

# Administering Avaya G450 Branch Gateway

© 2010-2022, Avaya Inc. All Rights Reserved.

#### Notice

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

#### 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: <a href="https://support.avaya.com/helpcenter/getGenericDetails?detailId=C20091120112456651010">https://support.avaya.com/helpcenter/getGenericDetails?detailId=C20091120112456651010</a> 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.

#### **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.

### **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: <a href="https://support.avaya.com">https://support.avaya.com</a> or such successor site as designated by Avaya.

#### **Documentation disclaimer**

"Documentation" means information published in varying mediums which may include product information, operating instructions and performance specifications that are generally made available to users of products. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of Documentation unless such modifications, additions, or deletions were performed by or on the express behalf of 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.

#### Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, <u>HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO</u>, 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 "YOÙ" 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 as set forth below in the Designated System(s) License (DS) section as applicable. 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 set of Designated Processors that hosts (physically or virtually) 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 <a href="https://support.avaya.com/LicenseInfo">https://support.avaya.com/LicenseInfo</a> 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. Unless otherwise stated, 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.

### How to Get Help

For additional support telephone numbers, go to the Avaya Support website: <a href="http://www.avaya.com/support">http://www.avaya.com/support</a>. If you are:

- Within the United States, click the Escalation Contacts link that is located under the Support Tools heading. Then click the appropriate link for the type of support that you need.
- Outside the United States, click the Escalation Contacts link that is located under the Support Tools heading. Then click the International Services link that includes telephone numbers for the international Centers of Excellence.

### **Providing Telecommunications Security**

Telecommunications security (of voice, data, and/or video communications) is the prevention of any type of intrusion to (that is, either unauthorized or malicious access to or use of) your company's telecommunications equipment by some party.

Your company's "telecommunications equipment" includes both this Avaya product and any other voice/data/video equipment that could be accessed via this Avaya product (that is, "networked equipment").

An "outside party" is anyone who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf. Whereas, a "malicious party" is anyone (including someone who may be otherwise authorized) who accesses your telecommunications equipment with either malicious or mischievous intent.

Such intrusions may be either to/through synchronous (time-multiplexed and/or circuit-based), or asynchronous (character-, message-, or packet-based) equipment, or interfaces for reasons of:

- Utilization (of capabilities special to the accessed equipment)
- Theft (such as, of intellectual property, financial assets, or toll facility access)
- · Eavesdropping (privacy invasions to humans)
- · Mischief (troubling, but apparently innocuous, tampering)
- Harm (such as harmful tampering, data loss or alteration, regardless of motive or intent)

Be aware that there may be a risk of unauthorized intrusions associated with your system and/or its networked equipment. Also realize that, if such an intrusion should occur, it could result in a variety of losses to your company (including but not limited to, human/data privacy, intellectual property, material assets, financial resources, labor costs, and/or legal costs).

### Responsibility for Your Company's Telecommunications Security

The final responsibility for securing both this system and its networked equipment rests with you - Avaya's customer system

administrator, your telecommunications peers, and your managers. Base the fulfillment of your responsibility on acquired knowledge and resources from a variety of sources including but not limited to:

- · Installation documents
- · System administration documents
- · Security documents
- · Hardware-/software-based security tools
- · Shared information between you and your peers
- · Telecommunications security experts

To prevent intrusions to your telecommunications equipment, you and your peers should carefully program and configure:

- Your Avaya-provided telecommunications systems and their interfaces
- Your Avaya-provided software applications, as well as their underlying hardware/software platforms and interfaces
- · Any other equipment networked to your Avaya products

#### **TCP/IP Facilities**

Customers may experience differences in product performance, reliability and security depending upon network configurations/design and topologies, even when the product performs as warranted.

#### **Product Safety Standards**

This product complies with and conforms to the following international Product Safety standards as applicable:

- IEC 62368-1, including all relevant national deviations as listed in the IECEE Bulletin—Product Category OFF: IT and Office Equipment.
- · CAN/CSA-C22.2 No. 62368-1 / UL 62368-1.

This product may contain Class 1 laser devices.

- · Class 1 Laser Product
- · Luokan 1 Laserlaite
- Klass 1 Laser Apparat

### **Electromagnetic Compatibility (EMC) Standards**

This product complies with and conforms to the following international EMC standards, as applicable:

- CISPR 32, including all national standards based on CISPR
- CISPR 35, including all national standards based on CISPR 35
- IEC 61000-3-2 and IEC 61000-3-3.

Avaya Inc. is not responsible for any radio or television interference caused by unauthorized modifications of this equipment or the substitution or attachment of connecting cables and equipment other than those specified by Avaya Inc. The correction of interference caused by such unauthorized modifications, substitution or attachment will be the responsibility of the user. Pursuant to Part 15 of the Federal Communications Commission (FCC) Rules, the user is cautioned that changes or modifications not expressly approved by Avaya Inc. could void the user's authority to operate this equipment

### Federal Communications Commission Part 15 Statement:

For a Class A digital device or peripheral:



#### Note

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the 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 and, if not installed and used in accordance with the

instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

For a Class B digital device or peripheral:



#### Note:

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- · Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

#### Equipment With Direct Inward Dialing ("DID"):

Allowing this equipment to be operated in such a manner as to not provide proper answer supervision is a violation of Part 68 of the FCC's rules.

Proper Answer Supervision is when:

- This equipment returns answer supervision to the public switched telephone network (PSTN) when DID calls are:
  - · answered by the called station,
  - · answered by the attendant,
  - routed to a recorded announcement that can be administered by the customer premises equipment (CPE) user
  - · routed to a dial prompt
- This equipment returns answer supervision signals on all (DID) calls forwarded back to the PSTN.

Permissible exceptions are:

- · A call is unanswered
- · A busy tone is received
- · A reorder tone is received

Avaya attests that this registered equipment is capable of providing users access to interstate providers of operator services through the use of access codes. Modification of this equipment by call aggregators to block access dialing codes is a violation of the Telephone Operator Consumers Act of 1990.

#### **Automatic Dialers:**

When programming emergency numbers and (or) making test calls to emergency numbers:

- Remain on the line and briefly explain to the dispatcher the reason for the call.
- Perform such activities in the off-peak hours, such as early morning or late evenings.

### **Toll Restriction and least Cost Routing Equipment:**

The software contained in this equipment to allow user access to the network must be upgraded to recognize newly established network area codes and exchange codes as they are placed into service.

Failure to upgrade the premises systems or peripheral equipment to recognize the new codes as they are established will restrict the customer and the customer's employees from gaining access to the network and to these codes.

#### For equipment approved prior to July 23, 2001:

This equipment complies with Part 68 of the FCC rules. On either the rear or inside the front cover of this equipment is a label that contains, among other information, the FCC registration number, and ringer equivalence number (REN) for this equipment. If requested, this information must be provided to the telephone company.

#### For equipment approved after July 23, 2001:

This equipment complies with Part 68 of the FCC rules and the requirements adopted by the Administrative Council on Terminal Attachments (ACTA). On the rear of this equipment is a label that contains, among other information, a product identifier in the format US:AAAEQ##TXXX. If requested, this number must be provided to the telephone company.

The REN is used to determine the quantity of devices that may be connected to the telephone line. Excessive RENs on the telephone line may result in devices not ringing in response to an incoming call. In most, but not all areas, the sum of RENs should not exceed 5.0.

L'indice d'équivalence de la sonnerie (IES) sert à indiquer le nombre maximal de terminaux qui peuvent être raccordés à une interface téléphonique. La terminaison d'une interface peut consister en une combinaison quelconque de dispositifs, à la seule condition que la somme d'indices d'équivalence de la sonnerie de tous les dispositifs n'excède pas cinq.

To be certain of the number of devices that may be connected to a line, as determined by the total RENs, contact the local telephone company. For products approved after July 23, 2001, the REN for this product is part of the product identifier that has the format US:AAAEQ##TXXX. The digits represented by ## are the REN without a decimal point (for example, 03 is a REN of 0.3). For earlier products, the REN is separately shown on the label.

#### Means of Connection:

Connection of this equipment to the telephone network is shown in the following table:

Manufactu rer's Port Identifier	FIC Code	SOC/ REN/ A.S. Code	Network Jacks
Off premises station	OL13C	9.0F	RJ2GX, RJ21X, RJ11C
DID trunk	02RV2.T	AS.2	RJ2GX, RJ21X, RJ11C
CO trunk	02GS2	0.3A	RJ21X, RJ11C
	02LS2	0.3A	RJ21X, RJ11C
Tie trunk	TL31M	9.0F	RJ2GX
Basic Rate Interface	02IS5	6.0F, 6.0Y	RJ49C
1.544 digital	04DU9.BN	6.0F	RJ48C, RJ48M
interface	04DU9.1K N	6.0F	RJ48C, RJ48M
	04DU9.1S N	6.0F	RJ48C, RJ48M
120A4 channel service unit	04DU9.DN	6.0Y	RJ48C

If this equipment causes harm to the telephone network, the telephone company will notify you in advance that temporary discontinuance of service may be required. But if advance notice is not practical, the telephone company will notify the customer as soon

as possible. Also, you will be advised of your right to file a complaint with the FCC if you believe it is necessary.

The telephone company may make changes in its facilities, equipment, operations or procedures that could affect the operation of the equipment. If this happens, the telephone company will provide advance notice in order for you to make necessary modifications to maintain uninterrupted service.

If trouble is experienced with this equipment, for repair or warranty information, please contact the Technical Service Center at 1-800-242- 2121 or contact your local Avaya representative. If the equipment is causing harm to the telephone network, the telephone company may request that you disconnect the equipment until the problem is resolved.

A plug and jack used to connect this equipment to the premises wiring and telephone network must comply with the applicable FCC Part 68 rules and requirements adopted by the ACTA. A compliant telephone cord and modular plug is provided with this product. It is designed to be connected to a compatible modular jack that is also compliant.

Connection to party line service is subject to state tariffs. Contact the state public utility commission, public service commission or corporation commission for information.

#### Installation and Repairs

Before installing this equipment, users should ensure that it is permissible to be connected to the facilities of the local telecommunications company. The equipment must also be installed using an acceptable method of connection. The customer should be aware that compliance with the above conditions may not prevent degradation of service in some situations.

Repairs to certified equipment should be coordinated by a representative designated by the supplier. It is recommended that repairs be performed by Avaya certified technicians.

#### FCC Part 68 Supplier's Declarations of Conformity

Avaya Inc. in the United States of America hereby certifies that the equipment described in this document and bearing a TIA TSB-168 label identification number complies with the FCC's Rules and Regulations 47 CFR Part 68, and the Administrative Council on Terminal Attachments (ACTA) adopted technical criteria.

Avaya further asserts that Avaya handset-equipped terminal equipment described in this document complies with Paragraph 68.316 of the FCC Rules and Regulations defining Hearing Aid Compatibility and is deemed compatible with hearing aids.

Copies of SDoCs signed by the Responsible Party in the U. S. can be obtained by contacting your local sales representative and are available by contacting Avaya Support website at: <a href="https://support.avaya.com">https://support.avaya.com</a>.

#### **Canadian Conformity Information**

This Class A (or B) digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe A (ou B) est conforme à la norme NMB-003 du Canada.

This product meets the applicable Industry Canada technical specifications/Le présent materiel est conforme aux specifications techniques applicables d'Industrie Canada.

### **European Union Declarations of Conformity**



Avaya Inc. declares that the equipment specified in this document bearing the "CE" (Conformité Europeénne) mark conforms to the European Union Electromagnetic Compatibility Directive (2014/30/EU), Low Voltage Directive (2014/35/EU) and RoHS Directive (2011/65/EU).

A copy of the Declaration may be obtained from <a href="https://support.avaya.com">https://support.avaya.com</a> or Avaya Inc., 2605 Meridian Parkway Suite 200 Durham, NC 27713 USA.

#### **European Union Battery Directive**



Avaya Inc. supports European Union Battery Directive 2006/66/EC. Certain Avaya Inc. products contain lithium batteries. These batteries are not customer or field replaceable parts. Do not disassemble. Batteries may pose a hazard if mishandled.

#### Japan

The power cord set included in the shipment or associated with the product is meant to be used with the said product only. Do not use the cord set for any other purpose. Any non-recommended usage could lead to hazardous incidents like fire disaster, electric shock, and faulty operation.

本製品に同梱または付属している電源コードセットは、本製品専用で す。本製品以外の製品ならびに他の用途で使用しないでください。火 災、感電、故障の原因となります。

#### If this is a Class A device:

This is a Class A product based on the standard of the Voluntary Control Council for Interference by Information Technology Equipment (VCCI). If this equipment is used in a domestic environment, radio disturbance may occur, in which case, 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誘す るよう要求されることがあります。

#### If this is a Class B device:

This is a Class B product based on the standard of the Voluntary Control Council for Interference from Information Technology Equipment (VCCI). If this is used near a radio or television receiver in a domestic environment, it may cause radio interference. Install and use the equipment according to the instruction manual.

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 B 情報技術装置です。この装置は、家庭環境で使用することを目的としていますが、この装置がラジオやテレビジョン受信機に近接して使用されると、受信障害を引き起こすことがあります。取扱説明書に従って正しい取り扱いをして下さい。

#### **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, its licensors, its suppliers, 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, Hosted Service(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 non-Avaya trademarks are the property of their respective owners.

### **Downloading Documentation**

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

### **Contact Avaya Support**

See the Avaya Support website: <a href="https://support.avaya.com">https://support.avaya.com</a> 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: <a href="https://support.avaya.com">https://support.avaya.com</a> (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

Chapter 1: Introduction	22
Purpose	
Change history	22
Chapter 2: Configurations	23
Basic configuration	
Port redundancy configuration	23
Port and switch redundancy configuration	
RSTP configuration	
RSTP and switch redundancy configuration	25
Chapter 3: Configuration overview	26
Defining the Console interface	
Defining the USB-modem interface	
Other interfaces	
Define other interfaces	27
Configuration using CLI	28
Configuration changes and backup	28
Saving configuration changes and backing them up	29
Firmware version control	29
Using an older version of firmware	29
Chapter 4: Branch Gateway access	30
CLI access	30
Logging to CLI	30
CLI contexts	30
Using CLI help	31
CLI access using the local network	32
Accessing CLI using a computer	
CLI access using modems	32
Accessing CLI using a USB modem	33
USB port settings	33
Branch Gateway serial modems	34
CM access	
Security overview	
Login permissions	
User account management	
Login authentication	
SSH protocol support	
SCP protocol support	
RADIUS authentication	
Special security features	43

	Commands used to configure Telnet access	43
	Gateway secret management	44
	DoS attacks	45
	Managed Security Services	47
	Enhanced Access Security Gateway (EASG)	52
	Managing EASG	52
	Viewing EASG product certificates	55
	Managing EASG site certificates	
	Viewing EASG status	. 57
	Viewing product id	
	Service logins with Enhanced Access Security Gateway (EASG) authentication	58
Ch	apter 5: Basic device configuration	59
	Defining an interface	. 59
	Primary Management Interface (PMI) configuration	60
	Setting the PMI of the Branch Gateway	60
	Active and configured PMI	61
	PMI configuration CLI commands	61
	Example of defining a default gateway	
	Branch Gateway Controller configuration	. 62
	Locating the Branch Gateway serial number	
	Survivability and migration options	
	MGC list configuration	
	About setting reset times	
	Example for setting reset times	
	Accessing the registered MGC	
	H.248 Registration Source Port	
	ICC or Survivable Remote Server monitoring	
	Summary of MGC list configuration commands	
	DNS resolver	
	DNS resolver features	
	Typical DNS resolver application – VPN failover	
	Configuring DNS resolver	
	Using DNS resolver to resolve a hostname	
	DNS resolver maintenance	
	DNS resolver configuration commands	
	Device status viewing	
	The show mm command	
	The show mm and show mg list config commands	
	Device status commands	
	OOB	
	oob-interface configuration	
	no oob-interface	
	show onh-interface	77

set non-oob-interfa	faces access	77
	e management	
	9	
	ware upgrades	
	ware uploads from the gateway	
	ocal Survivability (SLS)	
	tibility with SLS	
	ublity with SES	
	pported in SLS	
	onality in SLS mode	
	onality not supported by SLS	
	urvivability data sources and communication paths.	
•	e	
	ess	
· · · · · · · · · · · · · · · · · · ·	process	
•	JI OCESS	
	pecific Branch Gateway features	
•	ling in SLS mode	
	arances in SLS mode	
	erances in SES mode	
	es	
•	utton	
	ook button	
•	LS mode	
_	sure in SLS modeSoftphone in SLS mode	
	Softphone in SLS mode	
55 5	log entries and format	
•	log with contact closure	
•	log with contact closure	
_	rules	
9		
	or SLS Restriction (COR) permissions	
	` '.	
	ld descriptions for the Branch Gatewayage field descriptions	
,	•	
•	on in CI C	
	es in SLSusing the CLI to manually configure SLS administra	······································
•	ield descriptions	
טסו טווטעון pack II	เษเน นะอน เมเบเอ	129

Collecting signaling groups data	133
Signaling Group field descriptions	134
Collecting administered ISDN-BRI trunks data	134
ISDN-BRI Trunk field descriptions	135
Collecting Feature Access Codes data	136
Feature Access Code field descriptions	137
Collecting system parameters data	138
Codecs supported in SLS	139
General system parameters field descriptions	139
Collecting ARS dial patterns data	139
ARS Dial Patterns field descriptions	140
Collecting Incoming Call Handling data	140
Incoming call handling data field descriptions	140
Configuration of the SLS data through the CLI	141
Creating the SLS administration data set on the Branch Gateway	142
Administering station parameters	144
Class values in SLS station context	146
Module-port values in SLS station configuration mode	147
Administering DS1 parameters	147
ISDN Layer 3 country codes	149
ISDN Layer 3 country protocols for ISDN Primary Rate service	150
Administering BRI parameters	151
Trunk group assignment	153
Administering trunk-group parameters	153
Maximum number of members in a trunk group	158
SLS group type assignments	158
Module-port values in SLS trunk-group context for analog trunks	159
Trunk port values in SLS trunk-group context for digital trunks	159
Administering signaling-group parameters	160
Administering dial-pattern parameters	161
Administering incoming-routing parameters	162
Summary of SLS configuration commands	163
Chapter 7: Switch Ethernet port configuration	173
Ethernet ports on the Gateway switch	
Ethernet ports on the Branch Gateway router	173
Cables used for connecting devices to the fixed router	173
Roadmap for configuring switch Ethernet ports	174
Summary of switch Ethernet port configuration CLI commands	
Configuring the WAN Ethernet port	
Roadmap for configuring additional features on the WAN Ethernet port	176
WAN Ethernet port traffic shaping	
About backup interfaces	
Summary of WAN Ethernet port configuration CLI commands	177

	DHCP client configuration	178
	DHCP client applications	178
	Configuring the DHCP client	179
	Examples of DHCP lease release and renew	180
	Commands used for DHCP client maintenance	181
	Examples of configuring DHCP client logging messages	181
	Summary of DHCP client configuration CLI commands	
	LLDP configuration	182
	Supported TLVs	183
	Configuring LLDP	183
	Summary of LLDP configuration CLI commands	184
Ch	apter 8: System logging	186
	Types of logging sinks	186
	Syslog server configuration	187
	Defining Syslog servers	187
	Disabling Syslog servers	189
	Deleting Syslog servers	189
	Displaying the status of the Syslog server	
	Syslog sink default settings	
	Syslog message format	190
	Commands used to copy a syslog file	190
	Configuring a log file	190
	Disabling logging system messages to a log file	191
	Deleting current log file and opening an empty log file	191
	Log file message format	192
	set logging file retention	192
	show logging file retention	193
	Configuring a session log	193
	Example discontinuation of the display of system messages	194
	Example display of session logging configuration	194
	Session logging message format	
	Logging filter configuration	195
	Commands used to set the logging filters	195
	Severity levels	
	Default sink severity levels	
	Application filtering	
	Syslog server example	
	Log file example	198
	Session log example	
	Accessing diagnostic logs	
	Summary of logging configuration CLI commands	199
Ch	apter 9: VoIP QoS	
	RTP and RTCP configuration	201

	Header compression configuration	201
	Header compression configuration options	202
	Header compression support by interface	202
	Configuring IPHC	
	Summary of IPHC header compression CLI commands	204
	Configuring VJ header compression	
	Commands used to display and clear header compression statistics	206
	Commands used to configure QoS parameters	207
	Commands used to configure RTCP QoS parameters	
	Commands used to configure RSVP parameters	207
	Summary of QoS, RSVP, and RTCP configuration CLI commands	207
	Weighted Fair VoIP Queuing	
	Summary of WFVQ configuration CLI commands	208
	Priority queuing	209
	Summary of priority queueing configuration CLI commands	209
Cł	napter 10: Modems and Branch Gateway	211
	USB-modem interface configuration	
	Example of IP address to USB port assignment	211
	The ppp authentication command parameters	211
	Summary of CLI commands for configuring the USB port for modem use	212
	Console port and modem configuration	213
	Summary of CLI commands for configuring the Console port for modem use	213
Cł	napter 11: WAN interfaces	215
	Serial interface overview	215
	Layer 1 T1 port with two channel groups	215
	E1/T1 port channel group	
	USP port using PPP protocol	
	USP port using frame relay protocol	217
	Frame Relay multipoint topology support	217
	Configuring the initial WAN	217
	The Avaya MM340 E1/T1 WAN media module	218
	Configuring Avaya MM340 E1/T1 WAN media module	218
	E1/T1 default settings	220
	Commands used to reset and display controller counters	221
	Commands used to activate loopback mode on an E1/T1 line	221
	Summary of E1/T1 ports configuration commands	
	Avaya MM342 USP WAN media module	222
	Configuring Avaya MM342 USP WAN media module	222
	USP default settings	224
	Summary of USP port configuration commands	
	PPP configuration	
	PPPoE overview	
	Frame relay	230

	Configuring frame relay	230
	Commands used to reset and display frame relay interface counters	232
	Summary of frame relay commands	232
	WAN configuration and testing connectivity	233
	Commands used for WAN configuration and testing connectivity	233
	Summary of WAN configuration verification commands	234
	Backup interfaces	234
	Modem dial backup	236
	Modem dial backup logging messages	248
	Dialer Messages	
	Console messages	249
	USB Modem Messages	250
	PPP Messages	251
	Summary of modem dial backup commands	
	ICMP keepalive	
	Dynamic CAC	
	Object tracking	
	Frame relay encapsulation features	
	Priority DLCI	
Ch	apter 12: Emergency Transfer Relay	
•	ETR state configuration	
	Activating ETR manually	
	Deactiving ETR manually	
	Restoring ETR to automatic activation	
	Summary of ETR commands	
Ch	apter 13: SNMP	
CII	Agent and manager communication	
	SNMP versions	
	SNMPv1	
	SNMPv2c	
	SNMPv3	
	Users	
	Groups	
	Views	
	SNMP trap configuration	
	snmp-server host command parameters	
	Notification types	
	Summary of SNMP trap configuration commands	
	Summary of SNMP access configuration commands	
	Dynamic trap manager	
	Dynamic trap manager parametersSummary of dynamic trap manager configuration commands	
	SNMP configuration examples	
	SINIVIE CONTIQUIATION EXAMINATES	05

Chapter 14: Media encryption using AES-256	291
Screen for administering Media encryption using AES-256	291
Administering Media encryption using AES-256	
Detailed description	
Chapter 15: Encrypted SRTCP	293
Detailed description	
Encrypted SRTCP	293
Screen for administering Encrypted SRTCP	293
Administering Encrypted SRTCP	294
Interactions for Encrypted SRTCP	294
Chapter 16: Contact closure	295
Configuring contact closure hardware	295
Software contact closure	296
Contact closure modes	296
Configuring contact closure software	296
Showing contact closure status	297
Summary of contact closure commands	297
Chapter 17: Announcement files	
Uploading announcement files to a remote SCP server	298
Downloading announcement files from a remote SCP server	
Uploading announcement files to a remote FTP server	299
Downloading announcement files from an FTP server	299
Uploading an announcement file to a USB mass storage device	300
Downloading an announcement file from a USB mass storage device	300
Uploading announcement files to a remote HTTP or HTTPS server	300
Downloading announcement files from an HTTP or HTTPS server	301
Uploading announcement files to a remote SCP server via Avaya SBCE tunnel	
Downloading announcement files from a remote SCP server via Avaya SBCE tunnel	
Erasing an announcement file from the directory	
Renaming an announcement file in the directory	
Displaying the announcement files stored in the directory	
Displaying the status of a download process	
Displaying the status of an upload process	
Summary of announcement files commands	
Dynamic time slots allocation	
Summary of dynamic time slots allocation commands	305
Chapter 18: Advanced switching	306
VLAN configuration	306
VLAN Tagging	
Multi VLAN binding	
Gateway VLAN table	
Ingress VLAN Security	308
ICC-VLAN	308

	Configuring ICC-VLAN	308
	VLAN configuration examples	308
	Summary of VLAN commands	310
	Port redundancy	311
	Secondary port activation	311
	Switchback	312
	Port redundancy configuration commands	312
	Port redundancy configuration examples	312
	Summary of port redundancy commands	
	Port mirroring	313
	Port mirroring configuration examples	314
	Summary of port mirroring commands	314
	Spanning tree	314
	Spanning tree protocol	314
	Spanning tree per port	
	Rapid Spanning Tree Protocol (RSTP)	315
	Spanning tree configuration examples	317
	Summary of spanning tree commands	318
	Port classification	319
	Port classification configuration examples	319
	Summary of port classification commands	319
Ch	apter 19: Monitoring applications	320
	RMON	320
	RMON configuration examples	320
	Summary of RMON commands	321
	RTP statistics	322
	Configuring the RTP statistics application	323
	RTP statistics output	330
	RTP statistics examples	343
	Summary of RTP statistics commands	352
	Packet sniffing	353
	What can be captured	354
	Roadmap for configuring packet sniffing	354
	Configuring capture lists	
	Analyzing captured packets	
	About simulating packets	368
	Summary of packet sniffing commands	368
	Interface status reports	370
	Reporting of interface status	
	Summary of interface status commands	371
	Echo cancellation	371
	Summary of echo cancellation commands	372
	Integrated analog testing – Test and Heal	373

Hardware support for integrated analog testing	373
Types of tests	
Types of test lines	374
Setting up a test profile	374
Displaying and clearing profiles	375
Launching and cancelling a test	376
Displaying test results	376
Healing trunks	376
Displaying corrections	377
Summary of integrated analog testing commands	377
Service Level Agreement Monitor Agent	378
Chapter 20: Router	380
Enabling and disabling the router	
Interface configuration	
Router interface concepts	
Configuring an IP interface	
Interface configuration examples	
Summary of basic interface configuration commands	
Unnumbered IP interfaces	
Unnumbered IP on an interface configuration	
Configuring IP on an interface configuration	
Unnumbered IP examples	
Summary of unnumbered IP interface configuration commands	
Routing sources	
Routing table configuration	
Next hops	
Static route types	
Configuring multiple next hops	
Deleting a route and its next hops	
Via-interface static route	
Permanent static route	389
Discard routes	
Summary of routing table commands	
GRE tunneling	391
Packet routing to a GRE tunnel	392
Prevention of nested tunneling in GRE tunnels	
Optional GRE tunnel features	
Setting up a GRE tunnel	
GRE tunnel application example	
Summary of GRE tunneling commands	
DHCP and BOOTP relay	
DHCP	
ROOTD	400

DHCP/BOOTP relay	400
Summary of DHCP and BOOTP relay commands	401
DHCP server	402
Typical DHCP server application	403
Configuring the DHCP server	403
Deleting an IP address binding	406
DHCP pool configuration examples	406
Commands for displaying DHCP server information	407
Summary of DHCP Server commands	408
Broadcast relay	410
Directed broadcast forwarding	410
NetBIOS rebroadcast	410
Summary of broadcast relay commands	410
ARP table	411
Overview of ARP	411
Static and dynamic table entries	411
Adding static ARP table entries	412
Removing static and dynamic entries	412
Changing an entry in the ARP table	413
Summary of ARP table commands	413
Proxy ARP	413
Summary of Proxy ARP commands	413
ICMP errors	414
Summary of ICMP errors commands	414
RIP	414
RIPv1	415
RIPv2	415
RIPv1 vs. RIPv2	415
Prevention of routing loops in RIP	415
Commands used to prevent routing loops in RIP	415
RIP distribution access lists	416
Configuring a distribution access list example	416
RIP limitations	
Summary of RIP commands	417
OSPF	419
OSPF dynamic Cost	419
OSPF limitations	
Summary of OSPF commands	
Route redistribution	
Export default metric	
Summary of route redistribution commands	
VRRP	
VRRP configuration example	424

Summary of VRRP commands	425
Fragmentation	426
Summary of fragmentation commands	426
Chapter 21: IPSec VPN	428
Overview of IPSec VPN configuration	428
IPSec VPN configuration model	428
Overview of IPSec VPN components	429
IPSec VPN components	429
Summary of configuration commands	430
Site-to-site IPSec VPN	432
IPSec VPN maintenance	447
Typical installations for IPSec VPN	449
Typical failover applications	471
Introduction to the failover mechanism	471
VPN keepalives	472
Backup peer mechanism	472
Failover using GRE	472
Redundancy and load sharing modes	
Hub and spoke with hub redundancy/load sharing using GRE	473
Configuring VPN hub redundancy and load sharing topologies using GRE	474
VPN hub redundancy and load sharing topologies	474
VPN hub redundancy and load sharing topologies example	475
Failover using DNS	478
VPN DNS topology	478
Configuring the VPN DNS topology	478
VPN DNS topology example	480
Failover using a peer-group	483
Failover VPN topology using a peer-group	484
Configuring the failover VPN topology using a peer-group	484
Failover VPN topology using a peer-group example	486
Checklist for configuring site-to-site IPSec VPN	
Summary of VPN commands	492
Chapter 22: Policy lists	497
Types of policy lists	497
Access control lists	497
QoS lists	498
QoS list parts	498
Allowed values on QoS fields	
Use of policy-based routing	499
Policy list management	499
Policy list configuration	500
Creating or editing a policy list	500
Creating a list based on an existing list	500

Defining list identification attributes	501
Policy list attributes	501
Default actions	501
Deleting a policy list	502
Policy list attachments	502
Packets entering the interface	502
Packets exiting the interface	502
Policy lists to packets	502
Policy list attachment configuration	503
Attaching policy lists and access control lists	
Attaching policy lists and QoS lists	503
Removing a list	504
Device-wide policy lists	
Defining global rules	505
Policy rule configuration	505
Editing and creating rules	506
Policy lists rule criteria	506
Composite operations	510
Pre-configured composite operations for access control lists	510
Pre-configured composite operations for QoS lists	511
Configuring composite operations	512
Adding composite operation to an IP rule	512
Composite operation example	512
DSCP table	513
Changing an entry in the DSCP table	513
Policy list displays and tests	514
Policy list commands in context	514
Simulating packets	515
Simulated packet properties	516
Summary of access control list commands	516
Summary of QoS list commands	518
Chapter 23: Policy-based routing	522
Policy-based routing	
Chapter 24: Synchronization	524
Defining a stratum clock source	
Setting the synchronization source	
Disassociating a clock source	
Enabling and disabling automatic failover and failback	
Synchronization status	
Displaying synchronization status	
Summary of synchronization commands	
Chapter 25: TLS / Certificate Management	
TI Q	528

	TLS certificate stores	528
	Certificate validation	530
	Mutual authentication	530
Ch	apter 26: Federal Information Processing Standards (FIPS)	531
	Federal Information Processing Standards	
	FIPS Security Level of the Cryptographic Module	
	Determining FIPS Certified Firmware is installed	
	FIPS Approved Mode of Operation	
	Prerequisites for entering FIPS Approved Mode	
	Determining FIPS Approved Mode is enabled	
	Determining Configuration is FIPS Compliant	
	Backup and restore of Gateway configuration	
	Before Enabling or Disabling FIPS Approved Mode	
	Enabling FIPS Approved Mode	
	Maintaining FIPS Approved Mode	
	Disabling FIPS Approved Mode	
	Administration procedures	
	FIPS-related CLI commands	
	Non-compliant CLI Commands in FIPS Approved Mode	
	Warnings for unencrypted communication in FIPS Approved Mode	
	Enabling FIPS Approved Mode	
	Disabling FIPS Approved Mode	542
	FIPS Error States and LED Status Indicators	546
	Power-up Testing	546
	Error States	
	Zeroization Status during Error State 1	547
Ch	apter 27: Resources	549
	Branch Gateway documentation	
	Finding documents on the Avaya Support website	
	Accessing the port matrix document	
	Avaya Documentation Center navigation	
	Training	
	Viewing Avaya Mentor videos	
	Support	
Αp	pendix A: Traps and MIBs	
	Branch Gateway traps	
	Branch Gateway MIB files	
	MIB objects in the Load.MIB file	
	MIB objects in the RFC1315-MIB.my file	
	MIB objects in the Q-BRIDGE-MIB.my file	
	MIB objects in the ENTITY-MIB.my file	
	MIB objects in the IP-FORWARD-MIB.my file	
	·	570

MIB objects in the UTILIZATION-MANAGEMENT-MIB.my file file	5/1
MIB objects in the ENTITY-SENSOR-MIB.my file	572
MIB objects in the RSTP-MIB.my file	572
MIB objects in the APPLIC-MIB.my file	572
MIB objects in the DS1-MIB.my file	573
MIB objects in the PPP-IP-NCP-MIB.my file	574
MIB objects in the RFC1213-MIB.my file	575
MIB objects in the AVAYA-ENTITY-MIB.my file	578
MIB objects in the Rnd-MIB.my file	578
MIB objects in the XSWITCH-MIB.my file	578
MIB objects in the CROUTE-MIB.my file	579
MIB objects in the RS-232-MIB.my file	582
MIB objects in the RIPv2-MIB.my file	583
MIB objects in the IF-MIB.my file	583
MIB objects in the DS0BUNDLE-MIB.my file	584
MIB objects in the RFC1406-MIB.my file	
MIB objects in the DS0-MIB.my file	
MIB objects in the POLICY-MIB.my file	
MIB objects in the BRIDGE-MIB.my file	591
MIB objects in the CONFIG-MIB.my file	
MIB objects in the G700-MG-MIB.my file	
MIB objects in the FRAME-RELAY-DTE-MIB.my file	599
MIB objects in the IP-MIB.my file	
MIB objects in the Load12-MIB.my file	
MIB objects in the PPP-LCP-MIB.my file	
MIB objects in the WAN-MIB.my file	
MIB objects in the SNMPv2-MIB.my file	
MIB objects in the OSPF-MIB.my file	
MIB objects in the TUNNEL-MIB.my file	607
Appendix B: ASG authentication	609
ASG authentication CLI commands	609
Replacing the ASG authentication file.	609

# **Chapter 1: Introduction**

# **Purpose**

This document describes how to set up, configure, and maintain Branch Gateway. It is intended for system administrators and support personnel.

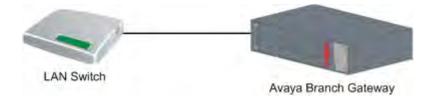
# **Change history**

Issue	Date	Summary of changes	
2	July 2022	Updated the following sections:	
		Branch Gateway Controller configuration on page 62	
		Branch Gateway MGC settings on page 65	
		Results from the set mgc list command on page 66	
		Showing the current MGC list on page 66	
1	December 2021	Initial 10.1 release.	

# **Chapter 2: Configurations**

# **Basic configuration**

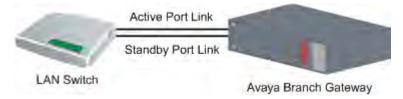
You can deploy the Branch Gateway basic configuration in a LAN. The basic configuration does not support redundancy. You can connect Branch Gateway to an external LAN switch using one of the two Ethernet LAN ports located on the front panel of the gateway.



# Port redundancy configuration

You can deploy the Branch Gateway port redundancy configuration in a LAN. You can connect Branch Gateway to an external LAN switch using both the Ethernet LAN ports located on the front panel of Branch Gateway.

Configure one of the ports on the Ethernet LAN as the active primary link and the other as the standby, disabled link. When the gateway determines a primary link failure, the gateway automatically fails over to the secondary link. Both LAN ports of the peer LAN switch ports must be enabled for the gateway to fail over to the secondary link.



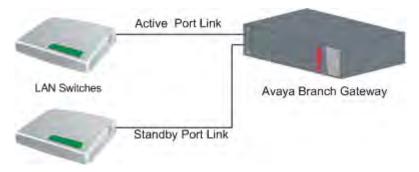
#### Related links

Port redundancy on page 311

### Port and switch redundancy configuration

You can deploy Branch Gateway in a LAN using the port and switch redundancy configuration. You can connect each LAN port on the front panel of Branch Gateway to two LAN switches.

Configure one of the ports on the Ethernet LAN as the active primary link and the other as the standby, disabled link. When the gateway determines a primary link failure or malfunction of the switch attached to it, the gateway automatically fails over to the secondary link to the backup switch. Both LAN ports of the peer LAN switch ports must be enabled for the gateway to fail over to the secondary link.



### Related links

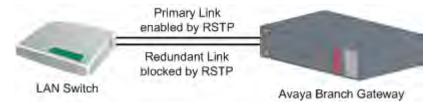
Port redundancy on page 311

# **RSTP** configuration

You can deploy Branch Gateway in a LAN using RSTP to provide redundancy. You can connect each Ethernet LAN port on the front panel of the Branch Gateway to an external LAN switch.

A spanning tree protocol blocks one of the links from Branch Gateway to the external LAN switch. The spanning tree protocol must be configured on the external LAN switch and the Ethernet LAN ports on Branch Gateway. When the gateway determines a primary link failure, the gateway automatically fails over to the secondary link. Both LAN ports of the peer LAN switch ports must be enabled for the gateway to fail over to the secondary link.

Compared to port redundancy method, Fast RSTP is better because Fast RSTP controls the state of the link between the gateway and the LAN switch based on the best LAN topology. However, Fast RSTP can have a time delay during RSTP convergence.



### Related links

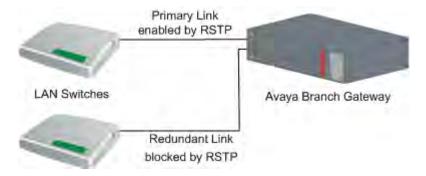
Spanning tree on page 314

# RSTP and switch redundancy configuration

You can deploy Branch Gateway in a LAN using RSTP and switch redundancy configuration. You can connect each Ethernet LAN port on the front panel of the Branch Gateway to an external LAN switch.

Spanning tree protocol blocks one of the links from Branch Gateway to the external LAN switch. Spanning tree protocol must be configured on both the external LAN switch and the Ethernet LAN ports on the Branch Gateway. When the gateway determines a primary link failure or malfunction of the switch attached to it, the gateway automatically fails over to the secondary link to the backup switch. Both LAN ports of the peer LAN switch ports must be enabled for the gateway to fail over to the secondary link.

Compared to port redundancy method, Fast RSTP is better because Fast RSTP controls the state of the link between the gateway and the LAN switch based on the best LAN topology. However, Fast RSTP can have a time delay during RSTP convergence.



### Related links

Spanning tree on page 314

# **Chapter 3: Configuration overview**

A new Branch Gateway has default configuration settings. Before using Branch Gateway, you must configure certain items according to the system specifications. Configure other items depending on network specifications.

A new Branch Gateway has three physical interfaces for management: Console interface, Services interface, and USB-modem interface.

Configure Branch Gateway based on different access methods.

### **Defining the Console interface**

### About this task

Configuring an IP address to the Console interface is the first task of configuring a new Branch Gateway instance. Configuring a subnet mask is optional.

### **Procedure**

- 1. Type interface console to enter the Console context.
- 2. Use the ip address command to define an IP address for the Console interface.



### Note:

For more detailed installation instructions, including information on obtaining IP addresses, refer to Installing and Upgrading Avaya G450 Media Gateway.

### **Example**

The following example shows the configuration of 10.3.3.1 as the IP address of the Console interface:

```
Gxxx-001(super) # interface console
Gxxx-001(super-if:Console)# ip address 10.3.3.1
```

### **Defining the USB-modem interface**

### **About this task**

Configure an IP address to the USB-modem interface to connect to Branch Gateway using a USB modem. Do not configure a subnet mask.

### **Procedure**

- 1. Type interface usb-modem to enter the USB-modem context.
- 2. Use the ip address command to define a new IP address for the USB-modem interface.

### **Example**

The following example shows the configuration of 10.3.3.2 as the IP address of the USB-modem interface:

```
Gxxx-001(super) # interface usb-modem
Gxxx-001(super-if:USB-modem) # ip address 10.3.3.2
Done!
```

The default IP address of the USB port is 10.3.248.253 255.255.255.252.

### Other interfaces

Your system specifications might require that you define other interfaces.

The Primary Management IP address (PMI) is the IP address assigned to Branch Gateway. Branch Gateway uses PMI for self-identification when communicating with other devices, particularly the Media Gateway Controller (MGC). Management data intended for the Branch Gateway is routed to the interface defined as PMI. You can use any interface as the PMI. The PMI address can be IPv4 or IPv6.

The MGC is a call controller server that controls telephone services on the Branch Gateway. The MGC can be internal or external and either IPv4 or IPv6.

#### Related links

Defining an interface on page 59

### **Define other interfaces**

You can perform most Branch Gateway configuration tasks using the Branch Gateway CLI. Avaya also provides several GUI applications using which you can perform the basic configuration tasks described in this section. To define other interfaces, you must first define a PMI and then register the Branch Gateway with an MGC.

After you have performed these steps, Branch Gateway is ready for use. You might have to perform other configuration tasks, but these tasks depend on the specifications of Branch Gateway and the network.

### Related links

Primary Management Interface (PMI) configuration on page 60 Branch Gateway Controller configuration on page 62

# **Configuration using CLI**

You can use the Branch Gateway CLI to manage Branch Gateway. As the CLI is a command prompt interface, you can type commands and view responses.

This guide contains information and examples about how to use CLI commands to configure the Branch Gateway.

For more information about the Branch Gateway CLI and a complete description of each CLI command, see Avaya Branch Gateway G450 CLI Reference.

### Related links

CLI access on page 30

# Configuration changes and backup

When you make changes to the configuration of Branch Gateway, you must save the changes to make them permanent. Branch Gateway has two sets of configuration information:

- Running configuration
- Startup configuration

Branch Gateway operates according to the running configuration. When Branch Gateway is reset, Branch Gateway erases the running configuration and loads the startup configuration as the new running configuration. When you change the configuration of Branch Gateway, your changes affect only the running configuration. If you do not save the changes and if Branch Gateway is reset, the changes are lost.

You can restore a backup copy of the configuration from the FTP or TFTP server or the USB flash drive. When you restore the backup copy of the configuration, the backup copy becomes the new running configuration on the Branch Gateway.



### Note:

In the FIPS mode, you can only restore from a backup that you perform on the same gateway. You cannot restore from a backup that you perform on a gateway that is in the non-FIPS mode.

### Saving configuration changes and backing them up

### **Procedure**

- 1. To save changes to the configuration of the Branch Gateway, enter copy running-config startup-config or copyedge running-config startup-config A copy of the running configuration becomes the new startup configuration.
- 2. Back up either the running configuration or the startup configuration to a FTP, TFTP, SCP, or an HTTPS server on your network, or to a USB flash drive.

### Firmware version control

Firmware is the software that runs Branch Gateway. Branch Gateway has two firmware banks:

- Bank A
- Bank B

Each firmware bank contains different versions of Branch Gateway firmware. The purpose of providing firmware banks is to provide firmware redundancy. You can save an old version of the firmware for future use, for example, when uploading new versions.

### Related links

Software and firmware upgrades on page 78

### Using an older version of firmware

### About this task

Use this procedure if you must use an older firmware version.

### **Procedure**

- 1. Enter set boot bank bank-X
- 2. Reset Branch Gateway to use the older version.

# **Chapter 4: Branch Gateway access**

You can gain access to Branch Gateway using CLI and Avaya Aura<sup>®</sup> Communication Manager (CM). You can manage login permissions by either configuring username and password or configuring Branch Gateway to use RADIUS authentication.

Branch Gateway supports recovery of user passwords, Telnet connections, and SYN cookies to prevent SYN attacks.

### **CLI access**

You can use CLI, a command prompt interface, to configure Branch Gateway and media modules.

You can use the following methods to access CLI:

- A console device connected to the Console port
- SSH to establish a secure remote session with the network, Services port, or dial up PPP network connection. SSH is enabled by default.
- Telnet connection with the network, Services port, or dial up PPP network connection. Telnet is disabled by default.

If you have a service contract with Avaya Services, Avaya Support engineers can connect remotely to service Branch Gateway with Telnet and SSH sessions. For higher security, you can configure Branch Gateway to authenticate remote service logins using the Enhanced Access Security Gateway (EASG) authentication instead of the password authentication.

### Logging to CLI

### **Procedure**

- 1. Log in to CLI with a username and password provided by your system administrator.
- 2. Use RADIUS authentication if your network has a RADIUS server.

#### Related links

Login permissions on page 35

### CLI contexts

CLI has various contexts. You can enter sets of related commands in these contexts. Contexts are nested in a hierarchy, with each context accessible from a parent context. The top level of the

CLI tree is called the general context. Each command has a related context. You can only use a command in the proper context.

### **Entering the Loopback interface**

### **Procedure**

To enter the Loopback interface context from the general context, enter the interface loopback 1 command.



### Note:

When you are in the Loopback interface context, you can enter the Loopback interface commands. You can use the tree command to view the list of commands in each context

### Using CLI help

### About this task

The help command or ? command displays the list of all CLI commands that you can use within the current context. The list includes a short explanation of each command.

### **Procedure**

To display the list of commands for the context you are in, type help or ?

### Specifically:

 You can view a list of all commands in the current context, which is similar to the command that you entered. You can accomplish the aforementioned by prefixing or postfixing the name of the command with help or ?.

For example, to view the list of IP commands available in the general context, enter help ip, ip help, ? ip, Or ip ?.

• To view the syntax of the command and parameters along with an example of the command, you can prefix or postfix the name of the command with help or ?.

You must be in the context of the command to use the help command to display information about the respective command.

• The TAB key can be used to complete the CLI commands, and if a parameter has multiple choices pressing the TAB key twice will list all the available choices.

### **Example**

Example: The user enters the vlan 1 interface context and uses the help command to view information about the bandwidth command.

```
Gxxx-001(super) # interface vlan 1
Gxxx-001(super-if:VLAN 1) # bandwidth ?
Bandwidth commands:
Syntax: bandwidth <kilobytes size>
                 <kilobytes size> : integer (1-10000000)
Example: bandwidth 1000
```

### CLI access using the local network

You can access CLI from a computer on the same local network as Branch Gateway by using SSH or, if Telnet is active, any standard Telnet program. You can use the IP address of any Branch Gateway interface as the host address.

### Accessing CLI using a computer

To access CLI from a computer, connect the computer either to the Console port or to the Services port.

Alternatively, connect the PC device to the Console port on the front panel of the Branch Gateway. Use only an approved Avaya serial cable. For more information about approved Avaya serial cables, see Overview for the Avaya Branch Gateway G450.

### Accessing Branch Gateway through the Services port

### **Procedure**

- 1. Use a computer with the SSH client software.
- 2. Use an Ethernet cable to connect the computer to the Services port located on the front panel of Branch Gateway.
- 3. Set the TCP/IP properties of the computer as follows:
  - a. IP address = 192.11.13.5
  - b. Subnet mask = 255.255.255.252
  - c. Disable DNS service
  - d. Disable WINS Resolution

Make a record of any IP addresses, DNS servers, or WINS entries that you change when you configure your laptop. Unless you use the NetSwitcher program or a similar program, you must restore these entries to connect to other networks.

