. For edge deployment, ERS8300 does not connect to BGP routers in a different AS. It only runs IBGP to form a maximum of 4 neighbors with BGP gateway routers in the same AS. It is unnecessary to support full BGP functions in ERS8300. Instead, IBGP and related functions are implemented in 4.2.0.1 release.

For more information, see *Avaya Ethernet Routing Switch 8300 Configuration — BGP Services, NN46200-521*.

IGMPv3 snooping

Release 4.2.0.1 supports IGMPv3 for SSM. With IGMPv3, a host can selectively request or filter traffic from sources within the multicast group. IGMPv3 enables SSM-snoop by default. IGMPv3 snoop uses only the SSM channel table. Any report record which is not consistent with the SSM channel table is ignored. For more information, see *Avaya Ethernet Routing Switch 8300 Configuration — IP Multicast Routing Protocols, NN46200-520*.

DHCP Snooping

Release 4.2.0.1 introduces DHCP Snooping. DHCP (Dynamic Host Configuration Protocol) Snooping is a security feature that provides network security by filtering un-trusted DHCP messages and by building and maintaining a DHCP binding table. For more information, see *Avaya Ethernet Routing Switch 8300 Configuration — Security, NN46200-605*.

Dynamic ARP inspection

Release 4.2.0.1 introduces Dynamic ARP inspection. Dynamic ARP (Address Resolution Protocol) inspection is a security feature that validates ARP packets in a network. It intercepts, logs, and discards ARP packets with invalid IP-to-MAC address bindings. This capability protects the network from certain man-in-the-middle attacks. For more information, see *Avaya Ethernet Routing Switch 8300 Configuration — Security, NN46200-605*.

IP Source Guard

Release 4.2.0.1 introduces IP Source Guard. IP Source Guard works closely with DHCP Snooping. When it is enabled on an untrusted port with DHCP Snooping enabled, IP filter entry is created for that port automatically based on IP information stored in the corresponding DHCP-Snooping Binding Table entry. A port's IP filter is changed if its corresponding Snooping Binding Table entry is created/deleted. IP Source Guard should only be enabled on a port where DHCP Snooping global, VLAN and ARP Inspection VLAN are enabled. For more information, see *Avaya Ethernet Routing Switch 8300 Configuration — Security, NN46200-605*.

IP spoof detection

Release 4.2.0.1 introduces IP spoof detection. You can prevent VLAN logical IP spoofing by blocking the external use of the switch IP address. A configurable option is provided on a port by port basis which detect a duplicate IP address (that is the same as the switch VLAN IP address), and block all packets with a source or destination address equal to that address. For more information, see *Avaya Ethernet Routing Switch 8300 Configuration — VLANs and Spanning Tree, NN46200-516*.

BPDU Filtering

Release 4.2.0.1 introduces BPDU Filtering. The Spanning Tree Protocol detects and eliminates logical loops in a bridged or switched network. Any bridge that participates in the spanning tree exchanges information with other bridges using configuration messages known as Bridge Protocol Data Units (BPDU). Based on the BPDU information exchange, the bridge with the lowest bridge ID becomes the root. This process is called the root selection process.

BPDU filtering, when enabled at a port level receiving a Spanning Tree BPDU, either shuts the port down for a specified or indefinite time period. Avaya recommends enabling Spanning Tree Fast Start in addition to BPDU filtering for all user access ports. If the port is set to shut down indefinitely, a manual disable and re-enable of the port state is required to bring the port back up.

For more information, see *Avaya Ethernet Routing Switch 8300 Configuration — VLANs and Spanning Tree, NN46200-516*.

Global VLACP MAC address configuration (ER Q01660095/ Q01958168)

Release 4.2.0.1 introduces the ability to configure VLACP MAC addresses globally. VLACP defaults to a IEEE reserved multicast MAC address for sourcing LACP PDU packets. The field desires a destination MAC address that flags the CPU while not flooding throughout MGID/ broadcast domain like an STP BPDU ex: 01:80:c2:00:00:0f. This allows the 8300 via VLACP to achieve hitless failover in the case of configuration loss in the core/distribution/edge level of a network where the 8300 is expected to reside, while minimizing the major overhead of configuring unique VLACP MAC addresses per link.

Premier trial license

You are provided a 60 day trial period of Ethernet Routing Switch 8300, 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 will be 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.

Enhanced local flow control for the 8248GTX module (ER Q01941996-02)

Local-Flow-Control improves performance on 8348GTX/8348GTX-PWR cards by reducing packets retransmission. 802.3x Flow Control must be enabled between the DX and EX chip for 8348GTX cards on the 8300 platform.

When the network port of the DC chip detects when its Ingress buffer is full, the port sends in FC message to its peer port. The FC message informs the peer port to inhibit packet transmissions for a period of time.

In addition. when the cascade port detects that its Ingress buffer reaches the Xoff threshold, the port sends an FC message to its peer port on the EX chip. The FC message informs the peer port to inhibit packet transmissions for a period of time.

Note:

Local-Flow-Control is only supported on 8348GTX and 8348GTX-PWR cards

Table 1: Command lines required for implementing flow control

Type	Command Line
CLI	config qos local-flow-control <slot list> {enable|disable} To show the configuration, execute the command: show config
ACLI	[no] qos local-flow-control <slot list> To show the configuration, execute the command: show running-config

TRUST-DSCP support (Q01971443-02)

TRUST-DSCP support has been added for all ERS 8300 modules. Previously this functionality only worked for certain module types.

The CLI command structure is:

config ethernet <port/portlist> qos trust-dscp <enable|disable>

Static multicast ARP configuration (Q01958122)

Static multicast ARP configuration functionality has been introduced.

Silent CPU reset (Q01978449)

The silent CPU reset situation is still open, but this code release contains extra instrumentation code in order to assist Avaya in understanding the situation. Under what has been labeled the “silent reset” condition, the switch switches over to standby SF with nothing in the system log to indicate why. This generally causes a 45 second to 1 or 2 minute outage for devices connected to this switch, in non-SMLT configurations. This situation has a repetitive time frame generally measured in months. Therefore if your network has not seen this situation to date (and most have not), then there is a very good probability that your network will not see this situation with any version of code.

The following functionality has been added to assist Avaya in analyzing ERS 8300 silent reset issues. These items are enabled by default (Q01978449).

- Monitor and log current and peak values for CPU utilization
- Enhancement for software watchdog routine to catch and log task related anomalies
- Monitor and log all interrupts for current and peak values
- Ability to monitor port and STP TCN flapping
- Additional error, warning and info log messages have now been added

Note:

New warning and info messages may appear during switch resets or boots. During these times, these log messages can be ignored, as they are part of the new instrumentation and normally occur during either reset or boot times. If these messages appear during normal switch operation, the user should contact Avaya and open a case with Avaya or their partner, appropriate to the user’s maintenance contract.

File names for this release

This section describes the Ethernet Routing Switch 8300 Software Release 4.2.0.1 software files and the hardware they support.