- 4. Configure the Internet browser settings of the computer to disable the proxy server.
- 5. Set the IP address of SSH to 192.11.13.6.



### Note:

By default, SSH is enabled and Telnet is disabled. If you wish to use Telnet, you must enable it.

### **CLI access using modems**

You can use a dialup PPP network connection to access CLI from a remote location through any standard SSH or Telnet program. You can use a USB modem connected to the USB port on the front panel of the Branch Gateway or a serial modem connected to the Console port on the front panel of the Branch Gateway. You must only use an approved Avaya serial cable. For more information about approved Avaya serial cables, see Overview for the Avaya Branch Gateway G450.

### Accessing CLI using a USB modem

### **Procedure**

- 1. Connect a modem to the USB port on the front panel of Branch Gateway.
  - Use a USB cable to connect the modem. Branch Gateway supports the Multitech MultiModem USB MT5634ZBA-USB-V92 and the USRobotics USB modem model 5637.
- 2. Ensure that the USB port is properly configured to be used with a modem.
- 3. From the remote computer, create a dialup network connection to Branch Gateway.
  - Use the TCP/IP and PPP protocols to create the connection. Configure the connection according to the configuration of the COM port of the remote computer. By default, Branch Gateway uses the RAS authentication. If your network has a RADIUS server, you can use the RADIUS authentication for the PPP connection.
- 4. Open any standard SSH/Telnet program on the remote computer.
  - Note:

Telnet is disabled on Branch Gateway by default. To enable Telnet, use the ip telnet command.

- 5. Open an SSH/Telnet session that is mapped to the IP address of the USB port on Branch Gateway.
  - To set the IP address of the USB port, that is, the USB-modem interface, use the ip address command.
- 6. Configure the serial connection on the remote computer to match the configuration of the USB port on Branch Gateway.

### Related links

USB-modem interface configuration on page 211

Login permissions on page 35

Summary of CLI commands for configuring the USB port for modem use on page 212

### **USB** port settings

Port setting	Value
Baud	-
Data bits	8
Parity	none
Stop bits	1
flow control	hardware

### **Branch Gateway serial modems**

The Branch Gateway supports the following serial modems:

- Multitech MultiModem ZBA, MT5634ZBA-V92.
- Multitech BRI-NT1 ISDN Modem w/ POTS, MTA128NT, for use in US and Canada.
- Multitech ISDN Modem w/ POTS, MTA128STBRI, for use in Europe and the rest of the world. The ISDN modems require DB-25 termination as well as the RJ-45 cable.

### Accessing the CLI using a serial modem

### **Procedure**

- Connect a modem to the Console port on the front panel of the Branch Gateway.
   Use an RJ-45 serial cable to connect the modem.
- 2. Make sure the Console port is properly configured for modem use.
- 3. From the remote computer, create a dialup network connection to the Branch Gateway.

  Use the TCP/IP and PPP protocols to create the connection. Configure the connection according to the configuration of the COM port of the remote computer. By default, the Branch Gateway uses PAP authentication. If your network has a RADIUS server, you can
- 4. Open any standard telnet program on the remote computer.

use RADIUS authentication for the PPP connection.

- 5. Open a telnet session to the IP address of the Console port on the Branch Gateway.
- 6. Configure the serial connection on the remote computer to match the configuration of the Console port on the Branch Gateway.

The Console settings are the same as the USB port settings except for the baud parameter that uses the highest possible setting.

### CM access

You can use the CM software to control telephone services provided by Branch Gateway. Run the CM software on a server. The network might have several servers that can control Branch Gateway. Access CM on any server that is a Media Gateway Controller (MGC) for Branch Gateway.

You can access CM with any of the following tools:

**SSH to port 5023 on the MGC:** For more information, see *Administrator Guide for Avaya Aura*® *Communication Manager.* 

### Related links

Branch Gateway Controller configuration on page 62

### **Security overview**

Branch Gateway includes a security mechanism through which the system administrator defines users and assigns each user a username, password, and privilege level. The privilege level of the user determines which commands the user can perform.

Branch Gateway also supports secure data transfer through SSH and SCP.

You can configure Branch Gateway to work with an external RADIUS server to provide user authentication. When you enable RADIUS authentication on Branch Gateway, the RADIUS server operates with Branch Gateway security mechanism. When the user enters a username, Branch Gateway first searches its own database for the username. If Branch Gateway does not find the username in its own database, it establishes a connection with the RADIUS server. The RADIUS server, then, provides the necessary authentication services.

### Login permissions

You can manage login permissions to enable different privilege levels for each user and to regulate the security features.

### **User account management**

You must provide a user name and password when you perform any of the following actions:

- · Access CLI.
- · Access CLI using a modem with dialup PPP.

You can configure various password parameters to enhance the system security. Parameters control password length, content, lockout and expiry policies.

When you access CLI, you must enter a user name. The user name that you enter sets your privilege level. The commands that are available to you during the session depend on your privilege level.

If your network has a RADIUS server, you can use the RADIUS authentication instead of a user name and password. A RADIUS server provides centralized authentication service for many devices on a network.

### Related links

CLI access on page 30

CLI access using modems on page 32

### Privilege level

When you access CLI, you must enter a user name. The user name that you enter sets your privilege level. The commands that are available to you during the session depend on your privilege level. If you use RADIUS authentication, the RADIUS server sets your privilege level.

The Gateway provides the following three privilege levels:

Read-only: Administering Avaya G430 Branch Gateway

The default user name falls under the Admin privilege level. For security reasons, the administrator usually changes the password of the default user name. For more information about privilege levels, see Avaya Branch Gateway G450 CLI Reference.

### Creating a user name, password, and privilege level

### About this task

When you create a new user, you must define the password and privilege level for the user. Enter a password that conforms with the password policies.



### Note:

You need an Admin privilege level to use the username and no username commands.

### **Procedure**

At the command prompt, type:

username <the username> access-type <access type>

### Example

g450ab2-025(super) # username john access-type read-write User account added.

### Changing user privileges

### About this task

To change the privilege level for a user name, remove the user name and add it again.

### **Procedure**

1. At the command prompt, type:

no username <the username>

At the command prompt, type username <the username > access-type <access type> Example:

Gxxx-001(super)# username john access-type read-write

### Commands to regulate password length and content

Use the following commands to regulate the password length and the characters:

- · login authentication min-password-length
- login authentication min-password-digit-chars
- login authentication min-password-lower-chars
- · login authentication min-password-upper-chars
- · login authentication min-password-special-chars
- login authentication max-password-class-repeated-chars

login authentication max-password-repeated-chars

For more information about these commands, see Avaya CLI Reference.

## Commands used to manage password lockout and disabling

When you lockout a user account, it remains locked out only for a specific time period. If you disable an account, an administrator must intervene to reenable the account. An administrator must run the username command and reconfigure the account using the same user name and password. Use the following commands to manage password lockout and disabling:

- · login authentication lockout
- login authentication inactivity-period

For information about parameters and default settings, see Avaya G450 CLI Reference.

## Password expiry management

You can force all passwords to expire within a certain time period after they are created. Accounts with expired passwords are locked and an administrator must reset the account using the username command. However, a user can change the password before expires using the password command.

## Changing a password

#### About this task

If a password expiration policy is being implemented, it is recommended to change your password before it expires. When you are 10 days or less than 10 days from the password expiration date, the system displays a warning message during log on. The message specifies that your password will expire in n days.

## **Procedure**

- 1. Use the password command to change your password.
  - Enter and confirm the new password.
- 2. Enter the copy running-config startup-config command so that the new password takes effect.

## Result

The new password you enter must match the password policies.

# Commands used to display user account information

Use the following commands to display the account information of the user:

- show username
- show login authentication

For a full description of the commands and their output fields, see *Avaya Branch Gateway G450 CLI Reference*.

## **User accounts CLI commands**

The following table lists the commands to manage user accounts. For more information about these commands, see *Avaya Branch Gateway G450 CLI Reference*.

Command	Description
login authentication change- password-on-first-login	The command forces a new user to change the password on first login.
login authentication inactivity-period	Disable a local user account after an inactivity period of 2 to 365 days.
login authentication lockout	Lock out or disable a local user account after successive failed login attempts.
	You can configure the lock out period between 30 to 3600 seconds. Both the lock out and the disabling policies come into effect after 1 to 10 successive failed login attempts.
login authentication min- password-digit-chars	Set the minimum number of digits and characters that a password must contain.
login authentication min-	Set the minimum password length.
password-length	The minimum password length must not be less than the sum of the minimum number of lowercase characters, uppercase characters, digit characters, and special characters.
login authentication min- password-lower-chars	Set the minimum number of lowercase characters that a password must contain.
login authentication min- password-special-chars	Set the minimum number of special characters that a password must contain.
	Special characters are any printable nonalphanumeric characters except for white characters, either blank or tab and double quotation marks ("), which is the ASCII character 34.  The default is zero special characters.
login authentication min- password-upper-chars	Set the minimum number of uppercase characters that a password must contain.
login authentication password-expire	Cause all local user passwords to expire after a specified number of days.
login authentication password- no-change-interval	Set the number of hours before a password can be changed again.
login authentication passwords-dont-reuse	Set the number of previous passwords that cannot be reused.
login authentication max- password-repeated-chars	Set the maximum number of consecutive repeated characters in a password (default not checked).
login authentication max- password-class-repeated-chars	Set the maximum number of consecutive characters of the same class (uppercase, lowercase, digits, symbols) in a password (default not checked).
password	Change the password of a user account.

Table continues...

Command	Description	
show login authentication	View the login authentication settings and information.	
	This includes information about the configured lockout period, inactivity period, expiration period, password length, and characters that must be included in the password.	
show username	Display information about the local user accounts.	
username	Add or remove a local user account.	

# Login authentication

## Examples for displaying Login authentication information Procedure

1. Display login authentication settings and information, using **show login** authentication.

## For example:

```
(super) # show login authentication
Services logins: On
Local craft: On
Lockout time: 180 seconds
Lockout attempt threshold: 3
Authentication response time: 120 seconds
CLI logout timeout: Off
Password expiration period: Off
Password inactivity period: Off
Previous passwords not reusable: 10 (default)
Min password change interval: 24 hours (default)
Password change on first login: Off (default)
Min password length: 14 (default)
Min upper case chars: 0 (default)
Min lower case chars: 1 (default)
Min special symbols chars: 0 (default)
Min digit chars: 1 (default)
Max repeated chars: 2 (default)
Max class repeated chars: 4 (default)
```

2. Display ASG authentication file information, using show auth-file info.



ASG authentication file is no longer supported from Release 7.1.2

## For example:

```
(super)# show auth-file info
Authentication File (AF) information:
AF-ID :7000012345
Date/time : 15:02:27 23-AUG-2015
Major release : 6.x
```

Display all locally defined user accounts, including services accounts and account type information such as authentication method, using show username.

## For example:

(super) # show username User account	Access level	Account type	Active
root snmpv3 craft inads init rasaccess sroot	admin admin admin tech dev read-only dev	local local Services Services Services Services Services	yes yes yes yes yes yes

4. View EASG status using EASGStatus

## For example:

```
super) # EASGStatus
EASG is Enabled.
```

## **Examples of configuring Login authentication**

You can perform the following login configurations:

- Block login access of Avaya Logins using EASGManage disableEASG. This deactivates all Avaya logins. To reactivate, use EASGManage enableEASG.
- You can set the time duration the gateway waits for a user to respond to authentication requests before timing out a connection. Use login authentication response-time time, where time is the time span in seconds following which the gateway aborts the connection if no response is received.

The following example shows a connection being timed out if no response arrives within 180 seconds of an authentication request:

```
(super) # login authentication response-time 180
```

Use no login authentication response-time to restore the response time span to the factory default of 120 seconds. The time value you enter is used for both:

- The response time interval between the user name prompt and the user name entry
- The response time interval between the challenge prompt and the challenge response
- Deactivate password authentication and activate EASG authentication of Avaya Services local connections to the Console port or Services port. To do this, use EASGManage disableEASG. To enable password authentication of Avaya Services local connections to the Console port or Services port, use EASGManage enableEASG. Enabling of password is set by default.
- Set a policy for blocking access to Branch Gateway following successive failed login attempts. To do this, use the login authentication lockout time attempt count command. time is the time duration for which the lockout is enforced and count is the number of failed attempts following which lockout is enforced. Use no login authentication lockout to return the lockout time and lockout attempt threshold to their default values. The default time span for lockout time and lockout attempt is 180 seconds and 3 seconds respectively.

The following example shows blocking access of Avaya Services to the device for 360 seconds following five failed login attempts:

```
(super) # login authentication lockout 360 attempt 5
```

This lockout affects locally defined user accounts and Avaya Logins. Remote users maintained centrally in a Radius server are not subject to the lockout sanction.

## SSH protocol support

Secure Shell (SSH) protocol is a network protocol that enables secure data communication between two computers over an insecure network. SSH accomplishes this by creating a transparent, encrypted channel between the local and remote devices. In addition to the remote shell, SSH provides secure file transfer between the local and remote devices. SSH is used for Secure Copy (SCP) file transfers. Branch Gateway supports three concurrent SSH users.

An SSH session can be established by password authentication. To determine the means by which an SSH session has been established on your Branch Gateway, enter show ip ssh.

Use the ssh-server-configuration CLI command to configure SSH ciphers, MACs, and key exchange algorithms. For details on SSH-server configuration, see Avaya Branch Gateway G450 CLI Reference quide.



## Note:

SSH supports IPv4 and IPv6.

## **Password authentication process**

Before data transfer between the client and Branch Gateway, the client needs to supply a user name and password to Branch Gateway. This process authenticates the user on the client side to Branch Gateway.

## **Enabling SSH on Branch Gateway**

#### Procedure

- 1. Use the hostname command to assign hostname identification.
- 2. To enable SSH to be used, you must also configure the server host key.

Use the crypto key generate rsa key-size 2048 command to generate an SSH host key pair.

3. Enter ip ssh to enable SSH authentication.

SSH is enabled by default.

# Disabling SSH on Branch Gateway

## **Procedure**

1. Use the disconnect ssh command to disconnect an existing SSH session.

- 2. Use the no ip ssh command to disable the SSH server that disconnects all active SSH sessions.
- 3. Use the **show ip ssh** command to display information on SSH configuration in addition to information about any active SSH sessions.

## **Summary of SSH configuration commands**

For more information about SSH configuration commands, see *Avaya Branch Gateway G450 CLI Reference*.

## **SCP** protocol support

In addition to data communication through an SSH session, the SSH protocol is used to support SCP for secure file transfer. When using SCP, Branch Gateway is the client, and an SCP server must be installed on the management station. After users are defined on the SCP server, Branch Gateway acts as an SCP client.

The process of establishing an SCP session is the same process as described in <u>SSH protocol</u> support on page 41, except that the roles of Branch Gateway and the client computer are reversed.

To perform file transfers secured by SCP, Branch Gateway launches a local SSH client using CLI. This establishes a secured channel to the secured file server. The Branch Gateway authenticates itself to the server by providing a user name and password. With a Windows-based SSH server (WinSSHD), the user name provided must be a defined user on the Windows machine with read/write privileges. The files transferred via SCP are saved in the C:\Documents and Settings\username directory.

The network element performs file transfer in unattended mode.

## Clearing the SSH of known host file content

## About this task

Each SCP client maintains a list of server fingerprints. If a key changes, the client's verification of the server's fingerprint fails, thereby preventing client access to the SCP server. If this happens, the following command erases the client server fingerprint list. This enables the client to access the server and begin to recreate its list of fingerprints with the SCP server's new fingerprint.

#### **Procedure**

Enter clear ssh-client known-hosts to clear the client's list of SCP server fingerprints.

## **RADIUS** authentication

If your network has a RADIUS server, you can configure the Branch Gateway to use RADIUS authentication. A RADIUS server provides centralized authentication service for many devices on a network. When you use RADIUS authentication, you do not need to configure usernames and passwords on the Branch Gateway. When you try to access the Branch Gateway, the Branch Gateway searches for your user name and password in its own database first. If it does not find them, it activates RADIUS authentication.

For additional information on RADIUS configuration and authentication, go to the Avaya website at <a href="http://www.avaya.com/support">http://www.avaya.com/support</a>, and search for the document *Avaya RADIUS Configuration Overview*.

## **Using RADIUS authentication**

## **Procedure**

- 1. Configure your RADIUS server with the usernames, passwords, and privilege levels that you want to use on the Branch Gateway.
- 2. Configure RADIUS authentication on the Branch Gateway.

## **RADIUS authentication configuration commands**

For more information about these commands, see Avaya Branch Gateway G450 CLI Reference.

Command	Description
clear radius authentication server	Clear the primary or secondary RADIUS server IP address
set radius authentication	Enable or disable RADIUS authentication
set radius authentication retry-number	Set the number of times to resend an access request when there is no response
set radius authentication retry-time	Set the time to wait before resending an access request
set radius authentication secret	Set the shared secret for RADIUS authentication
set radius authentication server	Set the IP address of the primary or secondary RADIUS authentication server
set radius authentication udp-port	Set the RFC 2138 approved UDP port number
show radius authentication	Display all RADIUS authentication configurations (shared secrets are not displayed)

# **Special security features**

Special security features allow you to establish incoming and outgoing Telnet connections, copy gateway configurations while keeping configuration secrets, and configure SYN cookies for preventing SYN attacks.

# **Commands used to configure Telnet access**

You can enable and disable the Branch Gateway's ability to establish incoming and outgoing Telnet connections using the following commands. These commands are secured commands and

are not displayed together with the running configuration (using the **show running-config** command). To see the status of these commands, use the **show protocol** command.

- ip telnet
- ip telnet-client
- ip telnet-services

## Telnet access configuration commands

For more information about these commands, see Avaya Branch Gateway G450 CLI Reference.

Command	Description
ip telnet	Enable the Branch Gateway to establish an incoming Telnet connection, or disable its ability to establish an incoming Telnet connection
no ip telnet	Disable the Branch Gateway's ability to establish an incoming Telnet connection
ip telnet-client	Enable the Branch Gateway to establish an outgoing Telnet connection, or disable its ability to establish an outgoing Telnet connection
	You can use this command only when accessing the Branch Gateway using a direct connection to the Console or Services port.
no ip telnet-client	Disable the Branch Gateway's ability to establish an outgoing Telnet connection.
ip telnet-services	Enable the Telnet server on the Services interface
	You can use this command only when accessing the Branch Gateway using a direct connection to the Console or Services port.
show ip telnet	Display the status of the Telnet server and the current Telnet connections
show protocol	Display the status of the Telnet or Telnet-client protocol
telnet	Initiate a login session via Telnet to a network host

# **Gateway secret management**

The Branch Gateway provides a mechanism for storage, backup, and restoration of sensitive materials (passwords and keys) maintained in the Branch Gateways.

All sensitive materials are encrypted using a Master Configuration Key (MCK), derived from a passphrase entered by an administrator. The secrets are then stored in the configuration file in an encrypted format. This enables copying configurations, including secrets, from one device to another. The only requirement is that the administrator must generate an identical MCK (by using the same passphrase) in the target device before executing the copy operation.

## Note:

All Gateways have the same default MCK. For security reasons, it is recommended to configure a new MCK immediately upon Branch Gateway installation.

# **Configuring the Master Configuration Key**

#### **Procedure**

- 1. Enter **key config-key password-encryption** followed by a phrase of 13 to 64 printable ASCII characters.
- 2. Copy the running configuration to the start-up configuration using the copy running-config startup-config command.

#### Result

The new MCK is now in effect.

## DoS attacks

The Branch Gateway provides various TCP/IP services and is therefore exposed to a myriad of TCP/IP based DoS attacks.

"DoS (Denial of Service) attacks" refers to a wide range of malicious attacks that can cause a denial of one or more services provided by a targeted host.

## **SYN** attack

Specifically, a SYN attack, or SYN flood attack, is a well-known TCP/IP attack in which a malicious attacker targets a vulnerable device and effectively denies it from establishing new TCP connections.

The SYN attack is characterized by the following pattern:

Using a spoofed IP address, an attacker sends multiple SYN packets to a listening TCP port on the target machine (the victim). For each SYN packet received, the target machine allocates resources and sends an acknowledgement (SYN-ACK) to the source IP address. The TCP connection is called a "half-open" connection at this point since the initiating side did not yet send back an acknowledgment (termed the third ACK).

Because the target machine does not receive a response from the attacking machine, it attempts to resend the SYN-ACK, typically five times, at 3-, 6-, 12-, 24-, and 48-second intervals, before de-allocating the resources, 96 seconds after attempting the last resend. Altogether, the target machine typically allocates resources for over three minutes to respond to a single SYN attack.

When an attacker uses this technique repeatedly, the target machine eventually runs out of memory resources since it holds numerous half-open connections. It is unable to handle any more connections, thereby denying service to legitimate users.

Moreover, flooding the victim with TCP SYN at a high rate can cause the internal queues to fill up, also causing a denial of service.

## SYN cookies

SYN cookies refers to a well-known method of protection against a SYN attack.

SYN cookies protect against SYN attacks by employing the following strategies:

- Not maintaining any state for half-open inbound TCP sessions, thus preventing the SYN attack from depleting memory resources.
  - SYN cookies can maintain no state for half-open connections by responding to SYN requests with a SYN-ACK that contains a specially crafted initial sequence number (ISN), called a cookie. The value of the cookie is not a pseudo-random number generated by the system, but the result of a hash function. The hash result is generated from the source IP, source port, destination IP, destination port, and some secret values. The cookie can be verified when receiving a valid third ACK that establishes the connection. The verification ensures that the connection is a legitimate connection and that the source IP address was not spoofed.
- Employing the SYN cookies method at a lower point in the network stack then regular TCP handling, closer to the start point of packet handling. This reduces the chances that a SYN attack will fill up the internal gueues.
- Performing SYN attack fingerprinting and alerting an administrator about a SYN attack as it
  occurs. This is implemented by keeping track of the rate at which half-open TCP connections
  are created, and sending an alert when the rate exceeds a certain threshold.

In addition, when the SYN cookies mechanism is active, a hostile port scan might be misled into concluding that all TCP ports are open.

## **Configuring SYN cookies**

## **Procedure**

- 1. Enter tcp syn-cookies.
- 2. Copy the running configuration to the start-up configuration using the copy running-config startup-config command.
- 3. Reset the device using the reset command.

#### Result

SYN cookies are now enabled on the device.

## SYN attack notification

When the SYN cookies feature is enabled, the Branch Gateway alerts the administrator to a suspected SYN attack as it occurs by sending the following syslog message:

SYN attack suspected! Number of unanswered SYN requests is greater than 20 in last 10 seconds.

## Commands used to maintain SYN cookies

Use the following commands to show and clear SYN cookies statistics:

- show tcp syn-cookies
- clear tcp syn-cookies

For more information about these commands, see Avaya Branch Gateway G450 CLI Reference.

## SYN cookies configuration commands

For more information about these commands, see Avaya Branch Gateway G450 CLI Reference.

Command	Description
clear tcp syn-cookies counters	Clear the SYN cookies counters
show tcp syn-cookies	Show SYN cookies statistics for inbound TCP connections
tcp syn-cookies	Enable or disable the TCP SYN cookies defense mechanism against SYN attacks

# **Managed Security Services**

Branch Gateway IP interfaces and gateway applications such as WAN routers, PoE switches, and VPN devices can be at risk for DoS attacks. The Branch Gateway identifies predefined or custom-defined traffic patterns as suspected attacks and generates SNMP notifications, referred to as Managed Security Services (MSS) notifications.

## MSS reporting mechanism

MSS notifications are sent to the active MGC by the dynamic trap manager. MSS notifications sent to the active MGC by the dynamic trap manager are converted to syslog messages by the SNMP trap manager on the MGC.

MSS notifications are intercepted and, if certain conditions are met, may be forwarded to the Avaya Security Operations Center (SOC) as INADS alarms. The SOC is an Avaya service group that handles DoS alerts, responding as necessary to any DoS attack or related security issue.

## Note:

The syslog messages on the active MGC are stored in the messages file on the MGC hard disk. You can view the syslog messages through the Avaya Maintenance Web Interface (MWI) if you want to debug security issues directly.

Any additional SNMP recipients defined with the security notification group enabled also receive the MSS notifications.

#### Related links

<u>Syslog server configuration</u> on page 187 <u>Viewing QoS traps, QoS fault traps, and QoS clear traps</u> on page 337

# **Configuring MSS**

#### About this task

The MSS feature is automatically enabled and monitors all IP interfaces, including WAN data interfaces, IPSEC tunnels, Ethernet LAN and WAN ports, VoIP engine interfaces, and Dialer and Serial PPP interfaces.

## **Procedure**

 Verify that the dynamic trap manager that automatically sets the IP address of the active MGC SNMP trap manager, is configured so that security notifications are sent to the active MGC.

By default, all types of notifications are enabled. You can enter **show snmp** to check which notification groups are configured to be sent to the active MGC. You can modify the dynamic trap manager configuration using the **snmp-server dynamic-trap-manager** command, setting the notification type to all or security.

2. If required, define additional notification recipients using the snmp-server group, snmp-server host, and snmp-server user commands, and activating the security notification filter.

## For example:

```
//define an SNMP group:
Gxxx-001(super)# snmp-server group MSS group v3 noauth read iso write iso
notify iso
Done!
//create a new snmp user belonging to the SNMP group:
Gxxx-001(super) # snmp-server user MSS MSS group v3
//identify an SNMP trap recipient, activating the security notification
filter:
Gxxx-001(super) # snmp-server host 5.5.5.2 traps v3 noauth MSS security
//view the SNMP configuration
Gxxx-001(super) # show snmp
Authentication trap disabled
Community-Access Community-String
read-only ****
read-write ****
SNMPv3 Notifications Status
Traps: Enabled
Informs: Enabled Retries: 3 Timeout: 3 seconds
SNMP-Rec-Address Model Level Notification Trap/Inform User name
5.5.5.2 v3 noauth all trap MSS
UDP port: 162
```

Use the set mss-notification rate command to modify the MSS reporting rate, if necessary.

The default is 300 seconds. The Branch Gateway counts events for each DoS class for the duration of the interval. At the end of each interval, if the count of each class of DoS events surpasses a defined threshold, the Branch Gateway generates an MSS notification, reporting on the event type, event parameters, and the number of occurrences. To display the current MSS reporting rate, use the show mss-notification rate command.

4. Ensure that INADS reporting is configured on the active MGC.

For information about configuring INADS reporting in CM, see Avaya Aura® Communication Manager documentation.

## **DoS** attack classifications

Traffic patterns meeting the DoS attack classifications are automatically reported in MSS notifications.

DoS Attack	Description
LAND_ATTACK	Land attack packets with the source IP the same as an IP address
TCP_URGENT_ATTACK	TCP packets with the URGENT option set
ICMP_RATE_LIMIT	ICMP (echo) requests exceeding a pre-defined rate
SMURF_ATTACK	ICMP echo packets with limited broadcast destination address
FRAGGLE_ATTACK	UDP packets with limited broadcast destination address
SYN-FLOOD	The number of unacknowledged TCP SYN-ACK exceeds a predefined rate
UNREACHABLE_PORT_ ATTACK	TCP/UDP IP packets sent to unreachable ports
MALFRAGMENTED_IP	Malfragmented IP packets on TO-ME interfaces
MALFORMED_IP	Malformed IP packets.
	The Branch Gateway reports malformed IP packets when:
	The IP version in the IP header is a value other than 4
	The IP header length is smaller than 20
	The total length is smaller than the header length
MALFORMED_ARP	ARP messages with bad opcode
SPOOFED_IP	For all routable packets, the Branch Gateway report reception of IP spoofed packets
UNKNOW_L4_IP_PROTOCOL	Packets with unknown (unsupported or administratively closed) protocol in IP packet with TO-ME interface as a destination
UNATHENTICATED_ACCESS	Failure to authenticate services

## **Custom DoS classifications**

You can define custom DoS attack classifications using access control list (ACL) rules. ACL rules control which packets are authorized to pass through an interface. A custom DoS class is defined by configuring criteria for an ACL rule and tagging the ACL with a DoS classification label.

## **Related links**

Policy lists on page 497

## Examples for defining a DoS class using ACLs

• Use the ip access-control-list command to enter the configuration mode of an ACL. For example:

```
Gxxx-001(super) # ip access-control-list 301
```

• Use the ip-rule command to enter the configuration mode of an ACL rule. For example:

```
Gxxx-001(super)# ip-rule 1
```

• Use the dos-classification command to configure the name of the DoS attack classification. Possible values are: fraggle, smurf, ip-spoofing, other-attack-100, other-attack-101, other-attack-102, other-attack-103, other-attack-104, and other-attack-105. For example:

```
Gxxx-001(super-ACL 301/ip rule 1)# dos-classification smurf Done!
```

• Use **destination-ip** or **ip-protocol** commands to define the packet criteria to which the ACL rule should apply.

You can use **destination-ip** to specify that the rule applies to packets with a specific destination address and you can use **ip-protocol** to specify that the rule applies to packets with a specific protocol:

```
Gxxx-001(super-ACL 301/ip rule 1) # destination-ip 255.255.255.255 0.0.0.0
Done!
Gxxx-001(super-ACL 301/ip rule 1) # ip-protocol icmp
Done!
```

• Use the composite-operation command to associate the ACL rule with the predefined operation "deny-notify," that tells the Branch Gateway to drop any packet received that matches the ACL rule, and send a trap upon dropping the packet. For example:

```
Gxxx-001(super-ACL 301/ip rule 1) # composite-operation deny-notify
Done!
```

Use the following example to exit the ACL rule:

```
Gxxx-001(super-ACL 301/ip rule 1)# exit
```

Use the following example to exit the ACL:

```
Gxxx-001(super-ACL 301)# exit
```

 An example for entering the configuration mode of the interface on which you want to activate the ACL:

```
Gxxx-001(super) # interface vlan 203
```

• An example for activating the configured ACL for incoming packets on the desired interface:

```
Gxxx-001(super-if:vlan 203) # ip access-group 301 in Done!
```

#### Related links

Policy lists rule criteria on page 506

## **Example of configuring MSS notifications using ACL rules**

The following example demonstrates the configuration of MSS notifications using ACL rules. In this example, smurf packets (ICMP packets that are sent to a limited broadcast destination) arriving at interface VLAN 203 are defined as a DoS attack to be reported in MSS notifications.

```
//create and enter the configuration mode of access control list 301:
Gxxx-001(super) # ip access-control-list 301
//create and enter the configuration mode of ip rule 1:
Gxxx-001(super-ACL 301/ip rule 1) # ip-rule 1
//set the rule criteria for the custom DoS classification:
//use dos-classification command to specify to report on receiving smurf
//packets (ICMP echo packets with limited broadcast destination address )
Gxxx-001(super-ACL 301/ip rule 1) # dos-classification smurf
//apply predefined composite-operation deny-notify, which drops the packet and
//causes the gateway to send a trap when it drops the packet
Gxxx-001(super-ACL 301)# composite-operation Deny-Notify
Done!
//specify that the ip rule applies to packets with this destination ip address.
Gxxx-001(super-ACL 301/ip rule 1)# destination-ip 255.255.255.255 0.0.0.0
//Specify that the ip rule applies to ICMP packets
Gxxx-001(super-ACL 301/ip rule 1) # ip-protocol icmp
Gxxx-001(super-ACL 301/ip rule 1)# exit
Gxxx-001(super-ACL 301) # show ip-rule
Index Protocol IP
                                  Wildcard Port
                                                           Operation
      DSCP
                                                           Fragment rule
                                             Any Type Deny-Notify
Any Code No
     icmp Src Any
Any Dst 255.255.255 Host
Dos classification: smurf
Deflt Any Src Any
Any Dst Any
                                               Any
                                                           Permit
      Any
                                               Any
Gxxx-001(super-ACL 301)# exit
Gxxx-001(super) # interface vlan 203
//activate Access Control list 301 for incoming packets on interface vlan 203:
Gxxx-001(super-if:VLAN 203)# ip access-group 301 in
```

## **MSS configuration CLI commands**

For more information about these commands, see Avaya Branch Gateway G450 CLI Reference.

Command	Description
composite-operation	Edit the specified composite operation. If the composite operation does not exist, it is created
destination-ip	Specify the destination IP address of packets to which the current rule applies
dos-classification	Set a label for a user-defined DoS attack classification to be reported in MSS notifications
ip access-control-list	Enter configuration mode for the specified policy access control list. If the specified list does not exist, the system creates it and enters its configuration mode.

Table continues...

Command	Description
ip-rule	Enter configuration mode for the specified rule. If the specified rule does not exist, the system creates it and enters its configuration mode.
ip-protocol	Specify that the current rule applies to packets having the specified IP protocol
set mss-notification rate	Set the rate at which the Branch Gateway sends Managed Security Services (MSS) notifications
show mss-notification rate	Show the interval time, in seconds, between MSS notifications
show snmp	Display SNMP configuration information
snmp-server dynamic-trap- manager	Modify the SNMP settings of the dynamic trap manager
snmp-server group	Define a new SNMPv3 group, or configure settings for the group
snmp-server host	Identify an SNMP management server, and specify the kind of messages it receives
snmp-server user	Configure settings for an SNMPv3 user

# **Enhanced Access Security Gateway (EASG)**

EASG provides a secure method for Avaya services personnel to access the Avaya Aura<sup>®</sup> application remotely and onsite. Access is under the control of the customer and can be enabled or disabled at any time. EASG must be enabled for Avaya Services to perform tasks necessary for the ongoing support, management and optimization of the solution. EASG is also required to enable remote proactive support tools such as Avaya Expert Systems<sup>®</sup> and Avaya Healthcheck.

# **Managing EASG**

# **Enabling EASG authentication**

## **About this task**

You can enable the EASG authentication for all Avaya logins.

## Before you begin

Login to the application CLI interface.

## **Procedure**

1. To enable the EASG authentication, run the command:

## EASGManage enableEASG

The system displays the following message:

By enabling Avaya Logins you are granting Avaya access to your system.

This is necessary to maximize the performance and value of you Avaya

support entitlements, allowing Avaya to resolve product issues in a timely manner.

In addition to enabling the Avaya Logins, this product should be registered with Avaya and technically onboarded for remote connectivity

and alarming. Please see the Avaya support site (support.avaya.com/registration) for additional information for registering products and establishing remote access and alarming. Do you want to continue (Y/N)?

2. When the system prompts, type Y.

The system displays the following message:

EASG is Enabled. Done!

## **Disabling EASG authentication**

#### About this task

You can disable the EASG authentication for all Avaya logins.

## Before you begin

Login to the application CLI interface.

## **Procedure**

1. To disable the EASG authentication, run the command:

#### EASGManage disableEASG

The system displays the following message:

By disabling Avaya Logins you are preventing Avaya access to your system.

This is not recommended, as it impacts Avaya's ability to provide support

for the product. Unless the customer is well versed in managing the

product themselves, Avaya Logins should not be disabled. Do you want to continue (Y/N)?

2. When the system prompts, type Y.

The system displays the following message:

EASG is disabled. Done!

## **Enabling EASG authentication for specified user**

#### About this task

You can enable the EASG authentication for a specified user.

## Before you begin

Login to the application CLI interface.

## **Procedure**

1. To enable the EASG authentication for a specified user, run the command:

```
EASGManage enable {user}
```

The system displays the following message:

```
You are about to enable EASG access for User "xxxx". Do you want to continue (Y/N)?
```

2. When the system prompts, type Y.

The system displays the following message:

```
EASG access for User "xxxx" is enabled. Done!
```

## Disabling EASG authentication for specified user

#### About this task

You can disable the EASG authentication for a specified user.

## Before you begin

Login to the application CLI interface.

#### **Procedure**

1. To disable the EASG authentication for a specified user, run the command:

```
EASGManage disable {user}
```

The system displays the following message:

```
You are about to disable EASG access for User "xxxx". Do you want to continue (Y/N)?
```

2. When the system prompts, type Y.

The system displays the following message:

```
EASG access for User "xxxx" is disabled. Done!
```

# Viewing available EASG users list

#### About this task

You can view the available EASG users list.

## Before you begin

Login to the application CLI interface.

## **Procedure**

To view the available EASG users list, run the command:

#### EASGManage listUsers

The system displays the available EASG users list.

# Viewing EASG product certificates

## Viewing EASG product certificate information

## About this task

You can view the EASG product certificate information.

## Before you begin

Login to the application CLI interface.

## **Procedure**

To view the EASG product certificate information, run the command:

## EASGProductCert

The system displays the following message:

```
Subject: CN=G450 Media Gateway 7.1.2, OU=EASG, O=Avaya Inc.
```

Serial Number: 10023

Start Date: Jul 27 23:04:02 2017 GMT (-60 days) Expiration Date: Jul 27 04:00:00 2032 GMT (5418 days)

Trust Chain:

- 1. O=Avaya, OU=IT, CN=AvayaITrootCA2
- 2. DC=com, DC=avaya, DC=global, CN=AvayaITserverCA2
- 3. O=Avaya Inc, OU=EASG, CN=EASG Intermediate CA
- 4. CN=Product EASG Intermediate CA, OU=EASG, O=Avaya Inc.
- 5. CN=G450 Media Gateway 7.1.2, OU=EASG, O=Avaya Inc.

# Managing EASG site certificates

## Copying and installing EASG site certificate using scp

## About this task

You can copy and install EASG site certificate using scp.

## Before you begin

Login to the application CLI interface.

#### **Procedure**

To copy and install EASG site certificate using scp, run the command:

## EASGSiteCertManage copy scp {filename} {ip-address}

The system copies and installs EASG site certificate.

## Copying and installing EASG site certificate using usb device

## About this task

You can copy and install EASG site certificate using usb device.

## Before you begin

Login to the application CLI interface.

#### **Procedure**

To copy and install EASG site certificate using usb device, run the command:

EASGSiteCertManage copy usb usb-device filename

The system copies and installs EASG site certificate using usb device.

## **Deleting installed EASG site certificate**

## About this task

You can delete the installed EASG site certificate.

## Before you begin

Login to the application CLI interface.

#### **Procedure**

To delete the installed EASG site certificate, run the command:

EASGSiteCertManage delete {installed pkcs7 name | all}

The system deletes the installed site certificate

## Viewing valid EASG site certificates list

#### About this task

You can view the valid EASG site certificates list.

## Before you begin

Login to the application CLI interface.

## **Procedure**

To view the valid EASG site certificates list, run the command:

## EASGSiteCertManage list

The system displays the following message:

```
Valid Site Certificates:
1. sitecertificatename.p7b
```

## Viewing valid installed EASG site certificate information

#### About this task

You can view the valid installed EASG site certificate information.

## Before you begin

Login to the application CLI interface.

#### **Procedure**

To view the valid installed EASG site certificate information, run the command:

## EASGSiteCertManage show {installed pkcs7 name}

#### The system displays the following message:

```
Subject: CN=Avaya Technician {username}, OU=EASG, O=Avaya Inc. Technician Name: rblechman
Start Date: Sep 7 21:09:08 2017 GMT (-13 days)Start Date: Sep 7 21:09:08 2017 GMT (-13 days)
Expiration Date: Sep 22 21:09:08 2017 GMT (1 days)
Trust Chain:
1. O=Avaya, OU=IT, CN=AvayaITrootCA2
2. DC=com, DC=avaya, DC=global, CN=AvayaITserverCA2
3. O=Avaya Inc, OU=EASG, CN=EASG Intermediate CA
4. CN=Site EASG Intermediate CA, OU=EASG, O=Avaya Inc.
5. CN=Avaya Technician rblechman, OU=EASG, O=Avaya Inc.
```

# **Viewing EASG status**

## Viewing EASG status

#### About this task

You can view the EASG status is enabled or disabled.

## Before you begin

Login to the application CLI interface.

#### **Procedure**

To view the EASG status, run the command:

#### **EASGStatus**

The system displays the following message:

EASG is Enabled.

# Viewing product id

## About this task

You can view the product id.

## Before you begin

Login to the application CLI interface.

## **Procedure**

To view the product id, run the command:

product-id

The system displays the following message:

39ad6805e054169a3da624581fd40976 Done! Done!

# Service logins with Enhanced Access Security Gateway (EASG) authentication

Branch Gateway supports EASG authentication for remote service logins. Branch Gateways, which are under service contract, do not have LSPs, and are controlled by external MGCs, need a remote connection of services. EASG is a more secure method of authentication than password authentication and does not require a static password.

EASG uses one-time tokens for authentication, in which a unique secret key is associated with each login. EASG authentication is a challenge-response mechanism. The remote user receives a challenge from the gateway and the user returns an EASG authenticated response that the gateway verifies before permitting access. A new challenge is used for each access attempt.

EASG authentication is supported for remote services connecting to the gateway using Telnet or SSH protocols. The remote logins could be via any of the following:

- Dial-up modem connected to the USB, Console, or Services port
- · Frame relay or leased line
- Secure gateway VPN
- Direct connection to the front panel Console port or Services port using the "craft" login

When EASG authentication is enabled on Branch Gateway, Branch Gateway recognizes any login attempts that use Avaya Services reserved user names as service logins. Branch Gateway requests EASG authentication from the user instead of a static user password.

The following user names are reserved for Avaya Services usage: rasaccess, sroot, init, inads, and craft.

When EASG authentication is enabled on Branch Gateway, all user accounts with user names similar to the reserved service logins are deactivated.

# **Chapter 5: Basic device configuration**

Basic device configuration lets you:

- Define a new interface and its IP address
- Configure parameters that identify the Branch Gateway to other devices
- Define a Gateway interface as the Branch Gateway's default gateway
- Configure an MGC to work with the Branch Gateway
- Configure DNS resolver for resolving hostnames to IP addresses
- View the status of the Branch Gateway
- Manage and upgrade software, firmware, configuration, and other files on the Branch Gateway
- Backup and restore the Branch Gateway

# Defining an interface

#### About this task

All interfaces on the Gateway must be defined by the administrator, after installation of the Branch Gateway.

## **Procedure**

1. Use the interface command to enter the interface context.

Some types of interfaces require an identifier as a parameter. Other types of interfaces require the interface's module and port number as a parameter.

## For example:

```
interface vlan 1
interface serial 3/1
interface fastethernet 10/2.0
```

- 2. Use the ip address command, followed by an IP address and subnet mask, to assign an IP address to the interface.
- 3. Use the load-interval command to set the load calculation interval for the interface.

For a list and descriptions of other interface configuration commands, see Interface configuration. For interface configuration examples, see Configuration example.

# **Primary Management Interface (PMI) configuration**

The Primary Management Interface (PMI) address is the IP address of an interface that you can specify on the Branch Gateway. The first IP address you configure on the Branch Gateway automatically becomes the PMI. You can subsequently assign any IP interface to be the PMI.

The PMI is used as the IP address of the Branch Gateway for the following management functions:

- Registration of the Branch Gateway to an MGC
- Sending SNMP traps
- Opening telnet sessions from the Branch Gateway
- · Sending messages from the Branch Gateway using FTP and TFTP protocol

You can designate any of the Branch Gateway's interfaces to serve as the Branch Gateway's PMI. The PMI must be an IP address that the MGC recognizes. If you are not sure which interface to use as the PMI, check with your system administrator.

# **Setting the PMI of the Branch Gateway**

## **Procedure**

1. Use the interface command to enter the context of the interface to which you want to set the PMI (primary management interface).

For example, to use the VLAN 1 interface as the PMI, enter interface vlan 1.



## ☑ Note:

If the interface has not been defined, define it now.

- 2. Enter
  - pmi for an IPv4 PMI
  - pmi6 for an IPv6 PMI.
- 3. To return to general context, enter the exit command.
- 4. To save the new PMI in the startup configuration file, enter the copy running-config startup-config command.
- 5. To reset the Branch Gateway, enter the reset command.



## Note:

Most configuration changes take effect as soon as you make the change, but must be saved to the startup configuration file in order to remain in effect after you reset the Branch Gateway. The PMI address is an exception. A change to the PMI does not take effect at all until you reset the Branch Gateway.

6. To verify the new PMI, enter **show pmi** in general context.

If you use this command before you reset the Branch Gateway:

- Active PMI, Active PMI6 and Configured PMI display
- Both the Active and the Configured PMI should be the same IP address.
- 7. Use the following commands to configure other identification information:
  - set system contact
  - set system location
  - set system name

# **Active and configured PMI**

If you use the **show pmi** command before you reset the Branch Gateway, two different PMIs display:

**Active PMI:** The IPv4 PMI that the Branch Gateway is currently using, as defined in the running configuration file.

**Configured PMI:** The PMI that the Branch Gateway is configured to use after reset, as defined in the startup configuration file.

**Active PMI6:** The IPv6 PMI that the Branch Gateway is currently using, as defined in the running configuration file.

# **PMI configuration CLI commands**

For more information about these commands, see Avaya Branch Gateway G450 CLI Reference.

Root level command	Command	Description
<pre>interface (fastethernet  serial tunnel  vlan loopback  dialer)</pre>	-	Enter configuration mode for the FastEthernet, Serial, Tunnel, VLAN, Loopback, or Dialer interface
-	pmi6 pmi6 [link-local]	Set the current interface as the Primary Management Interface for the system  Note:  You can define pmi6 or pmi6 link-local on a VLAN interface only.  You can define pmi and pmi6 simultaneously on the Gateway, but only on the same VLAN interface

Table continues...

Root level command	Command	Description
-	no pmi	-
	no pmi6	
set system contact	-	Set the contact information for this Branch Gateway system
set system location	-	Set the location information for this Branch Gateway system
set system name	-	Set the name of the Branch Gateway system
show pmi	-	Display the current Primary Management Interfaces

# Example of defining a default gateway

The Branch Gateway uses a default gateway to connect to outside networks that are not listed on the Branch Gateway's routing table. To define a default gateway, use the <code>ip default-gateway</code> command, followed by either the IP address or name (type and number) of the interface you want to define as the default gateway.

## **Example**

The following example defines the interface with the IP address 132.55.4.45 as the default gateway:

ip default-gateway 132.55.4.45

#### **Example**

The following example defines Serial interface 3/1:1 as the default gateway:

ip default-gateway serial 3/1:1

#### **Example**

To define a default gateway with IPv6 address 2001:db8:2179::2

Gxxx-001(super)# ipv6 default-gateway 2001:db8:2179::2

# **Branch Gateway Controller configuration**

Branch Gateway Controller (MGC) controls telephone services on Branch Gateway. You can use a server with the Communication Manager software as MGC. Branch Gateway supports External Call Controllers (ECC) and Internal Call Controllers (ICC). ECC is an external server communicating with Branch Gateway over the network. ICC is Avaya S8300 Server that you install in Branch Gateway as a media module.

When Branch Gateway uses ECC, it can use a local S8300 as a backup controller for Enhanced Local Survivability (ELS). S8300 functions in the Survivable Remote Server (SRS) mode. If ECC stops serving Branch Gateway, S8300 takes over the service.

Release 7.1 and later support the following commands:

- set allow-unencrypted: To allow or disallow media encryption requests from Communication Manager.
- set link-encryption: To specify what TLS versions the gateway offers when connecting to a server.

Media Gateway supports the following new enhancements from Release 10.1:

- Edge Gateway: With the Edge Gateway feature, endpoints and gateways can operate in local NAT address domains at the branch office sites, while the Avaya server products remain in the data centers. The data centers also operate in a private address space. Avaya Session Border Controller for Enterprise (ASBCE) is the conversion element that supports end-to-end communication from the data centers to public service provider networks and the branch office sites. For details on configuring the ASBCE Edge Gateway feature, see *Administering Avaya Session Border Controller for Enterprise*.
- Management link: Edge Gateway supports a new management link (MGSBC) with Session Border Controller. The link is required to support the following:
  - SNMP TRAP messages sent up a link to UDP port 162 on the host Communication Manager.
  - The transport of SSH administration and maintenance sessions between Communication Manager and Edge Gateway.

# **Locating the Branch Gateway serial number**

#### About this task

To register the Branch Gateway with an MGC, you need the Branch Gateway's serial number. You can find this serial number in either of the following ways:

## **Procedure**

- 1. Use the show system command
- 2. Look for a 12-character string located on a label on the back panel of the Branch Gateway

# Survivability and migration options

Several options exist to minimize network disruption if connectivity between the Branch Gateway and the server or media gateway controller (MGC) is lost.

**MGC list:** You must specify at least one, and up to four, MGCs in the list. The first MGC on the list is the primary MGC. If the Branch Gateway cannot connect with, or loses its connection with, the primary MGC, it attempts to connect with the other MGCs on the list.

#### Note:

When Standard Local Survivability (SLS) is enabled, the MGC list includes the SLS module as a fifth entry in the MGC list.

Standard Local Survivability (SLS): SLS consists of a module built into the Branch Gateway to provide partial backup MGC functionality in the event that the connection with the primary MGC is lost. This feature allows a local Branch Gateway to provide a degree of MGC functionality when no link is available to an external MGC. Alternatively, it can be configured on an individual Branch Gateway using the CLI.

Enhanced Local Survivability (ELS): ELS is available for the Branch Gateway using a local S8300 or S85XX functioning in LSP mode. If the ECC stops serving the Branch Gateway, the S8300 takes over the service.

Auto fallback to primary MGC: This feature provides a means by which a Branch Gateway being serviced by its LSP can return to its primary MGC automatically when the connection is restored between the Branch Gateway and the MGC. By migrating the Branch Gateway to the MGC automatically, a fragmented network can be made whole faster, without the need for human intervention. Auto fallback is configured via the CM. For details, see the Administrator Guide for Avaya Aura® Communication Manager.

#### Note:

Auto fallback does not include survivability. Therefore, there is a short period during registration with the MGC during which calls are dropped and service is not available. This problem can be minimized using the connection preservation feature described below.

Connection preservation: This feature enables the Branch Gateway to preserve the bearer paths of stable calls if the Branch Gateway migrates to another MGC (including an LSP), including migration back from an LSP to the primary MGC. A call for which the talk path between parties in the call has been established is considered stable. A call consisting of a user listening to announcements or music is not considered stable and is not preserved. Any change of state in the call prevents the call from being preserved. For example, putting a call on hold during MGC migration will cause the call to be dropped. Special features, such as conference and transfer, are not available on preserved calls. Connection preservation preserves all types of bearer connections except BRI. PRI trunk connections are also preserved. For details, see the Administering Network Connectivity on Avaya Aura® Communication Manager, 555-233-504.

Modem dial-backup: This feature can be used to provide redundant WAN connectivity between a Branch Gateway and its primary MGC using a serial modem. This connection uses a virtual interface called the Dialer interface. This feature recognizes that even if the Branch Gateway is configured for survivability via SLS or ELS, the best solution is to maintain the gateway's connection with its primary MGC whenever possible.

## **Related links**

Standard Local Survivability (SLS) on page 93 Modem dial backup on page 236

# **MGC** list configuration

Branch Gateway must be registered with MGC to provide telephony services. You can configure MGCs with the following commands:

- set mgc list: Create a list of valid MGCs.
- show mgc: Display the state and the setup parameters of the currently active MGC.
- show mgc list: Display the IP addresses of MGCs on the MGC list.
- clear mgc list: Remove one or more MGCs from the MGC list.

## **Branch Gateway MGC settings**

Use the set mgc list command to set Branch Gateway MGC. You can enter the IP addresses of up to four MGCs with the set mgc list command. The first MGC on the list is the primary MGC. Branch Gateway searches for the primary MGC first. If Branch Gateway cannot connect to the primary MGC, it searches for the next available MGC on the list. If the gateway is configured with IPv4 (PMI) and IPv6 (PMI6) addresses, you can set IPv4 and IPv6 addresses in the same index on the MGC list. Gateway first uses the IPv4 address when it tries to register to Communication Manager.

You can also use FQDN for the MGC list.

To enable Edge mode, provide the SBC@ip address parameter in the set mgc list command. For more information about enabling the Edge mode, see *Avaya Branch Gateway G450 CLI Reference*.

When you enable SLS, the MGC list includes the SLS module as a fifth entry on the MGC list.



If Communication Manager uses C-LANs, add the C-LAN address to the MGC list. Otherwise, use the processor Ethernet IP address. For duplicated Communication Managers, use the alias Communication Manager address.

#### Related links

Standard Local Survivability (SLS) on page 93

# **Example of setting Branch Gateway MGC**

In the following example of the set mgc list command, if the MGC with the IPv4 address 135.6.8.99 and IPv6 address 2001:db8::370:7334 is available, that MGC becomes the Branch Gateway's MGC. If that server is not available, the Branch Gateway searches for the next MGC on the list, and so on.

Gxxx-001(super)# set mgc list 135.6.8.99+2001:db8::370:7334,135.34.54.2,2001:db8::1428:5
7ab
Done!

## Results from the set mgc list command

To determine the result of the set mgc list command, use the show mgc command. This command has the following output:

Field	Description
Gateway Mode	Indicates whether the gateway is in <b>Enterprise</b> or <b>Edge</b> mode.
	If the IP address of the Primary or Secondary MGC Host start with the string "SBC@", then the gateway understands that the topology is in <b>Edge</b> mode.
Registered	Indicates whether Branch Gateway is registered with MGC (YES or NO).
Active Controller	Displays the IP address of the active MGC. If there is no active MGC (that is, if the set mgc list command failed to configure an MGC), this field displays 255.255.255.255.
H248 Link Status	Indicates whether the communication link between Branch Gateway and MGC is up or down.
H248 Link Encryption	Indicates whether the communication link with the MGC is encrypted or not, and the type of encryption (TLS, PTLS).
SBC	Displays the IP address of Avaya SBCE.
Management Link Status	Displays the status of the MGSBC management link between Edge Gateway and Avaya SBCE.
PRIMARY MGC HOST	IPv4 and IPv6 addresses of the primary MGC host.
SECONDARY MGC HOST	IPv4 and IPv6 addresses of the secondary MGC hosts

# **Showing the current MGC list**

## About this task

The **show mgc list** command shows the IP addresses of MGCs on the MGC list. It also shows whether SLS is enabled.

## **Procedure**

To view the current MGC list, run the command show mgc list.

## **Example**

To view media gateway controller operating in Enterprise Mode:

```
sls disabled
Done!
```

## To view media gateway controller operating in Edge Mode:

# Removing MGCs from the MGC list

## **Procedure**

Enter clear mgc list to remove one or more MGCs from the MGC list.

#### Specifically:

- To remove one or more MGCs from the MGC list, type the IP addresses of the MGC you want to remove as an argument to remove that MGC.
- To remove more than one MGC with one command, type the IP addresses of all the MGCs you want to remove, separated by commas.
- To remove all the MGCs on the list, enter clear mgc list with no arguments.

## **Changing the MGC list**

#### **Procedure**

- 1. Enter clear mgc list with no arguments to clear the MGC list.
- 2. Enter set mgc list with a different set of IP addresses.

If you use the  $set\ mgc\ list$  command without first clearing the MGC list, the Branch Gateway adds the new MGCs to the end of the MGC list.

# **About setting reset times**

If the connection between Branch Gateway and the registered MGC is lost, Branch Gateway attempts to recover the connection. Use the set reset-times primary-search command and the set reset-times total-search command to set the timeout for the Branch Gateway's search for the primary MGC and the other MGCs on its MGC list, respectively. Use the set reset-times transition-point command to configure the point at which the primary MGCs in the list end and the LSPs begin.

Use the **show recovery** command to display the reset times.

# **Example for setting reset times**

If there are three IP addresses in the MGC list and the third address is the LSP, the transition point should be 2.

The default time for the primary search is one minute. The default time for the total search is 30 minutes. The default transition point is 1.

## **Example**

```
Gxxx-001(super) # set reset-times primary-search 20
Done!
Gxxx-001(super) # set reset-times total-search 40
Done!
Gxxx-001(super) # set reset-times transition-point 1
Done!
```

In this example, in the event of a connection loss with the registered MGC, the Branch Gateway searches for the primary MGC on its MGC list for 20 minutes. If the Branch Gateway does not establish a connection with the primary MGC within this time, it searches for the other MGCs on the list for a total of 40 minutes.

# **Accessing the registered MGC**

#### **Procedure**

Access the MGC according to the following:

a. If the MGC is an S8300 Server, enter session mgc

The session mgc does not work on an IPv6-only Branch Gateway.

- b. If the MGC is an S88xx, Dell or HP, use the **set mediaserver** command to manually define the MGC's IP address, and then enter **session mgc** to access the MGC.
- c. If the Branch Gateway includes a local S8300, enter session icc to access the S8300. You can use this command whether the local S8300 is the Branch Gateway's registered MGC.

Both the session mgc command and the session icc command open a telnet connection to the MGC.

Use the session mgc on an S8300D running VSP.

d. To open a connection directly to the CM System Access Terminal (SAT) application in the MGC, add sat to the command.

#### For example:

```
Gxxx-001(super) # session mgc sat
```

e. To open a connection to the MGC's LINUX operating system, do *not* add sat to the command.

## For example:

```
Gxxx-001(super) # session mgc
```

# **H.248 Registration Source Port**

With the following CLI commands, you can define or view the source port range that the gateway uses to register to CM.

- · set registration source-port-range
- · show registration source-port-range
- · set registration default source-port-range

If you do not specify a range, the gateway will select a port within the default range of 1024 to 65535.

# ICC or Survivable Remote Server monitoring

When a local MGC controls telephone services on the Branch Gateway in ICC or Survivable Remote Server mode, the Branch Gateway monitors the connection with the MGC. If the connection with the MGC is lost, the Branch Gateway starts a recovery process.

- Use the **set icc-monitoring** command to control heartbeat monitoring of an ICC or Survivable Remote Server . The enable parameter enables heartbeat monitoring. The disable parameter disables heartbeat monitoring.
- Use the **show icc-monitoring** command to display the status of the ICC or Survivable Remote Server monitoring process.

# **Summary of MGC list configuration commands**

For more information about these commands, see Avaya Branch Gateway G450 CLI Reference.

Command	Description
clear mgc list	Remove one or more MGCs from the MGC list
session	Open a telnet connection to the MGC
set icc-monitoring	Enable or disable heartbeat monitoring of an MGC in ICC or Survivable Remote Server mode
set mediaserver	Set the MGC management address and ports
set mgc list	Create a list of valid Media Gateway Controller(s)
set reset-times	Set the timeout for the Branch Gateway's search for the primary MGC, or search for the other MGC's on the MGC list, or configure the point at which the primary MGCs in the list end and the Survivable Remote Servers begin
show icc-monitoring	Display the status of the ICC/Survivable Remote Server monitoring process
show mediaserver	Display MGC configuration information
show mgc	Display the state and setup parameters of the currently active MGC
show mgc list	Display the IP addresses of the MGCs on the MGC list
show recovery	Show the Branch Gateway connection recovery setup

## DNS resolver

A DNS resolver resolves hostnames to IP addresses by querying DNS servers according to an ordered list. The list of DNS servers is compiled using either DNS servers entered manually by the user, or DNS servers gathered automatically by means of DHCP or PPP protocols, or both.

The user can also optionally aid the DNS resolver by specifying a list of domain names that the DNS resolver adds as a suffix to non-Fully Qualified Domain Name (FQDN) names, to help resolve them to an IP address.

The DNS resolver feature is intended to provide a backup mechanism for VPN hubs using DNS.

#### Related links

IPSec VPN on page 428

## **DNS** resolver features

Branch Gateway supports the following DNS resolver features:

- Supports IPv4 and IPv6 it can resolve a hostname to IPv4 and IPv6 addresses.
- Fully compliant with RFC1034, RFC1035, and RFC1123
- Maintains a global DNS database for all interfaces. The database is compiled using:
  - Static (user-defined) DNS servers
  - Automatically-learned DNS servers. DNS servers can be automatically learned by the FastEthernet 10/2 interface when it is configured as a DHCP client or configured for PPP.



## Note:

The following PPP interfaces can be configured to automatically learn the DNS servers in the system:

- FastEthernet with PPPoE
- Dialer interface
- · Serial interface

The most common application of this configuration is for connecting Branch Gateway to the Internet and getting the DNS server information from the ISP. Therefore, interfaces configured to automatically learn the DNS servers in the system are usually the FastEthernet with PPPoE interface and the Dialer interface.

#### Related links

Configuring the DHCP client on page 179

# Typical DNS resolver application – VPN failover

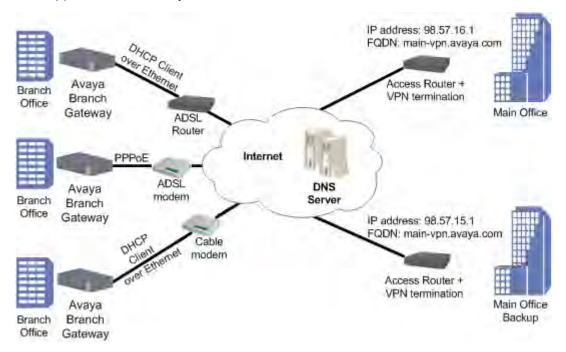
In this typical application, the DNS resolver feature is used to provide a VPN failover mechanism between two main offices. The failover mechanism is implemented as follows.

The VPN branch office(s) connect to two main offices (the VPN remote peers) that are configured with the same FQDN name, but have different IP addresses. When a branch office makes a

DNS query to resolve the VPN remote peer name to an IP address, it receives a list with the IP addresses of both main offices, selects the first one, and builds a VPN tunnel with it. If the first main office fails, the branch office sends another DNS query, and receives the IP address of the second main office in reply. It will then start a VPN tunnel with the second main office.

## Note:

VPN is supported in IPv4 only.



#### Related links

Failover using DNS on page 478

# **Configuring DNS resolver**

## **Procedure**

1. Enter ip domain name-server-list 1 to create the DNS servers list.

```
Gxxx-001(config) # ip domain name-server-list 1
Gxxx-001(config-name-server-list:1) #
```

2. Use the description command to specify a description for the list.

```
Gxxx-001(config-name-server-list:1) # description "All DNS servers"
Done!
Gxxx-001(config-name-server-list:1) #
```

- 3. Add a DNS server to the DNS servers list using the name-server command.
  - Assign an index number that ranks the DNS server by priority.
  - · Specify the IP address of the DNS server.
- 4. Repeat Step 3 to configure additional DNS servers in the list.

You can configure up to six DNS servers.

```
Gxxx-001(config-name-server-list:1) # name-server 1 1.1.1.1
Done!
Gxxx-001(config-name-server-list:1) # name-server 2 2001:DB8::21F:3CFF:FE14:6E25
Done!
```

5. Use the ip domain list command to configure a domain name.

This domain name will be used as a suffix to complete non-FQDN names (hostnames that do not end with a dot).

- Assign an index number that ranks the domain name by priority.
- · Specify the domain name.
- 6. Repeat Step 5 to configure additional domain names.

You can configure up to six domain names.

```
Gxxx-001(config) # ip domain list 1 avaya.com
Done!
Gxxx-001(config) # ip domain list 2 emea.avaya.com
Done!
```

7. Optionally, configure the number of DNS query retries, using the ip domain retry command.

The default value is 2.

```
Gxxx-001(config)# ip domain retry 4
Done!
```

8. Optionally, configure the timeout for a DNS query using the ip domain timeout command.

The default value is 3 seconds.

```
Gxxx-001(config) # ip domain timeout 4
Done!
```

The DNS resolver is enabled by default.

```
Gxxx-001(config)# ip domain lookup
Done!
```

- 10. If either DHCP Client or PPP are configured in the Branch Gateway, you do not need to configure DNS resolver because the DNS resolver is enabled by default. In addition, the DHCP Client and PPP discover DNS servers automatically, so the list of DNS servers include the automatically-learned DNS servers.
  - For DHCP Client, enable DHCP Client by entering ip address dhcp. For information about DHCP Client see Configuring the DHCP client.
  - For PPP, enable automatic discovery of DNS servers by entering ppp ipcp dns request.

#### **Example**

```
ip domain name-server-list
description
name-server 1
...
name-server 6
ip domain list 1
...
ip domain list 6
ip domain retry
ip domain timeout
show ip domain
ip domain lookup
```

### **DNS** resolver configuration example

The following example defines three DNS servers for the list of DNS servers, three domain names to add as suffixes to hostnames, a DNS query retry value, and a DNS query timeout value. The final command in the example enables the DNS resolver.

```
Gxxx-001(config) # ip domain name-server-list 1
Gxxx-001(config-name-server-list:1) # description "All DNS servers"
Gxxx-001(config-name-server-list:1) # name-server 1 1.1.1.1
Done!
Gxxx-001(config-name-server-list:1)# name-server 2 2.2.2.2
Done!
Gxxx-001(config-name-server-list:1) # name-server 3 2001:DB8::21F:3CFF:FE14:6E25
Gxxx-001(config-name-server-list:1) # exit
Gxxx-001(config) # ip domain list 1 support.avaya.com
Done!
Gxxx-001(config) # ip domain list 2 global.avaya.com
Done!
Gxxx-001(config) # ip domain list 3 avaya.com
Done!
Gxxx-001(config) # ip domain retry 4
Gxxx-001(config) # ip domain timeout 5
Gxxx-001(config) # ip domain lookup
```

### Using DNS resolver to resolve a hostname

#### About this task

Use the nslookup command, followed by a hostname, to resolve the hostname to an IP address.

### **DNS** resolver maintenance

There are various commands you can use to display DNS resolver information, clear DNS resolver counters, and display DNS resolver log messages.

### **Examples of viewing DNS resolver logging**

1. Enter set logging session enable to enable session logging to the terminal.

```
Gxxx-001# set logging session enable
Donel
CLI-Notification: write: set logging session enable
```

2. Enter set logging session condition DNSC to view all DNS resolver messages of level Info and above.

```
Gxxx-001# set logging session condition DNSC Info
CLI-Notification: write: set logging session condition DNSC Info
```



### W Note:

You can also enable logging messages to a log file or a Syslog server.

#### Related links

System logging on page 186

### **DNS** resolver configuration commands

For more information about these commands, see Avaya Branch Gateway G450 CLI Reference.

Root level command	Command	Description
clear ip domain statistics	-	Clear the DNS resolver's statistics counters
interface {dialer serial  console  FastEthernet  USB-modem}	-	Enter the interface configuration mode for a Dialer, Serial, Console, FastEthernet, or USB-modem interface
-	ppp ipcp dns request	Enable or disable requesting DNS information from the remote peer during the PPP/IPCP session
ip domain list	-	Specify static domain names (suffixes) to complete non-FQDN names (hostnames that do not end with a dot)
ip domain lookup	-	Enable or disable the DNS resolver
ip domain name- server-list	-	Enter the context of the DNS servers list, or set up the list
-	description	Set a name for the DNS servers list
-	name-server	Add a DNS server to the list of up DNS servers
ip domain retry	-	Set the number of retries for a DNS query
ip domain timeout	-	Set the timeout for a DNS query

Root level command	Command	Description
nslookup	-	Resolve a hostname to an IP address
show ip domain	-	Display the DNS resolver's configuration - the output shows the DNS servers that were statically configured and those which were gathered using DHCP or PPP protocols, as well as the list of domain suffixes  The output shows the DNS servers that were statically configured and those which were gathered using DHCP or PPP protocols, as well as the list of domain
		suffixes.
show ip domain statistics	-	Display the DNS resolver's statistics counters
show protocol	-	Display the status of a specific management protocol, or all protocols

### **Device status viewing**

This section describes the commands used to view the status of the Branch Gateway. For more information about these commands, see *Avaya G450 Branch Gateway CLI Reference*.

### The show mm command

Use the **show** mm command to view information about media modules that are installed on the Branch Gateway. To view information about a specific media module, include the slot number of the media module as an argument. For example, to view information about the media module in slot 2, enter **show** mm v2. The output of the command shows the following information:

- Slot number
- Uptime
- Type of media module
- Description
- Serial number and other hardware identification numbers.
- Firmware version
- · Number of ports
- · Fault messages

### The show mm and show mg list config commands

Use the show module command or enter show mg list\_config to view brief information about media modules that are installed in the Branch Gateway. To view brief information about a specific media module, include the slot number of the media module as an argument. For

example, to view information about the media module in slot 2, enter **show module v2**. The output of the command shows the following information:

- Slot number
- Firmware version
- Type of media module
- · Media module code

### **Device status commands**

For more information about these commands, see Avaya Branch Gateway G450 CLI Reference.

Command	Description
set utilization cpu	Enable CPU utilization measurements
show faults	Display information about currently active faults
show image version	Display the software version of the image on both memory banks of the device
show mg list_config	Display the current hardware and firmware configurations for the installed Branch Gateway equipment
show mgc	Display information about the Media Gateway Controller with which the Branch Gateway is registered
show module	Display brief information about the media modules installed in the Branch Gateway
show restart-log	Display information about the last time the Branch Gateway was reset
show system	Display information about the Branch Gateway
show temp	Display the device temperature
show timeout	Display the amount of time in minutes the terminal remains idle before timing out
show utilization	Display information about CPU and memory usage on the Branch Gateway
show voltages	Display power supply voltages

### OOB

### oob-interface configuration

The Out-of-Band Management interface can be used to access the gateway using CLI and SNMP and perform downloads or uploads. It is a dedicate management channel for device maintenance and provides separation between device management and user data. Having distinct channels isolates user and management/admin functions from data and allows more targeted auditing practices to be implemented to detect insider threats. The oob-interface command executed in the context of a FastEthernet or VLAN interface defines the interface as an Out-of-Band Management interface.

### Note:

- The Out-of-Band Management interface must be different from the PMI or PMI6 interface.
- An IP address must be defined on the interface before it can be configured as the Out-of-Band Management and a reboot is required after the Out-of-Band Management is configured.

### no oob-interface

The **no oob-interface** command removes a configured out of band interface. The command is denied if access on the other interfaces was disabled.



A reboot is required after the out-of-band management interface is removed.

### show oob-interface

The **show oob-interface** command displays the status of the Out-of-Band Management Interface.

### set non-oob-interfaces access

The set non-oob-interfaces access command is used to enable or disable access to the gateway from all interfaces except the out-of-band management interface. If the access is disabled then SSH, telnet, SNMP are only available on the Out-of-Band management interface.



The command is denied if an Out-of-Band interface is not configured.

### Software and firmware management

You can manage Avaya Branch Gateway software and firmware, either:

- Remotely, using an FTP, TFTP, SCP, or HTTPS server or
- Locally, using a USB mass storage device connected to the Avaya Branch Gateway USB port

### File transfer

Branch Gateway can be a client for the SCP, FTP, TFTP, and HTTPS protocols. Use either a USB device or the SCP, FTP, TFTP, or HTTPS protocols to transfer files between Branch Gateway and other devices. You can use file transfer to:

Install software and firmware upgrades on Branch Gateway

- · Install firmware upgrades on media modules
- Backup and restore configuration settings

To use SCP/FTP/TFTP/HTTPS file transfer, you need to have an SCP, FTP server, TFTP server or an HTTPS server on your network.

### Note:

If you use an SCP or FTP server, Branch Gateway prompts you for a username and password when you enter a command to transfer a file. Also, when opening an FTP connection to the S8300, all anonymous FTP file transfers are restricted to the /pub directory. Permission for anonymous FTP users to create files in other directories is denied.

### Software and firmware upgrades

You can upgrade software on Branch Gateway. Software used to control Branch Gateway itself and media modules installed on Branch Gateway is called firmware. Use a USB device or the SCP, FTP, TFTP, or HTTPS protocol to download a new version of software or firmware. You can upgrade the following types of software and firmware:

- Firmware for Branch Gateway
- Java applet for Branch Gateway
- · Firmware for media modules

### Note:

You can also use Branch Gateway to upgrade the firmware and configuration files for IP phones.

For details, see Installing and Upgrading the Avaya G450 Branch Gateway

### Firmware bank management

The Branch Gateway has two firmware banks:

- Bank A
- Bank B

Each firmware bank contains a version of the Branch Gateway firmware. These may be different versions. The purpose of this feature is to provide software redundancy. If one of the versions becomes corrupted, you can reset the Branch Gateway using the other version. This is particularly important when downloading new versions.

### Displaying firmware versions in the banks

#### **Procedure**

Use the **show image version** command to display the firmware version of the image on both memory banks of the Branch Gateway.

### Bank management changes

By default, when you turn on or reset the Branch Gateway, the Branch Gateway loads firmware from Bank B. To change the default bank from which firmware is loaded during startup, use the

set boot bank command. For example, to configure the Branch Gateway to load firmware from Bank A on startup, enter set boot bank bank-A. Now, when you reset the Branch Gateway, it will load firmware from Bank A.

To display the bank from which the Branch Gateway is currently set to load its firmware upon startup or reset, use the **show boot bank** command.

### Loading firmware from the non-default bank

#### About this task

Use the **ASB** button on the Branch Gateway front panel to load firmware from a bank other than the default bank during startup:

#### **Procedure**

- 1. Press and hold the **reset** button.
- 2. Press and hold the ASB button.
- 3. Release the **reset** button.
- 4. Release the ASB button.

#### Result

For example, if the Branch Gateway is configured to load firmware from Bank B, use the steps listed above to reset the Branch Gateway to load the firmware from Bank A instead.

### Software and firmware upgrades using SCP/FTP/TFTP/HTTPS

To upgrade software or firmware, you must obtain an upgrade file from Avaya. Place the file on your SCP, FTP, TFTP, or HTTPS server. Then, use one of the following commands to upload the file to Branch Gateway. For each of these commands, include the full path of the file and the IP address of the SCP, FTP, TFTP, or HTTPS host as parameters. When you enter the command, the CLI prompts you for a username and password.

When using SCP, FTP, TFTP, or HTTPS commands, you must use the specific path of the file on the SCP, FTP, TFTP, or HTTPS server according to the home directory of the service (SCP, FTP, TFTP, or HTTPS) that you are using.

### Example of an upgrade using SCP/FTP/TFTP/HTTPS

To upgrade the firmware of an MM710 media module in slot 2 from a TFTP server with the IP address 192.1.1.10, where the home directory is c:\home\ftp\ and the upgrade file is located in the directory c:\home\ftp\version, use the following command:

copy tftp module \version\mm710v3.fdl 192.1.1.10 2

#### Example

The following example downloads a firmware version with the path and file name  $C: g450\_sw\_41\_24\_0.bin$  from an FTP server with the IP address 149.49.134.153 to Bank A of Branch Gateway.

copy ftp SW imageA C:\g450 sw 41 24 0.bin 149.49.134.153

#### **Example**

The following example downloads a firmware version with the path and file name C:\g450v4 sw 41 24 0.bin from an FTP server with the IP address 149.49.134.153 to Bank A of Branch Gateway.

```
copy ftp SW imageA C:\g450v4 sw 41 24 0.bin 149.49.134.153
```

#### Example

The following example downloads a firmware version with the path and file name C:\q450v4 sw 41 24 0.bin from an SCP server with the IP address 149.49.134.153 to Bank A of Branch Gateway.

```
copy scp SW imageA g450/g450v4 41 24 0.bin 172.16.1.22
```



#### Note:

The G450 hardware vintage 4 uses a different software image. The filename starts with q450v4 sw. G450 hardware vintage 1 to 3 use a software image starting with q450 sw.

#### Example

The following example downloads the software image file, q450 sw 41 44 0.bin (for G450 or G430 hardware vintage 1.x, 2.x, 3.x) from the HTTPS server with URL my.webserver.com with the username dan:

```
g450-025(super) # copy http SW imageA https://dan@my.webserver.com/images/
g450 sw 41 44 0.bin
Enter WebServer Password: Resolving hostname to IP address
Press any key to stop the operation
```

### Upgrading software and firmware using a USB mass storage device

#### About this task

You can upgrade software and firmware using a USB mass storage device.

#### **Procedure**

- 1. Obtain an upgrade file from Avaya and place it on your PC.
- 2. Insert the USB mass storage device into the PC's USB port, and copy the software or firmware file(s) to the USB mass storage device.
- 3. Remove the USB storage device from the PC, and insert it in Branch Gateway USB port.
- 4. Copy the software or firmware files to Branch Gateway using one of the following commands:
  - · copy usb SW imageA
  - · copy usb SW imageB
  - · copy usb module
  - copy usb phone-imageA (Or imageB, Or imageC, Or imageD)
  - copy usb phone-scriptA (Or phone-scriptB)
  - · copy usb announcement-file

- · copy usb auth-file
- · copy usb startup-config
- · copy usb easg
- EASGSiteCertManage copy usb
- 5. Use the **show download software status** command to display the status of the firmware download process.

# Upgrading firmware using the USB mass storage device "restore" command About this task

The primary use of the **restore usb** command is to restore the entire Branch Gateway. If you use the command to upgrade firmware, take care to follow instructions carefully.

#### **Procedure**

1. Backup the Branch Gateway by entering backup config usb usbdevice0 backupname, where backup-name is the backup directory path and file name you are creating on the USB mass storage device.

A backup directory is created on the USB mass storage device.

- 2. Obtain the firmware upgrade file(s) from Avaya and place them on your PC.
- 3. Insert the USB mass storage device into the PC's USB port, and copy the firmware file(s) to the USB mass storage device as follows:
  - a. Copy Branch Gateway firmware files to the root directory.
  - b. Copy the Device Manager firmware file to the root directory.
  - c. Copy media modules' firmware files to the MM sub directory.
  - d. Copy IP phone firmware files to the IPPHONE sub directory.
- 4. Remove the USB mass storage device from the PC, and insert it in the Branch Gateway USB port.
- 5. Enter restore usb usbdevice0 backup-name, where backup-name is the root directory path and name on the USB mass storage device.
- 6. Enter show restore status to check the status of the restore operation.

The report lists the upgraded files.

#### Related links

Sample backup directory after backup on page 85

### Software and firmware uploads from the gateway

### Files copied to a USB mass storage device

You can use a USB mass storage device inserted into the Branch Gateway USB port to copy individual files to a USB mass storage device.

When you use the **copy file usb** command to upload a specific file from the gateway to the USB mass storage device, **file** can be any of the following types:

- · announcement-file. Announcements files
- phone-script. Phone script file A or B to the USB mass storage device
- startup-config. The startup configuration file
- · capture-file. The packet sniffing buffer
- · dhcp-binding. The DHCP binding file
- · syslog-file. The syslog file
- · cdr-file. A Call Detail Recording (CDR) file

### Files copied to an FTP/SCP/TFTP/HTTPS server

When you use the **copy file ftp** command to upload a specific file from the Branch Gateway to an FTP server, **file** can be any of the following types:

- · announcement-file. Announcements files
- · capture-file. The packet sniffing buffer
- · cdr-file. A Call Detail Recording (CDR) file
- · dhcp-binding. The DHCP binding file

When you use the **copy file scp** command to upload a specific file from the Branch Gateway to an SCP server, where **file** can be any of the following:

- · announcement-file. Announcements files
- capture-file. The packet sniffing buffer
- cdr-file. A Call Detail Recording (CDR) file
- · dhcp-binding. The DHCP binding file

When you use the **copy file tftp** command to upload a specific file from the Gateway to a TFTP server, where **file** can be any of the following:

- · announcement-file. Announcements files
- capture-file. The packet sniffing buffer
- cdr-file. A Call Detail Recording (CDR) file
- · dhcp-binding. The DHCP binding file

When you use the **copy file https** command to upload a specific file from the Gateway to a HTTPS server, where **file** can be any of the following:

- · announcement-file. The Announcements file
- capture-file. The packet sniffing buffer
- · startup-config. The configuration file

- dhcp-binding. The DHCP binding file
- syslog file

### Software and firmware management commands

For more information about these commands, see Avaya Branch Gateway G450 CLI Reference.

Command	Description
copy ftp module	Upgrade the firmware on a media module from an FTP server by entering this command followed by the module number of the module you want to upgrade.
copy ftp SW_imageA	Upgrade Branch Gateway firmware into Bank A from an FTP server.
copy ftp SW_imageB	Upgrade Branch Gateway firmware into Bank B from an FTP server.
copy tftp module	Upgrade the firmware on a media module from a TFTP server.
copy tftp SW_imageA	Upgrade Branch Gateway firmware into Bank A from a TFTP server.
copy tftp SW_imageB	Upgrade Branch Gateway firmware into Bank B from a TFTP server.
copy https module	Upgrade the firmware on a media module from a HTTP or HTTPS server.
copy https SW_imageA	Upgrade Branch Gateway firmware into Bank A from an HTTP or HTTPS server.
copy https SW_imageB	Upgrade Branch Gateway firmware into Bank B from an HTTP or HTTPS server.
copyedge scp module	Upgrade the firmware on a media module from an SCP server via Avaya SBCE tunnel.
copyedge scp SW_imageA	Upgrade Branch Gateway firmware into Bank A from an SCP server via Avaya SBCE tunnel.
copyedge scp SW_imageB	Upgrade Branch Gateway firmware into Bank B from an SCP server via Avaya SBCE tunnel.
copy usb announcement-file	Upgrade announcements files from the USB mass storage device.
copy https announcement-file	Upgrade announcements files from an HTTP or HTTPS server.
copyedge scp announcement-file	Upgrade announcements files from an SCP server via Avaya SBCE tunnel.
copy usb auth-file	Upgrade the authorization file from the USB mass storage device.
copy usb module	Upgrade the firmware on a media module from the USB mass storage device.
copy usb phone-image	Upgrade phone images from the USB mass storage device.
copy usb phone-script	Upgrade phone scripts from the USB mass storage device.
copy usb startup-config	Upgrade the startup configuration file from the USB mass storage device.
copy scp SW_imageA	Downloads a software image from an SCP server into Bank A. The command prompts for the username and password.

Command	Description
copy scp SW_imageB	Downloads a software image from an SCP server into Bank B. The command prompts for the username and password.
copy scp easg	Copy and install an EASG Site Certificate using scp.
copy usb SW_image	Upgrade Branch Gateway firmware into Bank A or into Bank B, from the USB mass storage device.
copy usb easg	Copy and install an EASG Site Certificate using a USB device.
dir	List all files in the USB mass storage device connected to Branch Gateway.
set boot bank	Set the default bank from which firmware is loaded during startup.
show boot bank	Display the bank from which Branch Gateway is currently set to load its firmware upon startup or reset.
show download software status	Display the status of the firmware download process.
show image version	Display the firmware version of the image on both memory banks of the device.

### Note:

Branch Gateway has four G450 hardware versions. Use the **show system** command to check the hardware version. If the Model is G450v4, it uses a different software image: g450v4 sw x y z.bin.

### Backup and restores using a USB mass storage device

You can use a USB flash drive and a USB externally-powered hub for backups and restores. Avaya Branch Gateway also supports USB 2.0 high speed (480 Mbits/sec) for faster file transfer between Branch Gateway and USB mass storage devices.

### Note:

An external USB hub is supported on Branch Gateways with hardware suffix.vintage C.1 or above. To check the hardware suffix and vintage, enter **show system** and check the HW suffix and HW vintage values.

CLI commands for backing up and restoring files to or from a USB mass storage device enable you to use a USB port for efficient restoration or replication of Branch Gateway and for replacing and upgrading media modules. Using the USB port you can back up or restore multiple files with one CLI command, which is simpler than the alternative TFTP/FTP/SCP/HTTPS method, in which files are copied and restored individually.

A single CLI command backs up all the administration and configuration files of Branch Gateway on USB mass storage device. Another single command restores all of the backed up files. If you need to completely replicate Branch Gateway, you can also download Branch Gateway firmware, media modules' firmware, Device Manager firmware, IP phone firmware, and Device Manager firmware to the USB mass storage device, and use the restore usb command to restore these files as well as the administration and configuration files.

### Note:

The CLI backup config usb and restore usb commands (for efficient backup/restore using a USB mass storage device) only run on Branch Gateways R4.0 and higher.

You can also use the USB mass storage device to copy individual Branch Gateway files to or from Branch Gateway.

### Tip:

Use a USB mass storage device with LED indication.

#### Related links

Upgrading software and firmware using a USB mass storage device on page 80

# Backing up administration and configuration files using a USB mass-storage device About this task

The following procedure backs up all the Branch Gateway configuration and administration files, but does not back up any firmware files.

Back up the Branch Gateway regularly to a USB mass-storage device. This backup can be very helpful in restoring the Branch Gateway's configuration if it becomes faulty, or in restoring the entire Branch Gateway.

Use at least a 128 MB USB mass-storage device since it can hold two full backup directories with all images and configuration files. You can create multiple backup directories as long as there is space in the USB mass-storage device.

#### **Procedure**

- 1. Connect a USB mass-storage device to the Branch Gateway USB port.
- 2. Type s to commit the current configuration to NVRAM.
- 3. Enter backup config usb usbdevice0 backup-name, where backup-name is the backup directory path and file name, you are creating on the USB mass-storage device.
  - A backup directory is created on the USB mass-storage device.
- 4. Before unplugging the USB mass-storage device, use the **safe-removal usb** command to safely remove the USB mass-storage device.
- 5. You can use the **show backup status** command to display information regarding the status of a backup of the Branch Gateway configuration to a USB mass-storage device.

### Sample backup directory after backup

After the backup, a backup directory is created on the USB mass-storage device with the following sample structure and file types:

Root directory	Sub-directory	Files	Comments
backup-23-Aug-2015	-	-	Backup directory name

Root directory	Sub-directory	Files	Comments
-	-	readme.txt	File with backup information
-	-	startup_config.cfg	Configuration file
-	-	audio.bin	Customer-specific VoIP parameters
-	-	auth-file.cfg	Authentication file
-	IPPHONE	-	IP phone scripts and images directory
-	-	46xxupgrade.scr	-
-	-	46xxsettings.txt	-
-	MM	-	Media modules file directory
-	GWANNC	-	Branch Gateway announcements and music-on-hold file
-	-	GeorgeAnnouncement.wav	-
-	-	GeorgiaAnnouncement.wav	-

## Restoring backed up configuration and administration files to Branch Gateway using a USB mass-storage device

#### **Procedure**

- 1. Make sure you have a backup of Branch Gateway on a USB mass-storage device.
- 2. Connect the USB mass-storage device to Branch Gateway USB port.
- 3. Enter restore usb usbdevice0 backup-name, where backup-name is the backup directory path and file name on the USB mass-storage device.
- 4. Before unplugging the USB mass-storage device, use the **safe-removal usb** command to safely remove the USB mass-storage device.

### Replicating Branch Gateway using a USB mass-storage device

#### About this task

The following procedure is useful for replicating Branch Gateway that has become faulty. Since the backup command backs up all the gateway configuration files, but does not back up any firmware files, the main task is to add the various firmware files before running restore.

### Important:

When adding files to a backup directory on a USB mass-storage device, follow the file and directory naming convention to enable a successful restore.

#### **Procedure**

1. Make sure you have a backup of the faulty Branch Gateway on a USB mass-storage device.

- 2. Transfer the media modules, including the S8300 if installed, from the faulty Branch Gateway into the corresponding slots of the new Branch Gateway.
- 3. Connect the new Branch Gateway to a power source.
- 4. In the new Branch Gateway, enter show image version to find out which of the two image banks holds the older Branch Gateway firmware version, and what version it is.
- 5. If the new Branch Gateway firmware version is below 26.x.y, you must replace it with firmware version 26.x.y or higher, in order to enable the restore option.
- 6. If the new Branch Gateway firmware version is 26.x.y or above, add Branch Gateway firmware to the USB mass-storage device, as follows:
  - a. From Avaya support Website, download to your PC the same version of Branch Gateway firmware as was running in the faulty Branch Gateway.
  - b. Insert the USB mass-storage device into the PC's USB port.
  - c. Copy Branch Gateway firmware file to the root backup directory in the USB massstorage device.
- 7. Add the firmware files of the media modules to the USB mass-storage device, as follows:
  - a. From Avaya support Website, download to your PC the firmware files of the media modules installed in the gateway.
    - For each media module, download all firmware corresponding to the various hardware vintage/suffix versions available for that module. If you are not sure which media modules you have, you can download the firmware files of all media modules. The restore operation uses only the files needed.
  - b. Insert the USB mass-storage device into the PC's USB port.
  - c. Copy the firmware files from the PC to the MM sub directory in the USB mass-storage device.
    - Do not change the firmware file names.
- 8. You can optionally add the firmware files of the IP phones to the USB mass-storage device, as follows:
  - a. From Avaya support Website, download to your PC the firmware files (booter and application) of up to two supported IP phones, as well as the <sup>1</sup> or <sup>2</sup> file.
  - b. Insert the USB mass-storage device into the PC's USB port.
  - c. Copy the IP phone files from the PC to the USB mass-storage device.

Place them in the IPPHONE sub directory under the root backup directory. Do not change the names of the downloaded files.



### ☑ Note:

You will need to reset the IP phones after the restore operation on the gateway.

<sup>&</sup>lt;sup>1</sup> 46xxupgrade.txt

<sup>&</sup>lt;sup>2</sup> 46xxupgrade.scr

- 9. You can optionally restore or add the Device Manager, as follows:
  - a. From Avaya support website, download to your PC the firmware file of the Device Manager.
  - b. Insert the USB mass-storage device into the PC's USB port.
  - c. Copy the Device Manager firmware file from the PC to the USB mass-storage device.

    Place it in the root backup directory. Do not change the name of the firmware file.
- 10. View the backup directory on the USB mass-storage device.
- 11. Enter **key config-key password-encryption** followed by the same passphrase that was used to create the Master Configuration Key (MCK) in the faulty gateway.

This creates on the new gateway an MCK identical to the MCK in the faulty gateway, which enables the restore operation to decrypt the secrets in the configuration file.

The restored configuration file will include all the configuration of the gateway, including user's names and passwords, IKE pre-shared keys, etc.

- 12. Insert the USB mass-storage device in the new Branch Gateway USB port.
- 13. Enter restore usb usbdevice0 backup-name, where backup-name is the backup directory path and file name on the USB mass-storage device.
- 14. Enter show restore status to check the status of the restore operation.

The report lists the files restored.

15. Update the S8300 on the new Branch Gateway with the serial number of the new gateway, otherwise the gateway is not able to register in the CM.

See Administrator's Guide for Avaya Aura® Communication Manager.

#### Result

The new Branch Gateway is now a restored, fully-operational Branch Gateway.

#### Next steps

Before unplugging the USB mass-storage device, use the **safe-removal usb** command to safely remove the USB mass-storage device.

#### **Related links**

Backing up administration and configuration files using a USB mass-storage device on page 85

### Sample backup directory after replication

After replicating Branch Gateway using a USB mass storage device, you can view the backup directory on the USB mass storage device. The file types and directory structure should match the following convention:

Root directory	Sub-directory	Files	Comments
backup-23-Aug-2015	-	-	Backup directory name

Root directory	Sub-directory	Files	Comments
-	-	readme.txt	File with backup info
-	-	startup_config.cfg	Configuration file
-	-	audio.bin	Customer-specific VoIP parameters
-	-	auth-file.cfg	Authentication file
-	-	g450_sw_41_24_0.bin	Branch Gateway hardware versions 1.x, 2.x, and 3.x
-	-	g450v4_sw_41_24_0.bin	Branch Gateway hardware version 4.x
-	IPPHONE	-	IP phone scripts and images directory
-	-	46xxupgrade.scr	-
-	-	46xxsettings.txt	-
-	-	4601dape1_82.bin	-
-	-	4601dbte1_82.bin	-
-	MM	-	Media modules file directory
-	-	mm722v2.fdl	-
-	-	mm714v67.fdl	-
-	-	mm711h20v67.fdl	-
-	-	mmanalogv67.fdl	-
-	GWANNC	-	Branch Gateway announcements and music- on-hold file directory
-	-	DanAnncouncement.wav	-
-	-	DanaAnncouncement.wav	-

### Replacing/adding/upgrading media modules using a USB mass-storage device Procedure

- 1. Backup Branch Gateway by entering backup config usb usbdevice0 backupname, where backup-name is the backup directory path and file name you are creating on the USB mass-storage device.
  - A backup directory is created on the USB mass-storage device.
- 2. From Avaya support Website, download to your PC the firmware files of the media modules you are adding or upgrading.
  - For each media module, download all firmware corresponding to the various hardware vintage/suffix versions available for that module. If you are not sure which files you need, you can download the firmware files of all media modules. The restore operation uses only the files needed.

3. Insert the USB mass-storage device into the PC's USB port, and copy the media modules' firmware files to the MM subdirectory under the root backup directory.

### **!** Important:

When adding files to a backup directory on a USB mass-storage device, it is important to follow the file and directory naming convention, in order to enable a successful restore.

- 4. Insert the USB mass-storage device into Branch Gateway USB port.
- 5. Enter restore usb usbdevice0 backup-name, where backup-name is the backup directory path and file name on the USB mass-storage device.
- 6. If you changed the placement of media modules in the slots, update the MGC managing Branch Gateway.

See Administrator's Guide for Avaya Aura® Communication Manager.



### ■ Note:

Before unplugging the USB mass-storage device, use the safe-removal usb command to safely remove the USB mass-storage device.

#### Related links

Sample backup directory after backup on page 85

### USB backup, restore, and replication commands

For more information about these commands, see Avaya Branch Gateway G450 CLI Reference.

Command	Description
backup config usb	Back up the Branch Gateway configuration to a USB mass-storage
copy usb sw_imageA	Download a software image from an external USB mass storage device into Bank A
copy usb sw_imageB	Download a software image from an external USB mass storage device into Bank B
dir	Display information regarding the status of a restore operation of Branch Gateway files from a USB mass-storage device
erase usb	Erase a file or directory on the USB mass-storage device
key config-key password-encryption	Change the default Master Key of the Branch Gateway, which is used to encrypt Branch Gateway secrets in the Branch Gateway configuration file
restore usb	Restore Branch Gateway files from a USB mass-storage device
safe-removal usb	Safely remove the USB mass-storage device
show backup status	Display information regarding the status of a backup of the Branch Gateway configuration to a USB mass-storage device
show image version	Display the software version of the image on both memory banks of the device

Command	Description
show system	Display information about the device
show usb	Display the USB devices connected to the Branch Gateway

### Configuration file backup and restore

A configuration file is a data file that contains a complete set of configuration settings for Branch Gateway. You can use configuration files to back up and restore the configuration of Branch Gateway. You can back up either the running configuration or the startup configuration to the server as a configuration file. When you restore a configuration file from a server, it becomes the startup configuration on Branch Gateway.

#### Note:

The startup configuration file stores Branch Gateway secrets (passwords, etc.) in an encrypted format. Thus, secrets do not have to be re-entered if you are copying a configuration file from one Branch Gateway to another.

#### You can:

- Use the FTP/TFTP/SCP/HTTPS copy commands to transfer a configuration file between Branch Gateway and a server on the network.
- Use a USB mass-storage device connected to Branch Gateway USB port to upload or download the startup configuration file of Branch Gateway. You can use either the USB copy commands, or use the USB backup and restore commands for a full backup and restore of Branch Gateway.

#### **Related links**

Configuration changes and backup on page 28

Gateway secret management on page 44

Backup and restores using a USB mass storage device on page 84

#### Configuration file backup and restore commands

For more information about these commands, see Avaya Branch Gateway G450 CLI Reference.