Table 2: Software files

Module or file type	Description	File name	Size in bytes
Software tar file	Tar file of all software files	v4.2.0.1.tar.gz	
Ethernet Routing Switch images			
Boot monitor image	Required SF/CPU firmware for the	p83b4201.img	1.1 MB

Module or file type	Description	File name	Size in bytes
	Ethernet Routing Switch 8300		
Runtime image	Required Ethernet Routing Switch 8300 image	p83a4201.img	9.4 MB
Runtime image for I/O modules	Runtime image required for I/O modules	p83r4201.dld	2.3 MB
Pre-boot monitor image	This pre-boot image file is only required to be loaded when upgrading from software release 2.0.0.1 and the pre-boot image version is below Release 3.7.	p83f4201.img	230 786
Software license	Needed for licensed features.	license.dat	variable
MIB (zip file)	Zip file containing MIBs. This compressed .mib file contains a file named “manifest”, which contains a list of the MIBs supported by the switch, including the private MIBs.	p83a4201.mib.zip p83a4201.mib (private MIB)	542 KB 3.3 MB
MD5 checksum file	Required for integrity check; contains Message Digest 5 (MD5) checksums for all files	p83a4201.md5	745
AES/SNMPv3 image	Encryption module required for SNMPv3 Advanced Encryption Standard (AES) and DES support	p83c4201.aes; only available from www.avaya.com/support	27 KB
3DES	Encryption module required for Secure Shell (SSH) Triple Data Encryption Standard (3DES) support	p83c4201.img; only available from www.avaya.com/support	52 MB

Module or file type	Description	File name	Size in bytes
Device Manager images			
Solaris for SPARC image	Required for Device Manager for Solaris	jdm_6170_solaris_sparc.sh	
Microsoft Windows image	Required for Device Manager for Windows	jdm_6170.exe	
Linux image	Required for Device Manager for Linux	jdm_6170_linux.sh	

Important information and restrictions

This section describes important information and restrictions.

Important information and restrictions navigation

- Ensuring Device Manager Online Help displays correctly on page 30
- Upgrading an advanced software license on page 31
- Upgrading the switch to Release 4.2.0.1 software on page 31

Ensuring Device Manager Online Help displays correctly

Avaya supports the following two browsers for Java Device Manager Online Help:

- Netscape
- Internet Explorer

If you use Netscape as your Web browser, to ensure that the topics and table of contents display correctly when you make a context call to on-product Help, perform the following procedure once before you request Help on a topic:

1. Start the Netscape browser.
2. From the Tools menu, select Options (An Options window opens.)
3. In the Security and Privacy panel of the Options window, click Site Controls. (An Options - Site Controls window opens.)
4. Ensure that the Site List tab is selected.
5. Select Local Files in the Master Settings area of the window.

6. Select Internet Explore in the Rendering Engine area of the window.
7. Click OK to close the Options - Site Controls window.

Upgrading an advanced software license

Under some circumstances, you may require a new license. This depends on the version of the license file you are currently using. If you are running a pre-4.2.0.1 Release, you can use the show license command to check your version number. If the version number has a non zero value, you will require a new Advanced or Premier license in order to properly function with Release 4.2.0.1. Note that the show license command in Release 4.2.0.1 no longer shows a version number field. If you have any issues running any licensed feature, before you contact Technical Support, first obtain an updated license. If this does not resolve the issue, then contact Technical Support.

For information about how to install a Premier license, see *Avaya Ethernet Routing Switch 8300 Administration, NN46200-604*.

Upgrading the switch to Release 4.2.0.1 software

For more information about the procedure to upgrade the switch to Release 4.2.0.1 software, see *Avaya Ethernet Routing Switch 8300 Upgrades — Software Release , NN46200-400*

This section discusses issues related to the upgrading of the Ethernet Routing Switch 8300 to the current software.

Note about DLD files

When the boot configuration is saved in runtime, the current bootp DLD image names are saved in the boot.cfg file. If you load a new image without removing the bootp DLD entry references from the boot.cfg, then the new version of the file is not downloaded to the I/O boards.

- On boot up, if a DLD file is not configured in boot.cfg, the CP code searches for a DLD file with the following file name:

  ```
  p83r<stream name><version>.dld
  ```

  The stream name and version must match the CP image being initialized. If this file is found, its checksum is verified and it is downloaded to the I/O boards. If the boot configuration is saved, this is the DLD file name saved in boot.cfg.
- If the CP does not find this DLD file name in its flash, it searches for the following default file name:

  ```
  p83r<stream name>.dld
  ```

Only the stream name must match the CP image being initialized. If this file is found, its checksum is verified and it is downloaded to the I/O boards. If the boot configuration is saved, this is the DLD file name saved in boot.cfg.

To make the system boot from the default DLD files, first clear the DLD file references made by boot.cfg:

1. Enter the boot monitor.
2. Enter the following command:

   ```
   bootp image default
   ```

   This clears the DLD file entries so that the new version of

   `p83r<stream name><version>.dld` or **`p83r<stream name>.dld`** is loaded.

   Caution:

   Do not interrupt the DLD download after it has started or IO modular failure can occur.

Supported software and hardware capabilities

This section lists the known limits for the Ethernet Routing Switch 8300 Software Release 4.2.0.1 and JDM 6.1.7.0 of the Ethernet Routing Switch 8300 Series software. These capabilities will be enhanced in subsequent software releases.

Feature	Maximum number supported	
Media Access Control (MAC)/forwarding data bases (FDB) Entries	Up to 16 000	**Important:** Dynamic ARP 2994 Static ARP 500
Address Resolution Protocol (ARP) Entries	Up to 2994	
Spanning Tree Groups (STG)	Up to 64	
VLANs	Maximum number of VLAN IDs 4000 By-Port up to 512 IP Based By-Port up to 2000 non-IP Based	

Feature	Maximum number supported	
MultiLink Trunk (MLT) Groups	Up to 31	**Important:** • For 8348TX, 8348TX-PWR and 8324FX ports, you can use only Link Aggregation Groups 1-7. • For 8348GB, 8324GTX, 8348GTX and 8348GTX-PWR ports and 8393SF/CPU, you can use Link Aggregation Groups 1-31.
Split Multilink Trunking (SMLT) Groups	Up to 30 with 1 IST group	
Max Number of Links per MLT/SMLT/interswitch trunking (IST) group	8	
Internet Protocol (IP) Interfaces	Up to 512	
Static Routes	Up to 1000	
Routing Information Protocol (RIP)	Up to 8000 RIP Routes	
Open Shortest Path First (OSPF)	Up to 6 OSPF areas Up to 80 adjacency Up to 8000 OSPF routes	
OSPF combinations	TBD	
Border Gateway Protocol (BGP)	Up to 8000 BGP Routers	
BGP neighbors	4	
Virtual Router Redundancy Protocol (VRRP) Instances	Up to 256	
Virtual Routing Forwarding Instances	Up to 128	**Important:** VRF OSPF Instances 12 VRF RIP Instances 24
Internet Group Management Protocol (IGMP) Snoop	Maximum number of IGMP Interfaces: 500 VLANs Maximum number of IGMP groups: 2000 IGMP Joins/sec: 200 IGMP Leaves/sec: 200	
Protocol Independent Multicast (PIM)	Up to 128 PIM neighbors Up to 512 (Source, Group) pairs	
Extensible Authentication Protocol over LAN (EAPoL) 802.1X supplicants	Up to 8 supplicants per port	

Feature	Maximum number supported	
Remote Access Dial-in User Service (RADIUS) Media Access Control (MAC) centralization clients	Up to 8 supplicants per port	
Link Layer Discovery Protocol (LLDP) Neighbors	Up to 384	
IP Filters		
ACL	Up to 512 (IP or non-IP based)	
ACT	With one ACL, up to 34 (IP or non-IP based)	
ACE	With one ACL and one ACT, up to 128 (IP or non-IP based)	
ACG	With one ACL, one ACT and one ACE, up to 1 024 (IP or non-IP based)	
Multicast VLAN Registry	Up to 256 receiver VLANs	

Supported Standards (IEEE, RFCs and others)

This section identifies the 802 standards, RFCs, and network management MIBs supported in this release.