Command	Description
copy ftp startup- config	Download a Branch Gateway configuration file from an FTP server to the Startup Configuration NVRAM
copy scp startup- config	Download a Branch Gateway configuration from an SCP server to the Startup Configuration NVRAM
copy tftp startup- config	Download a Branch Gateway configuration file from a TFTP server to the Startup Configuration NVRAM
copy usb startup- config	Download a Branch Gateway configuration file from a USB mass-storage device to the Startup Configuration NVRAM
copy https startup- config	Download a Branch Gateway configuration file from an HTTP or HTTPS server to the Startup Configuration NVRAM

Command	Description
copyedge scp startup- config	Download a Branch Gateway configuration from an SCP server via Avaya SBCE tunnel to the Startup Configuration NVRAM
copy running-config ftp	Upload the current Branch Gateway running configuration to a file on an FTP server
copy running-config scp	Upload the current Branch Gateway running configuration to a file on an SCP server
copy running-config tftp	Upload the current Branch Gateway running configuration to a file on a TFTP server
copy running-config https	Upload the current Branch Gateway running configuration to a file on an HTTP or HTTPS server
copyedge running- config scp	Upload the current Branch Gateway running configuration to a file on an SCP server via Avaya SBCE tunnel
copy startup-config ftp	Upload the current Branch Gateway startup configuration to a file on an FTP server
copy startup-config scp	Upload the current Branch Gateway startup configuration to a file on a SCP server
copy startup-config tftp	Upload the current Branch Gateway startup configuration to a file on a TFTP server
copy startup-config usb	Upload the current Branch Gateway startup configuration to a file on a USB mass-storage device
copyedge startup- config scp	Upload the current Branch Gateway startup configuration to a file on a SCP server via Avaya SBCE tunnel
copy startup-config	Upload the current Branch Gateway startup configuration to a file on a HTTP or HTTPS server
show download status	Display the status of the current Branch Gateway configuration file download process, as the file is being loaded into the device

### List of files on the Branch Gateway

Use the dir command to list all Branch Gateway files. When you list the files, you can see the version numbers of the software components. The dir command also shows the booter file that cannot be changed.

You can also use the dir command to list all files in the USB mass-storage device connected to the Branch Gateway.

# Chapter 6: Standard Local Survivability (SLS)

Standard Local Survivability (SLS) provides a local Branch Gateway with a limited subset of MGC functionality when there is no IP-routed WAN link available to an MGC, or no MGC is available.

SLS is supported on IPv4 only.

SLS is not a replacement for ELS or SRS (Survivable Remote Server) survivability, which offer full call-feature functionality and full translations in the survivable mode. Instead, SLS is a cost-effective survivability alternative offering limited call processing in survivable mode. Although the Branch Gateway can host an S8300 Server in ICC or SRS mode, SLS offers both local survivability and call control.

In contrast to the server-based survivability features, SLS operates entirely from the Branch Gateway and requires a data set comprised of CM translations (survivable ARS analysis and configuration data). This data set can be configured manually from individual Branch Gateways using CLI commands. For instructions on configuring SLS, see SLS configuration rules.

### Media module compatibility with SLS

SLS works on the Branch Gateway and its media modules only if they satisfy the minimum hardware vintage and firmware version requirements listed in the following table.

Media module	Minimum firmware version required
MM710	Vintage 16
MM711, hw v20+	Vintage 69
MM711, hw v30+	Vintage 84
MM712	Vintage 8
MM714, hw v1-v5	Vintage 69
MM714, hw v10+	Vintage 84
MM716	Vintage 84
MM717	Vintage 8
MM720	Vintage 7

Media module	Minimum firmware version required
MM721	Vintage 1
MM722	Vintage 7
G450	MG 4.1, build 27_x

### **SLS** features

- Call capability for analog, DCP, and IP phones
- · ISDN BRI/PRI trunk interfaces
- Non-ISDN digital DS1 trunk interfaces
- Outbound dialing through the local PSTN (local trunk gateway) from analog, DCP, and IP phones
- Inbound calls from each trunk to pre-configured local analog or IP phones that have registered
- · Direct inward dialing
- · Multiple call appearances
- · Hold and call transfer functions
- · Contact closure feature
- Local call progress tones (dial tone, busy, etc.)
- Emergency Transfer Relay (ETR) in cases of power loss
- Auto fallback to primary MGC
- · IP station registration

### Avaya telephones supported in SLS

Analog	DCP	IP
2500	2402	4601
-	2410	4602
-	2420	4602sw
-	6402	4610sw
-	6402D	4612
-	6408	4620

Analog	DCP	IP
-	6408+	4620sw (default)
-	6408D (default)	4621
-	6408D+	4622
-	6416D+	4624
-	6424D+	4625
-	8403B	-
-	8405B	-
-	8405B+	-
-	8405D	-
-	8405D+	-
-	8410B	-
-	8410D	-
-	8411B	-
-	8411D	-
-	8434D	-

The 96xx family and 16xx family of IP phones are not directly referenced in the Branch Gateway CLI. When you administer these phones using the CLI, use the following mapping:

Table 1: Mapping Avaya 96xx and 16xx IP phones for CLI administration

Module name	CLI interface name
1603	4610
1608	4610
1616	4620
9608	46203
9608G	<b>4620</b> 3
9610, FW V2.0 +	4606 <sup>3</sup>
9611G	<b>4620</b> 3
9620, FW V2.0 +	4610 <sup>3</sup>
9621G	46203
9630, FW V2.0 +	4620 <sup>3</sup>
9640, FW V2.0 +	4620 <sup>3</sup>
9641G	46203
9641GS	<b>4620</b> 3
9650, FW V2.0 +	4620 <sup>3</sup>

<sup>&</sup>lt;sup>3</sup> For R4.0, the firmware must be build 26 39 or newer. For R5.0, the firmware must be build 27 27 or newer.

### Call processing functionality in SLS mode

In survivable mode, SLS provides only a limited subset of CM call processing functionality:

- Limited call routing through a Survivable ARS Analysis Table (through the CLI) and COR calling permissions
- Inbound calls are directed in one of three ways:
  - Using the Incoming-Routing screen
  - Using the **Set Incoming-Destination** on the Trunk group screen that enables mapping to a given station
  - Inbound calls are directed to a previously-administered pool of available stations (the **Survivable Trunk Dest?** field is y on the Station screen). The search algorithm is circular so that the incoming calls are fairly distributed.

### Important:

SLS permits 911 calls, but the specific location information is not transmitted to the Public Service Answering Point (PSAP). Only the general trunk-identifying information is transmitted. Emergency personnel will have a general location associated with the trunk (for example, a building address), but nothing more specific (for example, a room or office number). Also, if a 911 call disconnects for any reason, emergency personnel cannot reliably call the originator back. A small business office's address is sufficient from the perspective of emergency routing.

- CM Feature Access Codes for ARS, contact closure, and Hold
- Acts as an H.323 Gatekeeper that enables IP endpoints to register simultaneously
- Direct Inward Dialing
- Multiple call appearances
- Hold and Call Transfer functions
- · Contact closure feature
- Call Detail Recording (CDR)
- Trunk Access Code (TAC) dialing
- Non-ISDN DS1 trunks (with in-band signaling)
- ISDN PRI/BRI trunks:
  - T1 robbed-bit: . All 24 channels serve as trunks without full 64 kbps transmission
  - E1 CAS: . All 31 channels serve as trunks with full 64 kbps transmission

#### Related links

SLS logging activities on page 106

### Call processing functionality not supported by SLS

- Many small business customers employ custom calling features such as call waiting, from the BOC/LEC, attempting a more PBX-like capability. These features are not supported by SLS.
- Non-ISDN signaling:
  - DMI BOS signaling for T1 and E1
  - R2-MFC signaling for E1
- · Calling party name/number information to digital station displays
- Caller ID on outgoing analog station calls
- · Caller ID on incoming analog loop-start trunk calls
- · Three party conferences
- Last Number Redial
- · Call Forwarding-Busy/Don't Answer
- No Music On Hold source or announcement playback
- Call Center features, including ASAI
- Connection Preserving Failover/Failback for Branch Gateways

### **Provisioning data**

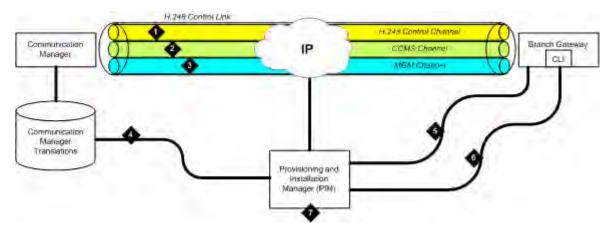
SLS requires that the Branch Gateway has connected to an MGC at least once and has received provisioning information, including:

- CM port information sent through the H.248 control channel:
  - Tone sources, including a distinctly different dial tone to inform users that the system is operating in survivable mode
  - Loss plan
- CM provisioning information for the options in the station and trunk media modules is sent through the CCMS channel
- The provisioning may be entered manually via an SNMP MIB browser or via the local Branch Gateway's CLI interface.

### Note:

The SLS data must be configured manually in the Branch Gateway using the Branch Gateway's CLI interface for SLS administration.

# Standard Local Survivability data sources and communication paths



#### Table 2: Figure notes:

- 1. 248 call signaling and configuration data
- 2. CCMS messages through Clear Channel
- 3. Branch Gateway Maintenance Channel
- 4. SLS MIB delivered to the Branch Gateway through SNMP
- 5. Security codes (passwords) sent over SSH connection to CLI

NOTE: The SLS data must be configured manually in the Branch Gateway.

The required CM translations for SLS include fields on the Station and Branch Gateway screens.

#### **Related links**

Configuring CM for SLS on page 108

### **SLS entry**

When SLS is enabled, the MGC list displays a fifth element called SLS. This element is always past the Transition Point. After the Link Recovery search concludes for the primary MGC list (entries above the Transition Point), it searches the alternate MGC list (entries below the Transition Point), ending with SLS, the last choice for the Branch Gateway.

When the Link Recovery search settles on the SLS entry in the MGC list, the Branch Gateway registers with SLS (resident on the Branch Gateway) for its call control.

SLS transitions between four possible SLS states: Unregistered, Setup, Registered, and Teardown.

### **Unregistered state**

This is the normal state in which SLS waits for an H.248 registration request from the Branch Gateway. When SLS receives the request, it registers the Branch Gateway and transitions to the Setup state.

### Setup state process

In this transitional state, SLS performs the following activities:

- 1. Checks for proper provisioning data. If there is insufficient provisioning, the registration request is denied, and SLS returns to the Unregistered state.
- 2. Initializes SLS components, such as Gatekeeper data (for example, IP endpoint's E.164 addresses and passwords), dial plan, and ARS routing.
- Registers with the Branch Gateway.
- 4. Creates the H.323 Gatekeeper socket after successful registration.

When Setup is complete, SLS transitions to the Registered state.

### Registered state process

SLS can only process calls while it is in the Registered state in which it performs the following:

- 1. Constructs endpoint objects based on board insertion and IP registration.
- 2. Tears down endpoint objects based on board removal and IP unregistration.
- Handles registration requests from H.323 endpoints that properly authenticate by using their extension number as a 'terminal alias', and the password as the registration encryption key.
- 4. Handles stimuli from all interfaces to establish and remove calls.

SLS remains in the Registered state as long as the socket to SLS is open.

### **Teardown state**

SLS transitions to the Teardown state whenever the following events occur:

- The Branch Gateway administrator uses the set sls disable command from the Branch Gateway CLI or manual MIB browser using the SNMP read/write attribute avSurvAdminState.
- The Branch Gateway closes the SLS socket after maintenance determines that it has completed an H.248 registration with the primary MGC.
- SLS determines that it needs to unregister with the Branch Gateway due to internal error conditions.

### **Teardown state process**

1. Tears down endpoint objects.

- 2. Sends unregistration requests to IP endpoints that are not on active calls. IP endpoints lose registration with SLS and display the discovered IP address during re-registration with an MGC.
- 3. Closes the H.323 Gatekeeper socket.

After Teardown is complete, SLS transitions to the Unregistered state and starts searching at the top of the MGC list for a controller.

### **SLS** interaction with specific Branch Gateway features

SLS interacts differently with the various Branch Gateway features.

### **Direct Inward Dialing in SLS mode**

Direct Inward Dialing (DID) is a service offered by telephone companies that enables callers to dial directly into an extension on a switch without the assistance of an operator or automated call attendant.



#### Note:

DID is a method of routing calls that applies to both analog and digital (T1/E1) lines. However, while the method is typically referred to as DID in the analog world, it is usually called Dialed Number Identification Service (DNIS) in the digital world. Despite the difference in names, the concept is the same.

The Branch Gateways support DID central office trunk interfaces, and the digit transmission from the central office is configurable when ordering the service:

Immediate: The DID signaling starts immediately after the central office seizes the analog DID trunk by closing the loop (across tip and ring). In addition, analog DID trunk lines only support inbound calls. For this reason, Customer Premise Equipment (CPE) utilizing DID trunk lines for inbound routing may utilize loop-start lines for outbound transmission.

Wink: The DID signaling starts after the Branch Gateway's analog trunk interface reverses the battery polarity and sends a "wink" to the central office.



### Warning:

An analog two-wire DID trunk line is different from a standard analog loop-start line. With analog DID trunk lines, the battery (power feed) to the line is supplied by the Branch Gateway's analog trunk interface. With a standard loop-start line, the power is supplied by the central office, which is why damage can occur from connecting a loop-start PSTN trunk to the DID port.

The number of sent digits (3 to 4 typically) and signaling type (Pulse/DTMF) are also configurable at ordering time.

### Multiple call appearances in SLS mode

When a Branch Gateway is in SLS mode, three call appearances, each with limitations, are supported:

- The first two call appearances are for incoming or outgoing calls. The first call appearance is the default
- The third call appearance is for outgoing calls only.

### Note:

"First", "second", and "third", refer to the order in which you use call appearances, not the order of the Call Appearance buttons on your phone.

#### Example

For example, User A chooses the third call appearance to dial User B, and then User C calls User A, which is sent to the first call appearance. In this situation, a subsequent inbound call to User A will be denied (busy) because the first and third call appearances are in use, and the second call appearance is only available for outbound calls.

### Hold in SLS mode

Using the Hold feature differs by user and by phone type, and the same is true of the Hold feature in Standard Local Survivability (SLS) mode. Some users return to a call on Hold by pressing the **Call Appearance** button, however, CM has an administrable parameter that allows users to release a call on hold by pressing the **Hold** button a second time (if only one call is held). The Hold feature also works differently in DCP and IP phones and analog phones in the survivable mode.

The Hold feature in SLS does not support:

- · Music on Hold
- Local mute on analog phones
- · Specialized treatment of E-911 calls
- · Call Hold indicator tones

### DCP and IP phones

When a Branch Gateway is in the survivable mode, you can release calls on Hold on all DCP and IP phones by either:

- Pressing the Hold button a second time if only one call is held
- Pressing the held Call Appearance button

### Analog telephones

Newer analog telephones (for example, Avaya 62xx series) have buttons with specific functions for placing a call on Hold:

**Hold button:** A hold function that is local to the telephone

Pressing the Hold button causes the analog station to place a hold bridge in both directions at the telephone set. No signaling notification is sent to the SLS call-engine and, therefore, there is no ability to notify the other party that they have been placed on hold. Pressing the Hold button a second time causes the analog phone to remove the hold bridge and the call path is restored. In essence, this hold operation is equivalent to using the Mute button on station sets.

Flash button: A function that sends a switchhook signal to the server

Switchhook (receiver on/off hook): A function that sends a disconnect signal to the server

### Using the Flash button

#### **Procedure**

1. Press the **Flash** button on the analog phone.

You hear a dial tone; the other party hears nothing.

You can leave the call on Hold or transfer the call. Press the **Flash** button twice to return to the call.

Dial the Feature Access Code (FAC) for Hold.

At this point you can leave the call on Hold or transfer the call.

3. To return to the call, press the **Flash** button again.

The call is re-established.



### ■ Note:

Either party can put the call on Hold or return to the call.

### Using the switchhook button

#### **Procedure**

1. Press the switchhook once.

You hear a dial tone.

2. Dial the FAC for Hold.

This places the call on Hard Hold which prevents you from transferring the call. To return to the call, dial the FAC for Hold.

- 3. Do one of the following:
  - Return to the call by dialing the FAC for Hold.

The call is re-established.

• Dial a third party by dialing the number and flashing the switchhook once (you will hear a stutter dial tone). Dial the FAC for Hold (the second call is now on Hold and the first call is re-established). If you want to toggle between the first and second calls, press the switchhook and dial the FAC for Hold once each time you want to change calls.

Hang up.

Your phone will ring to notify you that you have a call on Hold. When you lift the receiver you will hear a dial tone and can perform any of the activities listed in Step 3.

### Call Transfer in SLS mode

Using the Call Transfer feature differs by user and by phone type. The same is true of the Hold feature in Standard Local Survivability (SLS) mode. Call Transfer also works differently in DCP/IP phones and analog phones in the survivable mode. Some limitations of the Call Transfer feature are:

- The established call must be initiated from a local station (administered on this Branch Gateway) or from an incoming trunk. You can make only point-to-point call transfers to a phone that is local to the same Branch Gateway.
- Does not support E-911 calls
- Does not support the Conference button on any phone
- Does not support trunk-to-trunk transfer (for example, for voice messaging)

### Transferring a call on DCP and IP phones

#### **Procedure**

1. While talking on a call or while you have a call on Hold, press the **Transfer** button on your phone.

You hear a dial tone; the other party hears nothing.

- 2. Dial the third party's number on your phone.
- 3. You can either:
  - · Wait for the third party to answer and announce the call, then either press the Transfer button again or hang up.
  - Transfer the call before the third party answers by pressing the **Transfer** button again.

#### Result

The person you were talking to is transferred to the third party.

A message appears on your phone display to indicate that the call transfer is complete.



If you do not completely dial the string or if you hear a fast-busy or re-order (French siren) tone, only a Hard Hold call connection (if present) remains at the station.

If the third party does not answer, the call does not ring back to the originating party. If a transfer does not complete, the event is logged.

### Transferring an established call from an analog phone

#### About this task

Newer analog phones (for example, Avaya 62xx series) have buttons with specific functions for transferring a call. The switchhook (receiver on/off hook) sends a disconnect signal to the server. and the Transfer/Flash button sends a transfer message to the server.

#### **Procedure**

- 1. While on a call, press the switchhook once or press the **Transfer/Flash** button.
  - You hear a dial tone; the other party hears nothing.
- 2. Dial the third party's number on your phone.
- 3. You can either:
  - Wait for the third party to answer and announce the call, then hang up.
  - Transfer the call before the third party answers by hanging up.

#### Result

The person you were talking to is transferred to the third party.

A message appears on your phone display to indicate that the call transfer is complete. If the necessary call processing resources are not available, the transfer does not complete and the event is logged.



#### 🔀 Note:

Displays are not supported on analog phones unless they are supported locally by an analog phone.

### Using contact closure in SLS mode

### About this task

When the Branch Gateway is in survivable mode, contact closure works as follows:

#### **Procedure**

- 1. Lift the phone receiver and listen for the survivability dial tone.
- 2. Dial the appropriate contact closure FAC (Feature Access Code) open, close, or pulse — on the phone.
  - If you dial an invalid FAC code, then SLS plays an intercept tone and terminates the session.
  - If you dial a valid FAC code, then you will hear a standard dial tone and can proceed to Step 3 on page 104.
- 3. Dial the three-digit Branch Gateway number.
  - If you enter fewer than three digits, then SLS times out and you must restart this procedure from the beginning.

- If the Branch Gateway number matches the local Branch Gateway number, then SLS plays a standard dial tone and you can proceed to Step 4 on page 105.
- If the Branch Gateway number does not match the local Branch Gateway number, SLS plays an intercept tone and terminates the session.
- 4. Dial the contact closure code, for example 1 for contact pair #1, and 2 for contact pair #2.

You hear stutter tone and then silence, confirming these valid codes. If you dial an invalid contact closure number, you hear an intercept tone.

Contact closure feature activations appear in the CDR log.



#### Note:

If the contact closures are set to manual operation, the FAC operation will not work even though the confirmation tone is heard. However, an event will be logged.

#### Related links

Example of CDR log entries and format on page 106

#### Contact closure / SLS feature interactions

- There is no screening to authorize the use of the contact closure feature in SLS mode.
   Security is provided by limiting the number of users who know the correct key sequence required for the contact closure feature.
- You cannot use the Hold or Transfer features while dialing the contact closure FAC key sequence.
- Contact closure will not work until you dial the full digit sequence and it is processed.
- If two users try to simultaneously use contact closure, whoever dials the full FAC key sequence first gets precedence.
- Interdigit timing rules apply to the contact closure feature, so if you pause too long during the FAC key sequence, the feature times out.
- Call appearances are not released (available for calls) until you hang up.
- You cannot use the contact closure feature from outside trunk lines.

#### Related links

Contact closure on page 295

### Administering IP Softphone in SLS mode

#### About this task

The SLS mode supports shared administrative identity with the Avaya Softphone application, but requires specific station administration.

#### **Procedure**

1. Access the CM administrative SAT interface.

- 2. At the SAT interface, enter change station <extension > to display the Station screen.
- 3. Set the **Terminal Type** field to a 46xx IP phone.
- 4. Save the changes.



### Note:

If you administer the Terminal Type field as a DCP phone, shared administrative identity functionality in SLS mode is not supported.

#### Related links

Accessing the registered MGC on page 68

### **SLS logging activities**

SLS exports call-recording data in survivability mode. The Call Detail Record (CDR) log contains detailed information about each outgoing call that uses a trunk. This information can be stored in flash NVRAM or directed to an external server for later processing. It includes data for:

- Merged outgoing Trunk Access Codes (TACs), indicating successfully completed dialing
- Successfully completed ARS calls



### 🔀 Note:

The Syslog information is stored in a memory file that is configured as a FIFO with a length of 50 KB. Once the last entry in the memory is full, the newest log event overwrites the oldest entry. This provides for a storage of 667 call records that may be saved during SLS operation. If you have a Syslog server on a PC connected to the local area network of the branch office, then these Syslog messages can be immediately transported from the Branch Gateway to the Syslog server. This enables the capture period to run for an extended period.

Contact closure

### **Example of CDR log entries and format**

```
Gxxx-SLS(super) # show logging cdr file content
08/23/2015,10:46:35:CDR-Informational: 10:46 00:00 A 700 50029555 52001 v301 08/23/2015,10:45:46:CDR-Informational: 10:45 00:00 A 700 50029 52001 v301
08/23/2015,10:45:14:CDR-Informational: 10:45 00:00 A 700 52 52001 v301
08/23/2015,10:44:35:CDR-Informational: 10:44 00:00 A 700 445200 52001 v301
08/22/2015,13:20:23:CDR-Informational: 13:20 00:00 A 700 50029 52001 v301
08/22/2015,13:20:15:CDR-Informational: 13:20 00:00 A 700 50029 52000 v301 08/22/2015,13:20:05:CDR-Informational: 13:20 00:00 A 700 44 52000 v301
08/22/2015,13:19:59:CDR-Informational: 13:19 00:00 A 700 44500 52000 v301
```

An interpretation of the first entry is:

- **08/23/2015**: is the date of the log entry
- 10:46:35: is the time of the log entry

- CDR-Informational: is the category (to aid sorting)
- 10:46: is the time the call was placed
- **00:00:** is the duration of the call in hours and minutes or **99:99:** if the duration is greater than 99 hours
- A: is the condition code. Possible values are:
  - 7. Outgoing call
  - 9. Incoming call
  - A. Outgoing TAC call or emergency call
  - B. Used for contact closure
- 700: is the FAC or TAC number
- 50029555: is the dialed number
- 52001: is the extension that originated the call
- v301: indicates the port through which the call was routed

### **Example of CDR log with contact closure**

```
Gxxx-SLS(super) # show logging cdr file content 08/23/2015,03:59:24:(0 0 0:15:5)CDR-Informational: Aug 23 03:59 B 15840 PULSE 003 2
```

An interpretation of this entry is:

- Date (08/23/2015) and time (03:59:24) record when the feature was activated
  - **B:** is the condition code. Possible values are:
  - 7. Outgoing call
  - A. Outgoing TAC call or emergency call
  - B. Used for contact closure
- 15840: is the extension that activated the feature
- PULSE: indicates the contact closure operation (could also be OPEN: or CLOSE:)
- 003: is the Branch Gateway number
- 2: is the contact closure number

### **SLS** configuration

### **SLS** configuration rules

SLS is included as part of the resident firmware package that is installed as part of Branch Gateway firmware upgrade. However, for SLS to function correctly, the following conditions must be met:

- CM must be configured for SLS and Auto Fallback.
- Branch Gateway can be manually configured for SLS and Auto Fallback using the CLI.
- SLS must be enabled on Branch Gateway.
- To activate any saved changes within SLS, the disable and enable SLS commands must be used together.

#### Related links

<u>Prerequisites for using the CLI to manually configure SLS administration on the Branch Gateway</u> on page 121

Enabling SLS on page 120

Activating changes in SLS on page 121

### **Configuring CM for SLS**

#### About this task

You must configure CM for SLS using manual CLI entry of SLS administration. Perform the configuration during the initial administration of the host CM server.

#### **Procedure**

- 1. Access the CM administrative SAT interface.
- 2. At the SAT, enter change node-names ip to display the IP Node Names screen.

#### For example:

```
change ip-codec-set-1

IP NODE NAMES

Name

IP Address

Name

IP Address

Name

IP Address

Denver

Gateway1

192.168.1

.200

...

procr

192.168.1

.201

...

(X of X administered node-names were displayed)

Use 'list node-names' command to see all the administered node-names

Use 'change node-names ip xxx' to change a node-name 'xxx' or add a node-name
```

3. In the **Modem** field, type v150mr.

### Note:

Set the name of the Branch Gateway consistently with the **Name** field on the Media Gateway Administration screen in CM (add media-gateway) and with the name used in the set system name command (gateway CLI).

- 4. Type the IP address of the Branch Gateway in the IP Address field.
- 5. Submit the screen.
- 6. At the SAT, enter change system-parameters mg-recovery-rule 1 to display the System Parameters Media Gateway Automatic Recovery Rule screen.
- 7. Type a description of the rule in the **Rule Name** field.
- 8. Set the Migrate H.248 MG to primary field to immediately.

### Note:

The immediately value is only one of the four possible choices. See the *Administrator Guide for Avaya Aura*® *Communication Manager* for more information on the values for this field.

- 9. Submit the screen.
- 10. At the SAT, enter display media-gateway 1 to display the Media Gateway screen.
- 11. Verify the following fields:
  - Name field (20 characters maximum) must match the administered name of the gateway.
  - Max Survivable IP Ext field only appears when the Type field is Gxxx.

The current maximum product limits enforced by the SLS gateway's firmware module is 240.

These limits are enforced due to resource considerations in the given gateway.

### **!** Important:

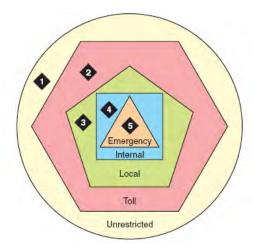
Since the VoIP resources on the Branch Gateway are limited, the **Max Survivable IP Ext** field should not exceed these values.

- 12. At the SAT, enter change station extension to display the Station screen.
- 13. Verify that the following fields are correct:
  - Survivable GK Node Name
  - Survivable COR
  - Survivable Trunk Dest
- 14. Submit the screen.

#### Related links

Accessing the registered MGC on page 68
Configuration of the SLS data through the CLI on page 141

### Inherited Class of Restriction (COR) permissions



COR permissions show the hierarchical relationship among the calling-restriction categories.

#### Table 3: Figure notes:

- 1. **Unrestricted:** Users can dial any valid routable number, except an ARS pattern specifically administered as **deny:** . ETR functionality and calls through the CO are permitted in this class.
- 2. Local: Users can only dial these call types:
  - loci: (public-network local number call)
  - op: (operator)
  - svc: (service)
  - hnpa: (7-digit NANP call)
- 3. Toll: Users can only dial these call types:
  - fnpa: (10-digit NANP call)
  - natl: (non-NANP call)
- 4. **Internal:** Users can only dial other stations within the Branch Gateway and the emergency external number (default)
- 5. **Emergency:** Users can only dial the emergency external number

### Station screen field descriptions for the Branch Gateway

### **Security Code**

The security code required by users for specific system features and functions are as follows:

- Extended User Administration of Redirected Calls
- · Personal Station Access

- Redirection of Calls Coverage Off-Net
- Leave Word Calling
- Extended Call Forwarding
- Station Lock
- · Voice Message Retrieval
- Terminal Self-Administration
- Enterprise Mobility User
- Extension to Cellular
- Call Forwarding
- Posted Messages
- Security Violation Notification
- Demand Printing

The required security code length is administered system wide.

### **Type**

Use this field to specify the telephone type. You must administer the station type for each station that you add to the system.

The following table lists the telephones, virtual telephones, and personal computers that you can administer on Communication Manager. Telephones that are not in the table require an alias to a supported set type.



#### Note:

If Terminal Translation Initialization is enabled, you cannot change the analog telephones administered with hardware to a virtual extension.

Telephone type	Model	Administered as
Single-line analog	500	500
	2500, 2500 with Message Waiting Adjunct	2500
	6210	6210
	6211	6210
	6218	6218
	6219	6218
	6220	6220
	6221	6220
CallerID	Analog telephone with Caller ID	CallrID

Telephone type	Model	Administered as
	7101A, 7102A	7101A
	7103A Programmable and Original	7103A
	7104A	7104A
	8110	8110
	DS1FD	DS1FD
	7302H, 7303H	7303S
	Voice Response Unit (VRU) with C&D tones	VRU
	VRU without C&D tones	2500
Single-line	DS1 device without forward disconnect	ops
DS1/DSO	VRU with forward disconnect without C&D tones	ds1fd or ds1sa
	VRU with forward disconnect without C&D tones	VRUFD or VRUSA
Terminals	510D	510
	515BCT	515
Multi-appearance	7303S	7303S, 7313H
hybrid	7305H	7305S
	7305S	7305S, 7316H, 7317H
	7309H	7309H, 7313H
	7313H	7313H
	7314H	7314H
	7315H	7315H
	7316H	7316H
	7317H	7317H
Multi-appearance	2402	2402
digital	2410	2410
	2420	2420
	6402	6402
	6402D	6402D
	6408	6408
	6408+	6408+
	6408D	6408D
	6408D+	6408D+
	6416D+	6416D+
	6424D+	6424D+

Telephone type	Model	Administered as
	7401D	7401D
	7401+	7401+
	7403D	7403D
	7404D	7404D
	7405D	7405D
	7406D	7406D
	7406+	7406+
	7407D	7407D
	7407+	7407+
	7410D	7410D
	7410+	7410+
	7434D	7434D
	7444D	7444D
	8403B	8403B
	8405B	8405B
	8405B+	8405B+
	8405D	8405D
	8405D+	8405D+
	8410B	8410B
	8410D	8410D
	8411B	8411B
	8411D	8411D
	8434D	8434D
	9404	9404
	9408	9408
	CALLMASTER I	602A1
	CALLMASTER II, III, IV	603A1, 603D1, 603E1, 603F1
	CALLMASTER VI	606A1
	IDT1	7403D
	IDT2	7406D

Telephone type	Model	Administered as
IP Telephone	4601+	4601+
	Note:	
	When you add a new 4601 IP telephone, you must use the 4601+ station type. This station type has the Automatic Callback feature enabled.	
	4602+	4602+
	Note:	
	When you add a new 4602 IP telephone, you must use the 4602+ station type. This station type has the Automatic Callback feature enabled.	
	4606	4606
	4610	4610
	4612	4612
	4620SW IP (G3.5 hardware)	4620
	4621	4621
	4622	4622
	4624	4624
	4625	4625
	4690	4690
	9608	9608
	9610	9610
	9611	9611
	9620	9620
	9621	9621
	9630	9630
	9640	9640
	9641	9641
	9650	9650

Telephone type	Model	Administered as
SIP IP Telephone	4602SIP with SIP firmware	4620SIP
	4610SIP with SIP firmware	
	4620SIP with SIP firmware	
	4620SIP CC (Call Center)	
	SIP Softphone/Avaya one-X Desktop	
	Toshiba SP-1020A	
	Note:	
	You must administer any telephone with SIP firmware used for SIP networking as a 4620SIP, 96xxSIP, or 16CC SIP telephone.	
	* Note:	
	Communication Manager Release 6.2 and later do not support 1616SIP CC and 4620SIP CC telephones.	
	9601SIP	9608SIP
	9620, 9630, 9630G 9640, 9640G with SIP firmware	96xx or 96xxSIP telephone
	9608 with SIP firmware	9608SIP
	9611 with SIP firmware	9611SIP
	9621 with SIP firmware	9621SIP
	9641 with SIP firmware	9641SIP
	9608 with SIP firmware (for call center)	9608SIPCC
	9611 with SIP firmware (for call center)	9611SIPCC
	9621 with SIP firmware (for call center)	9621SIPCC
	9641 with SIP firmware (for call center)	9641SIPCC
H.323 SoftPhone	application Road Warrior	H.323 or DCP type
	Native H.323	H.323
	Singleconnect	H.323 or DCP type
	Any NI-BRI (N1 and N2) telephone	NI-BRI
	7505D	7505D
	7506D	7506D
	7507D	7507D
	8503D	8503D
	8510T	8510T

Telephone type	Model	Administered as
	8520T	8520T
Personal computer	6300/7300	PC
(voice/data)	6538/9	Constellation
Test Line	ATMS	105TL
No hardware assigned at the time of administration.		Use XDID when Communication     Manager assigns a DID number to the station.
administration.		Use XDIDVIP when the administrator later assigns a DID number to the station.
		Use virtual to map the station and other extensions to one physical telephone.
Key telephone system interface	_	K2500
AWOH	any digital set	_
	CTI station	СТІ
CTI	CTI station	CTI
XMOBILE	EC500, DECT, PHS	XMOBILE
ISDN-BRI data module	7500	7500
SBS Extension	SBS test extension (no hardware)	sbs

### **Port**

The Auxiliary and Analog ports assigned to the station are as follows.

Valid Entry	Usage
01 to 64	The first and second numbers are the cabinet numbers.
A to E	The third character is the carrier.
01 to 20	The fourth and fifth characters are the slot numbers. G650 has 14 slots.
01 to 32	The sixth and seventh characters are the port numbers.
x or X	Indicates that there is no hardware associated with the port assignment since the switch was set up, and the administrator expects that the extension has a non-IP set. Or, the extension had a non-IP set, and it dissociated. Use x for Administered WithOut Hardware (AWOH) and Computer Telephony (CTI) stations, as well as for SBS Extensions.
IP	Indicates that there is no hardware associated with the port assignment since the switch was set up, and the administrator expects that the extension would have an IP set. This is automatically entered for certain IP station set types, but you can enter for a DCP set with softphone permissions. This changes to the s00000 type when the set registers.

Valid Entry	Usage
xxxVmpp	Specifies the Branch Gateway.
	xxx is the Branch Gateway number, which is in the range 001 to 250.
	m is the module number, which is in the range 1 to 9.
	• pp is the port number, which is in the range 01 to 32.
Analog Trunk port	Analog trunk port is available with:
	MM711 and MM714 media modules
	TN747 and TN797 circuit packs

#### Survivable GK Node Name

Any valid previously-administered IP node name. Identifies the existence of other H.323 gatekeepers located within gateway products that offer survivable call features. For example, the MultiTech MVPxxx-AV H.323 gateway family and the SLS function within the Branch Gateways. When a valid IP node name is entered into this field, Communication Manager adds the IP address of this gateway to the bottom of the Alternate Gatekeeper List for this IP network region. As H.323 IP stations register with Communication Manager, this list is sent down in the registration confirm message. With this, the IP station can use the IP address of this Survivable Gatekeeper as the call controller of last resort.

If blank, there are no external gatekeeper nodes within a customer's network. This is the default value.

Available only if the station type is an H.323 station for the 46xx or 96xx models.

#### Survivable COR

Sets a level of restriction for stations to be used with the survivable dial plan to limit certain users to only to certain types of calls. You can list the restriction levels in order from the most restrictive to least restrictive. Each level has the calling ability of the ones above it.

Available for all analog and IP station types.

Valid Entries	Usage
emergency	This station can only be used to place emergency calls.
internal	This station can only make intra-switch calls. This is the default.
local	This station can only make calls that are defined as locl, op, svc, or hnpa in the Survivable Gateway Call Controller's routing tables.
toll	This station can place any national toll calls that are defined as fnpa or natl on the Survivable Gateway Call Controller's routing tables.
unrestricted	This station can place a call to any number defined in the Survivable Gateway Call Controller's routing tables. Those strings marked as deny are also denied to these users.

#### **Survivable Trunk Dest**

Designates certain telephones as not being allowed to receive incoming trunk calls when the Branch Gateway is in survivable mode.

Available for all analog and IP station types.

Valid Entry	Usage
у	Allows this station to be an incoming trunk destination while the Branch Gateway is running in survivability mode. This is the default.
n	Prevents this station from receiving incoming trunk calls when in survivable mode.

#### Switchhook Flash

Valid Entry	Usage
У	Allows users to use the switchhook flash function to activate Conference/Transfer/Hold and Call Waiting. Required for H.323 station types.
n	Disables the flash function so that when the switchhook is pressed while active on a call, the call drops. Requires that Call Waiting Indication is disabled.

### **Expansion Module**

Indicates whether or not this telephone has an expansion module. Enables the administration of the buttons for the expansion module.

#### Name

The name of the person associated with this telephone or data module. The system uses this value to create the system directory.

### Note:

This field is supported by Unicode language display for the 4610SW,4620SW, 4621SW, and 4622SW telephones.

For more information on Unicode language display, see *Administering Avaya Aura*® *Communication Manager*.

### Note:

In the display for emergency notification when completing the **Name** field, fill the most important identifying information at the beginning of the field. When an emergency call is made and a crisis alert station with a 27-character display is notified, only 17 characters of the **Name** field appear on the first display line, followed by the extension. The second line contains the last three characters of the **Name** field, followed by the word EMERGENCY. Characters 18 through 24 of the **Name** field are not displayed at all.

### **SLS ARS Entry page field descriptions**

Use the following fields on the SLS ARS Entry page to administer an Automatic Route Selection in SLS.

### **Dialed String**

Communication Manager matches the dialed numbers with the entry in the **Dialed String** field that most closely matches the dialed number. You can enter up to 18 digits that the call-processing server analyzes. You can also enter the wildcard characters, x and X.

#### Min

Use this field to specify the minimum number of user-dialed digits that the system must collect to match the dialed string.

#### Max

Use this field to specify the maximum number of user-dialed digits that the system must collect to match the dialed string.

#### Del

Use this field to enter the number of digits that the system must delete from the starting of the dialed string.

### **Replacement String**

Use this field to specify the digit string that must replace the deleted portion of the dialed number.

Valid entry	Usage
blank	To delete the digits without replacement.
0 to 9, *	To type the digit string.
	The digit string can have up to 18 characters.
#	To indicate the end of dialing.

### Call Type (ARS only)

Use this field to enter the call type associated with each dialed string.

Valid entry	Usage	China Number 1, Call Type
intl	Use this option for public-network international calls.	toll-auto
alrt	Use this option to alert attendant consoles or other digital telephones when a user places an emergency call.	normal
emer	Use this option for emergency calls.	normal

Valid entry	Usage	China Number 1, Call Type
fnpa	Use this option for ten-digit North American Numbering Plan (NANP) calls.	attendant
hpna	Use this option for seven-digit NANP calls.	normal
lop	Use this option for international operator calls.	attendant
locl	Use this option for public-network local calls.	normal
lpvt	Use this option local private calls.	normal
natl	Use this option for non-NANP calls.	normal
npvt	Use this option for national private calls.	normal
nsvc	Use this option for national service calls.	normal
ор	Use this option for operator calls.	attendant
pubu	Use this option for public-network number (E.164)-unknown calls.	normal
svcl	Use this option for national(2) calls.	toll-auto
svct	Use this option for national(2) calls.	normal
svfl	Use this option for service call first party control calls.	toll
svft	Use this option for service call first party control calls.	local

### **Trunk Group**

Valid Entry	Usage
1 to 2000	Trunk-group number selected from the drop-down choices of trunk groups found in the SLS extract from the controlling CM server.

### **Permit / Deny**

Indicates whether the call should be permitted or denied.

### **Enabling SLS**

#### **Procedure**

To enable SLS on the Branch Gateway, enter set sls enable



If you enable SLS and then performed additional administration, you must first disable SLS and then re-enable it. This causes the SLS application to resynchronize its administrative database with the Branch Gateway's global CLI command database.

The Branch Gateway responds with the message, Survivable Call Engine is enabled.

### **Disabling SLS**

#### **Procedure**

To disable SLS on the Branch Gateway, enter set sls disable

The Branch Gateway responds with the message Survivable Call Engine is disabled.

### **Activating changes in SLS**

#### About this task

To activate changes you make in SLS, use the disable and enable SLS commands together. To activate changes in SLS, perform the following steps:

#### **Procedure**

- 1. Make any changes to SLS administration desired.
- 2. While still in SLS mode, enter set sls disable

The Branch Gateway responds with the message Survivable Call Engine is disabled.

3. Enter set sls enable

The Branch Gateway responds with the message Survivable Call Engine is enabled.

# Prerequisites for using the CLI to manually configure SLS administration on the Branch Gateway

Before configuring SLS administration on the Branch Gateway, ensure that:

- CM Release 6.3 or later is running on the host server
- · The Branch Gateway is registered with CM
- The SLS is enabled on the Branch Gateway through its CLI
- S8300 is not serving as a Survivable Remote Server
- Branch Gateway is not subtending to another external server (including Survivable Core Server or another Survivable Remote Server in another gateway)

### Note:

Do *not* run two SLS data update sessions concurrently. The SLS data can be administered locally using CLI or a SNMP MIB browser. This can cause a situation where one administrator can unknowingly undo the work of the other. For example, if a local administrator enters trunk-group context just before a remote administrator performs a SNMP write operation to change a trunk-group parameter, that parameter will be overwritten with the current CLI values when the local administrator exits the trunk-group context.

### **SLS** data set preparation

It is recommended to plan the SLS coverage and gather information from CM before creating the SLS administration data set at the Branch Gateway command line. Strategic selection of the stations and trunks that participate in SLS can ensure that vital communications are spared interruptions caused by network outages.

### **!** Important:

Since you can administer your system for SLS either from the SAT or from the Branch Gateway CLI, the two administration tasks must be synchronized with common data and port usage as well as system-defined capacities. For example, if a physical DCP station port number 10 is not administered on the CM server, even though the Branch Gateway's SLS engine has that port administered, the port is unusable during SLS operation on the Branch Gateway. This is because the hardware port configuration on the media modules is initially configured by CM in subtending gateway mode, by using the H.248 control channel to push information down to the Branch Gateway.

### SLS capacities

The maximum number of legacy stations and trunks that can be supported is dependent upon the slot-module configuration of what is installed.

Branch Gateway model	IP stations
G450 <sup>4</sup>	240

You can collect the CM data using the CM administrative SAT interface.

#### Related links

Accessing the registered MGC on page 68

### Collecting analog stations data

#### **Procedure**

- 1. At the SAT, enter list media-gateway to display a list of administered gateways.
- 2. Look for supported gateways in the **Type** field.
- 3. Once you know the Branch Gateway of interest, match the Branch Gateway model with the analog station ports.
  - MM711
  - MM714
  - MM716
- 4. At the SAT, enter display port port-number, where port-number is the analog station port on the Branch Gateway.

The system displays the extension number assigned to the port.

<sup>&</sup>lt;sup>4</sup> 340 stations maximum (all types)

- 5. Once you know the extension, enter **display station** *extension* to display the Station screen for this extension.
- 6. Gather the necessary information for the following fields:
  - Extension
  - Port
  - Type Only 2500 is the accepted Type
  - Survivable COR
  - Survivable Trunk Dest
  - Switchhook Flash
  - Name

#### **Related links**

Station screen field descriptions for the Branch Gateway on page 110

### **Collecting DCP stations data**

#### **Procedure**

- 1. At the SAT, enter list media-gateway to display a list of administered gateways.
- 2. Look for supported gateways in the **Type** field.
- 3. When you know the Branch Gateway of interest, match the gateway model with the digital station ports:
  - MM712
  - MM717
- 4. At the SAT, enter display port port-number, where port-number is the DCP station port on the gateway.

The system displays the extension number assigned to the port.

- 5. to display the Station screen for this extension, type display station extension.
- 6. Gather the necessary information for the following fields:
  - Extension
  - Port
  - · Security Code

(Optional) - used for the registration of an IP Softphone (RoadWarrior)

- Type as any of the following types:
  - 2402
  - 2410
  - 2420

- 6402
- 6402D
- 6408
- 6408+
- 6408D
- 6408D+
- 6416D+
- 6424D+
- 8403B
- 8405B
- 8405B+
- 8405D
- 8405D+
- 8410B
- 8410D
- 8411B
- 8411D
- 8434D
- Survivable COR
- Survivable Trunk Dest
- Expansion Module
- Name

For more information about these fields, see Station screen field descriptions for the branch gateway.

### **Collecting IP stations data**

#### **Procedure**

- 1. At the SAT, enter list media-gateway to display a list of administered gateways.
- 2. Look for supported gateways in the **Type** field.
- 3. Enter display media-gateway.
- 4. Read the reported IP address for this gateway.
- 5. Enter list node-name and compare the IP address of the Branch Gateway in the list with the IP address of the gateway that you are administering for SLS.

When you find a match in the node-name screen, read the assigned node-name. This will be used to do a pattern match with a field on the IP Station screen in Step 6 on page 125.

6. Enter list station type type, where type is one of the supported IP stations.

The report lists all IP phones that could have the **Survivable GK Node-Name** administered to the target media gateway. The **Survivable GK Node-Name** uniquely associates an IP phone with a particular Branch Gateway.

- 7. Once a match is made between the station screen's **Survivable GK Node-Name** and the target gateway's **Node-Name**, gather the values for the given IP station per:
  - Extension
  - · Security Code

(IP only) - used for the registration of the IP endpoint

- Type as any of the following types:
  - 4601
  - 4602
  - 4602SW
  - 4606
  - 4610SW
  - 4612
  - 4620
  - 4620SW
  - 4621
  - 4622
  - 4624
  - 4625
- Survivable COR
- Survivable Trunk Dest
- Expansion Module
- Name

#### Related links

Station screen field descriptions for the Branch Gateway on page 110

### Collecting trunk groups data

#### **Procedure**

1. At the SAT, enter list media-gateway to display a list of administered gateways.

- 2. Look for supported gateways in the **Type** field.
- 3. At the SAT, enter display media gateway to view the media modules that are assigned to the various slots.

Use the table in <u>SLS group type assignments</u> on page 158 as a reference to identify how the particular media module has been configured for serving as a trunk port, and then use the various list commands on CM to look for physical port matches in the various trunk SAT forms in order to discover what translation information is needed.

- 4. Identify the analog trunk ports.
- 5. Identify the BRI trunk ports.
- 6. Identify the digital DS1 trunk ports.
- 7. Identify the Branch Gateway modules and check for provisioned trunk ports.
- 8. At the SAT, enter **display port** *portid*, where *portid* is the trunks port on the target gateway.

The system reports the Trunk Group Number/Member Number for this particular port.

- 9. Once you know the Trunk Group Number, gather trunk-group information for the following fields:
  - Group Type
  - · Outgoing Dial Type
  - Trunk Group Number
  - TAC
  - Port
  - Digit Treatment
  - Digits
  - Trunk Type
  - Group Name
  - Codeset to Send Display
  - Codeset to Sent National IEs
  - Outgoing Channel ID Encoding
  - Digit Handling (in/out)
  - Network (Japan) Needs Connect Before Disconnect
  - Send Name
  - Send Calling Number
  - Incoming Calling Number Format
  - Incoming Destination

- Trunk Hunt
- Sig Grp

#### **Related links**

Module-port values in SLS trunk-group context for analog trunks on page 159 Trunk port values in SLS trunk-group context for digital trunks on page 159

### **Trunk Group screen field descriptions**

Name	Description
Group Type	This field specifies the type of trunks associated with this trunk group
Outgoing Dial Type	The only acceptable values are tone and rotary. If the field is set to automatic or mf, then the value of tone is used instead. Note that this does not apply to DS1 PRI links.
Trunk Group Number	This value is used in the routing table
TAC	This value is only necessary if the <b>Dial Access?</b> field is set to y. If that field is set to n, the TAC value is not pushed down to the media gateway.
Port	There may be more than one port within a trunk group definition that pertains to a given media gateway
Digit Treatment	This only applies for DID analog trunks or for DS1 tie trunks. Note that this does not apply to DS1 PRI tie trunks.
Digits	This field contains a value only when the <b>Digit Treatment</b> field is set to insert1, insert2, insert3, or insert4

Name	Description
Trunk Type	Depends on trunk signaling type:
	Analog trunks:
	- Loop-start
	- Ground-start
	- DID
	In-Band DS1 trunks with CO Group-Type:
	- Loop-start
	- Ground-start
	In-Band DS1 trunks with Tie Group-Type:
	- Wink/wink
	- Wink/immediate
	- Wink/auto
	- Immediate/Immediate
	- Auto/auto
	- Auto/wink
Group Name	Customer identification of trunk group
Codeset to Send Display	Describes which Q.931 code-sets are allowed to send Display IEs
Codeset to Send National IEs	Describes which Q.931 code-sets are allowed to send National supported IEs
Outgoing Channel ID Encoding	Used for encoding Channel ID IE
Digit Handling (in/out)	Defines overlap receiving and transmitting rules
Network (Japan) Needs Connect Before Disconnect	Sends a CONNECT message before sending a DISCONNECT message, if enabled
Send Name	Specifies whether the Group Name is to be specified with the message sent while connecting to the network
Send Calling Number	Specifies whether the Trunk Group Number is to be specified with the message sent while connecting to the network
Incoming Calling Number - Format	Specifies how to fill the Calling Party Number and Called Party Number IEs
Incoming Destination	Sets a destination station for routing incoming trunk group calls
Trunk Hunt	Determines the method in which the survivable-call- engine selects an available trunk from the trunk group pool

Name	Description
Sig Grp	Specifies the Signaling Group Number that is the manager of this ISDN trunk member

### **Collecting DS1 trunks data**

#### **Procedure**

- 1. At the SAT, enter display ds1 location to display the DS1 administration for a particular circuit pack location.
- 2. Gather the following DS1 information for each DS1 facility:
  - Name
  - Bit-Rate
  - · Signaling Mode
  - Channel Numbering
  - Connect
  - Interface
  - Side
  - Country Protocol
  - Protocol Version
  - DCP/Analog Bearer Capability
  - Interface Companding
  - ITN-C7 Long Timers
- 3. Repeat the display ds1 location command and press Enter for each circuit pack that you want to include in the SLS data set.

### DS1 circuit pack field descriptions

#### Name

Assigns a significant, descriptive name to the DS1 link. Use the vendor's circuit ID for the link in this field because that information helps troubleshoot problems with the link. This field can also be used to indicate the function or the destination of this DS1 facility. Accepts up to 15 characters.



Avaya BRI deskphones support only ASCII characters because non-ASCII characters, such as Eurofont and Kanafont, show up incorrectly.

#### **Bit Rate**



#### Note:

TN464C and later release circuit packs have an option switch that must be set to match this Bit Rate value.

Valid Entry	Usage
1.544	The maximum transmission rate for DS1 circuit packs that support T-1 service.
2.048	The maximum transmission rate for DS1 circuit packs that support E-1 service.

### **Signaling Mode**

Selects the signaling method used for the DS1 link. This mode must match the method used by the network services provider.

Valid Entry	Usage
CAS	Channel Associated Signaling. Out-of band signaling with E1 service. This setting yields 30 64-kbps B-channels for voice or data transmission. Channel 0 is used for framing while channel 16 carries signaling. Used for Enterprise Mobility User (EMU)/ EC500 administration.
robbed-bit	In-band signaling with T1 service. This setting yields 24 56-kbps B-channels for voice transmission.
isdn-pri	Either T1 or E1 ISDN service. This setting supports both Facility Associated Signaling and Non-Facility Associated Signaling.
isdn-ext	Either T1 or E1 ISDN service. This setting supports only Non-Facility Associated Signaling.
	* Note:
	NFAS is primarily a feature for ISDN-T1 connections offered by service providers in North America and Hong Kong. However, it can also be used on private-network connections, and in that context it is possible to set up NFAS using ISDN-E1 interfaces.
common-chan	Out-of-band signaling with T1 service. This setting yields 23 64-kbps B-channels for voice or data transmission. Channel 24 is used for signaling.

### **Channel Numbering**

The ETSI and ISO QSIG specifications require that B-channels on an E1 be encoded as 1 to 30 in the Channel ID IE. Prior to the existence of this field, Communication Manager only used this scheme for Country Protocols 2a (Australia) and 13a (Germany 1TR6). Available only with ISDN-PRI signaling on a private network. The interface must be peer master or peer slave.

#### 2.048 bit rate options:

- timeslot
- sequential

If Communication Manager is connected via QSIG trunks to a switch or server supporting the ETSI QSIG or ISO QSIG specifications, this field must be sequential.

#### Connect

To control communications at layers 2 and 3 of the ISDN-PRI protocol, this field to specifies what is on the far end of this DS1 link.

Available only for ISDN-PRI signaling.

Valid Entry	Usage
pbx	The DS1 link is connected to another switch in a private network.
line-side	Communication Manager is acting as the network side of an ISDN-PRI interface. Used to connect to Roll About Video equipment.
network	The DS1 link connects Communication Manager to a local telephone company central office or any other public network switch.
host	The DS1 link connects Communication Manager to a computer.

#### Interface

Controls how the server negotiates glare with the far-end switch. The servers at either end of the DS1 link must have complementary settings in this field. Otherwise, the D-channel cannot function. For example, if the Avaya S8XXX server at one end of the link is administered as network, the other end must be administered as user. Available only when this DS1 link is providing an ISDN-PRI connection in a private network.

### Private network applications in the U.S.

Valid Entry	Usage
network	The server overrides the other end when glare occurs, and when connecting the server to a host computer.
user	The server releases the contested circuit and looks for another when glare occurs, and when connecting the server to a public network.

#### Private network applications outside the U.S.

Valid Entry	Usage
peer-master	The switch overrides the other end when glare occurs.
peer-slave	The switch releases the contested circuit and looks for another when glare occurs.

#### Side

Use this field to control how Communication Manager must resolve glare at layer 3 over an ISDN-PRI link in QSIG private networks. The system displays this field only if the **Interface** type is peer-master or peer-slave.



#### Caution:

You must correctly pair with the administration of the far-end server. If the far-end server is administered as the b side, you must set the Side field to a, regardless of whether the layer 2 is peer-master or peer-slave, and vice versa.

Valid entry	Usage
а	The <b>Interface</b> is peer-master. Communication Manager overrides the far-end when glare occurs.
b	The <b>Interface</b> is peer-slave. Communication Manager releases the contested circuit and looks for another when glare occurs.

### **Country Protocol**

The country protocol used by the far-end server. For connections to a public network, your network service provider can tell you which country protocol they are using.

Available only with ISDN-PRI and CAS signaling.

Valid Entry	Usage
1 to 25	The country protocol used by the local telephone company central office at which this link terminates.
etsi	The network service provider uses the European Telecommunications Standards Institute (ETSI) protocol and the <b>Signaling Mode</b> is isdn-pri.

#### **Protocol Version**

Available only when:

- The Signaling Mode is isdn-pri and the Connect type is network.
- The **Signaling Mode** is isdn-pri, the **Connect** type is pbx, and the **Interface** type is user or network.

Valid Entry	Usage
a, b, c, d	Selects the protocol that matches the network service provider's protocol in countries whose public networks allow multiple layer-3 signaling protocols for ISDN-PRI service. Contact the network service provider to verify that the protocols match.



#### Warning:

The AT&T Switched Network Protocol prohibits restricted displays of connected numbers. Display problems occur if you administer the 1a country-protocol/ protocol-version combination on the DS1 screen and administer the ISDN-PRI Trunk Group to restrict sending the connected number.

### **DCP/ANALOG Bearer Capability**

Sets the information transfer capability in a bearer capability IE of a setup message to speech or 3.1kHz. Available only with the ISDN-PRI **Signaling Mode**.

Valid Entry	Usage
3.1kHz	Provides 3.1 kHz audio encoding in the information transfer capability.
speech	Provides speech encoding in the information transfer capability.

#### Interface

Controls how the server negotiates glare with the far-end switch. The servers at either end of the DS1 link must have complementary settings in this field. Otherwise, the D-channel cannot function. For example, if the Avaya S8XXX server at one end of the link is administered as network, the other end must be administered as user. Available only when this DS1 link is providing an ISDN-PRI connection in a private network.

#### Private network applications in the U.S.

Valid Entry	Usage
network	The server overrides the other end when glare occurs, and when connecting the server to a host computer.
user	The server releases the contested circuit and looks for another when glare occurs, and when connecting the server to a public network.

#### Private network applications outside the U.S.

Valid Entry	Usage
peer-master	The switch overrides the other end when glare occurs.
peer-slave	The switch releases the contested circuit and looks for another when glare occurs.

### **ITN-C7 Long Timers**

Controls the T302 and T303 timers.

Available only if the **Signaling Mode** is isdn-pri.

Valid Entry	Usage
у	Increases the length of the long timers.
n	Uses the default long timers.

### Collecting signaling groups data

- 1. Collect the following information from the Communication Manager Signaling Group screen for ISDN-PRI administration only:
  - · Trunk Group for Channel Selection
  - Associated Signaling
  - · Primary D-channel
  - · Trunk Board
  - · Interface Id

### **Signaling Group field descriptions**

### **Trunk Group for Channel Selection**

Available only if **Group Type** is atm, h.323, or isdn-pri.

Valid Entry	Usage
1 to 2000	Trunk group number used for channel selection.

### **Associated Signaling**

Available only if **Group Type** field is isdn-pri.

Valid Entry	Usage
у	Enables associated signaling.
n	Enables non-facility associated signaling.

### **Primary D-channel**

Specifies the gateway port ID where the D-channel is located. For the gateways, the first component is the three digit gateway number, followed by a 'v', the slot number, and 24 (T1) or 16 (E1).

#### **Trunk Board**

This is needed only if the Associated Signaling is set to no . This does not apply to SLS on the G250. Specifies the gateway port ID where the D-channel is located. For the gateways, the first component is the three digit gateway number, followed by a "v", and one numeric character for the slot number.

#### Interface Id

Needed only if the Associated Signaling is set to no. Specifies the channel of the DS1 circuit that carries the D-channel for ISDN signaling. This is an integer from 0 through 31.

### Collecting administered ISDN-BRI trunks data

#### **Procedure**

- 1. At the SAT, enter display bri-trunk-board location to display the DS1 administration for a particular circuit pack location.
- 2. Gather the following ISDN-BRI administration information for each location:
  - Name
  - Interface
  - Side
  - · Country Protocol

- DCP/Analog Bearer Capability
- · Companding Mode
- TEI
- · Directory Number A
- Directory Number B
- SPID-A
- SPID-B
- Endpt Init
- · Layer 1 Stable

### **ISDN-BRI Trunk field descriptions**

#### Name

The name used to identify the circuit pack. Accepts up to 15 alphanumeric characters.



Avaya BRI deskphones support only ASCII characters because non-ASCII characters, such as Eurofont and Kanafont, show up incorrectly.

#### **ISDN-BRI Trunk/Interface**

Determines glare handling.

#### ISDN-BRI Trunk/Side

QSIG glare handling, when Interface is peerSlave.

### **ISDN-BRI Trunk/Country Protocol**

Specifies the Layer 3 signaling protocol used by the country-specific service provider.

### ISDN-BRI Trunk/DCP/Analog Bearer Capability

Sets the Information Transfer capability in the Bearer Capability IE of the SETUP message.

### **Companding Mode**

Specifies the companding mode used by the far end switch.

#### TEI

LAPD address assignment for the TEI field.

### **Directory Number**

The directory numbers assigned to the interface and allocated to two separate endpoints. This field must be administered in pairs. Accepts up to 10 characters.

#### **SPID**

The Service Profile Identifier (SPID) expected by the far end. Accepts up to 12 characters. Communication Manager prevents changing this field unless the port is busied out or unadministered. The only protocol supported for SPID initialization is Country Code 1. Trunks are not put in service if SPID installation is unsuccessful. Leading zeroes are significant and must not be ignored.

### **Endpt Init**

Indicates whether the far end supports endpoint initialization. Communication Manager blocks you from changing this field unless the port is busied out or unadministered.

Valid Entry	Usage
У	Requires that an <b>SPID</b> be administered.
n	Requires that an SPID and Endpt ID not be administered.

### Layer 1 Stable

The system displays the field only if you set the **Termination Type** field to TE.

Valid Entry	Usage
у	The far-end network is stable at Layer 1.
n	The far-end network can drop Layer 1 after a call is completed and near-end ignores the Layer 1 disconnect message.

### **Collecting Feature Access Codes data**

#### **Procedure**

- 1. At the SAT, enter display system-parameters customer-options to display the Customer Options screen.
- 2. Scroll to page 5 and determine how the **Multinational Locations** or **Multiple Locations** fields are set:
  - If either of these fields is set to y (enabled), then proceed to Step 3 on page 137.
  - If these fields are set to n (disabled), at the SAT, enter display feature-access-codes and gather the following FAC information:
    - Contact Closure Open Code
    - Contact Closure Close Code
    - Contact Closure Pulse Code

- Auto Route Selection (ARS) Access Code1
- Auto Route Selection (ARS) Access Code2
- ARS FAC
- CAS Remote Hold/ Answer Hold-Unhold Access Code
- 3. Look up the location of the gateway, as follows:
  - a. At the SAT, enter list media-gateway to get the gateway's number.
  - b. At the SAT, enter display media gateway number, where number is the gateway number you obtained in Step a on page 137.

This provides you with the location field value.

- If the gateway has an administered location, at the SAT, enter display locations number, where number is the administered location number. If there is an ARS entry for the given location, you must use this value exclusively in the SLS data set.
- If there is no administered location, at the SAT, enter display feature—access—codes and gather the FAC information listed in Step 2 on page 136.

### **Feature Access Code field descriptions**

### **Contact Closure Open Code**

FAC used to open a contact closure relay. Contact closures control electrical devices remotely. Users use an FAC to activate electrical devices such as electrical door locks. If **Contact Closure Close Code** is administered, then **Contact Closure Open Code** must also be administered.

This value must conform to the FACs or dial access codes defined by the dial plan.

#### **Contact Closure Close Code**

FAC used to close a contact closure relay. Contact closures control electrical devices remotely. Users use an FAC to activate electrical devices such as electrical door locks. If **Contact Closure Open Code** is administered, then **Contact Closure Close Code** must also be administered.

This value must conform to the FACs or dial access codes defined by the dial plan.

#### Contact Closure Pulse Code

FAC used to pulse a contact closure relay.

This value must conform to the FACs or dial access codes defined by the dial plan.

### **Auto Route Selection (ARS) Access Code 1**

FAC used to access ARS. The system can automatically choose the least-expensive way to send a toll call. You can have one ARS access code for local and one for long distance, and route accordingly.

This value must conform to the FACs or dial access codes defined by the dial plan.

### Auto Route Selection (ARS) Access Code 2

Additional FAC used to access ARS.

This value must conform to the FACs or dial access codes defined by the dial plan.

#### **ARS FAC**

This is used instead of the Features screen ARS FAC entry if the Loc No. that correlates to the gateway has an entry in this screen that overrides the general ARS FAC(s).

#### CAS Remote Hold/Answer Hold-Unhold Access Code

FAC used by a Centralized Attendant Service (CAS) attendant to place calls on hold and answer calls held at a remote server running Communication Manager. This FAC can also be used by an analog station. Flashing the switch-hook for the proper interval (between 200 and 1000 ms) while talking on an existing call causes the existing call to be placed on soft hold, using which the analog user can dial the Answer Hold-Unhold FAC to Hard hold the call.

This value must conform to the FACs or dial access codes defined by the dial plan.

### **Collecting system parameters data**

#### **Procedure**

- 1. At the SAT, enter list media-gateway to display a list of administered gateways.
- 2. Look for supported gateways in the **Type** field.
- 3. Once you have determined the media gateway of interest, note its IP-Network-Region.
- 4. At the SAT, enter display ip-network-region *n*, where *n* is the gateway's administered IP-Network-Region.
  - Read the **Codec-set** field value from the IP Network Region screen.
- 5. At the SAT, enter display ip-codec-set n, where n is the **Codec-set** field value from the IP Network Region screen.
  - The report lists the supported codes in the **Audio Codec** field.
- 6. At the SAT, enter display system-parameters features to display the Feature Related System Parameters screen.
- 7. Scroll to page 10 and read the value of the **Date Format on Terminals** field.
- 8. At the SAT, enter **display media-gateway** *n*, where *n* is the administered number of the Media Gateway of interest, to display the Media Gateway screen.
- 9. Read the Max Survivable IP Ext field value.

### **Codecs supported in SLS**

There can be up to seven distinct codec-sets in use in the system. However, only one codec set is active for the network region in which the gateway is located.

SLS only supports two codecs:

- G.711 A-law
- G.711 U-law

### **General system parameters field descriptions**

For information about the fields on the IP codec set screen, see Avaya Aura<sup>®</sup> Communication Manager Screen Reference.

#### **Date Format on Terminals**

Applies to 64xx and 24xx DCP terminals, and to 46xx IP terminals.

#### Max Survivable IP Ext

This field describes the maximum IP phone registrations allowed.

### Collecting ARS dial patterns data

#### About this task

To gather the route patterns and ARS analysis in CM, you must first know which trunk groups are assigned to the gateway of interest. After verifying this information, perform the following steps:

#### **Procedure**

- 1. At the SAT, enter list route-pattern trunk-group *n*, where *n* is an administered trunk group, to display the administered route patterns.
- 2. For the first preference for this route-pattern entry, read the values of the following fields:
  - No Deleted Digits
  - Inserted Digits
- 3. At the SAT, enter list ars analysis to search the ARS Analysis table for row entries whose **Route Pattern** field matches the route-pattern values that were obtained in Step 1 on page 139. Once you discover a match with **Route Pattern**, use the entries from this row in the ARS Analysis table to complete the following three entries for the SLS Dial-Pattern table:
  - Min
  - Max
  - · Dialed String

### **ARS Dial Patterns field descriptions**

### No Deleted Digits

Specifies the number of dialed digits to be deleted from the beginning of the dialed string. The default is 0.

### **General system parameters/Inserted Digits**

Specifies the digit string to be inserted at the beginning of the dialed string. The default is blank.

#### Min

Use this field to specify the minimum number of user-dialed digits that the system must collect to match the dialed string.

#### Max

Use this field to specify the maximum number of user-dialed digits that the system must collect to match the dialed string.

### **Dialed String**

Communication Manager matches the dialed numbers with the entry in the **Dialed String** field that most closely matches the dialed number. You can enter up to 18 digits that the call-processing server analyzes. You can also enter the wildcard characters, x and x.

### **Collecting Incoming Call Handling data**

#### About this task

To gather the Incoming Call Handling Treatment and ARS Digit Conversion information in CM, you must first know which trunk groups are assigned to the gateway of interest. After verifying this information, perform the following steps:

#### **Procedure**

- 1. At the SAT, enter display inc-call-handling-trmt trunk-group n, where n is an administered trunk group.
- 2. For each entry, read the values of the following fields:
  - Called Number
  - · Called Len
  - Del
  - Insert

## Incoming call handling data field descriptions

#### **Called Number**

Valid Entry	Usage
1 to 16	Specifies the leading digits received for an incoming call.
blank	Matches any number associated with the specified service or feature.

#### Called Len

Valid Entry	Usage
0 to 21	The number of digits received for an incoming call. Zero is used when the Public Switched Telephone Network (PSTN) provider does not provide any "Number Digits" within the received <b>Called Party IE</b> , such as in Japan.
blank	When <b>Called Number</b> has also been set to blank, so that any length of digits associated with the <b>Called Party IE</b> of the Incoming SETUP message matches this field.

#### Del

Valid Entry	Usage
1 to 21	The number of leading digits to be deleted from the incoming Called Party Number.
blank	Calls of a particular type can be administered to be routed to a single destination by deleting all incoming digits and then administering the <b>Insert</b> field with the required extension.

#### Insert

Valid Entry	Usage
1 to 16	The number of digits prepended to the front of the remaining digits after any
*	optional digit deletions have been performed. The resultant number formed from digit deletion and insertion is used to route the call, provided night service is not in
#	effect.

### Configuration of the SLS data through the CLI

The command line interface (CLI) has a root-level context of sls for administering the SLS data set. After you enter sls at the CLI prompt, the prompt changes to indicate that you are in the sls context. Once in this context, seven additional sub-contexts provide for station and trunk administration, minimizing the need to type in a long command string:

- station context that is invoked by entering station <extension ><class> to enter a second-level sub-context for administering stations
- trunk-group context that is invoked by entering trunk-group <tgnum><group-type> to enter the second-level sub-context for administering trunk groups
- ds1 context that is invoked by entering ds1 <port-address> to enter the second-level subcontext for administering DS1 trunks
- sig-group context that is invoked by entering sig-group <sgnum> to enter the second-level sub-context for administering signaling groups

- bri context that is invoked by entering bri <port-address> to enter the second-level subcontext for administering ISDN BRI links
- dial-pattern context that is invoked by entering dial-pattern <dialed-string> to enter the second-level sub-context for administering dial pattern strings
- incoming-routing context that is invoked by entering incoming-routing routing <tgnum> <mode>
  cpattern —length> to enter the second-level sub-context for administering incoming routing

Enter exit to leave the second-level sub-contexts and return to the (super-sls)# context.

### Note:

Review <u>Summary of SLS configuration commands</u> on page 163 in its entirety before proceeding with SLS administration. This summary of SLS commands guides you in understanding the various sub-commands of each sub-context.

## Creating the SLS administration data set on the Branch Gateway

- 1. Log on to the Branch Gateway.
- 2. To administer the name, enter set system name <name>, where <name> is typed inside quotation marks ("").

To remove the administered name, enter set system name, and then rename the Branch Gateway using the set system name < name > command.

### Note:

Branch Gateway administered name must match the name in the CM administration.

- 3. At Branch Gateway command prompt, enter sls to begin entering SLS data.
  - The command line prompt changes to (super-sls)# to indicate that you are in SLS data entry mode. Entering exit ends the SLS data entry mode session, and the command line prompt returns to its original state.
- 4. If you want to change the maximum allowable IP registrations from the default, enter set max-ip-registrations *n*, where *n* is from 1 to 240.
- 5. Use the set date-format command to set a date format for the SLS data set.
- 6. Use the set ip-codec-set command to select the country-specific G.711 codec set within the SLS data set: g.711mu or g.711a.
- 7. Administer the slot configuration information by entering set slot-config <slot-number> <box> <box> <box> <box> down the slot where the Media Module is located and <box> <box> down the slot where the Media Module type.
- 8. Administer the station information.
- 9. Administer DS1 trunks as required.
- 10. Administer BRI links as required.

11. Administer the trunk groups.

Note that you can add members to the trunk group only after you administer the signaling group information.

- 12. Administer the signaling groups.
- 13. Administer ARS dial patterns for outgoing calls.
- 14. Administer digit treatment for incoming routed calls.
- 15. Optionally administer the attendant feature for the purpose of call routing by entering set attendant <access-code> <extension>, where <access-code> specifies the dial access code for the attendant feature, and <extension> specifies the station which serves as the branch office attendant position.

Incoming trunk calls that have dialed strings that cannot be completely routed, will now be routed by SLS to this attendant position. In addition, stations in the branch office may directly dial the attendant using the <access-code>.

- 16. Administer the Feature Access Codes (FACs) by entering set fac <feature> <fac>, where <feature> is one of the following:
  - ars1
  - ars2
  - hold
  - contact-open
  - · contact-close
  - contact-pulse

<fac> is a 1 to 4 digit string that includes the digits 0 through 9, excluding \* and # for
analog rotary phones. The <fac> string must be unique and must not conflict with station
extension numbers and Trunk Access Codes (TACs).

#### Examples

- set fac ars2 \*9
- set fac contact-close 8
- Note:

The "\*" and "#" characters are not available on rotary-dial, analog phones.

17. At the Branch Gateway command prompt, enter exit to leave the sls context.

The Branch Gateway command prompt reverts to that of the original login.

18. After all of the SLS features are administered, at the Branch Gateway command prompt enter set sls enable to enable SLS on the Branch Gateway.



### Note:

If you enabled SLS and then entered additional administration, you must first disable SLS by entering set sls disable, and then re-enable it by entering set sls enable. This will cause the SLS application to resynchronize its administrative database with the Branch Gateway's CLI command database.

19. At the Branch Gateway command prompt, enter copy running-config startupconfig to save the changes.

#### Related links

Administering DS1 parameters on page 147

Administering BRI parameters on page 151

Administering trunk-group parameters on page 153

Administering signaling-group parameters on page 160

Administering dial-pattern parameters on page 161

Administering incoming-routing parameters on page 162

Media module compatibility with SLS on page 93

### Administering station parameters

#### **Procedure**

1. At the Branch Gateway command prompt, enter station <extension> <class> to enter a second-level sub-context to administer each phone that you want covered by SLS.

In this command, <extension> is a 1 to 16 digit numeric string that may begin with 0, and class <class> is analog, dcp, or ip.

For example, station 1234567 ip administers an IP phone with the extension "1234567".

The command line prompt changes to sls-station <extension> to indicate that you are in the station context for SLS administration. Entering exit ends the station configuration mode, and the command line prompt returns to its original state. If you want to remove the station from the SLS administration, enter clear station <extension> at the command line interface. Enter exit to leave the second-level station context to return to the (super-sls)# context.

- 2. Depending on the class (analog, dcp, or ip, set in Step 1 on page 144), enter set type <model>, where <model>is a value from Class values in SLS station context on page 146.
  - For example, set type ip4620 sets the previously-administered extension "1234567" as an Avaya 4620 IP phone.
- 3. For analog and dcp classes only (set in Step 1 on page 144), enter set port < moduleport> for this station, where <module-port> is a value in Module-port values in SLS station configuration mode on page 147.

# Note:

This command is required only for stations that support physical media module ports. If the class is ip (set in Step 1 on page 144), you cannot run this command.

You cannot select these modules or ports if they are already assigned as DID trunks.

#### Examples:

- If an MM711 is inserted into slot V3 and an analog station is to be administered for port #5, then set port v305 sets the previously-administered analog station "1234567" to the fifth physical analog station port on the Branch Gateway's media module.
- If an MM712 is inserted into slot V2 and a DCP station is to be administered for port #1. then set port v201 sets the previously-administered dcp station "1234567" to the first physical DCP station port on the Branch Gateway's media module.
- 4. Enter set cor <cor type> to set the class of restriction (COR) for this extension, where <cor type> is one of the following:
  - emergency
  - · internal (default)
  - local
  - toll
  - unrestricted

There exists a hierarchical relationship among the calling-restriction categories. As you move from the most restricted COR (emergency) to the least restricted (unrestricted), each level increases the range of dialing abilities. For example, toll includes the dialing privileges of local, internal, and emergency.

For example, set cor unrestricted gives a station unrestricted dialing.

- 5. If this station is administered to be included into a pool of stations that are allowed to receive incoming analog loop-start trunk calls, enter set trunk-destination yes.
- 6. If this is an IP phone (set in Step 1 on page 144), enter set password password where <password> is from four to eight digits in length, to administer a password.

For example, set password 53136 establishes the password "53136" on a previouslyadministered IP phone.

The phone automatically registers to the Branch Gateway upon failure if the password and the extension number are the same as those administered in CM.



#### Note:

Passwords are not required for analog or DCP phones unless an IP Softphone is using the administrative identity of a DCP phone, in which case the password is required.

7. To enable DCP or IP phones (set in Step 1 on page 144) to have an expansion module, enter set expansion-module yes.

- 8. For analog phones (set in Step 1 on page 144) that you want SLS to recognize the switchhook flash signal (that offers subsequent transfer features), enter set swhookflash ves.
- 9. Enter set name < name > to identify the user name for the station.

Use the 1 to 27 character name as specified on CM. Type the name string inside double quotes.

10. Enter **show** to check the station administration of the station being programmed.

The report lists the station parameters. For example:

Extension	Type	Port	Cor	Trunk-Des	Exp-Mod	Flash	Password
49139	ip4620	IPaddr	local	У	n	_	*****
	ip stati	on regi	stered	at address	'aaa.bbb.ccc	.ddd'	



## Note:

For currently-registered IP phones or IP Softphones, the IP address displays.

11. Enter exit to leave the station context in SLS.

#### Related links

Inherited Class of Restriction (COR) permissions on page 110

# Class values in SLS station context

analog	dcp	ip	
analog2500 <sup>5</sup>	dcp2402	ip4601	
-	dcp2410	ip4602	
-	dcp2420	ip4602sw	
-	dcp6402	ip4610sw	
-	dcp6402D	ip4612	
-	dcp6408	ip4620	
-	dcp6408+	ip4620sw (default)	
-	dcp6408D (default)	ip4621	
-	dcp6408D+	ip4622	
-	dcp6416D+	ip4624	
-	dcp6424D+	ip4625	
-	dcp8403B	-	
-	dcp8405B	-	
-	dcp8405B+	-	
-	dcp8405D	-	

<sup>&</sup>lt;sup>5</sup> Since there is just one entry, the model is optional; analog2500 is the default value.

analog	dcp	ip
-	dcp8405D+	-
-	dcp8410B	-
-	dcp8410D	-
-	dcp8434D	-

# Module-port values in SLS station configuration mode

Gateway	Media module	Analog station ports*	DCP
G430 or G450	MM711	8 possible ports	-
	MM712	-	8 possible ports
	MM714	4 possible ports (ports 1-4)	-
	MM714B	4 possible ports (ports 1-4)	-
	MM716	24 possible ports	-
	MM717	-	24 possible ports

# Administering DS1 parameters

#### **Procedure**

1. Enter ds1 <slot-address>, where <slot-address> is any permitted port.

The command line prompt changes to super-sls/ds1-<port-address>. If you want to remove the ds1 trunk from the SLS administration, enter exit to leave the second-level ds1 context and return to the (super-sls)# context, and then enter clear ds1 slotaddress.



## Note:

If configuration changes affecting trunk provisioning (such as, signaling and bit-rate) are made to a DS1 trunk where the trunk and its associated signaling group have already been provisioned, an error message instructs you that the Administrative change is in violation with existing trunk member provisioning, and the configuration change is rejected.

2. Enter set name < name > to identify the user name for the DS1 trunk.

Use the 1 to 27 character name as specified on CM (add trunk-group n). Type the name string inside double quotes.

3. Enter set bit-rate < rate > to set the maximum transmission rate in Mbps for the DS1 facility.

The rate can be either 1544 (T1) or 2048 (E1).

- 4. Enter set signaling-mode <mode-type> to set the signaling mode for the DS1 facility, where <mode-type> is one of the following values:
  - cas. Out-of-band signaling for E1 service, yielding thirty 64 kbps B-channels for voice transmission
  - robbed bit. In-band signaling for T1 service, yielding twenty-four 56 kbps B-channels for voice transmission
  - isdnpri. T1 or E1 ISDN Primary Rate service (supports both FAS and NFAS)
  - isdnext, NFAS T1 or E1 ISDN service for:
    - T1 facility, in which all 24 channels are for bearer transport
    - E1 facility, in which all 31 channels are for bearer transport
- 5. Enter set channel-numbering <method> to select the channel-numbering method for B-channels on an E1 interface, where <method> is one of the following values:
  - seq. Sequential codes of B-channels 1-30 in the ISDN Channel Identification IE
  - tslot. Timeslot method
- 6. Enter set connect <far-end> to specify the equipment at the far-end of the DS1 link, where <far-end> is one of the following values:
  - host. Data application (computer or server)
  - lineside. Terminal equipment (video multiplexer)
  - · network. Central office
  - pbx. Private communication system (another pbx)
- 7. If the far-end equipment is specified as **pbx** (set in Step 6), enter **set interface** < glare-mode> to specify the glare-handling convention, where < glare-mode> can be one of the following values:

For non-QSIG calls:	For QSIG calls:
<ul> <li>network. If the Branch Gateway is connected to a host computer and encounters glare, it overrides the far-end</li> </ul>	peerMaster. SLS overrides the other end when glare occurs     peerSlave. SLS releases the
user. If the Branch Gateway is connected to a public network and encounters glare, it releases the circuit	circuit when glare occurs

- 8. If the DS1 link is employed with ISDN, and the glare-handling convention is specified as peerMaster or peerSlave for the ISDN link (set in Step 7).
- 9. Enter set side <side> to specify the glare mode: either a or b.
- 10. If the DS1 link is employed with ISDN, enter set country-protocol <country-code> to specify the ISDN Layer 3 country protocol type, where <country-code> is one of the values in ISDN Layer 3 country codes on page 149:

- 11. For countries whose public networks allow for multiple ISDN Layer 3 country protocols for ISDN Primary Rate service, enter set protocol-version <option> to specify the mode.
  - Verify that the protocol version matches the country specified in **set country**-**protocol** (set in Step 9).
- 12. If the DS1 link is employed with ISDN, enter set bearer-capability <bearer> to set the Information Transfer Rate field of the Bearer Capability IE, where <bearer> is one of the following values:
  - 3khz. 3.1 kHz audio encoding
  - · speech. Speech encoding
- 13. Enter set interface-companding <type> to set the interface to agree with the companding method used by the far-end of the DS1 circuit for SLS mode, where <type> is one of the following values:
  - alaw. A-law companding
  - · ulaw. U-law companding
- 14. Enter set long-timer yes | no to increase the duration of the T303 (call establishment) timer, where:
  - yes. The T303 timer is extended from 4 seconds to 13 seconds
  - no. The T303 timer remains at 4 seconds
- 15. Enter show to check the DS1 administration.

The report lists the DS1 parameters. For example:

```
Name = 'Willow Steet 2'
DS1 Rate Signaling Channel Connect Interface Side Protocol Ver Bearer Cmpd Ltm
--- --- v3 1544 isdnpri seq network user a countryl a speech ulaw no
```

16. Enter exit to leave the ds1 context in SLS.

#### Related links

ISDN Layer 3 country protocols for ISDN Primary Rate service on page 150

# ISDN Layer 3 country codes

Country Code	Country		
1	United States (AT&T mode, also known as 5ESS)		
2	Australia (Australia National PRI)		
3	Japan		
4	Italy		
5	Netherlands		

Country Code	Country
6	Singapore
7	Mexico
8	Belgium
9	Saudi Arabia
10	United Kingdom (ETSI)
11	Spain
12	France (ETSI)
13	Germany (ETSI)
14	Czech Republic
15	Russia
16	Argentina
17	Greece
18	China
19	Hong Kong
20	Thailand
21	Macedonia
22	Poland
23	Brazil
24	Nordic countries
25	South Africa
etsi	ETSI (no use of RESTART message)
qsig	QSIG

# ISDN Layer 3 country protocols for ISDN Primary Rate service

Country code	Description	Possible Values
Country 1 (United States)	AT&T mode (also known as 5ESS)	а
	National ISDN-1	b
	Nortel mode (also known as DMS)	С
	Telecordia (NI-2)	d
Country 2 (Australia)	Australia National PRI	а
	ETSI	b
	invalid	С
	invalid	d

Country code	Description	Possible Values
Country 10 (United	DASS	а
Kingdom)	ETSI	b
	invalid	С
	invalid	d
Country 12 (France)	French National PRI	а
	ETSI	b
	invalid	С
	invalid	d
Country 13 (Germany)	German National PRI	а
	ETSI	b
	invalid	С
	invalid	d
ETSI	Full message set, including RESTART	а
	No RESTART message	b
	invalid	С
	invalid	d

# **Administering BRI parameters**

#### **Procedure**

1. Enter bri <slot-address>, where <slot-address> is any permitted port.

The command line prompt changes to sls-bri <slot-address>. If you want to remove the BRI link from the SLS administration, enter exit to leave the second-level bri context and return to the (super-sls)# context, and then enter clear bri <slot-address>.

2. Enter set name < name > to identify the user name for the DS1 trunk.

Use the 1-27 character name, as specified on CM (add trunk-group n). Type the name string inside double quotes.

3. Enter set interface <glare-mode> to specify the glare-handling convention.

<glare-mode> can be one of the following values:

For non-QSIG calls:	For QSIG calls:
<ul> <li>network. If the Branch Gateway is connected to a host computer and encounters glare, it overrides the far-end</li> </ul>	<ul> <li>peerMaster. SLS overrides the other end when glare occurs</li> <li>peerSlave. SLS releases the</li> </ul>
user. If the Branch Gateway is connected to a public network and encounters glare, it releases the circuit	circuit when glare occurs

- 4. If the BRI link is employed with ISDN, and the glare-handling convention is specified as peerMaster or peerSlave for the ISDN link (set in Step 3),
- 5. Enter **set side <side>** to specify the glare mode: either a or b.
- 6. If the BRI link is employed with ISDN, enter set country-protocol <country-code> to specify the ISDN Layer 3 country protocol type, where <country-code> is any of the values listed in ISDN Layer 3 country codes on page 149.
- 7. If the BRI link is employed with ISDN, enter set bearer-capability <br/>bearer> to set the Information Transfer Rate field of the Bearer Capability IE, where bearer is one of the following values:
  - 3khz. 3.1 kHz audio encoding
  - · speech. Speech encoding
- 8. Enter set interface-companding <type> to set the far-end companding method, where <type> is one of the following values:
  - alaw. A-law companding
  - ulaw. U-law companding
- 9. If the BRI link is employed with ISDN, enter set tei-assignment <tei> to select the method by which the Layer 2 (LAPD) protocol obtains its Terminal Endpoint Identification (TEI) address.

tei is one of the following values:

- · auto. TEI is assigned by the network provider
- zero. TEI is fixed administratively
- 10. Enter **set directory-number-a** < number> to assign a directory number to the B1 channel of the BRI link.
  - <number> is the provisioned number received from the network provider. The number
    value must be identical to the number the network provider has assigned to the circuit.
- 11. Enter set directory-number-b < number> to assign a directory number to the B2 channel of the BRI link.
  - <number> is the provisioned number received from the network provider. The number
    value must be identical to the number the network provider has assigned to the circuit.
- 12. Enter set spid-a number to assign an SPID to the B1 channel of the BRI link.
- 13. Enter set spid-b number to assign an SPID to the B2 channel of the BRI link.
  - Note:

All BRI links must have SPIDs properly configured for the link to function. SPIDs are received from the network service provider.

14. If the BRI link is employed with ISDN, enter set-endpoint-init {yes | no} to determine whether or not the far-end supports endpoint initialization.

15. If the BRI link is employed with ISDN, enter set layer1-stable {yes | no} to determine whether or not to keep the physical layer active (stable) between calls.

Some European countries require that the physical layer is deactivated when there is no active call.

16. Enter show to check the BRI administration.

The report lists the BRI parameters. For example:

17. Enter exit to leave the bri context in SLS.

# Trunk group assignment

You can create a trunk group that does not have any assigned members. Once a valid port is assigned as a trunk group member, this trunk group then becomes active and may be employed by SLS call processing for incoming/outgoing trunk operation. The slot-configuration table is used, together with the port capacity for the given module, to determine the validity of a port assignment at administration time.

As a result, there may not be more active trunk groups than there are physical trunk members within a given Branch Gateway. In addition, a combo-port may only be used for one active assignment. For example, the analog station/DID trunk ports may be either allocated to serve as an analog station or as an analog DID trunk, but not both.

The maximum limits for a given trunk type are defined by the slot-configuration assignment for the Branch Gateway. The maximum number of ports allowed per interface module is defined in <u>SLS</u> group type assignments on page 158.

#### Example

trunk-group 1 loop-start establishes an analog loop-start trunk group number 1.

# Administering trunk-group parameters

#### **Procedure**

- 1. Enter trunk-group <tgnum> <group-type>, where tgnum is any number from 1 to 2000 and <group-type> can be one of the following:
  - · loop-start (analog)
  - · did (analog)
  - ground-start (analog)
  - bri (ISDN basic rate)
  - t1-isdn (ISDN primary rate on 1.544 Mbps facility)

- e1-isdn (ISDN primary rate on 2.048 Mbps facility)
- t1-inband (non-ISDN rate on 1.544 Mbps facility)
- e1-inband (non-ISDN rate on 2.048 Mbps facility)

The command line prompt changes to super-sls/trunk-group-<tqnum>. If you want to remove the trunk group from the SLS administration, enter exit to leave the secondlevel trunk-group context and return to the (super-sls)# context, and then enter clear trunk-group <tgnum>.

2. Enter set dial <dial-type>, where <dial-type> is either rotary or dtmf.

For example, set dial dtmf establishes that the trunk group uses DTMF signaling.

3. Enter set tac <tac>, where <tac> is a 1 to 4 digit numeric value (plus initial # and \* on all but rotary dial phones) for this trunk's access code (TAC).

The TAC value must be unique among all trunk groups, extension numbers, and ARS Feature Access Code (FAC) strings.

For example, set tac 88 establishes access to this trunk group by dialing "88".

4. Enter add port <module> <port> <sig-group> to specify the port that is compatible with the device and/or media module.

The <sig-group> argument is necessary for a digital ISDN-PRI trunk. It is an integer number from 1 to 650 that specifies the signaling group associated with the management of this trunk member.



#### Note:

Administer the signaling group and DS1 information before you add any ports to the trunk group.

#### Example 1

If an MM711 is inserted into slot V3 and an analog loop-start trunk is to be administered for port 4, then add port V304 administers an analog loop-start trunk through port V304.

#### Example 2

If an MM722 is inserted into slot V2 and an ISDN BRI trunk is to be administered for port 1, then add port v201 adds a BRI trunk for the first physical port of the Branch Gateway media module to a trunk group using one B-channel of the BRI link.



## Note:

You cannot mix BRI and PRI trunks within the same trunk group. If you attempt to assign more than the maximum number of trunks to a trunk group, an error message instructs you to delete a trunk member before adding a new trunk. A physical trunk can be a member of only one trunk group.

5. For an analog DID trunk group, enter set supervision <sup-type> to set the incoming signaling supervision mode.

<sup-type> can be either immediate or wink.

For example, **set supervision wink** assigns wink-start incoming signaling supervision to a DID trunk group.

- For a non-ISDN digital trunk (t1-inband or e1-inband), enter set supervision <suptype> to set the incoming signaling supervision mode, where <sup-type>can be one of the following:
  - loop-start
  - · ground-start
  - wink-wink
  - · wink-immediate
  - · wink-auto
  - · immediate-immediate
  - · auto-auto
  - auto-wink
- 7. For an analog DID trunk group or DS1 non-ISDN tie trunk group, enter set digit-treatment <digit-treat>, where <digit-treat> can be one of the following values:
  - blank (use this value to prevent any absorb or insert digit treatment from being applied)
  - absorb1
  - absorb2
  - · absorb3
  - absorb4
  - absorb5
  - insert1
  - insert2
  - insert3
  - insert4

#### **Examples**

For example:

- set digit-treatment absorb1 removes the first digit from the incoming DID trunk
- set digit-treatment blank removes any digit treatment from the trunk group
- 8. For analog DID trunk groups or DS1 tie trunk groups, enter set digits <digits > to define the inserted digit string, where digits is the number of digits.

## Note:

The number of digits must comply with the digit-treat parameter in the set digit-treatment command. If the digit-treat parameter is insert3, then the digits parameter for this command must be three digits in length.

- 9. Enter set name < name > to identify the user name for the trunk group.
  - Use the 1 to 27 character name as specified on CM (add trunk-group n). Type the name string inside double quotes.
- 10. For ISDN trunks, enter set codeset-display <codeset> to identify which Q.931 codesets are allowed to send display information to the user phone: codeset0, codeset6, or codeset7.
- 11. For ISDN trunks, enter set codeset-national <codeset> to identify which Q.931 codesets are allowed to send National Information Elements (IEs, or display information) to the user phone: codeset6 or codeset7.
- 12. For ISDN trunks, enter set channel-preference <type> to define how the Channel **Identification IE** field is encoded, where <*type*> can be one of the following:
  - exclusive. The central office must have the ability to grant a call on this channel or reject the call attempt
  - preferred. The central office might offer the call request on another available channel
- 13. For ISDN trunks, enter set digit-handling method to define the order of reception/ transmission to be considered with the flow of inbound/outbound:
  - · enbloc-enbloc
  - enbloc-overlap
  - overlap-enbloc
  - overlap-overlap

Enbloc requires sending the entire collected digit string in one block. Overlap sends the digits one at a time as they are collected.

- 14. For ISDN trunks, enter set japan-disconnect <yes | no> to specify whether to perform a disconnect sequence (CONNECT message followed by a DISCONNECT message).
- 15. For ISDN trunks, enter set send-name < method > to define whether or not the calling, connected, called, or busy party's administered name is sent to the network on outgoing or incoming calls.

<method> can be one of the following:

- no. The name is not sent to the network for incoming or outgoing calls
- yes. The name is sent to the network for incoming or outgoing calls
- restricted. The name is sent to the network as "Presentation restricted"

# Note:

For this release, specify <method> as no, since sending a Calling Party Name is a future feature.

16. For ISDN trunks, enter set send-number <method> to define whether or not the calling, connected, called, or busy party's administered number is sent to the network on outgoing or incoming calls.

<method> can be one of the following:

- no. The number is not sent to the network for incoming or outgoing calls
- yes. The number is sent to the network for incoming or outgoing calls
- restricted. The number is sent to the network as "Presentation restricted"

# **Note:**

For this release, specify <method> as no, since sending a Calling Party Number is a future feature.

17. For ISDN trunks, enter **set numbering-format** < type> to specify the numbering plan for this trunk in Standard Local Survivability (SLS).

The numbering plan encodes the **Numbering Plan Indicator** and **Type of Number** fields in the Calling/Connected Party Number IE in the ISDN protocol.

<type>can be one of the following:

- unknown. Both the Numbering Plan Indicator and Type of Number are unknown
- public. The Numbering Plan Indicator meets the E.164 standard and the Type of Number is national

# Note:

The SLS application is intended to operate into PSTN trunk interfaces. For this reason, the only two choices for network numbering plans identification are public (E.464) and unknown (no particular plan). For this release, specify type as unknown since SLS does not currently support an administrative table to calculate the Calling Party Number that is consistent with the numbering plan of the PSTN service provider.

- 18. For non-ISDN digital trunks, analog loop-start and analog ground-start trunks, enter set incoming-destination extension to identify an extension to directly receive an incoming trunk call, for example, an attendant or a voice response/recording system.
- 19. For non-ISDN digital trunks, enter **set incoming-dialtone** yes | no> to specify
  whether to provide a dial tone in response to far-end trunk group seizures.
- 20. For a DS1 circuit, enter **set trunk-hunt** < type> to specify the trunk-hunting search within a facility in an ISDN trunk group or through a non-ISDN digital trunk group, where < type> is one of the following:
  - ascend. A linear search from the lowest to the highest numbered available channels

- circular. A circular search beginning with the point at which the search previously ended. When the search has reached the top of the channel list, it resumes at the bottom of the list in wrap-around fashion
- descend. A linear search from the highest to the lowest numbered available channels
- 21. Enter **show** to check the trunk-group administration.