Supported Standards	
802.1D	MAC Bridges (Spanning Tree Protocol)
802.1p	Traffic Class Expediting
802.1Q	Virtual LANs
802.1X	Port-Based Network Access Control (Extensible Authentication Protocol)
802.1AB	Station and Media Access Control Connectivity Discovery (LLDP)
802.3	10BASE-T (ISO/IEC 8802-3, Clause 14)
802.3u	100BASE-T (ISO/IEC 8802-3, Clause 25)

Supported Standards	
802.3u	Auto-Negotiation on Twisted Pair (ISO/IEC 8802-3, Clause 28)
802.3x	100Mb/s Full Duplex Operation
802.3z	Gigabit Ethernet (1000BASE-X)
802.3ab	1000BASE-T
802.3ae	10Gb/s Ethernet (10GBASE-X)

Supported IPv4 standards	
RFC 768	User Datagram Protocol (UDP)
RFC 783	Trivial File Transfer Protocol (TFTP) v2
RFC 791	IP
RFC 792	Internet Control Message Protocol (ICMP)
RFC 793	Transmission Control Protocol (TCP)
RFC 826	Ethernet Address Resolution Protocol
RFC 854	Telnet protocol
RFC 903	Reverse ARP
RFC 1058	RIP
RFC1112	Host Extensions for IP Multicasting
RFC1157	Simple Network Management Protocol (SNMP)
RFC1213	TCP/IP Management Information Base (MIB)-II
RFC1493	Bridge MIB
RFC 1519	Classless Inter-Domain Routing (CIDR)
RFC1541	Dynamic Host Configuration Protocol (DHCP)
RFC1542	Bootstrap Protocol (Clarifications and Extensions)
RFC1591	Domain Name System
RFC1657	Definitions of Managed Objects for the Fourth Version of the Border Gateway Protocol (BGP-4)
RFC1745	BGP4/IDRP for IP---OSPF Interaction
RFC1757	Remote Network Monitoring

Supported IPv4 standards	
RFC1771	A Border Gateway Protocol 4 (BGP-4)
RFC1812	IPv4 Router Requirements
RFC1850	OSPFv2 MIB
RFC1866	HyperText Markup Language v2
RFC1997	BGP Communities Attribute
RFC1998	An Application of the BGP Community Attribute in Multi-home Routing
RFC 2068	Hypertext Transfer Protocol (HTTP) v1.1
RFC 2138	RADIUS Authentication
RFC2139	RADIUS Accounting
RFC 2328	OSPFv2
RFC 2236	IGMPv2
RFC2338	VRRP
RFC 2362	Protocol Independent Multicast-Sparse Mode (PIM-SM)
RFC2385	Protection of BGP Sessions via the TCP MD5 Signature Option
RFC2453	RIPv2
RFC2474	Differentiated Services in IPv4 and IPv6
RFC2475	Differentiated Services
RFC2570	Simple Network Management Protocol (SNMP)v3
RFC2571	SNMP Frameworks
RFC2572	SNMP Message Processing and Dispatching
RFC2573	SNMPv3 Applications
RFC2574	SNMPv3 User-based Security Model (USM)
RFC2575	SNMPv3 View-based Access Control Model (VACM)
RFC2576	SNMP Coexistence of v1, v2, & v3 of Internet Network Management Framework
RFC2597	Assured Forwarding per hop behavior (PHB) Group
RFC2598	Expedited Forwarding PHB

Supported IPv4 standards	
RFC2665	Ethernet MIB
RFC2737	Entity MIBv2
RFC2787	VRRP MIB
RFC 2819	Remote Monitoring (RMON) MIB
RFC2863	Interfaces Group MIB
RFC3917	IPFIX

The Ethernet Routing Switch 8300 is an SNMPv1/v2/v2c/v3 agent with Industry Standard MIBs, as well as private MIB extensions, which ensures compatibility with existing network management tools.

These MIBs are provided with different versions of code. Consult the Avaya website where a file named mib.zip contains all these MIBs, and a special file named manifest for the order of the MIB compilation.

Standard MIB name	IEEE	File name
802.1ab	802.1ab	ieee8021ab.mib ieee8021ab1x.mib ieee8021ab3x.mib ieee8021abMed.mib
EaPoL (802.1X)	802.1X	ieee8021x.mib

Standard MIB name	RFC	File name
IANA Interface type	n/a	iana_if_type.mib
SMI	RFC1155	rfc1155.mib
SNMP	RFC1157	rfc1157.mib
MIB for network management of TCP/IP based Internet MIBs	RFC 1213	rfc1213.mib
A convention for defining traps for use with SNMP	RFC 1215	rfc1215.mib
RIP version 2 MIB extensions	RFC1389	rfc1389.mib
Definitions of Managed Objects for Bridges	RFC1493	rfc1493.mib
Evolution of the Interface Groups for MIB2	RFC1573	rfc1573.mib

Standard MIB name	RFC	File name
Definitions of Managed Objects for the Ethernet-like Interface types	RFC1643	rfc1643.mib
Definitions of Managed Objects for the Fourth Version of the Border Gateway Protocol (BGP-4) using SMIv2	RFC1657	rfc1657.mib
RIP version 2 MIB extensions	RFC1724	rfc1724.mib
Remote Network Monitoring Management Information Base (RMON) Note: Ethernet Routing Switch 8300 supports Alarms, Events, Statistics and History.	RFC1757/RFC2819	rfc1757.mib
OSPF Version 2 Management Information Base	RFC1850	rfc1850.mib
Management Information Base of the Simple Network Management Protocol (SNMPv2)	RFC1907	rfc1907.mib
Remote Network Monitoring Management Information Base (RMON) version 2 using SMIv2	RFC2021	rfc2021.mib
IP Forwarding Table MIB	RFC2096	rfc2096.mib
The Interfaces Group MIB using SMIv2	RFC2233	rfc2233.mib
An Architecture for Describing SNMP Management Frameworks	RFC2571	rfc2571.mib
Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)	RFC2572	rfc2572.mib
SNMP Applications	RFC2573	rfc2573.mib
User-based Security Model (USM) for version 3 of the Simple Network	RFC2574	rfc2574.mib

Standard MIB name	RFC	File name
Management Protocol (SNMP)		
Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework	RFC2576	rfc2576.mib
Definitions of Managed Object for Bridges with Traffic Classes, Multicast Filtering, and Virtual LAN extensions	RFC2674	rfc2674.mib
Textual Conventions for Internet Network Addresses	RFC2851	rfc2851.mib
The Interface Group MIB	RFC2863	rfc2863.mib
Internet Group Management Protocol MIB	RFC2933	rfc2933.mib
The Advanced Encryption Standard (AES) Cipher Algorithm in the SNMP Used-based Security Model	RFC3826	rfc3826.mib
VRRP (Virtual Router Redundancy Protocol)	RFC2787	rfc2787.mib

Supported Standards	
Rapid City MIB	rapid_city.mib
Rapid City MIB	synro.mib
Other SynOptics definitions	s5114roo.mib
Other SynOptics definitions	s5tcs112.mib
Other SynOptics definitions	s5emt103.mib
IGMP MIB	rfc_igmp.mib
VRRP MIB	vrrp_rcc.mib
MIB definitions	wf_com.mib
OSPF Version 2 Management Information Base-	rfc1850t_rcc.mib

Ethernet Routing Switch 8010/8006 chassis support

With Releases 4.2.0.1 and later, Avaya does not recommend or support the use of Ethernet Routing Switch 8300 modules in an Ethernet Routing Switch 8010 or Ethernet Routing Switch 8006 chassis.