The following example shows all four trunk members assigned to one trunk-group:

#### The following example shows twelve port members assigned as t1-inband signaling:

The report lists the trunk-group parameters.

22. Enter exit to leave the trunk-group context in SLS.

# Maximum number of members in a trunk group

You can assign a maximum of 255 members to analog and digital trunks.

# SLS group type assignments

Group type	Media module	Number of ports/ channels	Description of trunks that may be assigned
loop-start ground- start did	MM711	8	Ports 1-8
loop-start ground- start	MM714 or MM714B	4	Ports 5, 6, 7, 8
did	MM714or MM714B	4	Ports 1, 2, 3, 4
did	MM716	24	Ports 1-24
bri	MM720	16	Eight physical ports, each offering B1 and B2 channels

Group type	Media module	Number of ports/ channels	Description of trunks that may be assigned
bri	MM721	16	Eight physical ports, each offering B1 and B2 channels
bri	MM722	4	Two physical ports, each offering B1 and B2 channels
t1-isdn	MM710	23	D-channel is associated with this facility (FAS)
t1-isdn	MM710	24	D-channel is not associated with this facility (NFAS), and the DS1's signaling-mode is set to isdnext
e1-isdn	MM710	30	D-channel is associated with this facility (FAS)
e1-isdn	MM710	31	D-channel is not associated with this facility (NFAS), and the DS1's signaling-mode is set to isdnext
t1-inband	MM710	24	T1 Robbed-bit signaling application
e1-inband	MM710	30	E1 CAS signaling application

# Module-port values in SLS trunk-group context for analog trunks

Group Type	Media Module	Number of Ports/ Channels	Description
loop-start did ground- start	MM711	8	ports 1-8
loop-start ground-start	MM714 or MM714B	4	ports 5,6,7,8
did	MM714 or MM714B	4	ports 1,2,3,4
did	MM716	24	ports 1-24

# Trunk port values in SLS trunk-group context for digital trunks

Group Type	Media Module	Maximum Ports/Channels
bri	MM720	16
bri	MM721	16
bri	MM722	4
t1-isdn	MM710	23 (FAS)
		24 (NFAS)
e1-isdn	MM710	30 (FAS)
		31 (NFAS)
t1-inband	MM710	24
e1-inband	MM710	30

# Administering signaling-group parameters

#### **Procedure**

- 1. Enter sig-group <sgnum>, where <sgnum> is any number from 1 to 650.
  - The command line prompt changes to <code>sls-sig-group</code> <code><sgnum></code>. If you want to remove the signaling group from the SLS administration, enter <code>exit</code> to leave the second-level siggroup context and return to the (super-sls)# context, and then enter <code>clear sig-group sqnum</code>.
- 2. Enter set trunk-group-chan-select <tgnum> to specify the trunk-group number that accepts incoming calls where the **Information Channel Selection** field does not specify a preferred channel for bearer transport.
  - This is useful if the signaling group controls more than one trunk group (in cases where you wish to manage a DS1 facility with more than one trunk group).
- 3. Enter set primary-dchannel <circuit-number>, where <circuit-number> is an identifier for a Branch Gateway, slot, or T1/E1 circuit, to select the primary D-channel number.
  - For the value of *<circuit-number>*, you can use a 3-digit Branch Gateway identifier (for example, 005), a 2-character slot identifier (for example, v2), or a 2-digit circuit number (24 for T1-ISDN, 16 for E1-ISDN).
- 4. If your trunk is provisioned without a D-channel for signaling, enter set associated-signaling no to use Non-Facility Associated Signaling (NFAS).

## Note:

- NFAS is primarily a feature for ISDN-T1 connections offered by service providers in North America and Hong Kong. However, it can also be used on private-network connections, and in that context it is possible to set up NFAS using ISDN-E1 interfaces. If you are using NFAS, enter add nfas-interface gateway module interface-id, where gateway is the 3-digit Branch Gateway identifier, module is the 2-character slot identifier, and interface-id is the DS1 circuit number associated with the NFAS group. The value of interface-id is received from the network service provider.
- The North American Public Network Service Providers do not allow any part of a T1 to be shared outside of this NFAS-trunk group. In other words, they do not allow one of the T1 interfaces (of this NFAS group) to be fractionalized into two or more uses. It must be dedicated to this given customer. Therefore, the following usage rules apply:
- All members of an NFAS DS1 (that are administered) must belong to the same trunkgroup
- All members of this trunk-group must belong to a single signaling group
- 5. Enter **show** to check the signaling groups administration.

The report lists the signaling groups parameters. For example:

Sig-group	Tg-Select	Assoc-Sig	Prime-Dchan	Nfas-Modules/Nfas-Id
10	98	yes	005v424	<del>-</del>

6. Enter exit to leave the sig-group context in SLS.

# Administering dial-pattern parameters

#### **Procedure**

1. Enter dial-pattern < dialed-string>, where < dialed-string> is a dial pattern to be used on outgoing calls.

The command line prompt changes to super-sls/dial-pattern <dialed-string>. If you want to remove the incoming routing treatment from the SLS administration, enter exit to leave the second-level dial-pattern context and return to the (super-sls)# context, and then enter clear dial-pattern < dialed-string>.

2. Enter set type <dial-type>, where <dial-type> specifies the type of outbound call and the dialing privileges available for outbound calls.

Each level of call includes the previous level's dialing privileges. For example, loc1 has the calling privileges of iop, intl, etc.

- 3. Enter set max-length </error
  - This must be set prior to the minimum length if the minimum length is larger than the default value.
- 4. Enter set min-length < length > to define the minimum length of the dialed string.
- 5. Enter set tgnum <tgnum > to designate a trunk-group for which this dialed string is assigned.
- 6. Enter set deny no to permit stations to originate outgoing trunk calls.
- 7. At the command-line enter set insert-digits < digits > to define the digits to insert into a dialed string, if required.
- 8. Enter set delete-digits < digits > to define the number of digits to be deleted from a dialed string, if required.



#### ■ Note:

You can either insert or delete digits, but not both.

9. Enter **show** to check the outbound dial-pattern string administration.

The report lists the dial-pattern parameters. For example:

Dialed-String/Deny	Min/Max Length 	Туре	Delete/Insert Digits
5381000/n 5385000/n	- , -	locl	1/303 1/720

10. Enter exit to leave the dial-pattern context in SLS.

#### Related links

Inherited Class of Restriction (COR) permissions on page 110

# Available call types

emer: Emergency calls only

**fnpa:** 10-digit North American Numbering Plan calls **hnpa:** 7-digit North American Numbering Plan calls

intl: Public-network international number calls

iop: International operator calls

locl: Public-network local number calls

natl: Non-North American Numbering Plan calls

op: Operator callssvc: Service calls

# Administering incoming-routing parameters

#### About this task

The incoming-routing parameters are useful for mapping DNIS numbers directly into the station extension numbers when the Service Provider's DNIS plan does not directly reflect the station extension number length used in the Branch Gateway's dial plan.

#### **Procedure**

1. Enter incoming-routing <tgnum><mode>, where <tgnum> is an existing ISDN trunk group number and mode is the protocol used for receiving incoming digits.

<mode> can be either enbloc or overlap.

The command line prompt changes to sls-incoming-routing <tgnum>. If you want to remove the incoming routing treatment from the SLS administration, enter exit to leave the second-level incoming-routing context and return to the (super-sls)# context, and then enter clear internal-routing <tgnum> <mode>.

- 2. If the mode is set to enbloc (in Step 1), you must:
  - Enter set delete-digits < digits > to define the number of digits to be deleted from a
    dialed string.
  - Enter set insert-digits < digits > to define the number of digits to be inserted at the beginning of a dialed string.
  - Enter set match-pattern <pattern>to define the beginning digit pattern of an incoming alphanumeric dial string to be matched against.

- Enter set length </endth> to define the length of the dialed string.
- 3. If the mode is set to overlap (in Step 1), you may configure only one of the following options:
  - Enter set delete-digits < digits > to define the number of digits to be deleted from a dialed string.
  - Enter set insert-digits < digits > to define the number of digits to be inserted at the beginning of a dialed string.

# Note:

This action takes place after the deletion task has been completed for the enbloc-receiving mode.

- 4. Enter exit to leave the incoming-routing context in SLS.
- 5. Enter **show** to check the incoming-routing administration.

The report lists the incoming-routing parameters for all dial patterns that have been administered. For example:

Match_pattern	Length	Del	Insert-digits	Mode	tgnum
234	7	3	5381000	enbloc	98
235	7	3	5381001	enbloc	99

# **Summary of SLS configuration commands**

For more information about these commands, see Avaya Branch Gateway G450 CLI Reference.

Root Level Commands	First Level Context Commands	Second Level Context Commands	Description
set sls	-	-	Enable or disable SLS
show sls	-	-	Display SLS status: enabled or disabled
sls	-	-	Enter the sls context
-	bri	-	Administer an ISDN Basic Rate Interface (BRI) port for SLS
-	-	set bearer- capability	Set the Information Transfer Rate field of the Bearer Capability IE in SLS
-	-	set country- protocol	Specify the ISDN Layer 3 country protocol type in SLS
-	-	set directory- number-a	Assign a directory number to the B1 channel of the BRI interface in SLS

Root Level Commands	First Level Context Commands	Second Level Context Commands	Description
-	-	set directory- number-b	Assign a directory number to the B2 channel of the BRI interface in SLS
-	-	set endpoint-init	Determine whether or not the far-end supports endpoint initialization in SLS
-	-	set interface	Specify the glare-handling convention for a BRI link in SLS
-	-	set interface- companding	Set the interface to agree with the companding method used by the far-end of the DS1 circuit for SLS mode
-	-	set layer1-stable	Determine whether or not to keep the physical layer active (stable) between calls in SLS
-	-	set name	Identify the user name for an ISDN facility in SLS
-	-	set side	Specify the glare-handling conditions when the set interface command is administered as peerMaster or peerSlave for the ISDN link in SLS
-	-	set spid-a	Assign a Service Profile Identifier (SPID) to the B1 channel of the BRI link in SLS
-	-	set spid-b	Assign a Service Profile Identifier (SPID) to the B2 channel of the BRI link in SLS
-	-	set tei- assignment	Select the method by which the Layer 2 (LAPD) protocol obtains its Terminal Endpoint Identification (TEI) address in SLS
-	-	show	List all BRI SLS parameters for this BRI port
-	clear attendant	-	Delete the administered attendant provisioning in SLS
-	clear bri	-	Delete the administration for a given BRI channel in SLS

Root Level Commands	First Level Context Commands	Second Level Context Commands	Description
-	clear dial- pattern	-	Delete a single dialed string pattern entry in the SLS data set
-	clear ds1	-	Delete the administration for a specific DS1 channel in SLS
-	clear fac	-	Delete an administered Feature Access Code for SLS
-	clear incoming- routing	-	Delete an entry for a particular incoming routed string that is associated with a given trunk group in SLS
-	clear sig-group	-	Delete the administration for a given ISDN signaling group in SLS
-	clear slot-config	-	Delete the slot and the board administration in the Branch Gateway for SLS
-	clear survivable- config	-	Set the SLS parameters to their default values
-	clear station	-	Delete a particular extension number in the SLS data set
-	clear trunk-group	-	Delete a trunk group entry from the SLS data set
-	dial-pattern	-	Administer ARS dial patterns for SLS
-	-	set delete-digits	Specify the number of digits to be deleted from the beginning of the dialed string for an outbound call in SLS
-	-	set deny	Permit or deny access to an outbound trunk in SLS
-	-	set insert-digits	Specify the number of digits to be inserted at the beginning of the dialed string for an outbound call in SLS
-	-	set max-length	Establish the maximum length of the dialed string in SLS
-	-	set min-length	Establish the minimum length of the dialed string in SLS
-	-	set tgnum	Designate the trunk-group number in SLS

Root Level Commands	First Level Context Commands	Second Level Context Commands	Description
-	-	set type	Administer the type of outbound call in SLS
-	-	show	List all dial-pattern SLS parameters
-	ds1	-	Administer DS1 trunks for SLS
-	-	set bearer- capability	Set the Information Transfer Rate field of the Bearer Capability IE in SLS
-	-	set bit-rate	Set the maximum transmission rate for the DS1 facility in SLS
-	-	set channel- numbering	Select the channel-numbering method for B-channels on an E1 interface in SLS
-	-	set connect	Specify the equipment at the far-end of the DS1 link in SLS
-	-	set country- protocol	Specify the ISDN Layer 3 country protocol type in SLS
-	-	set interface	Specify the glare-handling convention for a DS1 link in SLS
-	-	set interface- companding	Set the interface to agree with the companding method used by the far-end of the DS1 circuit for SLS mode
-	-	set long-timer	Increase the duration of the T303 (call establishment) timer in SLS
-	-	set name	Identify the user name for a DS1 facility in SLS
-	-	set protocol- version	Specify country protocol for countries whose public networks allow for multiple ISDN Layer 3 country protocols for ISDN Primary Rate service in SLS
-	-	set side	Specify the glare-handling conditions when the set interface command has been administered as peerMaster or peerSlave for the ISDN link in SLS

Root Level Commands	First Level Context Commands	Second Level Context Commands	Description
-	-	set signaling- mode	Set the signaling mode for the DS1 facility in SLS
-	-	show	List all SLS parameters for this DS1 interface
-	incoming-routing	-	Administer digit-treatment for incoming routed calls in SLS
-	-	set delete-digits	Specify number of digits to be deleted from the beginning of the dialed string for an inbound trunk call in SLS
-	-	set insert-digits	Specify number of digits to be inserted at the beginning of the dialed string for an inbound trunk call in SLS
-	-	set length	Specify the length of the dialed string in SLS
-	-	set match-pattern	Specify the beginning digit pattern of the incoming alphanumeric dial string to be matched against in SLS
-	-	show	List all incoming-routing SLS parameters
-	set attendant	-	Specify the dial access code for the attendant feature, and specify the station which serves as the branch office attendant position
-	set date-format	-	Set a date format for the SLS data set
-	set fac	-	Administer the Feature Access Code for SLS
-	set ip-codec-set	-	Configure an IP codec set within the SLS data set
-	set max-ip- registrations	-	Configure the maximum number of IP registrations allowed in the SLS data set
-	set slot-config	-	Define the slot and the board type in the Branch Gateway for SLS
-	show attendant	-	Display the administered attendant provisioning

Root Level Commands	First Level Context Commands	Second Level Context Commands	Description
-	show bri	-	List the administered BRI parameters for SLS
-	show date-format	-	Display the current date format for the SLS data set
-	show dial-pattern	-	List all dial-pattern strings in the SLS data set
-	show ds1	-	List the administered DS1 parameters for SLS
-	show fac	-	List the administered Feature Access Codes for SLS
-	show incoming- routing	-	Show all of the administered dial patterns in SLS for trunk groups
-	show ip-codec-set	-	List the codec set entries for SLS
-	show max-ip- registrations	-	Display the maximum IP registration administration in the SLS data set
-	show sig-group	-	List all administered signaling groups in SLS
-	show slot-config	-	Define the slot and the board administration in the Branch Gateway for SLS
-	show station	-	Display extension-specific SLS data parameters
-	show trunk-group	-	Display trunk group administration in SLS
-	sig-group	-	Administer signaling groups for SLS
-	-	add nfas- interface	Identify a list of DS1 modules that are controlled by the primary D-channel in SLS
-	-	remove nfas- interface	Remove a member from a NFAS-managed DS1 group in SLS
-	-	set associated- signaling	Specify whether the D-channel is physically present in the DS1 interface in SLS
-	-	set primary- dchannel	Identify the D-channel number in SLS

Root Level Commands	First Level Context Commands	Second Level Context Commands	Description
-	-	set trunk-group- chan-select	Specify the trunk-group number that can accept incoming calls in cases where the <b>Information Channel Selection</b> field does not specify a preferred channel for bearer transport in SLS
-	-	show	List all SLS parameters for this signaling-group
-	station	-	Administer stations for SLS
-	-	set cor	Administer the class-of- restriction values for each station that uses SLS
-	-	set expansion- module	Administer a DCP or IP station for an expansion module in SLS
-	-	set name	Identify the user name for a station in SLS
-	-	set password	Administer a station password in SLS for DCP and IP station sets
-	-	set port	Administer the port on a station for SLS
-	-	set swhook-flash	Enable SLS to recognize the switchhook flash signal from a particular analog station and to provide a subsequent transfer service
-	-	set trunk- destination	Administer a station extension to be included in a pool of stations that can receive incoming analog loop-start trunk calls in circular queuing in SLS
-	-	set type	Administer specific phone models for SLS
-	-	show	List all Station SLS parameters for this station
-	trunk-group	-	Administer trunks for SLS
-	-	add port	Administer the port appropriate for SLS

Root Level Commands	First Level Context Commands	Second Level Context Commands	Description
-	-	clear tac	Remove a trunk access code (TAC) assignment from a trunk group in SLS
-	-	remove port	Remove the port assignment from a trunk group in SLS
-	-	set busy- disconnect	Specify whether the SLS analog trunk call state machine will monitor the trunk for the presence of a busy tone, and disconnect the call if a busy tone is detected
-	-	set cbc	Specify whether the ISDN trunk group will operate by declaring the service type explicitly on a call-by-call basis
-	-	set cbc-parameter	Specify the type of service or feature being declared in the Network Services Facility information element
-	-	set cbc-service- feature	Define what class of service is being specified, as part of the <b>scocs</b> service declared in the Network Services Facility information element
-	-	set channel- preference	Define how the <b>Channel Identification IE</b> field is encoded in SLS
-	-	set codeset- display	Specify which Q.931 codesets are allowed to send display information to the user phone in SLS
-	-	set codeset- national	Specify which Q.931 codesets are allowed to send National Information Elements to the user phone in SLS
-	-	set dial	Define the method for sending outbound digits in SLS
-	-	set digit- handling	Define how the inbound/ outbound calls handle the transmission/reception of the dialed pattern in SLS

Root Level Commands	First Level Context Commands	Second Level Context Commands	Description
-	-	set digits	Define the inserted dial string that is added to the beginning of the received DID incoming dial string for analog DID trunks or for DS1 TIE trunks using inband signaling in SLS
-	-	set digit- treatment	Define the incoming digit treatment for analog DID trunks or for DS1 TIE trunks using in- band signaling in SLS
-	-	set incoming- destination	Identify an extension to directly receive an incoming trunk call in SLS
-	-	set incoming- dialtone	Provide a dial tone in response to far-end trunk group seizures in SLS
-	-	set japan- disconnect	Perform a disconnect sequence (CONNECT message followed by a DISCONNECT message) in SLS
-	-	set name	Identify the user name for a trunk group in SLS
-	-	set numbering- format	Specify the numbering plan for this trunk in SLS
-	-	set send-name	Define whether or not the calling, connected, called, or busy party's administered name is sent to the network on outgoing or incoming calls in SLS
-	-	set send-number	Define whether or not the calling, connected, called, or busy party's administered number is sent to the network on outgoing or incoming calls in SLS
-	-	set supervision	Define the incoming signaling supervision mode for analog DID trunks or DS1 tie trunks only in SLS
	-	set tac	Administer the trunk-access codes for SLS

Root Level Commands	First Level Context Commands	Second Level Context Commands	Description
-	<del>-</del>	set trunk-hunt	Specify the trunk-hunting search within a facility in an ISDN trunk group or through a non-ISDN digital trunk group in SLS
-	-	show	List all trunk-group SLS parameters for this trunk-group

# Chapter 7: Switch Ethernet port configuration

# **Ethernet ports on the Gateway switch**

The switch on the Gateway has 10/100/1000 Mbps fixed switch ports on the front panel (ports 10/5 and 10/6).

# **Ethernet ports on the Branch Gateway router**

The router on the Branch Gateway has 10/100 Mbps fixed router ports on the front panel (ports 10/2 and 10/4).

# Cables used for connecting devices to the fixed router

Use a standard network cable when you connect one of the following devices to the fixed router port:

- · WAN endpoint device
- Switch
- Router

Use a crossover network cable when you connect a computer or other endpoint device to the fixed router port. For all other Ethernet ports on the Branch Gateway, you can use either a standard network cable or a crossover network cable to connect any device.

# Roadmap for configuring switch Ethernet ports

For basic configuration of a switch Ethernet port, use the commands listed below. You can also configure the following features on a switch Ethernet port:

- Advanced switching features, including VLANs.
- VoIP queuing. To configure VoIP queuing on a switch port, configure a VLAN for the port. Then configure VoIP queuing on the VLAN.
- Access control policy lists and QoS policy lists. To configure policy lists on a switch port, configure a VLAN for the port. Then configure policy on the VLAN.
- SNMP Link Up and Link Down traps.

#### Related links

Advanced switching on page 306

Commands used to configure QoS parameters on page 207

Policy lists on page 497

SNMP trap configuration on page 285

# Summary of switch Ethernet port configuration CLI commands

For more information about these commands, see Avaya Branch Gateway G450 CLI Reference.

Command	Description
set port auto-negotiation- flowcontrol-advertisement	Set the flow control advertisement for the specified Gigabit Ethernet ports when performing auto-negotiation
set port duplex	Configure the duplex type (full or half-duplex) of an Ethernet or Fast Ethernet port or range of ports
	You can configure Ethernet and FastEthernet interfaces to either full-duplex or half-duplex. The duplex status of a port in auto-negotiation mode is determined by auto-negotiation. When auto-negotiation is enabled, an error message is generated if you attempt to set the transmission type of auto-negotiation Fast Ethernet ports to half-duplex or full-duplex mode.
set port enable   disable	Enable or disable a port or a range of ports
set port flowcontrol	Set the send/receive mode for flow control frames (IEEE 802.3x or proprietary) for a full-duplex port
set port level	Set the default packet priority level for untagged packets
set port name	Configure a name for a port

Command	Description	
set port negotiation	Enable or disable auto-negotiation on the port	
set port speed	Set the speed of a port or range of ports	
show port auto-negotiation-flowcontrol-advertisement	Display the flow control advertisement for a Gigabit port used to perform auto-negotiation	
show port edge state	Display the edge state of a port	
show port flowcontrol	Display port flow control information	

Command	Description	
set port duplex	Configure the duplex type (full or half-duplex) of an Ethernet of Fast Ethernet port or range of ports	
set port edge admin state	Determine whether the port is an edge port, for the purposes of RSTP (Rapid Spanning Tree Protocol)	
	Edge port is a treatment assigned to ports for the purposes of RSTP (Rapid Spanning Tree Protocol). For more information about using this command and RSTP configuration in general, see Rapid Spanning Tree Protocol (RSTP).	
set port enable   disable	Enable or disable a port or a range of ports	
set port flowcontrol	Set the send/receive mode for flow control frames (IEEE 802.3x or proprietary) for a full-duplex port	
	Each direction (send or receive) can be configured separately. Use the show port flowcontrol command to display port flow control information.	
set port level	Set the default packet priority level for untagged packets	
	Packets traveling through a port set at normal priority should be served only after packets traveling through a port set at high priority are served.	
set port name	Configure a name for a port	
set port negotiation	Enable or disable auto-negotiation on the port	
	When negotiation is enabled, the speed and duplex of a Fast Ethernet port is determined by auto-negotiation. If negotiation is disabled, the user can set the speed and duplex of a Fast Ethernet port.	
set port point-to-point admin status	Set the connection type of the port to one of the following arguments:	
	force-true. The port is treated as if it were connected point-to-point	
	force-false. The port is treated as if it were connected to shared media	
	auto. The Branch Gateway tries to automatically detect the connection type of the port	

Command	Description
set port speed	Set the speed of a port or range of ports
	An error message is generated if you attempt to set the speed when auto-negotiation is enabled.
show port edge state	Display the edge state of a port
show port flowcontrol	Display port flow control information

# **Configuring the WAN Ethernet port**

#### **Procedure**

- 1. Use the interface fastethernet 10/2 or interface fastethernet 10/4 command to enter the context of the port interface.
- 2. Perform basic configuration of the interface.
- 3. Use the Ethernet WAN port configuration commands in the context of the port interface.

#### Related links

Interface configuration on page 381

# Roadmap for configuring additional features on the WAN Ethernet port

- Primary Management Interface (PMI).
- · Advanced router features.
- VoIP queuing.
- Access control policy lists and QoS policy lists.
- SNMP Link Up and Link Down traps.

#### Related links

Primary Management Interface (PMI) configuration on page 60

Router on page 380

Commands used to configure QoS parameters on page 207

Policy lists on page 497

SNMP trap configuration on page 285

# WAN Ethernet port traffic shaping

You can use traffic shaping to determine the data transfer rate on the WAN Ethernet port. To set traffic shaping, use the traffic-shape rate command in the interface context. To disable traffic shaping, use the no form of the traffic-shape rate command. Traffic shaping works in tandem with the configured bandwidth. If you change the traffic shape rate, this automatically

changes the bandwidth. Similarly, if you change the bandwidth, this automatically changes the traffic shape rate.



#### Note:

The traffic shape rate is determined in bits. The bandwidth is determined in kilobytes.

#### Related links

Commands used to configure QoS parameters on page 207

# **About backup interfaces**

You can configure backup relations between a pair of any Layer 2 Serial interfaces, including the FastEthernet interface.

#### **Related links**

Backup interfaces on page 234

# **Summary of WAN Ethernet port configuration CLI commands**

For more information about these commands, see Avaya Branch Gateway G450 CLI Reference.

Root level command	Command	Description
interface fastethernet		Enter interface fastethernet configuration mode
	autoneg	Set the port speed and duplex to auto-negotiation mode
	no autoneg	Disable the auto-negotiation mode
	duplex	Set the duplex setting (full or half) for the interface
	keepalive-track	Bind an object tracker to the interface to check whether it is up
		When activated, the object tracker sends health check packets at defined intervals to the other side of the interface. If the configured number of consecutive keepalive requests are not answered, the interface track state changes to down. The object tracker continues monitoring the interface, and when its track state changes to up, the interface state changes to up.
	shutdown	Set the administrative status of the current interface to down or up
	no shutdown	Restore the administrative status of the interface to up.
	speed	Set the speed for the interface
	traffic-shape rate	Configure traffic shaping for outbound traffic on the current interface

# **DHCP** client configuration

You can configure Branch Gateway to function as a DHCP (Dynamic Host Configuration Protocol) client.

DHCP client enables Branch Gateway to receive an IP address from a DHCP server, according to the DHCP client-server protocol. The DHCP server grants Branch Gateway DHCP client an IP address for a fixed amount of time, called the lease. After the lease expires, Branch Gateway DHCP client is required to stop using the IP address. Branch Gateway DHCP client periodically sends requests to the server to renew or extend the lease.

In addition to receiving an IP address, Branch Gateway DHCP client can optionally request to receive a domain name, a list of default routers, and a list of available DNS servers.

# Note:

Branch Gateway can function as both a DHCP server and a DHCP client simultaneously. That is, you can connect a cable modem for an Internet connection to the WAN Fast Ethernet in order to use Branch Gateway as a DHCP client. At the same time, you can activate the DHCP server on Branch Gateway for use by clients, such as, IP phones and PCs connected to the LAN ports. The DHCP server on Branch Gateway does *not* serve Internet devices connected over the WAN Fast Ethernet ports.

You can also enable the DHCP client on the VLAN interface.

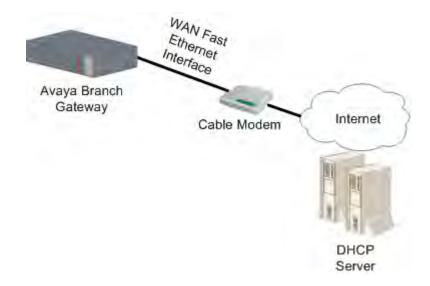
The DHCP client only supports IPv4.

#### Related links

**DHCP server** on page 402

# **DHCP** client applications

The typical application of DHCP client in Branch Gateway involves requesting and receiving an IP address from the service provider's DHCP server, to enable a broadband Internet connection via cable modem.



# **Configuring the DHCP client**

#### **Procedure**

1. Enter the context of the FastEthernet interface.

#### For example:

```
Gxxx-001# interface fastethernet 10/2
Gxxx-001(config-if:FastEthernet 10/2)#
```

2. Optionally, configure DHCP client parameters.

If you do not configure these parameters, their default values are used:

- Use the ip dhcp client client-id command to set the client identifier for the DHCP client. By default, the client identifier is usually the MAC address of the Branch Gateway FastEthernet interface.
- Use the ip dhcp client hostname command to set the hostname for the DHCP client. By default, the DHCP client uses the Branch Gateway's hostname.
- Use the ip dhcp client lease command to set the lease requested by the DHCP client. The lease is the length of time that the IP address provided by the DHCP server remains in effect. By default, the client does not request a specific lease from the DHCP server and uses the lease set by the DHCP server.
- Use the ip dhcp client request command to determine which DHCP options the DHCP client requests from the DHCP server. By default, the DHCP client requests all DHCP options.

#### For example:

```
Gxxx-001(config-if:FastEthernet 10/2) # ip dhcp client client-id hex
01:00:04:0D:29:DC:68
Done!
Gxxx-001(config-if:FastEthernet 10/2) # ip dhcp client hostname "Gxxx-A"
Done!
Gxxx-001(config-if:FastEthernet 10/2) # ip dhcp client lease 1 4 15
```

```
Done!

Gxxx-001(config-if:FastEthernet 10/2) # no ip dhcp client request domain-name

Done!
```

3. Optionally, use the ip dhcp client route track command to apply an object tracker to monitor the DHCP client's default route.

The object tracker continuously checks the validity of the default route, that is, whether data can be transmitted over the default route. Whenever the object tracker determines that the default route has become invalid, the route is dropped from the routing table and traffic is routed to alternate routes. If the default route becomes valid again, it is added back to the routing table.

Note that if several default routers are learned from a specific interface, the object tracker tracks only the first one.

#### For example:

```
Gxxx-001(config-if:FastEthernet 10/2)#ip dhcp client route track 3
Done!
```

4. Enable the DHCP client by entering ip address dhcp.

A message appears, displaying the IP address and mask assigned by the DHCP server. For example:

```
Gxxx-001(config-if:FastEthernet 10/2) # ip address dhcp
Done!
Interface FastEthernet 10/2 assigned DHCP address 193.172.104.161, mask
255.255.255.0
```

# Note:

Whenever you change the value of a DHCP client parameter (such as, client-id, or client hostname), enter ip address dhcp again to re-initiate DHCP address negotiation using the new values.

5. Use the show ip dhcp-client command to view the DHCP client parameters.

#### Related links

Object tracking provisioning on page 262

Typical application – tracking the DHCP client default route on page 269

Summary of DHCP Server commands on page 408

# **Examples of DHCP lease release and renew**

The release dhcp command example:

```
(super)# release dhcp FastEthernet 10/2
Done!
```

• The renew dhcp command example:

```
(super) # renew dhcp FastEthernet 10/2 Done!
```

A message appears displaying the IP address and mask assigned by the DHCP server. For example:

```
Interface FastEthernet 10/2 assigned DHCP address 193.172.104.161, mask
255.255.255.0
```

For a description of these commands, see Avaya G450 Branch Gateway CLI Reference.

### Commands used for DHCP client maintenance

- show ip dhcp-client
- show ip dhcp-client statistics
- clear ip dhcp-client statistics

For a description of these commands, see Avaya Branch Gateway G450 CLI Reference

# **Examples of configuring DHCP client logging messages**

• set logging session enable command example.

```
Gxxx-001# set logging session enable
Done!
CLI-Notification: write: set logging session enable
```

• set logging session condition dhcpc example:

```
Gxxx-001# set logging session condition dhcpc Info
Done!
CLI-Notification: write: set logging session condition dhcpc Info
```

### Note:

You can also enable logging messages to a log file or a Syslog server.

For a description of these commands, see Avaya G450 Branch Gateway CLI Reference.

### Related links

System logging on page 186

# **Summary of DHCP client configuration CLI commands**

For more information about these commands, see Avaya Branch Gateway G450 CLI Reference.

Root level command	Command	Description
clear ip dhcp-client statistics	-	Clear the DHCP client statistics counters
interface fastethernet	-	Enter interface fastethernet configuration mode
-	clear ip dhcp-client statistics	Clear the DHCP client statistics counters

Root level command	Command	Description
-	ip address dhcp	Enable or disable IP address negotiation via DHCP (applies to WAN FastEthernet interfaces only)
-	ip dhcp client client- id	Set the client identifier for the DHCP client
-	ip dhcp client hostname	Set the client hostname for the DHCP client
-	ip dhcp client lease	Set the lease requested by the DHCP client
-	ip dhcp client request	Specify which DHCP options the DHCP client requests from the DHCP server
-	ip dhcp client route track	Apply object tracking in order to monitor the DHCP client's default route
-	show ip dhcp-client	Display the configuration of the DHCP client
-	show ip dhcp-client statistics	Display the DHCP client statistics counters
release dhcp	-	Releases a DHCP lease for an interface. This effectively releases the client IP address, and no IP address is allocated to the specified interface.
renew dhcp	-	Renews a DHCP lease for an interface. This is effectively a request to renew an existing IP address, or the start of a new process of allocating a new IP address.
show ip dhcp- client	-	Display the configuration of the DHCP client
show ip dhcp-client statistics	-	Display the DHCP client statistics counters

# **LLDP** configuration

IEEE 802.1AB Link Layer Discovery Protocol (LLDP) simplifies troubleshooting of enterprise networks and enhances the ability of network management tools to discover and maintain accurate network topologies in multi-vendor environments. It defines a set of advertisement messages, called TLVs, a protocol for transmitting and receiving the advertisements, and a method for storing the information contained in the received advertisements.

The LLDP protocol allows stations attached to a LAN to advertise information about the system (such as, its major capabilities and its management address) and information regarding the station's point of attachment to the LAN (port ID and VLAN information) to other stations attached to the same LAN. These can all be reported to management stations via IEEE-defined SNMP MIBs.

LLDP information is transmitted periodically. The IEEE has defined a recommended transmission rate of 30 seconds, but the transmission rate is adjustable. An LLDP device, after receiving an LLDP message from a neighboring network device, stores the LLDP information in an SNMP MIB. This information is valid only for a finite period of time after TLV reception. This time is defined by the LLDP "Time to Live" (TTL) TLV value that is contained within the received packet unless refreshed by a newly received TLV. The IEEE recommends a TTL value of 120 seconds, but you can change it if necessary. This ensures that only valid LLDP information is stored in the network devices and is available to network management systems.

LLDP information is associated with the specific device that sends it. The device itself is uniquely identified by the receiving party port via chassis ID and port ID values. Multiple LLDP devices can reside on a single port, using a hub for example, and all of the devices are reported via MIB. You can enable (Rx-only, TX-only, and Rx or Tx) or disable LLDP mode of operation on a per-port basis.

# Supported TLVs

### **Mandatory TLVs**

- End-of-LDPDU
- Chassis ID
- Port ID
- Time to Live

### **Optional TLVs**

- Port description
- System description
- · System name
- System capabilities
- Management address

# **Optional 802.1 TLVs**

- VLAN name
- Port VLAN

# **Configuring LLDP**

### **Procedure**

1. Enable the LLDP agent globally using the set 11dp system-control command.

### For example:

Gxxx-001(super)# set lldp system-control enable
Done!

The device's global topology information, including all mandatory TLVs, is now available to neighboring devices supporting LLDP.

2. Optionally, configure the administrative LLDP port status using the **set port 11dp** command.

The default value is rx-and-tx.

The device now sends LLDP TLVs and accepts LLDP TLVs from neighboring devices supporting LLDP on the specified port.

### For example:

```
Gxxx-001(super) # set port lldp 10/3 rx-and-tx Done!
```

3. Optionally, configure additional TLVs transmission using the set port 11dp tlv command.

This allows you to advertise additional data about the device's and port's VLAN information, VLANs, and system capabilities. Additional TLVs are disabled by default.

### For example:

```
Gxxx-001(super) # set port lldp tlv 10/3 enable all Done!
```

The device now advertises all mandatory and optional TLVs to neighboring network devices supporting LLDP.

- 4. If required, change any of the following timing parameters:
  - The interval at which the device transmits LLDP frames, using the command set 11dp tx-interval. The default is 30 seconds
  - The value of TxHoldMultiplier, using the command set lldp tx-hold-multiplier. TxHoldMultiplier is a multiplier on the interval configured by set lldp tx-interval that determines the actual TTL value sent in an LLDP frame. The default value is 30. The time-to-live value transmitted in TTL TLV is expressed by: TTL = min(65535, TxInterval \* TxHoldMultiplier).
  - The minimal delay between successive LLDP frame transmissions, on each port, using the command set 11dp tx-delay. The default is 30 seconds.
  - The delay from when a port is set to LLDP "disable" until re-initialization is attempted, using the command set 1ldp re-init-delay. The default is 2 seconds.
- 5. Verify LLDP advertisements using the **show 11dp** command.

# Supported ports for LLDP

You can configure only ports 10/5 and 10/6 to support LLDP.

# **Summary of LLDP configuration CLI commands**

For more information about these commands, see Avaya Branch Gateway G450 CLI Reference.

Command	Description
set lldp re-init-delay	Set the delay from when a port is set to LLDP "disable" until re-initialization is attempted
set lldp system-control	Enable or disable the LLDP application globally per device or stack
set lldp tx-delay	Set the TxDelay, which is the minimal delay in seconds between successive LLDP frame transmissions, on each port
set lldp tx-hold-multiplier	Set the TxHoldMultiplier, which is a multiplier on the TxInterval that determines the actual TTL value sent in an LLDP frame
set lldp tx-interval	Set the TxInterval, the interval at which the device transmits LLDP frames
set port lldp	Change the administrative LLDP status of a port
set port lldp tlv	Enable or disable the transmission of the optional TLVs on a per port basis
show 11dp	Display the LLDP information received on each port
show lldp config	Display the global LLDP configuration
show port 11dp config	Display port-level LLDP configuration
show port lldp vlan-name config	Show the VLANs that are being transmitted on a specific port

# **Chapter 8: System logging**

System logging is a method of collecting system messages generated by system events. The Branch Gateway includes a logging package that collects system messages in several output types. Each of these types is called a sink. When the system generates a logging message, the message can be sent to each sink that you have enabled.

System messages do not always indicate problems. Some messages are informational, while others may help to diagnose problems with communications lines, internal hardware, and system software.

By default, all sinks are disabled. When enabled, log file and Syslog sink settings can be saved by using the command: copy running-config startup-config to save the running configuration to the startup configuration. However, the Session sink and its settings are deleted when the session is terminated.

You can define filters for each sink to limit the types of messages that the sink receives.

The logging facility logs configuration commands entered through the CLI or SNMP, and system traps and informative messages concerning the functioning of various processes. However, a user with user privileges who enables the log can only see the entered commands. For example, a user with read-only privileges cannot see entered commands having a read-write user level. In addition, the log does not display confidential information, such as, passwords and VPN pre-shared keys.

### Related links

Logging filter configuration on page 195

# Types of logging sinks

Sink	Description
Syslog	Logging messages are sent to up to three configured servers, using Syslog protocol as defined in RFC 3164. Messages sent to the Syslog server are sent as UDP, TCP, and TLS messages.
Log file	Logging data is saved in the flash memory. These compressed, cyclic files serve as the system logging database.

Sink	Description
Session	Logging messages are sent to the terminal screen as follows:
	For a local connection, messages appear online on the local terminal.
	For a remote Telnet/SSH connection, messages appear online on the remote terminal.
	This sink is deleted whenever a session ends.

# Syslog server configuration

A Syslog server is a remote server that receives logging messages using the Syslog protocol. This enables storage of large log files that you can use to generate reports.

# **Defining Syslog servers**

### About this task

You can define up to three Syslog servers with either IPv4 or IPv6 addresses..

### **Procedure**

1. Define the Syslog server by entering **set logging server** followed by the IP address of the server and optionally the transport (UDP, TCP or TLS) and server port.

For example (UDP Syslog server):

```
Gxxx-001(super)# set logging server 147.2.3.66
Done!
```

### or (TLS Syslog server and certificate for TLS connection):

```
Gxxx-001(super)# set logging server 2001:db8::2179::1
tls
Gxxx-001(super)# copy scp root-ca syslog syslogcert.crt 172.16.1.22
Done!
```

Enable the Syslog server by entering set logging server enable followed by the IP address of the Syslog server.

When you define a new Syslog server, it is defined as disabled, so you must use this command in order to enable the server.

### For example:

```
Gxxx-001(super)# set logging server enable 147.2.3.66
Done!
```

 Optionally, define an output facility for the Syslog server by typing the set logging server facility command, followed by the name of the output facility and the IP address of the Syslog server.

If you do not define an output facility, the default local7 facility is used.

### For example:

Gxxx-001(super) # set logging server facility auth 147.2.3.66 Done!

The following is a list of possible facilities:

- · auth. Authorization
- · daemon. Background system process
- · clkd. Clock daemon
- · clkd2. Clock daemon
- · mail. Electronic mail
- local0 local7. For local use
- ftpd. FTP daemon
- kern, kernel
- · alert. Log alert
- · audi. Log audit
- ntp. NTP subsystem
- Ipr. Printing
- sec. Security
- · syslog. System logging
- uucp. Unix-to-Unix copy program
- · news. Usenet news
- user. User process
- 4. Optionally, limit access to the Syslog server output by typing the set logging server access-level command, followed by an access level (read-only, read-write, or admin) and the IP address of the Syslog server.

If you do not define an access level, the default read-write level is used.

### For example:

```
Gxxx-001(super)# set logging server access-level read-only 147.2.3.66
Done!
```

Only messages with the appropriate access level are sent to the Syslog output.

5. Optionally, define filters to limit the types of messages received.

### **Related links**

Logging filter configuration on page 195

# **Disabling Syslog servers**

### **Procedure**

Enter set logging server disable followed by the IP address of the Syslog server.

For example

```
Gxxx-001(super)# set logging server disable 147.2.3.66
Done!
```

# **Deleting Syslog servers**

#### About this task

You can delete a Syslog server from the Syslog server table.

### **Procedure**

Enter clear logging server followed by the IP address of the Syslog server you want to delete.

For example:

```
Gxxx-001(super)# clear logging server 147.2.3.66
Done!
```

# Displaying the status of the Syslog server

### **Procedure**

Enter show logging server condition followed by the IP address of the Syslog server.

If you do not specify an IP address, the command displays the status of all Syslog servers defined for the Branch Gateway.

### **Example**

As the following example illustrates, the command displays whether the server is enabled or disabled, and lists all filters defined on the server:

# Syslog sink default settings

**Severity:** Warning **Facility:** Local 7

Access level: Read-write

# Syslog message format

Syslog messages are arranged chronologically and have the following format:

```
<34> Oct 11 22:14:15 host LINKDOWN [005ms, SWICHFABRIC-Notification:Port 10/3 Link, ID=1234567890
```

The message provides the following information:

- A priority (<34> in this example) that is calculated based on the syslog facility and the severity level.
- A header (Oct 11 22:14:15 host LINKDOWN in this example), providing the date and time, the hostname, and a message mnemonic.
- A message (005ms, SWICHFABRIC-Notification: Port 10/3 Link in this example), detailing the milliseconds, the application being logged, the severity level, the message text, and an Authentication File Identification number (AFID).

# Commands used to copy a syslog file

You can copy the syslog file from Branch Gateway to another location using FTP, SCP, TFTP, or HTTPS or locally to a USB mass storage device.

Use any of the following commands to copy a syslog file:

```
• copy syslog-file ftp.
```

- copy syslog-file scp
- copy syslog-file tftp
- · copy syslog-file usb
- copy syslog-file https
- · copyedge syslog-file scp

For more information about these commands, see Avaya Branch Gateway G450 CLI Reference.

#### **Related links**

Summary of logging configuration CLI commands on page 199

# Configuring a log file

### About this task

A log file is a file of data concerning a system event, saved in the flash memory. The log files serve as the system logging database, keeping an internal record of system events.

### **Procedure**

1. Enter set logging file enable.

```
Gxxx-001(super)# set logging file enable
Done!
```

2. Optionally, define filters to limit the types of messages received.

#### Related links

Logging filter configuration on page 195

# Disabling logging system messages to a log file

### **Procedure**

Enter set logging file disable.

```
Gxxx-001(super) # set logging file disable
Done!
```

# Deleting current log file and opening an empty log file

### **Procedure**

Enter clear logging file

```
Gxxx-001(super)# clear logging file
Done!
```

### **Example display of log file messages**

The **show logging file content** command displays the messages in the log file. Note that the user enabling the log sees only entered commands with a user-level no higher than the user's privileges. A user with read-only privileges does not see entered commands having a read-write user level.

### **Example**

```
(super) # show logging file content
<190>Aug 23 16:28:32 149.49.77.11 -NoTag: -NoUTC 2015 055 1
mediagateway.g430 | 0 coldStart[BOOT-Informational: System boot up
from cold reset, ID=N/A
<187>Aug 23 16:28:32 149.49.77.11 -NoTag: -NoUTC 2015 525 1
mediagateway.g430 | 0 MSY-TRPMAJNA[VOICE-Error: No Call Controller
Found, ID=N/A
<190>Aug 23 14:30:25 149.49.77.11 -NoTag: -NoUTC 2015 965 1
mediagateway.q430 | 0 BOOT MESSAGE[BOOT-Informational: Booting from
bank B with firmware version 29.22.50, ID=N/A
<190>Aug 23 14:30:25 149.49.77.11 -NoTag: -NoUTC 2015 965 1
mediagateway.q430 | 0 coldStart[BOOT-Informational: System boot up
from cold reset, ID=N/A
<187>Aug 23 14:30:25 149.49.77.11 -NoTag: -NoUTC 2015 425 1
mediagateway.g430 | 0 MSY-TRPMAJNA[VOICE-Error: No Call Controller
Found, ID=N/A
```

# Example display of conditions defined for the file output sink

The following example shows the output from the show logging file condition command.

### **Example**

```
(super)# show logging file condition
*********************
*** Message logging configuration of FILE sink ***
Sink Is Enabled
Sink default severity: Informational
```

# Log file message format

Log file messages appear in first-in, last-out order. They have the following format:

```
08/23/2015,10:55:09:CLI-Notification: root: set port disable 10/6 08/23/2015,10:49:03:SWITCHFABRIC-Notification: Port Connection Lost on Module 10 port 5
```

Each message provides the following information:

- Severity
- The date and time (if available)
- · The logging application
- The process ID (if available)
- The UTC offset (if available)
- The year
- Milliseconds
- · Log format
- · The severity level
- The Branch Gateway type
- The message text

### set logging file retention

Defines the period of time in days that log content will be retained.

### **Syntax**

```
set logging file retention {retention_days}
retention days must be either:
```

- · A value between 1 and 9999, inclusive
- Unlimited

### **Example:**

```
# set logging file retention unlimited
Log retention time is unlimited.
Done!

# show logging file retention
Log retention time is unlimited.
Done!

# set logging file retention 30
Log retention time is 30 days.
Done!

# show logging file retention
Log retention time is 30 days.
Done!

# st logging file retention
Log retention time is 30 days.
Done!

# set logging file retention 10000
Error: Parameter 1 (<retention_days>) value (10000) > maximum value(9999)
set logging file retention -- Set log retention time in days
Syntax: set logging file retention <retention days>
```

# show logging file retention

Shows the period of time in days that has been set using the set logging file retention command

### **Syntax**

show logging file retention

### **Example:**

```
# set logging file retention 30
Log retention time is 30 days.
Done!
# show logging file retention
Log retention time is 30 days.
Done!
```

# Configuring a session log

### About this task

A session log is the display of system messages on the terminal screen. It is automatically deleted when a session ends.