Supported SFPs

This section lists the transceivers supported by the Ethernet Routing Switch 8300.

SFP order number	SFP type	Reach
AA1419013	LC type 1000BASE-SX	Up to 550 m
AA1419014	MT-RJ type 1000BASE-SX	Up to 550 m
AA1419015	LC type 1000BASE-LX	Up to 5 km
AA1419025	1470nm/Gray 1000BASE CWDM	Up to 40 km
AA1419026	1490nm/Viole t 1000BASE CWDM	Up to 40 km
AA1419027	1510nm/Blue 1000BASE CWDM	Up to 40 km
AA1419028	1530nm/Green 1000BASE CWDM	Up to 40 km
AA1419029	1550nm/Yellow 1000BASE CWDM	Up to 40 km
AA1419030	1570nm/Orange 1000BASE CWDM	Up to 40 km
AA1419031	1590nm/Red 1000BASE CWDM	Up to 40 km
AA1419032	1610nm/Brown 1000BASE CWDM	Up to 40 km
AA1419034	1490nm/Violet 1000BASE CWDM	Up to 70 km
AA1419035	1510nm/Blue 1000BASE CWDM	Up to 70 km
AA1419036	1530nm/Green	Up to 70 km

SFP order number	SFP type	Reach
	1000BASE CWDM	
AA1419037	1550nm/Yellow 1000BASE CWDM	Up to 70 km
AA1419038	1570nm/Orange 1000BASE CWDM	Up to 70 km
AA1419039	1590nm/Red 1000BASE CWDM	Up to 70 km
AA1419040	1610nm/Brown 1000BASE CWDM	Up to 70 km
AA1419043	RJ-45 Type 1000BASE-T	Up to 100 m
AA1419069 **Important:** Release 3.0 is required for recognition of this SFP.	1-port 1000BASE-BX Small Form Factor Pluggable GBIC (mini-GBIC, connector type: LC) - 1310nm Wavelength. Must be paired with AA1419070	Up to 10 km
AA1419070 **Important:** Release 3.0 is required for recognition of this SFP.	1-port 1000BASE-BX Small Form Factor Pluggable GBIC (mini-GBIC, connector type: LC) - 1490nm Wavelength. Must be paired with AA1419069	Up to 10 km
AA1419071	1-port 1000BaseEX SFP-LC 1550 nm	Up to 120 km
AA1419076	1000Base-BX10 1310 nm, bidirectional single fiber	Up to 40 km
AA1419077	1000Base-BX10 1490 nm, bidirectional single fiber	Up to 40 km
AA1419048-E6	1-port 1000Base-SX Small Form Factor Pluggable (SFP) Gigabit Ethernet Transceiver, connector type: LC. Digital Diagnostic Monitoring Interface	
AA1419049-E6	1-port 1000Base-LX Small Form Factor Pluggable (SFP) Gigabit Ethernet Transceiver, connector type: LC.	
AA1419050-E6	1-port 1000BaseXD Small Form-factor Pluggable (SFP)	

SFP order number	SFP type	Reach
	Gigabit Ethernet Transceiver - 1310nm.	
AA1419051-E6	1-port 1000BaseXD Small Form-Factor Pluggable (SFP) Gigabit Ethernet Transceiver - 1550nm.	
AA1419052-E6	1-port 1000BaseZX Small Form-Factor Pluggable (SFP) Gigabit Ethernet Transceiver 1550nm.	
AA1419053E6	1-port 1000BaseCWDM Small Form Factor Pluggable GBIC (mini-GBIC, connector type: LC) - 1470nm Wavelength	Up to 40 km
AA1419054-E6	1-port 1000BaseCWDM Small Form Factor Pluggable GBIC (mini-GBIC, connector type: LC) - 1490nm Wavelength	Up to 40 km
AA1419055-E6	1-port 1000BaseCWDM Small Form Factor Pluggable GBIC (mini-GBIC, connector type: LC) - 1510nm Wavelength	Up to 40 km
AA1419056-E6	1-port 1000BaseCWDM Small Form Factor Pluggable GBIC (mini-GBIC, connector type: LC) - 1530nm Wavelength	Up to 40 km
AA1419057-E6	1-port 1000BaseCWDM Small Form Factor Pluggable GBIC (mini-GBIC, connector type: LC) - 1550nm Wavelength	Up to 40 km
AA1419058-E6	1-port 1000BaseCWDM Small Form Factor Pluggable GBIC (mini-GBIC, connector type: LC) - 1570nm Wavelength	Up to 40 km
AA1419059-E6	1-port 1000BaseCWDM Small Form Factor Pluggable GBIC (mini-GBIC, connector	Up to 40 km

SFP order number	SFP type	Reach
	type: LC) - 1590nm Wavelength	
AA1419060-E6	1-port 1000BaseCWDM Small Form Factor Pluggable GBIC (mini-GBIC, connector type: LC) - 1610nm Wavelength	Up to 40 km
AA1419061-E6	1-port 1000BaseCWDM Small Form Factor Pluggable GBIC (mini-GBIC, connector type: LC) - 1470nm Wavelength	Up to 70 km
AA1419062-E6	1-port 1000BaseCWDM Small Form Factor Pluggable GBIC (mini-GBIC, connector type: LC) - 1490nm Wavelength	Up to 70 km
AA1419063-E6	1-port 1000BaseCWDM Small Form Factor Pluggable GBIC (mini-GBIC, connector type: LC) - 1510nm Wavelength	Up to 70 km
AA1419064-E6	1-port 1000BaseCWDM Small Form Factor Pluggable GBIC (mini-GBIC, connector type: LC) - 1530nm Wavelength	Up to 70 km
AA1419065-E6	1-port 1000BaseCWDM Small Form Factor Pluggable GBIC (mini-GBIC, connector type: LC) - 1550nm Wavelength	Up to 70 km
AA1419066-E6	1-port 1000BaseCWDM Small Form Factor Pluggable GBIC (mini-GBIC, connector type: LC) - 1570nm Wavelength	Up to 70 km
AA1419067-E6	1-port 1000BaseCWDM Small Form Factor Pluggable GBIC (mini-GBIC, connector type: LC) - 1590nm Wavelength	Up to 70 km
AA1419068-E6	1-port 1000BaseCWDM Small Form Factor Pluggable	Up to 70 km

SFP order number	SFP type	Reach
	GBIC (mini-GBIC, connector type: LC) - 1610nm Wavelength	
AA1419071	1-port 1000BaseEX SFP-LC 1550 nm	Up to 120 km
AA1419076	1000Base-BX10 1310 nm, bidirectional single fiber	Up to 40 km
AA1419077	1000Base-BX10 1490 nm, bidirectional single fiber	Up to 40 km

For detailed information about SFPs, refer to *Avaya Ethernet Routing Switch 8300 Installation — SFPs and XFPs* (NN46200-307)

Supported XFPs

XFPs are hot-swappable input/output enhancement components designed for use with Avaya products to allow 10 Gigabit Ethernet ports to link with other 10 Gigabit Ethernet ports. Digital diagnostic monitoring (DDM) provides real-time access to device operating parameters. All XFPs come with DDM capability.

All Avaya XFPs use LC connectors to provide precision keying, low interface losses, and space savings.

Table 3: XFP models on page 44 lists and describes the Avaya XFP models:

Table 3: XFP models

Model number	Product name	Description
10GBASE-SR	AA1403005-E5	850 nanometers (nm). The range is up to • 22 m using 62.5 micrometer (µm), 160 megaHertz times km (MHz-km) MMF • 33 m using 62.5 µm, 200 MHz-km MMF • 66 m using 62.5 µm, 500 MHz-km MMF • 82 m using 50 µm, 500 MHz-km MMF • 82 m using 50 µm, 500 MHz-km MMF

Model number	Product name	Description
		:
10GBASE-LR/LW	AA1403001-E5	1310 nm SMF. The range is up to 10 km.
10GBASE-ER/EW	AA1403003-E5	1550 nm SMF. The range is up to 40 km.
10GBASE-ZR/ZW	AA1403006-E5	1550 nm SMF. The range is up to 80 km.
10GBASE-LRM	AA1403007-E6	1310 nm MMF. The range is up to 220m.

Hot-removal/hot-insertion of Ethernet Routing Switch 8300 modules

In general, after you hot-insert or hot-remove an Ethernet Routing Switch 8300 module, you must wait 30 seconds before performing another hot-insertion or hot-removal of a module.

Hot-removal of master CPU

In a dual CPU configuration, both CPUs require the same set of images at all times. When you insert a new CPU in the Ethernet Routing Switch 8300, ensure that it has the same set of boot and runtime images as the existing CPU.

Removing the master CPU can result in a configuration loss for the removed CPU if it is replaced in the Ethernet Routing Switch 8300. To avoid this situation, follow these instructions if you need to remove a master CPU from an 8300 chassis:

1. Use the save to standby option to automatically save both the boot and the configuration files to both CPUs (master and standby).
2. If you are using the out-of-band Ethernet port of the 8393SF/CPU or 8394SF/CPU module for management, add a virtual IP address.

   The virtual IP address allows access to the master CPU whether the master CPU is slot 5 or slot 6.
3. Perform a soft reset on the master CPU to cause failover to occur.
4. Wait until the new master comes up and the old master becomes the standby.
5. Remove the standby CPU.

   If you need to reinsert this CPU, you must wait at least 60 seconds.

Note that if you remove the master CPU without following this procedure and then save the configuration after removal, the new configuration does not contain the removed CPU configuration. You then need to reconfigure the CPU ports.

To avoid this issue, back up the existing configuration file before saving any configuration. After you insert the removed CPU, you can then reboot the switch with the backup configuration file to restore the configuration. For more information about warm standby, see *Avaya Ethernet Routing Switch 8300 Planning and Engineering Network Design Guidelines* (NN46200-200).

Chapter 5: Resolved issues

Use the information in this section to learn about all issues fixed for Release 4.2.0.1.

Resolved issues navigation

Platform resolved issues

Table 4: Platform resolved issues

CR references	Description
Q01654805	Shapers can now be configured without affecting other ports on the same module. When configured, the TX-Q is reduced from 8 to 4
Q01040803	Changing the management IP address for a switch from the command line interface no longer causes inconsistent switch behavior.
Q01992990	System instability which could be observed in certain scenarios where some protocols like RIP were configured has now been resolved.
Q01992958	System instability when a large (greater than 500) number of vlans were added to the IST MLT is now resolved.

CR references	Description
Q01993351	The issue where ping from VRF uses the management port to route the response is now resolved.
Q01992961	When a configuration with 500+ vlans associated to SMLT/IST was sourced, the config loading time was long (around 9 minutes]. This is now resolved.
Q01969631	System instability which was observed after a CPU switchover had been done is now resolved.
Q01997246	An error message was encountered while configuring an Ip address to a vlan which is in the same subnet as the route configured in the bootconfig, but the configurations were still saved in the config file. This issue is resolved.

CLI and ACLI resolved issues

Table 5: CLI and ACLI resolved issues

CR references	Description
Q01958122-01	The static-mcastmac functionality allows the binding of a server NLB cluster multicast mac with a static set of ports (which are a subset of the port members for the vlan). The static-mcastmac entry needs to be enabled either on the vlan at L2 (if the switch is only performing L2 on that vlan) or as a static ARP entry at L3 (if the switch needs to IP route traffic into the vlan where the NLB Server cluster is). The 4.2.0.1 release enables the commandfor enabling the static-mcastmac entry as a static ARP entry at L3.

Device Manager resolved issues

Table 6: Device Manager resolved issues

CR references	Description
Q01858129-01	Non-printable ASCII characters (symbols) used for a configuration parameter value now displays correctly. This removes the problem of having the system consider the configuration file as corrupt.

Layer 2 resolved issues

Table 7: Layer 2 resolved issues

CR references	Description
Q00860990	If you remove a module that has associated static FDB or FDB-filter entries, the CLI command **`show vlan info all`** shows informationfor ports that are no longer present. This is a display issue onlyand does not affect the operation of the Ethernet Routing Switch 8300.

Multicast resolved issues

Table 8: Multicast resolved issues

CR references	Description
Q01749914-01	You can now configure PIM BSR on a circuitless IP (CLIP) from both CLI and ACLI.

IP Unicast resolved issues

Table 9: IP Unicast resolved issues

CR references	Description
Q01948850-01	Operation of the more-specific-non-local-route functionality has been improved to cover some situations where it previously did not route as desired.

Bandwidth management resolved issues

Table 10: Bandwidth management resolved issues

CR references	Description
No related issues.	

Security resolved issues

Table 11: Security resolved issues

CR references	Description
No related issues.	

MLT/SMLT resolved issues

Table 12: MLT/SMLT resolved issues

CR references	Description
Q01967344	It is now possible to create an MLT using 10G ports that have different types of XFPs. Previously the system would not allow this and return message of “MLT ports different types”.
Q01986567	IST flapping could previously occur when a VLAN was added or removed from the IST MLT. This is now resolved.
Q01997305	VRRP virtual Mac address for a non-SMLT connection were not being learnt properly over the IST. This issue specific situation is now resolved. There can be other MACs not properly learned under this situation. These other MAC situations will be resolved in a future release.

Switch management resolved issues

Table 13: Switch management resolved issues

CR references	Description
No related issues.	

Chapter 6: Known issues

Use the information in this section to learn more about known issues in Ethernet Routing Switch 8300 Release 4.2.0.1. These are to be resolved in a future release. Where applicable, use the workarounds provided for the known issues.

Known issues navigation

CLI/ACLI known issues

Table 14: CLI/ACLI known issues

CR References	Description
Q02073189/ Q02073577	If a switch set for ACLI mode is re-booted, and both the verify config and debug config flags are set true (non-default settings), then the switch will boot not with the proper configuration, but instead into a factory default configuration. Avaya recommends not to perform this action at this time. If the switch configuration, for a switch set to [Passport] CLI mode, is first saved in verbose mode (not the default setting; a user option) and then the switch is re-booted with both the verify config and debug config flags enabled (again not the default settings), the switch will boot with a factory default configuration instead of the correct configuration. Avaya recommends to not save config with verbose mode when using the CLI for the time being. These situations will be corrected in a future software release. Please note that the above situations are most likely present in older code as well; these are not introduced situations with 4.2.0.1 code.