### **Procedure**

1. Enter set logging session enable.

```
Gxxx-001(super) # set logging session enable
Done!
```



### Note:

If the device is connected to several terminals, a separate session log is established for each terminal.

Optionally, define filters to limit the types of messages received.

# Example discontinuation of the display of system messages

The following output is an example of the **set logging session disable** command used to discontinue the display of system messages to the terminal screen.

### Example

```
(super) # set logging session disable Done!
```

# **Example display of session logging configuration**

The following output is an example of the **show logging session condition**. command that displays whether session logging is enabled or disabled, and lists all filters defined for session logging.

### Example

```
(super)# show logging session condition
***********************
*** Message logging configuration of SESSION sink ***
Sink Is Enabled
Sink default severity: Warning
Session source ip: 172.16.1.231
```

# Session logging message format

Session logging messages are arranged chronologically and have the format shown in the following example:

```
08/23/2015,10:49:03:SWITCHFABRIC-Notification: Port Connection Lost on Module 10 port 5 was cleared 08/23/2015,10:55:09:CLI-Notification: root: set port disable 10/6
```

Each message provides the following information:

- The date and time (if available)
- · The logging application
- · The severity level
- · The message text

### Note:

The user enabling the log only sees entered commands with a user-level no higher than the user's own privileges. For example, a user with read-write privileges cannot see entered commands with an admin user level.

# Logging filter configuration

You can use filters to reduce the number of collected and transmitted messages. The filtering options are based on message classification by severity for each application. For a specified sink, you can define the threshold severity level for message output for each application. Messages pertaining to the specified applications, that have a severity level stronger than or equal to the defined threshold, are sent to the specified sink. Messages with a severity level weaker than the defined threshold are not sent.

# Commands used to set the logging filters

For each sink, you can set logging filters by specifying a severity level per application, as follows:

- set logging server condition application severity ip address creates a filter for messages sent to a specified Syslog server.
- set logging file condition application severity creates a filter for messages sent to a log file.
- set logging session condition application severity creates a filter for messages sent to a session log on a terminal screen where:
  - application is the application for which to view messages (use all to specify all applications).
  - **severity** is the minimum severity to log for the specified application (use none to disable logging messages for the specified application).
  - ip address is the IP address of the Syslog server.

### For example:

```
Gxxx-001(super) # set logging server condition dialer critical 147.2.3.66
Done!
Gxxx-001(super) # set logging file condition dhcps warning
Done!
Gxxx-001(super) # set logging session condition ISAKMP Information
Done!
```

You can also filter the show logging file content command by severity for each application, using the same variables as in the set logging file condition command. In addition, you can limit the number of messages to display.

For example, to display the 50 most recent messages from the QoS application with a severity level of critical or higher, enter the following command:

```
Gxxx-001(super) # show logging file content critical qos 50
```

# Severity levels

Severity level	Code	Description
emergency	0	System is unusable
alert	1	Immediate action required

Severity level	Code	Description
critical	2	Critical condition
error	3	Error condition
warning	4	Warning condition
notification	5	Normal but significant condition
informational	6	Informational message only
debugging	7	Message that only appears during debugging

# **Default sink severity levels**

Syslog: Warning

Log file: Informational

Session from terminal: Informational
Session from telnet/ssh: Warning

# **Application filtering**

You can define filters for any application listed in the following table.

Application	Description
arp	Address Resolution Protocol mechanism
boot	System startup failures
cdr	Call Detail Recording. Registers the active calls in SLS mode.
cli	CLI
config	Configuration changes
console	Serial modem messages
dhcp-relay	DHCP requests relaying
dhcpc	DHCP client package
dhcps	DHCP server package
dialer	Dialer interface messages
dnsc	DNS client package
fan	Cooling system
filesys	File system problem (flash)
ids	IDS events, specifically a SYN attack heuristic employed by the SYN cookies feature
iphc	IP header compression
ipsec	VPN IPSEC package
isakmp	VPN IKE package

Application	Description
ospf	Open Shortest Path First protocol
policy	Policy package
ppp	PPP protocol
pppoe	PPP over Ethernet
proxy-arp	Proxy ARP
qos	QoS messages
router	Core routing system failures
rtp-stat	RTP MIB statistics
saa	RTR-probes messages
security	Secure logging (authentication failure)
snmp	SNMP agent
stp	Spanning tree package
supply	Power supply system
switchfabric	Switch fabric failures
system	Operating system failures
tftp	Internal TFTP server
threshold	RMON alarms
tracker	Object tracker messages
usb	USB devices messages
usb-modem	USB modem messages
vj-comp	Van Jacobson header compression messages
vlan	VLAN package
voice	Voice failures
wan	WAN plugged-in expansion

# Syslog server example

The following example defines a Syslog server with the following properties:

- IP address 147.2.3.66
- · Logging of messages enabled
- Output to the Kernel facility
- Only messages that can be viewed by read-write level users are received
- Filter restricts receipt of messages from all applications to those less severe than error

```
Gxxx-001(super) # set logging server 147.2.3.66
Done!
Gxxx-001(super) # set logging server enable 147.2.3.66
Done!
Gxxx-001(super) # set logging server facility kern 147.2.3.66
Done!
```

```
Gxxx-001(super) # set logging server access-level read-write 147.2.3.66
Done!
Gxxx-001(super) # set logging server condition all error 147.2.3.66
Done!
```

# Log file example

The following example enables the logging of system messages to a log file in the flash memory and creates a filter to restrict the receipt of messages from the boot application to those with severity level of informational or more severe, and messages from the cascade application to those with severity level of alert or more severe.

```
Gxxx-001(super)# set logging file enable
Done!
Gxxx-001(super)# set logging file condition boot informational
Done!
Gxxx-001(super)# set logging file condition cascade alert
Done!
```

# Session log example

The following example enables a session log for a user wishing to debug the ISAKMP application, while only receiving messages of severity level error or stronger for all other applications. Therefore, the user sets the default severity level for all applications to error, and then sets the severity of the ISAKMP application to informational. Finally, the user displays the filter settings.

# Accessing diagnostic logs

### About this task

Use this procedure to capture log files.

### **Procedure**

- 1. Log on to the gateway as root.
- 2. Enable screen capture logging in your terminal emulation program.
- 3. Run the show all logs command.

 Send a copy of the screen capture log file to Avaya through an email or as an attachment.
 For more information about accessing diagnostic logs, see CLI Reference Avaya Branch Gateway G450, 03-602056.

### For example:

```
iW}ZH\sim YL{}Z(^E^M)=}EsZ^E}Z
ZH~YL{}Zj^M}ZZZZZZDZJ@ 3
Z1 { ~=ZNLMR } EZZZZZZDZw3
Z1 \sim '=; ^E ZK Esz \sim NZDZ''@:w: 3
Z!lzjLMR}EZZZZZZZZZDZ0:w
ZiW}Zl^>}YZn^=^ZzsDZ
))))))))))))))))))))))))))))))))))))
Z###Z.dizM}DZwD0TD0 Z###Z
?qlqiZA~/2z{}Z}Md=OZ
ZZg??onZZZZHHpnn WWDMMDss:WsZZZZgKgjiZhtjnAgZZZZZZg??j+ZZZZZZZt.qwZZZZZZZt.q0
     Z
               Z
                          Ζ
ZZZZZZZZZZZZZ
G450-gloin-031(super)#
```

# **Summary of logging configuration CLI commands**

For more information about these commands, see Avaya Branch Gateway G450 CLI Reference.

Command	Description
copy syslog-file ftp	Copy the syslog file to a remote server using FTP
copy syslog-file scp	Copy the syslog file to a remote server using SCP
copy syslog-file tftp	Copy the syslog file to a remote server using TFTP
copy syslog-file usb	Upload the syslog file from the Branch Gateway to the USB mass storage device
copy syslog-file https	Copy the syslog file to a remote server using HTTPS
copyedge syslog-file scp	Copy the syslog file to a remote server using SCP via Avaya SBCE tunnel

Command	Description
clear logging file	Delete the message log file being stored in non-volatile memory (NVRAM), including the history log, and open a new, empty log file
clear logging server	Delete the specified Syslog message server from the Syslog server table
set logging file	Manage the logging of system messages to non-volatile memory (NVRAM)
set logging server	Define a new Syslog output server for remote logging of system messages
set logging server access- level	Set the access level associated with a Syslog server sink
set logging server condition	Set a filter for messages sent to the specified Syslog server. Messages can be filtered by source system, severity, or both.
set logging server enable   disable	Enable or disable a specific Syslog server
set logging server facility	Define an output facility for the specified Syslog server
set logging session	Manage message logging for the current console session
show logging file condition	Display all conditions that have been defined for the file output sink
show logging file content	Output the messages in the log file to the CLI console. Note that the user enabling the log sees only entered commands with a user-level no higher than the user's privileges. A user with read-only privileges does not see entered commands having a read-write user level.
show logging server condition	Display the filter conditions defined for the Syslog output sink
show logging session condition	Display the filter conditions defined for message logging to the current console session

# **Chapter 9: VolP QoS**

Branch Gateway provides voice services over IP data networks using VoIP. VoIP is a group of protocols for transmitting and receiving various types of voice data over an IP network. VoIP includes protocols for transmitting and receiving the following types of information:

- · Digitally encoded voice data
- · Call signalling information
- · Call routing information
- QoS information

VoIP uses the RTP and RTCP protocols to transmit and receive digitally encoded voice data.

You can use many types of telephones and trunks that do not directly support VoIP. Branch Gateway translates voice and signalling data between VoIP and the system used by the telephones and trunks.

# RTP and RTCP configuration

VoIP uses the RTP and RTCP protocols to transmit and receive digitally encoded voice data. RTP and RTCP are the basis of common VoIP traffic. RTP and RTCP run over UDP and incur a 12-byte header on top of other (IP, UDP) headers. Running on PPP or frame relay, these protocols can be compressed.

# **Header compression configuration**

Header compression reduces the size of packet headers, thus reducing the amount of bandwidth needed for data. The header compression method is based on the fact that most of the header fields remain constant or change in predictable ways throughout the session. Thus, instead of constantly retransmitting the header, each side keeps a context table of the sessions (the normal headers), and while sending and receiving packets it replaces the full-length headers with one or two bytes CID (context-id) plus unpredictable deltas from the last packet.

The Branch Gateway offers both RTP header compression, for reducing the amount of bandwidth needed for voice traffic, and TCP and UDP header compression, for reducing the amount of bandwidth needed for non-voice traffic.

For header compression purposes, any UDP packet with an even destination port within a user-configurable range of ports, is considered an RTP packet.

The Branch Gateway enables decompression whenever compression is enabled. However, when enabling header compression on a Frame Relay interface, you must first verify that the remote host is also employing header compression. Header compression on a Frame Relay interface does not check what the remote host is employing. Thus, it may compress headers even when the remote host is not configured to decompress headers.

You can configure how often a full header is transmitted, either as a function of time or of transmitted compressed packets.

# Header compression configuration options

The Branch Gateway offers two options for configuring header compression:

- IP Header compression (IPHC) method, as defined by RFC 2507. IPHC-type compression applies to RTP, TCP, and UDP headers.
- Van Jacobson (VJ) method, as defined in RFC 1144. VJ compression applies to TCP headers only.

### Note:

VJ compression and IPHC cannot co-exist on an interface, and IPHC always overrides VJ compression. Thus, if you define both VJ compression and IPHC, only IPHC is enabled on the interface regardless of the order of definition.

# Header compression support by interface

Interface type		Supported compression methods
Serial	-	-
-	PPP	IPHC and VJ
-	Sub-Frame-Relay with IETF encapsulation	IPHC only
-	Sub-Frame-Relay with non-IETF encapsulation	RTP header compression using the IPHC method, and TCP header compression using the VJ method
Dialer		IPHC and VJ



Non-IETF encapsulation is compatible with other vendors.

# **Configuring IPHC**

### About this task

IHPC applies to RTP, TCP, and UDP headers.

### Note:

You cannot specify IPHC for a Frame Relay non-IETF interface.

### **Procedure**

1. Optionally, configure the following header compression parameters.

If you do not configure these parameters, their default values are used.

- ip rtp compression-connections
- ip tcp compression-connections
- ip rtp max-period
- ip rtp max-time
- ip rtp non-tcp-mode

IETF mode is not compatible with non-IETF mode.

• ip rtp port-range

### For example:

```
Gxxx-001(config-if:Serial 4/1:1) # ip rtp compression-connections 48
Gxxx-001(config-if:Serial 4/1:1)# ip tcp compression-connections 48
Done!
Gxxx-001(config-if:Serial 4/1:1)# ip rtp max-period 512
Gxxx-001(config-if:Serial 4/1:1) # ip rtp max-time 20
Done!
Gxxx-001(config-if:Serial 4/1:1) # ip rtp non-tcp-mode ietf
Gxxx-001(config-if:Serial 4/1:1) # ip rtp port-range 40000 50000
```

2. Use the ip rtp header-compression command if you want to enable RTP, TCP, and UDP header compression on the current interface.

The compression method employed is IPHC. Alternatively, you can use the following equivalent command: ip tcp header-compression iphc-format

### For example:

```
Gxxx-001# interface dialer 1
Gxxx-001(config-if:Dialer 1)# ip rtp header-compression
Done
```



### Note:

Once header compression is enabled, any change to a header compression parameter is effective immediately.

3. To disable IPHC on an interface, use the no form of the command you employed (in the interface context): no ip rtp header-compression or no ip tcp headercompression.

# **Summary of IPHC header compression CLI commands**

For more information about these commands, see Avaya Branch Gateway G450 CLI Reference.

Root level command	First level command	Description
clear ip rtp header-compression	-	Clear IP RTP header compression statistics for all enabled interfaces or for a specific interface. To clear RTP compression statistics for all endabled interfaces, do not enter an interface type and number. Clearing the statistics does not cause renegotiation of parameters.
clear ip tcp header-compression	-	Clear TCP header compression statistics for all enabled interfaces or for a specific interface. To clear TCP compression sttistics for all enabled interfaces, do not enter an interface type and number. Clearing the statistics does not cause renegotiation of parameters.
<pre>interface (dialer  serial)</pre>	-	Enter the Dialer or Serial interface context
-	ip rtp compression- connections	Control the number of Real-Time Transport Protocol (RTP) connections supported on the current interface. Use the no form of this command to restore the default value of 16. This command also sets the number of connections in the non-TCP space, not just RTP
-	ip rtp header- compression	Enable both RTP and TCP header compression on the current interface
-	ip rtp max-period	Set the maximum number of compressed headers that can be sent between full headers
-	ip rtp max-time	Set the maximum number of seconds between full headers
-	ip rtp non-tcp-mode	Set the type of IP header compression to ietf or non-ietf. When set to ietf, the command performs IP header compression according to IPHC RFCs. When set to non-ietf, the command performs IP header compression compatible with other vendors, which do not strictly follow the RFCs. The default header compression mode is non-ietf.
-	ip rtp port-range	Set the range of UDP ports considered as RTP on the current interface
-	ip tcp compression- connections	Set the total number of TCP header compression connections supported on the current interface. Use the no form this command to restore the default value of 16.

Root level command	First level command	Description
show ip rtp header- compression	-	Display header compression statistics for a specific interface. If no interface is specified, statistics for all interfaces are displayed.
show ip rtp header- compression brief	-	Display a subset of header compression statistics in the form of a table
show ip tcp header- compression	-	Display TCP header compression statistics for a specific interface
show ip tcp header- compression brief	-	Display a subset of TCP header compression statistics in the form of a table

# Configuring VJ header compression

### About this task

VJ header compression applies to TCP headers only.



### Note:

You cannot specify VJ header compression for a Frame Relay IETF interface.

### **Procedure**

1. Optionally, use the ip tcp compression-connections command to control the number of TCP header compression connections supported on the interface.

Use the no form of this command to restore the default value of 16 connections.

### For example:

```
Gxxx-001(config-if:Dialer 1) # ip tcp compression-connections 24
```

2. Use the ip tcp header-compression command to enable TCP header compression on the current interface.

The compression method employed is the VJ compression.



### Note:

- The ip rtp header-compression command always overrides the ip tcp header-compression command. Both commands enable TCP header compression, but they differ in the methods employed.
- The ip tcp header-compression iphc-format command always overrides the ip tcp header-compression command, and activates IPHC-type compression.

### For example:

```
Gxxx-001# interface dialer 1
Gxxx-001(config-if:Dialer 1)# ip tcp header-compression
Done!
```

### Note:

Once header compression is enabled, any change to a header compression parameter is effective immediately.

3. To disable VJ TCP header compression on an interface, use the no ip tcp headercompression command in the interface context.

### **Summary of Van Jacobson header compression CLI commands**

For more information about these commands, see Avaya Branch Gateway G450 CLI Reference.

Root level command	First level command	Description
clear ip tcp header- compression	-	Clear TCP header compression statistics for all enabled interfaces or for a specific interface
<pre>interface (dialer  serial)</pre>	-	Enter the Dialer or Serial interface context
-	ip tcp compression- connections	Set the total number of TCP header compression connections supported on the current interface
-	ip tcp header- compression	Enable TCP header compression on the current interface
show ip tcp header- compression	-	Display TCP header compression statistics for a specific interface. If no interface is specified, statistics for all interfaces are displayed. Use this command regardless of which compression method is employed.
show ip tcp header- compression brief	-	Display a subset of TCP header compression statistics in the form of a table

# Commands used to display and clear header compression statistics

For more information about these commands, see Avaya Branch Gateway G450 CLI Reference.

- show ip rtp header-compression
- show ip tcp header-compression
- clear ip rtp header-compression
- clear ip tcp header-compression

# Commands used to configure QoS parameters

Branch Gateway uses MGCP (H.248) protocol for call signalling and call routing information. Use the following commands to configure QoS for signalling and VoIP traffic.

- set qos control
- set qos signal
- show qos-rtcp
- set qos bearer

For more information about these commands, see Avaya Branch Gateway G450 CLI Reference.

# Commands used to configure RTCP QoS parameters

Use the following commands to set the RTCP QoS parameters.

- set qos rtcp
- show qos-rtcp

For more information about these commands, see Avaya Branch Gateway G450 CLI Reference.

# Commands used to configure RSVP parameters

VoIP can use the RSVP protocol to reserve network resources for voice data while communicating with other Gateways and other VoIP entities, such as, IP phones and Softphones.

- set qos rsvp
- show qos-rtcp

For more information about these commands, see Avaya Branch Gateway G450 CLI Reference.

# Summary of QoS, RSVP, and RTCP configuration CLI commands

For more information about these commands, see Avaya Branch Gateway G450 CLI Reference.

Command	Description
set qos bearer	Permit the setting of VoIP QoS-bearer related parameters for the Media Gateway Processor and VoIP engines. The parameters you define using this command may conflict with the default QoS list (400).
set qos control	Define the source for QoS control parameters: local or remote
set qos rsvp	Set values for the RSVP parameters of the VoIP engines. The parameters that can be set include enabled/disabled, refresh rate (seconds), failure retry (y or n), and service profile (Guaranteed or Controlled).

Command	Description
set qos rtcp	Set values for RTCP parameters. The RTCP parameters that can be set include enabling or disabling RTCP reporting capability, setting the IP address of the monitor, setting the reporting period (the default is five seconds), and defining the listening port number. This command supports IPv4 and IPv6.
set qos signal	Set QoS signaling parameters (DSCP or 802.1Q) for the Media Gateway Processor.
show qos-rtcp	Display QoS, RSVP, and RTCP parameters for IPv4 and IPv6.

# Weighted Fair VoIP Queuing

Weighted Fair VoIP Queuing (WFVQ) combines weighted fair queuing (WFQ) for data streams and priority VoIP queuing to provide the real-time response time that is required for VoIP.

WFQ is applied to data streams to provide fair bandwidth distribution among different data streams, with faster response times for shorter packets that are typical for interactive applications, such as, telnet. Priority VoIP queuing is applied to VoIP bearer and signaling traffic.

WFVQ is the default queuing mode for all serial interfaces for which frame relay traffic-shaping is not enabled, and all FastEthernet interfaces for which traffic-shaping is enabled. It is also the only queueing mode available on a per-PVC basis for serial interfaces when frame relay traffic shaping is enabled.

# **Summary of WFVQ configuration CLI commands**

For more information about these commands, see Avaya Branch Gateway G450 CLI Reference.

Root level command	Command	Description
interface (serial) fastethernet (dialer)	-	Enter the Serial, FastEthernet, or Dialer interface configuration context
-	fair-queue-limit	Specify the maximum number of packets that can be queued in the weighted fair queue. The upper and lower limits of this command depend on the amount of bandwidth configured for the interface.  Use this command only for troubleshooting.
-	fair-voip-queue	Enable Weighted Fair VoIP Queuing (WFVQ) on the current interface. WFVQ is the recommended queuing mode for interfaces.
		The no form of the fair-voip-queue command does not exist. If you enter the command no fair-voip-queue, it will actually enable WFVQ if WFVQ is not already enabled.

Root level command	Command	Description
-	priority-queue	Enable or disable priority queuing mode in a Serial or FastEthernet interface.
-	show queue	Display information about the real-time status of output queues for the current interface
-	voip-queue	Enable or disable custom queueing for VoIP traffic. If you disable custom queueing, WFVQ is reenabled.
show queueing	-	Display the WFVG configuration

# **Priority queuing**

Priority queuing enables you to queue packets according to the priority of each packet. There are four levels of priority. The total number of packets in all queues cannot exceed 5000.

You can enable priority queueing on the following interfaces:

- Serial (DS1 PPP L2-L3, DS1 PPP L2, USP PPP L2, USP PPP L2-L3)
- FastEthernet (L2, L2-L3) when Traffic Shaping is configured
- Serial (DS1 FR L2, USP FR L2) when Frame Relay Traffic Shaping is not configured
- Dialer (L2, L2-L3)

Priority queueing is disabled by default, since the default and recommended queueing method is WFVQ.

The high priority queue can be further split into two parts for voice traffic: control packets and bearer packets. This is called VoIP queueing. When VoIP queuing is enabled, the bearer queue size is calculated to meet the estimated queueing delay, which is 20 ms by default. You can re-estimate the queueing delay, which results in a change in the bearer queue size.

# Summary of priority queueing configuration CLI commands

For more information about these commands, see Avaya Branch Gateway G450 CLI Reference.

Root level command	Command	Description
interface (serial)	-	Enter the Serial, FastEthernet, or Dialer interface
fastethernet		configuration context
dialer)		

Root level command	Command	Description
-	priority-queue	Enable or disable priority queuing mode in a Serial or FastEthernet interface.
		By default, priority queuing is off, and WFVQ is enabled on all serial interfaces and all FastEthernet interfaces for which traffic-shaping is enabled.
-	no priority-queue	Disable priority queing and re-enable WFVQ.
-	queue-limit	Set the size of any of the four priority queues, in packets, for a given interface or interface type. The default sizes depend on the bandwidth of the interface.
-	no queue-limit	Restore the packet size to its default value, using the interface bandwidth
-	voip-queue	Enable or disable custom queueing for VoIP traffic.
-	no voip-queue	Disable VoIP queueing and re-enable WFVQ
-	voip-queue-delay	Set the maximum query delay for which to estimate the high priority queue size necessary to meet the queuing delay.
show queueing	-	Display the priority queue configuration

# Chapter 10: Modems and Branch Gateway

You can connect either a USB or a serial modem to Branch Gateway. A USB modem must be connected to the USB port on Branch Gateway chassis. A serial modern must be connected to the Console port (CONSOLE) on Branch Gateway chassis.

The USB port and the Console port require configuration for modem use.

For more information about these commands, see Avaya Branch Gateway G450 CLI Reference.



### Note:

If you have an Avaya Service contract, no configuration of the USB port is necessary for Services personnel to remotely access Branch Gateway through a USB modem.

# **USB-modem interface configuration**

By default, the USB interface is enabled. Its default parameter values are:

• Interface status: = up

• PPP timeout absolute: = 10

• ppp authentication: = ras

• ip address: = 10.3.248.253 255.255.255.252

### Example of IP address to USB port assignment

The following example describes how the ip address command assigns the IP address 192.168.22.33 to the USB port: (if:USB)# ip address 192.168.22.33 255.255.255.0

The default IP address for the USB port is 10.3.248.253 255.255.255.252.

### The ppp authentication command parameters

The ppp authentication command is used with any of the following parameters:

- pap. Password Authentication Protocol. An unencrypted password is sent for authentication.
- · chap. Challenge Handshake Authentication Protocol. An encrypted password is sent for authentication. To configure this password, use the ppp chap-secret command.

### ■ Note:

If the Branch Gateway firmware is replaced by an earlier firmware version, the ppp chap-secret is erased, and must be re-configured.

- ras. Remote Access Service mode is being used for authentication. This is the default.
- none. No password is sent

### Note:

The ppp authentication command changes the PPP authentication parameters of the Console port as well as the USB port, even if you use the command in USB-modem interface context.

# Summary of CLI commands for configuring the USB port for modem use

For more information about these commands, see Avaya Branch Gateway G450 CLI Reference.

Root level command	Command	Description
interface usb-	-	Enter USB-modem interface configuration context
-	async modem-init- string	Change the default modem initialization string
-	async reset-modem	Reset the connected modem. You can use this command from within an active PPP session over the USB modem
-	ip address	Assign an IP address and mask to an interface. This is the IP address to which a remote user can connect using SSH/Telnet.
-	ip peer address	Change the IP address offered to a requesting calling host during PPP/IPCP connection establishment. By default, the interface offers its own IP address plus one.
-	ppp authentication	Configure the authentication method used when starting a client session on the PPP server.
-	ppp chap-secret	Configure the shared secret used in PPP sessions with CHAP authentication
-	ppp timeout authentication	Set the maximum time to wait for an authentication response
-	show ppp authentication	Display PPP authentication status
-	shutdown	Disconnect an active PPP session and shut down the modem

Root level command	Command	Description
-	timeout absolute	Set the number of minutes until the system automatically disconnects an idle PPP incoming session. By default, the timeout value is 10 minutes.
show interfaces	-	Display interface configuration and statistics for a particular interface or all interfaces
show interfaces	usb-modem	Display the USB-modem interface parameters, the current status of the USB port, and the identity of any USB modem connected to the USB port.

# Console port and modem configuration

The Console port is labeled CONSOLE. The Console port is an RJ-45 socket that functions as a serial port. You can connect a console device or serial modem to the Console port to access the CLI.

You can set the Console port so that it automatically detects whether a console device or a modem is connected to it. Enter async mode interactive to set the Console port to use modem mode every time an Avaya proprietary modem cable is plugged into the Console port. If you do not want the Console port to automatically detect when a modem is connected to it, enter async mode terminal to disable interactive mode.

### Note:

By default, async mode is set to terminal.

### Related links

CLI access on page 30

# Summary of CLI commands for configuring the Console port for modem use

For more information about these commands, see the Avaya Branch Gateway G450 CLI Reference

Root level command	Command	Description
interface console	_	Enter Console interface configuration context. Use the no form of this command to set the console parameters to their default values.
-	async mode interactive	Enter modem mode every time the proprietary modem cable is plugged into the Console port

Root level command	Command	Description
-	async mode terminal	Disable interactive mode on the Console
-	async modem-init- string	Change the default modem initialization string
-	async reset-modem	Reset the connected modem
-	ip address	Assign an IP address and mask to an interface. This is the IP address to which a remote user can connect using Telnet.
-	ip peer address	Change the IP address offered to a requesting calling host during PPP/IPCP connection establishment. By default, the interface offers its own IP address plus one.
-	ppp authentication	Configure the authentication method used when starting a client session on the PPP server
-	ppp chap-secret	Configure the shared secret used in PPP sessions with CHAP authentication
-	ppp timeout authentication	Set the maximum time to wait for an authentication response
-	show ppp authentication	Display PPP authentication status
-	shutdown	Disconnect an active PPP session and shut down the modem
-	speed	Set the PPP baud rate to be used by asynchronous PPP ports.
-	timeout absolute	Set the number of minutes until the system automatically disconnects an idle PPP incoming session. By default, there is no timeout.

# **Chapter 11: WAN interfaces**

You can use an MM340 E1/T1 media module or an MM342 USP media module as an endpoint for a WAN line on Branch Gateway. You can use a Fast Ethernet port on Branch Gateway chassis as the endpoint for a WAN line by configuring the FastEthernet interface for PPP over Ethernet (PPPoE). Branch Gateway serves as a router, as well as the endpoint, for the WAN line.



### Note:

The WAN interface modules are no longer available and the G450 version 4 does not support the MM340 and MM342 WAN interfaces.

#### Related links

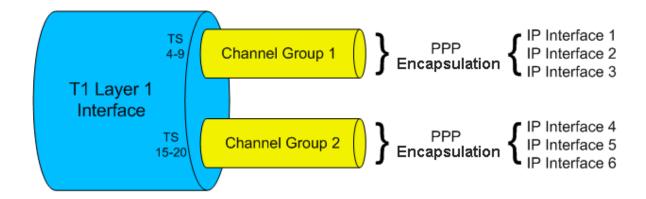
Router on page 380

# Serial interface overview

A Serial interface is a virtual interface that is created over a portion of an E1/T1 or USP port on a WAN media module. Serial interfaces support PPP and frame relay encapsulation protocols.

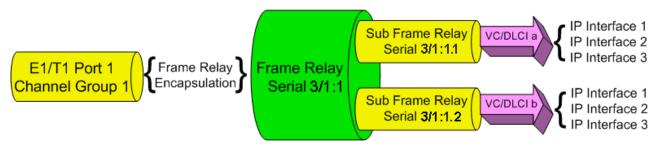
# Layer 1 T1 port with two channel groups

The following figure illustrates a Layer 1 T1 port with two channel groups defined. All data from each channel group is encapsulated using PPP protocol, and is distributed over the multiple IP interfaces defined for each channel group.



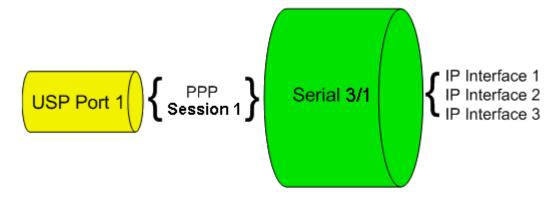
# E1/T1 port channel group

The following figure illustrates an E1/T1 port channel group. All data from the channel group is encapsulated using frame relay protocol. The data is sent via a frame relay Serial interface and sub-interfaces over the multiple IP interfaces defined using Data Link Connection Identifier (DLCI).



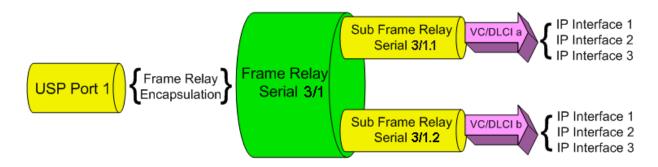
# **USP port using PPP protocol**

The following figure illustrates a USP port. All data from the USP port is encapsulated using the PPP protocol, and is sent via a Serial interface over the multiple IP interfaces defined for the Serial interface.



### USP port using frame relay protocol

The following figure illustrates a USP port. All data from the USP port is encapsulated using the frame relay protocol, and is sent through a frame relay Serial interface and sub-interfaces over the single IP interfaces defined using DLCI.



### Frame Relay multipoint topology support

Branch Gateway supports point-to-point frame relay connections. To enable you to use the Gateway as an endpoint in a Point to Multi-Point (PTMP) topology, Branch Gateway supports inverse ARP replies. Branch Gateway responds to inverse ARP queries received on frame relay sub-interfaces with the proper inverse ARP replies.

When you connect Branch Gateway as an endpoint in a PTMP configuration, you need to increase the OSPF timers manually. Use the ip ospf network point-to-multipoint command in Serial interface context to increase the OSPF timers with the following values:

- Increase the OSPF Hello Interval to 30 seconds
- Increase the OSPF Dead Interval to 120 seconds

#### Related links

OSPF on page 419

### Configuring the initial WAN

#### **Procedure**

- 1. Add one of the following WAN media modules:
  - Avaya MM340 E1/T1 media module
  - Avaya MM342 USP media module



#### Note:

You can also use the Fast Ethernet port on the Branch Gateway chassis as the endpoint for a WAN line by configuring this interface for PPPoE.

2. Connect the WAN line to the media module.

For more information see

For more information, see *Installing and Upgrading the Avaya Branch Gateway G450*.

- 3. Configure the WAN interface on the WAN media modules MM340 and MM342.
- 4. By default, a Branch Gateway WAN interface uses Point-to-Point Protocol (PPP).
- 5. If you want frame relay encapsulation on the WAN, configure frame relay.
- 6. Test the WAN configuration.
  - See WAN configuration and testing connectivity section.
- 7. Enter copy running-config startup-config to save the configuration.

#### Related links

Configuring PPPoE on page 227

### The Avaya MM340 E1/T1 WAN media module

### Configuring Avaya MM340 E1/T1 WAN media module

#### About this task

Use this procedure to configure Avaya MM340 E1/T1 WAN media module.

#### **Procedure**

- 1. Optionally, use the show controllers command to display the current settings.
- 2. Enter **show ds-mode** to check whether the Branch Gateway is configured for E1 or T1 operation.
- 3. Use the ds-mode command to set the mode of the Branch Gateway to E1 or T1.
  - Changing the line type requires resetting the module. The default value is T1.
- 4. Use the controller {e1 | t1} module\_number/port\_number command to enter Controller context for the port to be configured.
  - The prompt changes to:(super-if:Serial s/p)#, where s is the slot number of the media module, and p is the port number.
- 5. Use the following commands to change the clock source, frame type, linecode, or cable length parameters from the default settings:
  - For T1 mode:
    - clock source line|internal (default is line)
    - framing sf|esf (default is sf)

- linecode ami|b8zs (default is ami)
- cablelength long|short (default is long, gain26, 0db)

### **Note:**

Use the cablelength command to configure the cable's transmit and receive levels. If the cable is longer than 655 feet, use the command cablelength long gain26|gain36 -15db|-22.5db|-7.5db|0db (default is gain26, 0db). If the cable is 655 feet or less, use the command cablelength short 133ft|266ft|399ft|533ft|655ft (default is 133ft). When using the cablelength short form of the command, the transmit attenuation is configured using the loop length.

- fdl ansi|att|both (default is both)

### Note:

The **fdl** command defines the type of Facility Data Link loopback that the remote line is requested to enter. This command can only be used when ESF framing is defined.

- For E1 mode:
  - clock source line|internal (default is line)
  - framing crc4|no-crc4|unframed (default is crc4)
  - linecode ami|hdb3 (default is hdb3)
- 6. Use the **channel-group** command to specify the channel group and time slots to be mapped, as well as the DS0 speed.

#### Example:

- For T1 mode: channel-group 1 timeslots 1,3-5,7 speed 64 configures time slots numbered 1, 3-5, and 7 to be mapped in channel-group number 1, and sets the DS0 speed to 64 kbps. The default DS0 speed for T1 mode is 56
- For E1 mode: channel-group 1 timeslots 1,3-5,7 speed 64 configures time slots numbered 1, 3-5, and 7 to be mapped in channel-group number 1, and sets the DS0 speed to 64 kbps. The default DS0 speed for E1 mode is 64.
- 7. Enter exit to return to general context.

The prompt returns to:

Gxxx-001(super)#

8. Use the interface serial command to enter the Serial interface context.

Specify the slot number of the media module, the port number, the channel group number, and optionally, the IP interface number.

If you do not specify an IP interface number for the first Serial interface that you define on a channel group, the Branch Gateway automatically assigns IP interface number 0. For

each additional Serial interface that you define on the channel group, use a different IP interface number.

#### For example:

- interface serial 3/1:1. Enter a serial interface on the media module in slot number 3, on port number 1, with channel group number 1.
- interface serial 4/1:2.3. Enter a serial interface on the media module in slot number 4, on port number 1, with channel group number 2, and with IP interface number 3.

### Note:

If you use the framing unframed command in Step 5 for an E1 port, a channel group is automatically created on the entire E1 bandwidth. The channel group has the number 0. In Step 8, enter interface serial s/p:0, where s is the slot number and p is the port number.

### Note:

After the Serial interface is created, its default encapsulation is PPP.

- 9. Configure the interface encapsulation.
  - By default, the Serial interface uses PPP encapsulation.
- 10. Use the **ip address** command to configure the IP address and subnet mask of the interface.
- 11. Enter exit to return to general context.

The prompt returns to:

Gxxx-001(super)#

- 12. If needed, repeat Step 8 through Step 10 to configure additional IP interfaces on the same channel group.
- 13. If needed, repeat Step 6 through Step 10 to configure additional channel groups on the same E1 or T1 port.
- 14. Test the WAN configuration.

See WAN configuration and testing connectivity.

15. Enter copy running-config startup-config to save the configuration.

### E1/T1 default settings

Function	Default setting
DS mode	T1
E1 framing	CRC4

Function	Default setting
T1 framing	SF
E1 linecode	HDB3
T1 linecode	AMI
Clock source	Line
T1 cable length	Long, Gain 26,0 db
Speed	E1: 64kbps
	T1: 56kbps

### Commands used to reset and display controller counters

Use the following commands to reset counters on a controller interface:

- · clear controller counters
- remote

Use the following commands to display counters on a controller interface:

- show controllers
- show controllers remote

For a full description of the commands and their output fields, see *Avaya Branch Gateway G450 CLI Reference*.

### Commands used to activate loopback mode on an E1/T1 line

Use the following loopback commands to activate or deactivate loopback mode for an E1 or T1 line.

- · loopback diag
- · loopback local
- · loopback remote

### **Summary of E1/T1 ports configuration commands**

For a full description of the commands and their output fields, see *Avaya Branch Gateway G450 CLI Reference*.

Root level command	Command	Description
clear controller counters	-	Reset the controller counters
controller	-	Enter configuration mode for a specific controller

Root level command	Command	Description
-	cablelength long(T1)	Set transmit and receive levels for a cable longer than 655 feet
-	cablelength short(T1)	Set transmit levels for a cable of length 655 feet or shorter
-	channel-group	Create a channel group logical interface for a PPP or Frame Relay session
-	clock source	Set the clock source for an E1 or T1 controller
-	fdl	Define the type of Facility Data Link loopback that the remote line is requested to enter
-	framing	Set the frame type for an E1 or T1 data line
-	linecode	Set the type of line-code transmission for the E1 or T1 line
-	loopback	Put a T1 or E1 line into loopback mode or disable loopback mode
-	loopback remote	Request a remote station to activate or deactivate a line or payload loopback signal on the controller interface. This command is applicable only to a T1 line.
ds-mode	-	Set the mode of the controller: e1 or t1
interface serial	-	Enter Serial interface or sub interface configuration context
-	ip address	Configure the IP address and subnet mask of the interface
show controllers	-	Display status information about a controller interface
show controllers remote	-	Display controller statistics from a peer station
show ds-mode	-	Display the current mode of the controller

## Avaya MM342 USP WAN media module

# Configuring Avaya MM342 USP WAN media module

#### **Procedure**

1. Use the interface serial command to enter the context of the interface.

Specify the slot number of the media module, the port number, and optionally the IP interface number.

If you do not specify an IP interface number for the first Serial interface that you define on a port, the Branch Gateway automatically assigns IP interface number 0. For each additional Serial interface that you define on the port, use a different IP interface number.

#### For example:

- interface serial 3/1. Enter a serial interface on the media module in slot number 3, on port number 1.
- interface serial 4/1.2. Enter a serial interface on the media module in slot number 4, on port number 1, with IP interface number 2.

Gxxx-001(super)# interface serial 3/1

#### The prompt changes to:

Gxxx-001(super-if:serial 3/1)#

- 2. Use the following commands to change the idle characters, transmitter delay, encoding type, bandwidth parameters, line monitoring, and from their default settings:
  - idle character flags | marks. Set the bit pattern used to indicate an idle line. Use the no form of this command to restore the default value (flags).
  - transmitter-delay number. Set the minimum number of flags to be sent between successive packets. Use the no form of the command to restore the transmitter-delay value to the default (0).

### Note:

The transmitter-delay command is usually used when the DCE equipment that is connected directly to the Gateway, or the router on the WAN have a receive buffer that is not large enough to hold the traffic sent by the Gateway. In this case, configure transmitter-delay on the DCE equipment or the remote router in order to preserve the high performance that you had when transmitter-delay was configured to 0 on the Gateway.

- nrzi-encoding. Enable the non-return-to-zero inverted (NRZI) line coding format on the specified interface. Use the no form of the command to disable NRZI encoding.
- bandwidth kbps. Set the bandwidth parameter manually for the interface. Use the no form of this command to restore the bandwidth parameter to its default value (2,048). The manually specified bandwidth value overrides the dynamically calculated bandwidth during route cost calculations.

### **₩** Note:

If you are using the USP port as a clock source, configure the port's bandwidth to match the DCE clock rate.

• ignore dcd. Specify how the system monitors the line to determine if it is up or down. Specify ignore dcd to ignore DCD signals, and instead use DSR/CTS signals to determine the line's status. Use the no form of the command to specify that DCD signals are used to determine line status.

- invert txclock. Invert the transmit clock signal from the data communications equipment (DCE). Use the no form of the command to restore the signal to not inverted.
- 3. Configure the interface encapsulation.
- 4. Enter exit to return to general context.

The prompt returns to:

Gxxx-001(super)#

- 5. Repeat Step 1 to configure additional Serial interfaces on the USP port.
- 6. Test the WAN configuration.
- 7. Enter copy running-config startup-config to save the configuration.

#### Related links

Configuring frame relay on page 230

Commands used for WAN configuration and testing connectivity on page 233

### **USP** default settings

Function	Default setting
Encoding	NRZ
Bandwidth	2,048 kbps
Line-up indicator signal	DCD

### **Summary of USP port configuration commands**

For more information about these commands, see Avaya Branch Gateway G450 CLI Reference.

Root level command	Command	Description
interface serial	-	Enter Serial interface or sub interface configuration context
-	bandwidth	Set the bandwidth parameter manually for this interface
-	idle-character	Set the bit pattern used to indicate an idle line
-	ignore dcd	Specify how the system monitors the line to determine if it is up or down
-	invert txclock	Invert the transmit clock signal from the data communications equipment (DCE)
-	ip address	Configure the IP address and subnet mask of the interface
-	nrzi-encoding	Enable or disable the non-return-to-zero inverted (NRZI) line coding format on the interface

Root level command	Command	Description
-	transmitter-delay	Set the minimum number of flags to be sent between successive packets
		between successive packets

### **PPP** configuration

### **Configuring PPP**

#### About this task

PPP is the default encapsulation on a WAN port. If the encapsulation has been changed to frame relay and you want to restore PPP encapsulation, or to change the PPP parameters:

#### **Procedure**

- 1. Ensure that you are in the context of a serial interface that is defined on the port.
  - If you are not in the context of a serial interface, use the interface serial command. To view all Serial interfaces that are defined, use the show interfaces serial command.
- 2. If the interface is not already configured to use PPP encapsulation, enter **encapsulation ppp** to change the encapsulation to PPP.
- 3. (Optional) Change the queuing mode of the interface.
- 4. Use the following commands to change the interface parameters:
  - ip address. Configure the IP address and subnet mask of the interface.
  - ppp timeout ncp. Set the maximum time to wait for the network layer to negotiate. If this time is exceeded, the Gateway restarts the PPP session.
  - ppp timeout retry. Set the maximum time to wait for a response during PPP negotiation.
  - **keepalive**. Enable keepalive or change the interval to which keepalive is set. When activated, keepalive performs the initial negotiation and sends health checks at defined intervals to the other side of the interface. To deactivate keepalive, use the **no** form of the command or set the health check interval to 0.
- Enter exit to return to general context.

The prompt returns to:

Gxxx-001(super)#

- 6. Test the WAN configuration.
- 7. Enter copy running-config startup-config to save the configuration.

#### **Related links**

Weighted Fair VoIP Queuing on page 208

Commands used for WAN configuration and testing connectivity on page 233

### **Summary of PPP configuration commands**

For more information about these commands, see the Avaya Branch Gateway G450 CLI Reference.

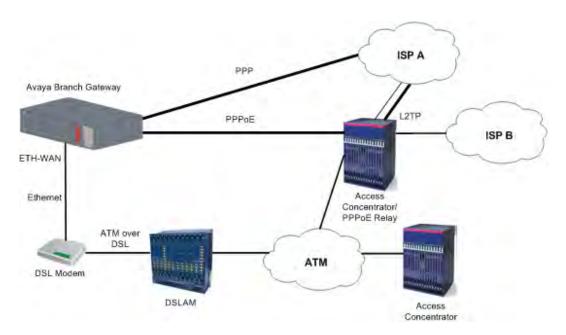
Root level command	Command	Description
interface serial	-	Enter Serial interface or sub interface configuration context
-	encapsulation	Set the encapsulation mode for a Serial interface: PPP or frame relay
-	ip address	Configure the IP address and subnet mask of the interface
-	keepalive	Enable PPP keepalive, in order to maintain a persistent connection
-	ppp timeout ncp	Set the maximum time, in seconds, that PPP allows for negotiation of a network layer protocol
-	ppp timeout retry	Set the maximum time to wait for a response during PPP negotiation
show interfaces	-	Display interface configuration and statistics for a particular interface or all interfaces

### **PPPoE** overview

You can configure ETH WAN Fast Ethernet ports as a WAN port using PPPoE (PPP over Ethernet). PPPoE offers dialup style authentication and accounting and allows subscribers to dynamically select their ISP.

PPPoE is a client-server protocol used for carrying PPP-encapsulated data over Ethernet frames. A PPPoE client can establish a tunnel that carries PPP frames between a dialing host (the Branch Gateway) and an access concentrator. This enables the use of PPP authentication protocols (CHAP and PAP). Unlike other tunneling protocols such as L2TP and PPTP, PPPoE works directly over Ethernet rather than IP.

A typical broadband access network is based on ADSL modems configured as transparent Ethernet bridges. ADSL modems use ATM protocol, and the transparent bridging is done to a well known ATM VC. On the other side of the telephone line is a device called a DSLAM. The DSLAM terminates the ADSL physical layer, collects the ATM cells from the various ADSL subscribers, and places them on the SP ATM infrastructure. The Ethernet frames from the customer's host device can reach one or more access concentrators, which are the remote access servers.



### **Configuring PPPoE**

#### **Procedure**

- 1. Enter the FastEthernet interface context with the interface fastethernet 10/2 command.
- 2. Enter encapsulation pppoe to change the encapsulation to PPPoE.

You must change the encapsulation to PPPoE before configuring an IP address on the interface.



#### Note:

You cannot use PPPoE if:

- An IP address must not be configured on the interface
- Dynamic CAC is not enabled on the interface.
- The interface is not part of a primary-backup interface pair.
- 3. Use the **ip address** command to configure an IP address and subnet mask for the interface.

In most cases, PPPoE tunnels require a 32-bit subnet mask.

Alternatively, you can enter ip address negotiated to obtain an IP address via PPP/IPCP negotiation.



#### Note:

You cannot configure PPP/IPCP address negotiation if DHCP address negotiation is already configured on the interface.