CR References	Description
Q02074197	If a switch set for ACLI mode receives an invalid SSH login request, a logout trap is sent instead of an authentication failure trap message. This operation works fine in CLI mode.
Q02073222	If you set a switch for ACLI mode is programmed with snmp-v3 parameters (target address and t-parameter entries), save configuration, the reboot the switch, the programmed snmp parameters will display as junk characters, even via JDM. Prior to reboot (and config reload), all snmp parameters will display fine for both ACLI and JDM. This operation works fine under CLI mode.
Q2012615/ Q02073194	If a switch set for ACLI mode is rebooted, the dld images boot.cfg file are populated to match the file name of the booted "a" image. Correct behavior is for the boot.cfg file to remain blank. This can cause extra work for future upgrades, as these fields may now need to be changed (config bootconfig bootp default), versus just always matching the booted "a" image by default. This operation works fine under CLI mode, except for some specific scenarios. Avaya recommends when upgrading to always check and configure as needed the proper bootconfig and bootp values when upgrading. This would recommendation continues even after this situation is corrected in a future software release.

MLT/SMLT known issues

Table 15: MLT/SMLT known issues

CR References	Description
Q02069216	If multiple SLTs (single link SMLT connections) are configured within an RSMLT VLAN, incorrect SLT IDs are displayed via the command show ip rsmlt infodisplay. This is a display issue only with the SLT IDs, and has no affect on RSMLT behavior or operation. Use JDM or SNMP as an alternative to view this information.

Switch Management known issues

Table 16: Switch Management known issues

CR References	Description
Q02071642	JDM does not properly allow for a MSTP associated VLAN configuration on a switch configured for MSTP mode. This operation works fine under either CLI or ACLI.

Miscellaneous known issues

Table 17: Miscellaneous known issues

CR references	Description
Q01140665	BGP-only fields that are not applicable to RIP under the CLI Route Policies node are being displayed and need to be hidden or removed.
Q01927341	BGP cannot currently build a neighbor when the connected link is updown after a massive route import.
Q01949115	An unknown unicast traffic inject has been observed to cause traffic forwarding loss over the 8394 master CP.
Q02016391	When an SFP is incorrectly insertion (180 degrees out of rotation) the switch may no longer recognize the SFP after proper insertion; the actually SFP operation is fine. An error message will be generated for the improper insertion, if indeed the improper insertion is even possible. A switch re-boot will clear the condition, or better yet, take care when inserting SFPs and perform this action properly.
Q01996142	Hot swapping of a SFP may cause it to be not recognized by the switch. A system re-boot will clear the condition.
Q02027489	10Gbase-ZX XFP transceiver is currently wrongly displayed as a 10GbLR type.
Q01984215-02	IP/MAC address learning in SMLT network designs may not always function properly in that certain MACs may point to being learned on the IST instead of the proper SMLT/SLT links. It is suggest that the FDB ageout time be set to 21601 seconds (assuming default ARP ageout time is left at 360 minutes). This parameter is set on a per VLAN basis, so the parameter needs to be changed for all VLANs within the system; default timer value is 300 seconds. This setting causes MACs to never be aged

CR references	Description
	out by the FDB timer, but instead by only the ARP timer; value of 21601 is 1 second higher than 360 minutes. This parameter setting has no negative affect and re-learning of MAC moves continues to be sub-second. If this behavior is seen in a live production network, perform either a MAC/FDB flush on the VLAN or an IP/ARP flush on the system.
Q01482076	LLDP-MED does not current interoperate with ADAC – user must choose one or the other at the port level at this time.
Q01998418	ERS 8300 does not allow SSH Access to Standby CPU or to any remote switch; SSH client support is currently not in the product, just SSH server. This is an enhancement request targeted for a future release. At this time, use either telnet or rlogin instead, if either or both are enabled.
Q01988391	Certain ERS 8300 filters will work fine when associated with a 8324GTX port but function abnormally when associated with a 8348GTX-PWR port. Suggestion is to currently not associate any of these types of filters with any 8348GTX-PWR ports.
Q02032997	ERS 8300 RSMLT peer may drop traffic for greater than 10 seconds when the other RSMLT peer comes back up after being down for longer than the hold-up timer (very rare situation). Setting the hold-up timer to infinity will currently mask this situation, but that value can not always be used, depending upon ones specific SMLT/RSMLT network design.

Known documentation issues

This section contains known issues in published documentation for Release 4.2.0.1. This information will be added to the documentation for the next release.

Installation — AC Power Supply (NN46200-301)

This document does not list the Mean Time Before Failure (MTBF) value for the 8302AC power supply. The MTBF for the 8302AC is 238,322 hours.

Chapter 7: Known limitations

Use the information in this section to learn more about known limitations. These CRs are classified as operation not to be changed.

Known limitations navigation

Hardware/software known limitations

Table 18: Hardware/software known limitations

CR references	Description
Q01813362	The 8348GTX&8348GTX-POE modules adopted an advanced technology to provide better efficiency and effectivity. There is a hardware limitation on this architecture: when a QoS shaper is configured on one port, this configuration will actually affect four related ports (3 additional ports). This affect is in groups of 4 ports like <1,5,9,13>, <2,6,10,14>, <3,7,11,15> etc. So any such configuration on any one of the same group port, affects all 4 ports. Similarly (for example), such a configuration on port 7, affects ports 3, 11 and 15.

Hardware known limitations

Table 19: Hardware known limitations

CR references	Description
Q00961155	The current Ethernet Routing Switch 8300 software does not support a modular automatic power pruning function. When the total Available Power for allocation is 0 and an additional PoE module is inserted, the additional module will not receive any PoE power even if it is configured with Critical Priority. Workaround: Avaya recommends that you manually administratively disable a selected PoE module in order to release the power to the higher priority module.
Q01943495	With the 8308 or 8394 blades, the mirror traffic and original traffic (double traffic) is limited on the link between PP uplink and FA. When traffic is over 63%, there is traffic loss on FA VOQ, and when traffic over 67%, PP suffers a traffic loss. Rec not to enable port mirroring on ports running greater than 50% line rate.
	An Egress Q-tag is only possible when the output/sniffer (mirroring) port is on a Tiger module. Available Tiger modules are 8348GTX (and PWR), 8348GB, 8308XL and 8394SF. A pre-existing chassis configuration with just Twist-D modules (any module beside Tiger list), can never see Q-tag from mirroring. Ingress Q-tags are not possible.

Platform known limitations

Table 20: Platform known limitations

CR references	Description
Q00851722	When the CP rate limit feature is required on MLT ports, the user must configure the rate on all MLT ports manually.
Q01439225	Modifications or deletions of an OSPF area aggregate entry do not take effect unless you globally disable and then re-enable OSPF, Workaround:If you delete or dynamically modify an area aggregate, Avaya recommends that you globally disable and then reenable OSPF.
Q01356776	If you use the port mirroring feature while monitoring LLDP packets, the mirrored packets can miss four bytes from Ethertype and chassis ID TLV.

CR references	Description
Q01403458	Tracing of LLDP task 68 above level 1 to the console can block Telnet, SNMP, and transmission and reception of LLDP frames, Ping responses and the ability to respond to ARP Workaround: If trace level 68 is needed for debugging purposes, Avaya recommends that you run only level 1.
Q01370691	When you run port mirroring with the mirroring and mirrored ports on different I/O modules, the traffic analyzer can sometimes see a 4 byte tag on untagged packets. Workaround: Avaya recommends that if you see this situation, configure port mirroring on the same I/O module.
Q00755304	When you enable the VCT test, the PHY waits a fixed amountof time before sending out the TDR test pulse. This is to ensure thatthe link is broken and that the link partner is not sending 10/100/1000Mbpstraffic. As soon as the VCT test is finished, the PHY automaticallyresumes normal operation. This means that auto-negotiation may startagain and the link is then re-established, which will take some time.
Q01951986	If IGMP is enabled on VLAN w/ tagged ports, IGMP should be enabled on all VLANs that are part Recommended: Ifa port is tagged and belongs to an IGMP VLAN, other all other VLANSit belongs to should also be IGMP enabled. Else, extraneous trafficwill hit the CPU.
Q01985635	For 8348GTX, 8348GTX-PWR and 8348GB, the DWR function works properly only when the egress ports at 1Gbps speed. Otherwise, the proportion of each stream does not accord with the weights.

Device Manager known limitations

Table 21: Device Manager known limitations

CR references	Description
Q00834504	The 802.1p-to-dscp table is not available in the Device Manager. However, it is available in the CLI and ACLI.
Q00802165	You cannot convert a MAC auto-learned entry to manual via the CLI and ACLI. You can only do so via the Device Manager using the VLAN > Mac Learning > VlanMacLearning dialog boxes. You cannot convert a MAC autolearned entry to manual through the CLI and ACLI. You can only do so through Device Manager using the VLAN, Mac Learning, VlanMacLearning dialog boxes.

CLI AND ACLI known limitations

Table 22: CLI and ACLI known limitations

CR references	Description
Q01041504	You can use decimal as well as hex input for the user-definedPID when configuring user-defined protocol-based VLANs. CLI and ACLI help text does not indicate that you can use both.
Q01010343	In the ACLI, the command **`eapol re-authenticate`** displays some garbage (incorrect) characters along with the EAP authentication messages. In the ACLI, the command **`eapol re-authenticate`** displays some incorrect characters along with the EAP authentication messages.
Q00816522	You cannot display the auto-learned MAC for a specific port in the ACLI. Instead, it only shows the number of MACs learned. When you enter **`show interfaces vlan autolearn`**, it does not provide an option to specify a port. You cannot display the autolearned MAC for a specific port in the ACLI. Instead, the ACLI only shows the number of MACs learned. When you enter **`show interfaces vlan autolearn`**, the display does not provide an option to specify a port.

Layer 2 known limitations

Table 23: Layer 2 known limitations

CR references	Description
Q01436928	Unlike other I/O modules, 8348GB card sends out a shutdown LLDP PDU before it goes down when administratively disabled.
Q00841632	If you delete selected ports bound to multicast MAC filtering and then source the configuration (**`source config.cfg`**), the deleted ports do not get restored as originally configured. The reason for this is that the MAC is already learned before you source the configuration. Thus, the port does not get added to the MAC. If you delete selected ports bound to multicast MAC filtering and then source the configuration (**`source config.cfg`**), the deleted ports are not restored as originally configured. This is because the MAC is

CR references	Description
	already learned before you source the configuration. Thus, the port does not get added to the MAC.
Q00802887	The autolearned MAC entry does not get re-learned after a conversion to manual entry and deletion until the FDB entry ages out. When you convert, you delete the manually entered MAC entry in the unknown MAC discard table. However, the FDB entry itself is not deleted. The autolearned MAC entry is not relearned after a conversion to manual entry and deletion until the FDB entry ages out. When you convert, you delete the manually entered MAC entry in the unknown MAC discard table. However, the FDB entry itself is not deleted.

QoS known limitations

Table 24: QoS known limitations

CR references	Description
Q01256112	When two different Scheduling groups are used, traffic flow is not expected. For example, if we are egressing traffic from two 8348GTX-PWR Gigabit ports into one 8348GTX-PWR Gigabit port and the two transmit streams have a QoS level of 3 and 4, if level 3 and 4 have the same scheduling group (say both are dwrr1,dwrr0 or strict priority), then traffic arrives as expected. However, if we change level 3 to DWRR1 and level 4 to DWRR0, the highest priority traffic always has less drops even though it is in a lower scheduling group i.e, 4 has a higher priority even though it has lower scheduling group. There are 8 hardware priority queues. By default, all queues are configured to use DWRR1 scheduling group. It is not recommend that the user change a higher priority queue to use DWRR0 while the lower priority queues still use DWRR1

Multicast known limitations

Table 25: Multicast known limitations

CR references	Description
Q00889744	IGMP static receivers are not supported in the Ethernet Routing Switch 8300.

CR references	Description
Q00791636	In the ACLI and CLI, **`show ip igmp interface`** displays the IGMP snoop interfaces. Those interfaces that are not IGMP-enabledare shown as inactive if the interface is IP-enabled, or was previously IGMP snoop enabled.
Q00737617	On an IGMP snoop device, the sender is available only if the traffic is unregistered. In other words, no receiver exists locally on the device. Otherwise, sender information will not be available on a snoop device . On an IGMP snoop device, sender information is available only if the traffic is unregistered (In other words, no receiver exists locally on the device.). If the traffic is registered, sender information is not available on an IGMP snoop device.
Q01595453	The user cannot flush FDB entries learned on an MLT by flushingMAC on an MLT member.
Q01536016	When IGMP Snooping is running in a multicast square SMLT, if one of the IST trunk fails, traffic can be lost and only recovers when the IST trunk comes back up.
Q01659446	When IGMP snooping is enabled, NLB multicast mode may floodmulticast traffic.
Q01548125	Multicast group IP cannot map to the same MAC address as reserved multicast IP. Avaya recommends not to use a multicast group for user traffic for which the MAC address of that multicast IP is mapped to a reserved multicast address. Workaround: Avaya recommends that you do not use a multicast group for user traffic for which the MAC address of that multicast IP is mapped to a reserved multicast address.

Bandwidth management known limitations

Table 26: Bandwidth management known limitations

CR references	Description
Q00879816	The VLAN ID range 1–4000 is supported under VLAN configurationfor data traffic. The remainder of the VLAN ID range that displaysis reserved for network control traffic. Do not configure filtersto match the reserved VLAN ID range.
Q00831460	A common pool of 128 records exists for both policies (policers) and filter stats. If this pool is exhausted and an additional record is requested, an error message like the following appears: `QOS ERROR gtcmCreateTcEntry: Failed, status = 20` Workaround:

CR references	Description
	Avaya recommends that if the error message appears, you must delete one filter stat instance or policer before adding anoter.
Q00803181	You can configure different filter remarking values for ports within an MLT. Workaround: Avaya recommends that you configure the same remarking values across all ports in an MLT.
Q00799518	When you use remark-user-priority, filter counters and stats can show invalid values.
Q00797808 Q00806856	Partial masking of Access-Template fields is not supported. For example, Access-Template Src Mac field defined as `00:00:00:ff:ff:ff` is not a supported configuration.
Q00788755	There is no provision in the Ethernet Routing Switch 8300 Layer2 commands to look up the DSCP value based on the .p bit.
Q00787044	If you enter **`show filter access-list statistics`** in the CLIwhen ACE MatchCountMode is disabled, an error message should appearindicating that the feature is not enabled. Currently, the consoleshows all 0 counters without any traffic or warning messages.
Q00785991	No statistics are available for traffic shaping.
Q00785950	In some configurations, egress counters for multicast trafficshow the counter values for unicast traffic when a port belongs toa protocol-based VLAN. In such instances, these counters are not shownunder the unicast counter values.
Q00785103	You can apply fdb-filters to ports but they act only on VLANs.For example, if you assign an fdb-filter to a port in a VLAN, allports in that VLAN will act on the filter. If the port to which thefdb-filter is assigned is disabled or goes down unexpectedly, thefilter remains in effect for all other ports in the VLAN.
Q00783246	When you poll statistics for the QoS egress-counter-set, counters are reset to zero. You cannot gather a cumulative number of packets over a period of time using this feature if you execute **`show qos egress-stats`**. When you poll statistics for the QoS egress-counter-set, counters are reset to zero. You cannot gather a cumulative number of packets over a period of time using this feature if you use the **`show qos egress-stats`** command.
Q00783246 Q00783234	The Policing remarking feature does not work when you use the **`remark-user-priority`** command for DiffServ remarking.
Q00765155	As it appears in the CLI, the maximum value of the committedand peak burst rate is misleading. The Ethernet Routing Switch 8300 shows onlya fixed maximum value of 65535, which does not change based on theconfiguration. The actual maximum value is calculated from the committedand peak information rates.

CR references	Description
Q00755441	In the Ethernet Routing Switch 8300, the VLAN QoS level is supported only on protocol-based VLANs.
Q00730427	QoS shaping does not perform correctly at lower rates. There is a 10–20% variation in the actual traffic rate as compared with the configured rate.
Q00697474	The 802.1p bit is not overwritten for untrusted Layer 2 ports. You can use filters to perform the same functions.

OSPF known limitations

Table 27: OSPF known issues

CR references	Description
Q01420932	If you set the transit delay higher than 900, the neighbors can get stuck in OSPF exchange state. Workaround: Avaya recommends that you set the transit delay timer to 900 or less.

Security known limitations

Table 28: Security known limitations

CR references	Description
Q01271108	The RADIUS accounting UDP port configuration change cannotbe saved. The default port for RADIUS accounting is 1813, which worksfor all the current RADIUS servers and is the port to use accordingto RFCs. After a reboot or config source, the port returns to thedefault of 1813.
Q00819777	Note that tagging and EAP are mutually exclusive. If you enable EAP on a port, using auto or force-authorize, you cannot enable tagging on the port, and vice versa. Tagging and EAP are mutually exclusive. If you enable EAP on a port, using auto or force-authorize, you cannot enable tagging on the port, and conversely.

Miscellaneous limitations

Table 29: Miscellaneous limitations

CR references	Description
Q01140665	BGP-only fields that are not applicable to RIP under the CLIRoute Policies node are being displayed and need to be hidden or removed.
Q01131665	A `save config` success message can follow a failure message. Workaround: Check flash to ensure sufficient free space and then redo the save config.
Q00773426	If you enable port mirroring on a tagged interface, the mirroredpackets will not contain the 802.1Q header.

Chapter 8: Customer Service

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

Navigation

- Getting technical documentation on page 67
- Getting product training on page 67
- Getting help from a distributor or reseller on page 67
- Getting technical support from the Avaya Web site on page 68

Getting technical documentation

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

Getting product training

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

Getting help from a distributor or reseller

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

Getting technical support from the Avaya Web site

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

Chapter 9: Translations of Safety Messages

This section contains translations of precautionary notices that you must read and follow for safe operation of the Ethernet Routing Switch 8300.

Electromagnetic interference caution statement

⚠ **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.

⚠ **Caution:**

ATTENTION

Le périphérique est un produit de Classe A. Le fonctionnement de cet équipement dans une zone résidentielle risque de causer des interférences nuisibles, auquel cas l'utilisateur devra y remédier à ses propres frais.

⚠ **Caution:**

ACHTUNG

Dies ist ein Gerät der Klasse A. Bei Einsatz des Geräts in Wohngebieten kann es Störungen des Radio- und Fernsehempfangs verursachen. In diesem Fall muss der Benutzer alle notwendigen Maßnahmen ergreifen, die möglicherweise nötig sind, um die Störungen auf eigene Rechnung zu beheben.

⚠ **Caution:**

PRECAUCIÓN

Este es un producto clase A. El uso de este equipo en áreas residenciales puede causar interferencias nocivas, en cuyo caso, se requerirá que los usuarios tomen cualquier medida necesaria para corregir la interferencia por cuenta propia.

⚠ **Caution:**

CUIDADO

Este dispositivo é um produto Classe A. Operar este equipamento em uma área residencial provavelmente causará interferência prejudicial; neste caso, espera-se que os usuários tomem as medidas necessárias para corrigir a interferência por sua própria conta.

⚠ **Caution:**

ATTENZIONE

Questo dispositivo è un prodotto di Classe A. Il funzionamento di questo apparecchio in aree residenziali potrebbe causare interferenze dannose, nel cui caso agli utenti verrà richiesto di adottare tutte le misure necessarie per porre rimedio alle interferenze a proprie spese.

Electrostatic discharge caution statement

⚠ **Electrostatic alert:**

ESD

To prevent damage from electrostatic discharge, always wear an antistatic wrist strap connected to an electrostatic discharge (ESD) jack when performing maintenance on this product. Ensure that the wrist strap makes contact with your skin.

⚠ **Electrostatic alert:**

ATTENTION

ESD (décharge électrostatique)

Pour prévenir tout dommage dû à une décharge électrostatique, vous devez toujours porter un un bracelet antistatique connecté à une prise pour décharge électrostatique (ESD) lors de l'exécution d'opérations de maintenance sur ce produit. Assurez-vous que le bracelet antistatique est en contact avec votre peau.

⚠ **Electrostatic alert:**

ACHTUNG

ESD

Um Schäden durch elektrostatische Entladung zu verhindern, tragen Sie bei der Instandhaltung dieses Produkts immer ein antistatisches Band am Handgelenk, das mit einer ESD-Buchse verbunden ist. Stellen Sie

⚠ **Electrostatic alert:**

PRECAUCIÓN

ESD (Descarga electrostática)

Para prevenir el daño producido por una descarga electrostática, use siempre una pulsera antiestática conectada a un enchufe de descarga electrostática (ESD) al realizar el mantenimiento de este producto. Asegúrese de que la pulsera antiestática haga contacto con su piel.

⚠ **Electrostatic alert:**

CUIDADO

ESD

Para evitar danos com descarga eletrostática, sempre use uma pulseira antiestática que esteja conectada a uma tomada de descarga eletrostática (ESD) quando estiver realizando a manutenção deste produto. Certifique-se de que a pulseira esteja em contato com sua pele.

⚠ **Electrostatic alert:**

ATTENZIONE

ESD

Per evitare danni derivanti da scariche elettrostatiche, indossare sempre un polsino antistatico collegato a una presa di scarico elettrostatico (ESD) durante la manutenzione del prodotto. Accertarsi che il polsino sia a contatto con la pelle.

Index