- 4. Configure an authentication method and parameters:
  - For PAP authenticating, enter ppp pap-sent username followed by a user name and password. For example:

```
Gxxx-001(super-if:FastEthernet 10/2)# ppp pap-sent username avaya32 password
******
Done!
```

• For CHAP authentication, enter ppp chap hostname followed by a hostname, and ppp chap password followed by a password. For example:

```
Gxxx-001(super-if:FastEthernet 10/2)# ppp chap hostname avaya32
Done!
Gxxx-001(super-if:FastEthernet 10/2)# ppp chap password ******
Done!
```

5. If the Branch Gateway is connected to the Internet via the FastEthernet interface configured for PPPoE, and you define a VPN tunnel which specifies remote hosts by name, it is recommended to use the ppp ipcp dns request command.

The command requests the list of available DNS servers from the remote peer during the PPP/IPCP session. The DNS servers are used by the DNS resolver to resolve hostnames to IP addresses.

6. Enter exit to return to general context.

The prompt returns to:

```
Gxxx-001(super)#
```

7. Test the configuration.

See WAN configuration and testing connectivity.

- 8. Enter copy running-config startup-config to save the configuration.
- 9. Optionally, shut down the port and the PPPoE client, if configured, with the **shutdown** command in the interface context.

#### **Related links**

Dynamic CAC on page 256

Backup interfaces on page 234

**DHCP client configuration** on page 178

### **Summary of PPPoE commands**

For more information about these commands, see Avaya Branch Gateway G450 CLI Reference.

Root level command	Command	Description
interface fastethernet	-	Enter the FastEthernet interface context
-	encapsulation pppoe	Change the encapsulation to PPPoE

Root level command	Command	Description
-	ip address	Configure an IP address and subnet mask for the interface
-	ip address negotiated	Obtain an IP address via PPP/IPCP negotiation
-	keepalive	Enable PPP keepalive, in order to maintain a persistent connection
-	keepalive-track	Bind interface status to an object tracker to check whether the interface is up
-	mtu	Set the interface's MTU to 1492, which ensures that overall packet size for the PPPoE interface does not exceed 1500, which is the MTU for Ethernet
-	ppp chap hostname	Override the device hostname for PPP CHAP authentication
-	ppp chap password	Set the CHAP password for authentication with a remote peer
-	ppp chap refuse	Prevent the device from authenticating with CHAP after the device is requested by the remote peer
-	ppp ipcp dns request	Enable or disable requesting the list of available DNS servers from the remote peer during the PPP/IPCP session
-	ppp pap refuse	Prevent the device from authenticating with PAP after the device is requested by the remote peer
-	ppp pap-sent username	Set the Password Authentication Protocol (PAP) password for authentication with the remote peer
-	ppp timeout ncp	Set the maximum time, in seconds, that PPP allows for negotiation of a network layer protocol
-	ppp timeout retry	Set the maximum time to wait for a response during PPP negotiation
-	pppoe-client persistent delay	Set the interval between pppoe-client dial attempts
-	pppoe-client persistent max- attempts	Limit the number of consecutive connection establishment retries
-	pppoe-client service- name	Set the PPPoE Client service-name

Root level command	Command	Description
-	pppoe-client wait- for-ipcp	Set the amount of time (in seconds) between establishment of the PPPoE tunnel and establishment of the IPCP tunnel. If this time is exceeded, the PPPoE client terminates the PPPoE tunnel.
-	shutdown	Shut down the port, and the PPPoE client, if configured

### Frame relay

### **Configuring frame relay**

#### **Procedure**

- 1. Ensure that the port is configured on the media module.
- 2. Ensure that you are in the context of a serial interface that is defined on the port.

If you are not in the context of a serial interface, use the interface serial command. To view all Serial interfaces that are defined, use the show interfaces serial command.

3. Use the encapsulation frame-relay command to change the encapsulation to frame

You can optionally specify the encapsulation type: IETF (RFC1490/RFC2427) or non-IETF. The default encapsulation type is IETF.



### Note:

Non-IETF encapsulation is compatible with other vendors.

- 4. If needed, use the frame-relay lmi commands to change the Local Management Interface (LMI) parameters from their default values, or enter frame-relay trafficshaping to activate traffic shaping on the frame relay interface.
- 5. Optionally, change the queuing mode of the interface.
- Enter exit to return to general context.

The prompt returns to:

Gxxx-001 (super) #

7. Enter interface serial if.fr-sub-if point-to-point to create a frame relay sub-interface and enter the context of the interface.

#### For example:

- interface serial 3/1:2.1 point-to-point. Create frame relay sub-interface number 1 on the E1/T1 media module in slot number 3, on port number 1, with channel group number 2
- interface serial 4/1:2.3.2 point-to-point. Create frame relay subinterface number 3 on the E1/T1 media module in slot number 4, on port number 1, with channel group number 2, and with IP interface number 2
- interface serial 3/1.2 point-to-point. Create frame relay sub-interface number 2 on the USP media module in slot number 3, on port number 1
- interface serial 4/1.2.1 point-to-point. Create frame relay sub-interface number 2 on the USP media module in slot number 4, on port number 1, with IP interface number 1

### Note:

Currently only point-to-point frame relay sub-interfaces are supported.

8. Enter frame-relay interface-dlci DLCI-number to configure a Data Link Connection Identifier (DLCI) for the frame relay sub-interface.

You can optionally specify the encapsulation type: IETF (RFC1490/RFC2427) or non-IETF. The default encapsulation type is IETF.

### Note:

Non-IETF encapsulation is compatible with other vendors.

9. If required, use the **frame-relay priority-dlci-group** command to configure a Priority DLCI group.

The arguments for this command are the DLCIs you want to assign to high, medium, normal, and low priority traffic, respectively. For example, the command frame-relay priority-dlci-group 17 18 19 assigns DLCI 17 to high priority traffic, DLCI 18 to medium priority traffic, and DLCI 19 to normal and low priority traffic.

- 10. Use the ip address command to configure an IP address and subnet mask for the frame relay sub-interface.
- 11. Enter exit to return to general context.

The prompt returns to:

Gxxx-001(super)#

- 12. If needed, repeat Step <u>7</u> on page 230 through Step <u>11</u> on page 231 to configure additional frame relay sub-interfaces on the same Serial interface.
- 13. If needed, repeat Step 2 on page 230 through Step 12 on page 231 to configure frame relay encapsulation for other Serial interfaces on the same WAN port.
- 14. Test the WAN configuration.

15. Enter copy running-config startup-config to save the configuration.

#### **Related links**

Configuring Avaya MM342 USP WAN media module on page 222 Configuring Avaya MM340 E1/T1 WAN media module on page 218 Frame relay traffic shaping and FRF.12 fragmentation on page 271 Weighted Fair VoIP Queuing on page 208

# Commands used to reset and display frame relay interface counters

- clear frame-relay counters
- show interfaces

For a full description of the commands and their output fields, see *Avaya Branch Gateway G450 CLI Reference*.

### **Summary of frame relay commands**

For more information about these commands, see Avaya Branch Gateway G450 CLI Reference.

Root level command	Command	Description
clear frame-relay counters	-	Clear the frame relay counters
interface serial	-	Enter Serial interface or sub interface configuration mode
-	encapsulation	Set the encapsulation mode for a Serial interface
-	frame-relay class- dlci	Associate a Virtual Channel with a named QoS or Traffic shaping template (map-class)
-	frame-relay interface-dlci	Associate a frame relay Virtual Channel with the current interface
-	frame-relay lmi- n391dte	Set the number of status enquiry intervals that pass before issuing a full status enquiry message
-	frame-relay lmi- n392dte	Set the maximum number of unanswered status enquiries the equipment accepts before declaring the interface down
-	frame-relay lmi- n393dte	Set the number of status polling intervals over which the error threshold is counted (the monitored event count)
-	frame-relay lmi-type	Manually define the type of the Local Management Interface (LMI) to use

Root level command	Command	Description
-	frame-relay priority- dlci-group	Assign Virtual Channels to priority classifications, for supporting traffic separation
-	frame-relay traffic- shaping	Turn on or off traffic shaping and frame relay fragmentation
-	ip address	Configure an IP address and mask for the interface
show interfaces	-	Display interface configuration and statistics for a particular interface or all interfaces

### WAN configuration and testing connectivity

### Commands used for WAN configuration and testing connectivity

After configuring the new interface, you can perform the following tests to verify that the new interface is operating correctly.

• For E1/T1 interfaces, use the **show controllers** command to view the status of the interface's controller. Verify that the controller is up, and that all error counters do not increase.

For all serial interfaces (E1/T1 and USB-modem), use the **show interfaces serial** command to verify that the interface and line protocol are both up. For example:

```
Serial x/y:z is up, line protocol is up
```

• For the USB-modem interface and the Fast Ethernet interface, use the **show interfaces** command to verify that all line signals are up. For example:

```
DCD = up DSR = up DTR = up RTS = up CTS = up
```

- Use the show frame-relay pvc command to view detailed PVC information, or show frame-relay pvc brief for a brief summary of PVC configuration.
- Use the following commands for more information about frame relay configuration:
  - **show frame-relay fragment**. Display frame relay fragmentation statistics and configuration on all PVCs associated with the interface.
  - show frame-relay 1mi. Display LMI statistics for the interface.
  - **show frame-relay map**. Display a summary table of frame relay sub-interfaces and DLCIs associated with the sub-interfaces.
  - **show frame-relay traffic**. Display frame relay protocol statistics, including ARP requests and replies sent and received over the interface.
  - show map-class frame-relay. Display the map-class Frame Relay table.
- Use the **show traffic-shape** command to view traffic shaping and frame relay traffic shaping configuration parameters for all interfaces.

- Use the **show ip interface** command to display information about IP interfaces. To display information about a specific interface, include the name of the interface as an argument. To display information about the interface of a specific IP address, include the IP address as an argument.
- Enter show running-config to display the configuration running on the device.
- Enter show startup-config to display the configuration loaded at startup.
- Use the ping command to send ICMP echo request packets from the Branch Gateway to the interface Serial peer IP address and verify that it responds.

### Summary of WAN configuration verification commands

For more information about these commands, see Avaya Branch Gateway G450 CLI Reference.

Command	Description	
ping	Check host reachability and network connectivity	
show controllers	Display status information about a controller interface	
show frame-relay fragment	Display frame relay fragmentation statistics and configuration on all PVCs, all PVCs associated with an interface, or a specific PVC	
show frame-relay lmi	Display LMI statistics for a particular interface or for all interfaces.  The output displayed differs depending on the type of interface.	
show frame-relay map	Display a summary table of Frame Relay sub-interfaces and DLCIs associated with the sub-interfaces	
show frame-relay pvc	Display detailed PVC information	
show frame-relay pvc brief	Display brief PVC information	
show frame-relay traffic	Display frame relay protocol statistics, including ARP requests and replies sent and received over Frame Relay interfaces	
show interfaces	Display interface configuration and statistics for a particular interface or all interfaces	
show ip interface	Display information about an IP interface	
show map-class frame- relay	Display the map-class Frame Relay table	
show traffic-shape	Display traffic shaping and frame relay traffic shaping configuration information	

### **Backup interfaces**

You can configure backup relations between a pair of any Layer 2 Serial interfaces. A backup interface is activated when the primary interface fails. The backup interface is deactivated when the primary interface is restored. A PPP session, frame relay interface, frame relay sub-interface, Dialer interface, FastEthernet interface, or Loopback interface can serve as a backup interface to any other Serial interface on the same module including interfaces on different serial ports.

### Note:

A frame relay interface in a primary or backup role overrides the role of its sub-interfaces.

If the FastEthernet interface serving as a backup interface is configured as a DHCP client, it sends no DHCP packets. Therefore, its IP address is not renewed until it becomes the primary interface. If the FastEthernet interface serving as a primary interface is configured as a DHCP client, the expiry of the leases on its IP address or no reception of an IP address does not activate the backup interface.

### **Backup delay configuration**

Configurable activation and deactivation delays provide a damping effect on the backup interface pair. This eliminates primary-to-backup switching in case of fluctuating underlying Layer 2 interfaces. You can configure the following backup delays with the backup delay command:

- failure delay. The time in seconds between the primary interface going down and the backup interface activation. The default is 0 seconds. The maximum is 3600 seconds.
- secondary disable delay. The time in seconds between the primary interface restoration and the backup interface deactivation. The default is 0 seconds. The maximum is 3600 seconds. Both interfaces are active during this time to enable a smooth transition for the routing protocols. To keep the backup interface active indefinitely, use never as the secondary disable delay.

#### **Example**

You can use the following command to switch over immediately to the backup interface in case of failure, and pause 60 seconds before reverting to the primary interface:

```
Gxxx-001(super)# interface fastethernet 10/2
Gxxx-001(super-if:FastEthernet 10/2)# backup delay 0 60
Done!
Gxxx-001(super-if:FastEthernet 10/2)#
```

### Interface backup relations rules

- Each interface can have only one backup interface.
- A backup interface can serve as a backup for only one other interface.
- Only one member of a primary and backup pair is active at any given time. An interface is automatically deactivated when configured as backup.
- The backup implementation does not protect against the failure of both interfaces. Therefore, if a backup interface fails while active, no switch to the primary interface is attempted.

When using frame relay encapsulation, the frame relay interface is considered down when its primary DLCI is down. The switchover back to the main interface occurs when the primary Data Link Connection Identifier (DLCI) is restored.

### Note:

The backup interface is not activated when the primary interface is administratively disabled.

### Summary of backup interfaces commands

For more information about these commands, see Avaya Branch Gateway G450 CLI Reference.

Root level command	Command	Description
interface (fastethernet  loopback  serial  tunnel)	-	Enter FastEthernet, Loopback, Serial, or Tunnel interface configuration context
-	backup delay	Set the time to wait before switching over to the backup interface, in case of failure. You can also use this command to set a delay before reverting back to the primary interface.
-	backup interface	Set a backup interface for the current interface followed by the interface type and number. You must use this command from the context of the interface for which you are setting a backup interface.

### Modem dial backup

The modem dial backup feature allows Branch Gateway to utilize a modem to provide redundant connectivity between Branch Gateway and IP phones in a small branch office and their primary Media Gateway Controller (MGC) at the headquarters or a regional branch office.

Even if Branch Gateway has Standard Local Survivability (SLS), or Enhanced Local Survivability (ELS) using a local S8300 in Survivable Remote Server mode, it is always preferable to continue working with the primary MGC, since features are lost when the system is fragmented.

Analog modems have limited bandwidth and high latency, and are therefore unfit for carrying VoIP traffic. However, using Dynamic Call Admission Control (CAC), Branch Gateway can be configured to report zero bandwidth for bearer traffic to the MGC when the primary WAN link fails. A matching configuration on the MGC allows it to block new calls, if their bearer is about to go over the modem dial backup interface, and to alert the user with a busy tone. In this case, the user is still able to place external calls manually if local PSTN trunks are available. Furthermore, CM 3.0 Inter-Gateway Alternate Routing (IGAR) may be configured to become active in such a case and to use the PSTN for transporting the voice bearer transparently between the sites, transparently to the user. For information about IGAR, see *Administrator Guide for Avaya Aura® Communication Manager*.

Modem dial backup is a generic data dial backup feature that can carry not only signalling but every type of IP traffic. However, the low bandwidth of an analog modem would be likely to cause congestion. The administrator must therefore ensure that VoIP signaling has priority over the Dialer interface. This can be performed using access control lists (ACL), QoS lists, and Weighted Fair Queuing (WFQ) priority schemes. The administrator should apply these tools in both Branch Gateway and the Remote Access Server (RAS).

You can configure modem dial backup to dial to an enterprise-owned RAS or to the Internet via an Internet Service Provider (ISP). Most ISPs mandate the use of the internal IPSec VPN gateway process to encrypt the traffic as it goes over the Internet.

### Note:

IPSec VPN adds overhead to each packet, further reducing available bandwidth.

Under ideal conditions, the bandwidth of the analog modem can reach 56 kbps for downlink (53 kbps in the US) and 33.6 kbps for uplink. However, sub-optimal PSTN quality may degrade the downlink bandwidth to 33.6 kbps, or even 28 kbps. This may not be enough to carry a single ISDN-PRI 64 kbps D-Channel for signalling over H.248 to and from the MGC, even without considering the need to support IP phones and/or analog or DCP trunks.

VoIP signaling consumes bandwidth when setting up and tearing down calls. However, calculations, testing, and field experience show that an analog modem can easily support a small branch office when the expected Busy Hour Call Completion (BHCC) is limited.

### Note:

The low bandwidth and high Round-Trip-Time (RTT) of analog modems (~100 ms) may lead to acceptable changes in Post-Dial-Delay (PDD) and offhook-to-dialtone delays.

Modem dial backup uses Branch Gateway backup interface functionality to activate the Dialer interface for modem dial backup when the primary interface fails and to deactivate the Dialer interface when the primary interface is up again. Currently, modem dial backup does not support such features as Dial On Demand Routing (DDR), callbacks, or RAS. Modem dial backup cannot receive backup calls.

### Note:

You can only backup one interface with modem dialer backup.

Using Branch Gateway backup interface functionality, you can designate the Dialer interface as the backup for the main WAN link. However, this method is not always available, since an 'up' WAN link status does not ensure connectivity, and the main WAN link may not even be directly connected to Branch Gateway.

The workaround is to use Branch Gateway object tracking feature to verify connectivity to the primary MGC using Respond Time Reports (RTRs) and object trackers. Configure object tracking to change the state of the Loopback interface accordingly, and configure the Dialer interface as a backup to the Loopback interface.

Modem dial backup uses a modem connected directly to Branch Gateway USB or Console port. The modem can also be used to access Branch Gateway CLI from a remote location. The modem cannot do both at the same time.

Finally, IP routing must be configured so that traffic to and from the site uses the Dialer interface when the primary interface is down. The Dialer interface can work both with static and dynamic routing (OSPF and RIP). Note that the latter mandates the use of unnumbered IP interfaces.

#### Note:

Modem dial backup has complex interactions with other configuration modules within Branch Gateway and on your network. Before configuring modem dial-backup, Avaya recommends reading Application Note - VoIP Network Resiliency. This document discusses the issues of network design for maximum resiliency, capacity planning for optimum performance, configuration options for network devices, strategies for implementing routing across the network, and security concerns. Based on your existing network design, several redundancy scenarios featuring modem dial backup are available.

Modem dial backup does not support backup dial-ins or callbacks. Some backup configurations require the remote host to receive a request for connection, acknowledge, end the connection, and dial back the requester. This configuration is not supported.

#### Related links

Dynamic CAC on page 256

Policy lists on page 497

Weighted Fair VoIP Queuing on page 208

Backup interfaces on page 234

Object tracking on page 258

CLI access using modems on page 32

Unnumbered IP interfaces on page 384

Modem dial backup interactions with other features on page 242

### Typical installations

The Branch Gateways were designed for small branch offices of a larger enterprise. Consequently, the same RAS may serve many branch offices, and, therefore, many Branch Gateways. A reasonable assumption is that not all branch offices would need modem dial backup at the same time. Therefore, the ratio of modem channels at the RAS to Branch Gateways at branch offices can be less than 1:1. There are several practical ways to configure the RAS server for use with modem dial backup Dialer interfaces:

- The RAS can assign an IP address to the calling Branch Gateway. This requires the RAS to identify the call gateway using the PAP/CHAP username, and install an appropriate static route to the branch office subnets accordingly. The username, password, and static route can be configured in an external RADIUS/TACACS+ server.
- The RAS server can use OSPF to learn the branch office subnets. This is much simpler to configure as all branch offices can share the same username and password. The Branch Gateway is configured to advertise the branch office subnets with OSPF. This feature requires the use of unnumbered IP addresses at the Branch Gateway and the RAS. Since the Dialer and the primary interfaces are not expected to be up at the same time, the RAS server can use passive-OSPF-interface and the Branch Gateway can use static via routes.
- The Branch Gateway can call an ISP RAS (which is likely to assign it a dynamic IP address) and open an IPSec VPN tunnel to an enterprise-owned VPN gateway.

While using OSPF and calling an ISP RAS are expected to be the most common scenarios, they involve complex interaction with IP routing and the remote RAS server. For more detailed configuration examples, see *Application Note - VoIP Network Resiliency*.

### Prerequisites for configuring modem dial backup

- At least one dialer string, which determines the phone number(s) of the remote modem(s) dialed by the Dialer interface
- · A configured interface to be backed up
- · Read/write or admin access level
- A modem: Multitech MultiModem ZBA (MT5634ZBA), or MultimodemUSB (MT5634ZBA-USB), or USRobotics USB modem (5637)

### Note:

Make sure policy is configured properly at the RAS server to ensure that signaling has priority over regular traffic.

Use the maximum UART speed for the serial modem (115400 BAUD).

### **Configuring modem dial backup**

#### **Procedure**

- 1. From the general context, use the show interfaces console or show interfaces USB-modem command to verify that the modem is connected. You may be required to enable the modem.
- 2. Enter interface dialer, followed by the identifier, to create the Dialer interface.

#### For example:

```
Gxxx-001(super)# interface dialer 1
Gxxx-001(if:dialer 1)#
```

The Dialer interface is created and can now be defined as a backup interface for an existing WAN interface.

3. Enter up to five dialer strings, using the dialer string command.

#### For example:

```
Gxxx-001(if:dialer 1)# dialer string 1 555555
Done!
Gxxx-001(if:dialer 1)# dialer string 2 1234567
Done!
```

When the Dialer interface is activated, the Dialer first attempts to dial the number associated with dialer string 1. If that attempt fails, the Dialer attempts to connect to the number associated with the next dialer string, and so on.

4. Set the IP address of the Dialer interface with the ip address command.

There are three options:

 Manually set the IP address and subnet mask. Use this option when you know to which server the dialed string is going to connect. For example:

```
Gxxx-001(if:dialer 1)# ip address 4.5.6.7 255.255.255.0 Done!
```

- Enter ip address negotiated.
- Enter ip unnumbered interface, where interface is the name of another interface in the gateway (for example, the WAN interface) from which an IP address for the Dialer interface is borrowed. Use this command when you do not know who will eventually be your peer and you want to run dynamic routing protocols (for example, OSPF or RIP) over the dialup link.
- 5. Enter dialer persistent initial delay, with the value 30 seconds, to prevent dialup after boot, before the WAN link is fully functional.

#### For example:

```
Gxxx-001(if:dialer 1)# dialer persistant initial delay 30
Done!
```

- 6. If needed, set any of the following parameters:
  - Use the dialer persistent max-attempts command to set the maximum number of dial attempts. For example:

```
Gxxx-001(if:dialer 1) # dialer persistent max-attempts 10
Done!
```

The Dialer interface dials each number associated with a dialer string, in order, until either a connection is made, or the number configured in the dialer persistent max-attempts command is reached.

• Use the dialer persistent re-enable command to enable and configure a timer to re-enable dial attempts after the maximum number of dial attempts has been reached. For example:

```
Gxxx-001(if:dialer 1)# dialer persistent re-enable 3600
Done!
```

• Use the dialer order command to set which dial strings are used upon a new dial trigger event. The default is to restart from the beginning of the dial list. For example:

```
Gxxx-001(if:dialer 1)# dialer order last-successful
Done!
```

• Use the dialer persistent command to force the dialer to attempt to reconnect every second, or at another redial interval, which you can configure using the dialer persistent delay command. By default, redialing is disabled. For example:

```
Gxxx-001(if:dialer 1) # dialer persistent
Done!
Gxxx-001(if:dialer 1) # dialer persistent delay 10
Done!
```

• Use the dialer wait-for-ipcp command to set the maximum time the dialer waits between dialing a number to successfully establishing PPP/IPCP. The default is 45 seconds. For example:

```
Gxxx-001(if:dialer 1)# dialer wait-for-ipcp 100
Done!
```

- 7. Configure an authentication method and parameters, if required:
  - For PAP authenticating, enter ppp pap sent-username followed by a username and password. For example:

```
Gxxx-001(if:dialer 1)# ppp pap sent-username avaya32 password ******
Done!
```

• For CHAP authentication, enter ppp chap hostname followed by a hostname, and ppp chap password followed by a password. For example:

```
Gxxx-001(if:dialer 1) # ppp chap hostname avaya32
Done!
Gxxx-001(if:dialer 1) # ppp chap password 123456
Done!
```

8. From the general context, use **show interfaces dialer** 1 to verify that the Dialer interface has connected to the remote peer.

#### For example:

```
Gxxx-001(super) # show interfaces dialer 1
Dialer 1 is down, line protocol is down
Internet address is 4.5.6.7, mask is 255.255.255.0
MTU 1500 bytes, Bandwidth 28 kbit
 IPSec PMTU: copy df-bit, Min PMTU is 300
 Reliability 1/255 txLoad 255/255 rxLoad 255/255
Encapsulation PPP
Link status trap disabled
Keepalive track not set
 Keepalive set (10 sec)
 LCP Starting
 IPCP Starting
 Last dialed string:
 Dial strings:
    1: 5555555
    2: 1234567
 Dialing order is sequential
 Persistent initial delay 5 sec
 Wait 45 sec for IPCP
 Weighted Fair VoIP queueing mode
 Last input never, Last output never
Last clearing of 'show interface' counters never
 5 minute input rate 0 bits/sec, 0 packets/sec
```

This command shows the interface status, including a summary of its definitions and settings. The status also tells you whether the interface is up and the dialup succeeded. In the example status, the interface is down and inactive.

9. Enter the context of the interface which the Dialer is to back up, and use the **backup interface** command to configure the Dialer interface as the backup interface.

#### For example:

```
Gxxx-001(if:serial 3/1:1)# backup interface dialer 1
```

Interface Dialer 1 is now selected as the backup interface to the selected interface. The Dialer interface is activated in the event of a failure of the primary interface. Upon activation, the Dialer interface dials the number associated with the first dialer string.

10. From the general context, use the ip default-gateway dialer command to configure backup routing.

The following example configures a simple low priority via static route:

```
Gxxx-001(super)# ip default-gateway dialer 1 1 low
Done!
```



### Note:

Define multiple routes to ensure that traffic reaches the Dialer interface.

### Modem dial backup interactions with other features

Optimal modem dial backup configuration is a complex undertaking, dependent on a large number of factors. For an extensive discussion of network design, capacity planning, routing configuration, device configuration, and security considerations, see Application Note - VoIP Network Resiliency. Device and network configuration features that need to be taken into account include:

- The backup interface command allows you to designate the Dialer interface as the backup to an existing WAN interface on the Branch Gateway. When the Branch Gateway reports the primary WAN interface down for a specified period of time, the Dialer interface is automatically activated and the modem dials.
- The Branch Gateway's Console port is an RJ-45 asynchronous port that can be used to support the modem for dial backup. Thus, the Dialer can use the same serial modem that is used for remote access to the device. Asynchronous dialing and modem recognition options must be set on the Console port to support creation of the Dialer interface.
- A Branch Gateway USB port can be used to support a USB modem for dial backup. Thus, the Dialer can use the same USB modem that is used for remote access to the device. Asynchronous dialing and modem recognition options must be set on the USB port to support creation of the Dialer interface.
- The Dialer interface supports PAP and CHAP authentication for PPP connections. In addition, the Dialer interface can be configured to be a member of a VPN, allowing encryption of the modem traffic. Van Jacobsen compression is available for encrypted traffic over the Dialer interface, allowing optimal use of bandwidth.
- It is recommended to filter traffic through the Dialer interface to permit only those packets necessary for continued interaction with the CM server. Filtering can be accomplished using access control lists, which specify traffic permissible through a selected interface.
- Dynamic CAC can be used in conjunction with IGAR to provide a stable backup path for continued IP phone function in the event of a dial backup scenario. Dynamic CAC notifies the CM server that no bandwidth is available for bearer traffic, keeping the dial circuit from becoming fully congested. IGAR provides a path for gateway-to-gateway traffic destined for

a remote CM server by forcing voice calls to and from the branch office to use the PSTN for bearer traffic. For more information on configuring IGAR, see *Administrator Guide for Avaya Aura*® *Communication Manager*.

- Static IP addressing for the Dialer interface may not be feasible. Dynamic IP addressing is
  available to enable you to connect to the remote network through an ISP. ISPs commonly
  provide IP addressing for connected ports on an as-needed basis. IP unnumbered links are
  available to supply addressing in situations where you wish to run routing over your network
  link without committing a subnet.
- Object tracking can be used with the Loopback interface to provide an alternative method for activating the Dialer interface when connectivity with the main office is lost. This is useful in configurations where the WAN interface is not connected directly to the Branch Gateway. Use object tracking to configure RTRs to verify connectivity with the main office. If the RTR fails, the object tracker can be configured to change the status of the Loopback interface to down. If the Dialer interface is configured as the backup for the Loopback interface, the Dialer interface will automatically dial when connectivity fails.

### Note:

In a situation where the same modem is used for inbound Avaya Service calls and outbound dial backup calls, only one call can be active at any time.

Refer to <u>www.multitech.com</u> for a listing of modem AT commands used to configure the modem directly.

#### Related links

Backup interfaces on page 234

Console port and modem configuration on page 213

PPPoE overview on page 226

Header compression configuration on page 201

Policy lists on page 497

Dynamic CAC on page 256

Dynamic local peer IP on page 453

**Unnumbered IP interfaces** on page 384

Object tracking on page 258

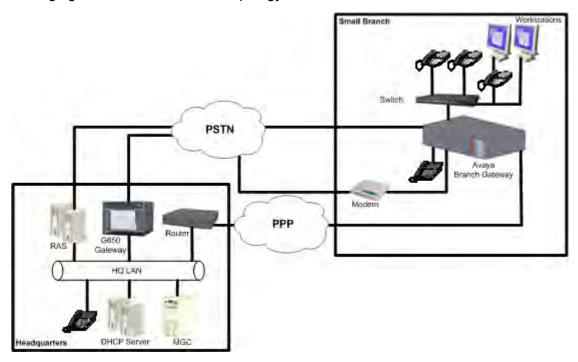
### **Configuration example**

This example sets up a modem dial backup for the WAN link between a branch office and the headquarters data center. The branch office is connected to the corporate network using a Branch Gateway. IP phone users in the branch office connect to an MGC located in the headquarters data center, and an RAS is located in the headquarters data center, with multiple phone lines available for dial access. The primary WAN connection is a PPP link connected to the serial 3/1 port. The Dialer PPP session uses CHAP encryption. The corporate network is routed using OSPF. An analog trunk connects the branch office to the PSTN for non-corporate bearer traffic.

#### Note:

When using a broadband modem (either xDSL or cable), it is recommended to run the VPN application.

The following figure shows the network topology.



#### **Command sequence**

```
!Step 1
Gxxx-001(super-if:Loopback 1) # exit
Gxxx-001(super) # interface loopback 1
Gxxx-001(super-if:Loopback 1) # ip address 149.49.4.5 255.255.255.252
Done!
Gxxx-001(super-if:Loopback 1)# exit
Gxxx-001(super)#
!Step 2
Gxxx-001(super) # ip access-control-list 305
Gxxx-001(super-ACL 305) # name "Block-RTP-to Modem-bkp"
Done!
Gxxx-001(super-ACL 305)# ip-rule 20
Gxxx-001(super-ACL 305/ip rule 20)# composite-operation "Deny"
Gxxx-001(super-ACL 305/ip rule 20)# ip-protocol udp
Done!
Gxxx-001(super-ACL 305/ip rule 20) # dscp 46
Done!
Gxxx-001(super-ACL 305/ip rule 20) # description "Block-VoIP-Bearer"
Gxxx-001(super-ACL 305/ip rule 20)# exit
Gxxx-001(super-ACL 305) # exit
Gxxx-001(super)#
!Steps 3-10 (Each command is an individual step)
Gxxx-001(super) # interface dialer 1
Gxxx-001(super-if:Dialer 1)# ppp chap hostname "area5"
Done!
```

```
Gxxx-001(super-if:Dialer 1) # dialer persistent initial delay 5
Done!
Gxxx-001(super-if:Dialer 1)# dialer persistent delay 5
Done!
Gxxx-001(super-if:Dialer 1) # dialer string 1 3035384867
Gxxx-001(super-if:Dialer 1) # dialer string 2 7325213412
Gxxx-001(super-if:Dialer 1) # dialer modem-interface console
Done!
Gxxx-001(super-if:Dialer 1) # ip unnumbered 1 Loopback 1
Done!
Gxxx-001(super-if:Dialer 1) # ip access-group 305 out
Done!
Gxxx-001(super-if:Dialer 1) # exit
Gxxx-001(super)#
!Step 11
Gxxx-001(super) # interface console
Gxxx-001(super-if:Console) # async mode interactive
Gxxx-001(super-if:Console) # async modem-type MultiTech-ZBA
Done!
Gxxx-001(super-if:Console) # exit
Gxxx-001(super)#
Step 12
Gxxx-001(super) # interface serial 3/1:1
Gxxx-001(if:serial 3/1:1) # backup interface Dialer 1
Gxxx-001(if:serial 3/1:1) # exit
Gxxx-001(super)#
Step 13
Gxxx-001(super) # router ospf
Gxxx-001(super router:ospf)# network 149.49.4.4 0.0.0.3 area 0.0.0.5
Gxxx-001(super router:ospf) # exit
Gxxx-001(super)#
```

#### **Command sequence explanation**

#### **Procedure**

1. Assign an IP address to the Loopback interface for use with modem dial backup using the interface loopback command.

This step allows the Dialer interface to be configured as an IP unnumbered link and still participate in OSPF routing.

Create an access control list with the ip access-control-list command.

The access control list determines which traffic is permitted to use the interface. In this example, access control list 305 is configured to block all traffic other than VoIP signalling traffic. The primary purpose of the access control list is to block bearer traffic from using the Dialer interface. The Dialer interface generally has insufficient bandwidth to support bearer traffic.

3. Create the Dialer interface using the interface dialer command.

The Dialer interface is created and is available as a backup link for a WAN interface. Only one Dialer interface can be created on the Branch Gateway.

4. Assign a PPP authentication method with the ppp chap hostname command.

The Dialer interface authenticates its PPP sessions to the remote RAS server using CHAP authentication and a username of area5. The username area5 must be configured on the RAS as a legitimate user.

5. Assign an initial delay for dialing with the dialer persistent initial delay command.

The initial delay prevents the Dialer from dialing out unnecessarily on reboot. The primary WAN interface often requires a few moments to register itself as up, and during that period, the initial delay prevents the device from activating the Dialer.

6. Assign a reset delay for the dialer string list using the dialer persistent delay command.

The reset delay determines the amount of time between cycles of call attempts, once all dialer strings have been attempted.

7. Enter up to five dialer strings using the dialer string command.

When the Dialer interface is activated, the Dialer first attempts to connect to the number associated with dialer string 1. If the connection attempt fails, the Dialer attempts to connect to the number associated with the next dialer string. These strings represent hunt group phone numbers configured on the RAS server in the headquarters data center.

8. Associate the Dialer interface with its physical port with the dialer modem-interface command.

The Dialer interface must be configured to use a physical interface on the device to which the modem is connected. Modem dial backup is supported on both the Console port and the USB port.

9. Configure the modem to participate in network routing with the ip unnumbered command.

An unnumbered interface uses the IP address of the interface configured in the command. In this example, the Loopback interface has been created for the Dialer interface to use its IP information. This IP information allows the unnumbered interface to forward and receive IP traffic without actually assigning a static IP address to the Dialer interface.

10. Assign an access control list to the Dialer interface using the ip access-group command.

All traffic passing through the Dialer interface must meet the conditions of the access control list associated with this access group or be rejected. In this example, the access-group references access control list 305, which is created to block all outgoing traffic across the Dialer interface other than the VoIP signalling traffic between the branch office gateway and the MGC in the headquarters data center.

11. Configure the Console port to support the modem with the interface console command.

The physical interface must be configured to use the attached modem. Each modem type has different initialization requirements. The only modems supporting modem dial backup are the MultiTech ZBA series modems.

12. Assign the Dialer interface to the interface you want to back up with the backup interface dialer command.

For example, interface Dialer 1 is selected as the backup interface to interface Serial 3/1:1, the primary WAN connection to the headquarters network. The Dialer activates in the event of a failure of the serial port and all permitted traffic transverses the Dialer interface.

13. Configure the Loopback interface to participate in the OSPF network using the router ospf command.

For example, a group of branch offices are assigned to OSPF area 5. This configuration allows filtering to take place at the border points and minimizes topology updates on the headquarters data center routers.

#### Related links

Policy lists on page 497

Modems and Branch Gateway on page 211

Backup interfaces on page 234

OSPF on page 419

### Modem dial backup maintenance

The Branch Gateway generates specific log messages for Dialer interface activity when configured to do so. Certain dialer-related log messages are generated to aid you in troubleshooting problems with modem dial backup. In addition, messages generated by the modem and the PPP session are available to help with troubleshooting modem dial backup issues.

### Commands used to activate session logging

To activate session logging for modem dial backup functions, type the following commands. Logging messages will be sent to the terminal screen.

- set logging session condition dialer information
- set logging session condition console information
- set logging session condition usb-modem information
- set logging session condition ppp information

### Note:

Not all logging messages indicate problems. Some are generated to provide information on normal working activity of the Dialer interface.

Syslog and log file logging are also available.

#### Related links

System logging on page 186

### Severity levels of the logging session

The **set logging** commands must include a severity level. All logging messages with the specified severity and higher are displayed. The following are the available severity levels:

**Information:** This message is for informational purposes and requires no action on your part.

**Debug:** This message provides information that can be useful in debugging certain problems, but requires no action itself.

Warning: This message indicates a condition requiring user intervention and troubleshooting.

### Modem dial backup logging messages

### **Dialer Messages**

Dialer Messages are messages generated by the Dialer interface.

Log Message	Severity	Possible cause	Action
Dialer 1 state is <state></state>	Debug	The Dialer interface generates a message when a change in its operational state has been detected. The default state for the Dialer interface when it is used as a backup interface for a WAN link is Standby. When the primary WAN link has failed and the backup interface mechanism is invoked, the state of the Dialer interface changes to Up.	None required.
Dialer 1 trigger is <on off=""></on>	Informational	In a modem dial backup scenario, the event triggering the Dialer interface is a failure of the primary WAN interface for which the Dialer interface has been configured as the backup interface. When the primary WAN interface has been determined to be down, a message is sent indicating the occurrence of the triggering event for the Dialer. When the primary WAN interface is returned to an operational state, a message is generated indicating that the conditions for triggering the Dialer are no longer being met, and that the Dialer can be brought down.	None required.

Log Message	Severity	Possible cause	Action
Dialer 1 string <string_id> <dialer_string></dialer_string></string_id>	Informational	The value of <i>string_ID&gt;</i> is equal to the ID of the string configured using the dialer string command. The value of <i>dialer_string&gt;</i> is equal to the phone number associated with the dialer string. For example, if you configured dialer string 3 to associate with the phone number 5551314, and the modem is attempting to connect using dialer string 3, the message received would be Dialer 1 string 3 5551314.	None required.
Dialer 1 timer expired	Debug	When the Dialer interface is configured with the dialer persistent re-enable command, a timer is created. This timer determines when the Dialer interface attempts to begin dialing again after a failure to connect in as many attempts as were configured in the dialer persistent max-attempts command. For example, if you configured the value of dialer persistent max-attempts as 10, and dialer persistent re-enable is configured for the Dialer interface, after the Dialer has made ten unsuccessful attempts to connect to the remote modem, the timer begins. When the timer expires, the Dialer 1 timer expired message is sent, and the Dialer begins attempting to connect to the remote modem again.	None required.
Dialer 1 Modem is not ready	Warning	This message is generated when the Dialer interface has been triggered and the operational state of the Dialer is up, but the Dialer is unable to communicate with the modem.	<ul> <li>Troubleshooting steps:</li> <li>Check modem cable connection to serial port.</li> <li>Check modem cable connection to modem.</li> <li>Check power to modem.</li> </ul>

### **Console messages**

Console Messages are messages generated by a serial modem attached to the Console port.

quired.
shooting steps:
modem cable ction to modem.
e that modem is ed on.
modem lights for rm.
quired.
shooting steps:
modem uration for proper zation string.
shooting steps:
modem cable ction to serial port eseat cable if sary.
quired.
ct es

## **USB Modem Messages**

USB Modem Messages are messages generated by a USB modem.

Log Message	Severity	Possible cause	Action
USB modem was detected	Informational	When the USB modem is discovered by the device and the initialization string is successful, a message is generated indicating that the device is ready to dial.	None required.
USB modem - Connection established	Informational	When the USB modem successfully connects to a remote modem and a PPP session is fully established, a message is sent indicating that the PPP is ready to transmit and receive traffic.	None required.
USB modem -	Warning	This message is generated when a	Troubleshooting steps:
Unplugged		modem cable is connected to the USB port, but no modem is detected.	Check modem cable connection to modem and to USB port and re- seat if necessary.
USB modem - Initialization string error	Warning	This message is generated when the USB modem attempts to dial and has an incorrect initialization string. The attempt to dial fails.	Troubleshooting steps:     Check modem     configuration for proper     initialization string.

## **PPP Messages**

PPP Messages are messages generated by the PPP session.

Log Message	Severity	Possible cause	Action
LCP Up/Down	Informational	LCP is used by PPP to initiate and manage sessions. LCP is responsible for the initial establishment of the link, the configuration of the session, the maintenance of the session while in use, and the termination of the link. LCP is considered Up when the link is being established and configured, and is considered down once the session is fully established and passing traffic. LCP then comes up to pass Link Maintenance packets during the session, and goes down after the maintenance is complete. LCP comes up when a termination request is sent, and goes down when the link is terminated.	None required.

Log Message	Severity	Possible cause	Action
PAP passed/failed	Debug	This message is sent when the authenticating station responds to the PAP authentication request.	None required.
CHAP passed/ failed	Debug	This message is sent when the authenticating station responds to the CHAP authentication request.	None required.
IPCP Up/Down	Debug	PPP uses IPCP to define the IP characteristics of the session. IP packets cannot be exchanged until IPCP is in the Up state.	None required.
IPCP IP reject	Warning	This message is generated when IPCP attempts to define the IP characteristics for a PPP session, but does not have the IP address of the local interface to define the session. Without IP address information on both sides of the session, the PPP session cannot begin passing IP traffic.	Troubleshooting steps:  • Check Dialer interface configuration to ensure an IP address is configured, either as a static address or through Dynamic IP addressing or through IP unnumbered.

### Summary of modem dial backup commands

For more information about these commands, see Avaya Branch Gateway G450 CLI Reference.

Root level command	Command	Description
interface dialer	-	Enter the Dialer interface configuration context
-	dialer modem- interface	Associate a Dialer with a modem interface
-	dialer order	Set which dial strings are used upon a new dial trigger event
-	dialer persistent	Force the Dialer to attempt to reconnect every second
-	dialer persistent delay	Set the redial interval
-	dialer persistent initial delay	Set the minimum delay from boot to persistent dialing
-	dialer persistent max-attempts	Set the number of consecutive dial attempts for the dial list
-	dialer persistent re-enable	Set the persistent re-enable timer after the maximum number of dial attempts has been reached
-	dialer string	Add a phone number to the dial list

Root level command	Command	Description
-	dialer wait-for- ipcp	Set the maximum time the Dialer waits between dialing a number to successfully establishing PPP/ IPCP
-	ip address	Assign an IP address and mask to an interface
-	ip address negotiated	Enable obtaining an IP address via PPP/IPCP negotiation
-	ip unnumbered	Configure an interface to borrow an IP address from another interface
-	ppp ipcp dns request	Enable requesting DNS information from the remote peer during the PPP/IPCP session
<pre>interface (fastethernet  loopback  serial  tunnel)</pre>	-	Enter the Console, FastEthernet, Loopback, Serial, or Tunnel interface configuration context
-	backup interface dialer	Set the Dialer interface as the backup interface for the current interface
ip default- gateway	-	Define a default gateway (router)
router ospf	-	Enable OSPF protocol on the system and to enter the Router configuration context
set logging session	-	Manage message logging for the current console session
show interfaces	-	Display interface configuration and statistics for a particular interface or all interfaces

# **ICMP** keepalive

The ICMP keepalive feature, formerly known as extended keepalive, is available for WAN FastEthernet interfaces. ICMP keepalive is a mechanism for determining if a certain IP address is reachable. The source interface sends test packets (ping) and waits for a response. If no response is received after a certain number of tries, the connection is declared to be down.

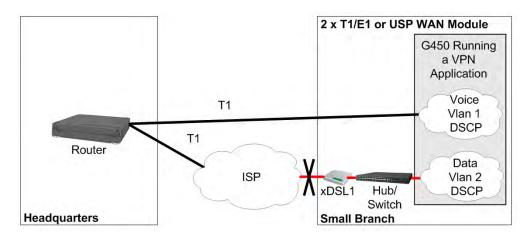
This feature provides a quick means to determine whether the interface is up or down. This is especially important for policy-based routing, in which it is important to determine as quickly as possible whether the next hop is available. See Policy-based routing section.

# Note:

ICMP keepalive has been replaced by the object tracking feature that supports keepalive probes over WAN, FastEthernet, Loopback, PPPoE, Dialer PPP interfaces, and Frame relay sub-interfaces. ICMP keepalive is still supported for backward compatibility.

Normal keepalive is sufficient for testing the status of a direct connection between two points. However, in many situations, the system needs to know the status of an entire path in order to ensure that packets can safely traverse it.

ICMP keepalive is a mechanism that reports on the status of an IP address and its next hop. The destination interface is only declared to be alive if the next hop is also reachable. This feature is critical for mechanisms such as policy-based routing that must guarantee service on a particular path.



For example, your branch office may have an Branch Gateway that connects to Headquarters over a T1 line and via an xDSL connection to the Internet. The T1 line is used for voice traffic, while data packets are sent over the xDSL line. If the Fast Ethernet line protocol is up but the xDSL connected to it is down, then ICMP keepalive, which checks the next hop, correctly reports that the WAN path is down. Policy-based routing, which relies on the interface status to determine how packets are routed, can use ICMP keepalive to know the status of the interfaces on its next hop list.

### Note:

ICMP keepalive is not used with a GRE Tunnel interface. The GRE tunnel has its own keepalive mechanism.

You cannot configure both DHCP Client and ICMP keepalive on the WAN FastEthernet interface. You cannot configure both DHCP Client and ICMP keepalive on the same WAN FastEthernet interface.

### Related links

Object tracking on page 258

GRE tunneling on page 391

DHCP client configuration on page 178

# Command used for enabling the ICMP keepalive feature

Use the keepalive-icmp command in the context of the interface to enable the ICMP keepalive feature.

For more information about this command, see Avaya Branch Gateway G450 CLI Reference.

# Commands used to define the ICMP keepalive parameters

Use the following commands to define the ICMP keepalive parameters.

```
• keepalive-icmp timeout
```

- keepalive-icmp success-retries
- keepalive-icmp failure-retries
- keepalive-icmp interval
- keepalive-icmp source-address
- show keepalive-icmp

For more information about these commands, see Avaya Branch Gateway G450 CLI Reference.

# **Example of configuring ICMP keepalive**

The following example configures ICMP keepalive on interface fastethernet 10/2 to send keepalive packets to IP address 135.64.2.12 using MAC address 11.22.33.44.55.66, at five second intervals. If a response is not received within one second, the keepalive packet is considered to have failed. After three consecutive failed packets, the interface is declared to be down. After two consecutive successful packets, the interface is declared to be up.

```
Gxxx-001# interface fastethernet 10/2
Gxxx-001(super-if:FastEthernet 10/2)# keepalive-icmp 135.64.2.12
11.22.33.44.55.66
Gxxx-001(super-if:FastEthernet 10/2)# keepalive-icmp interval 5
Gxxx-001(super-if:FastEthernet 10/2)# keepalive-icmp timeout 1
Gxxx-001(super-if:FastEthernet 10/2)# keepalive-icmp failure-retries 3
Gxxx-001(super-if:FastEthernet 10/2)# keepalive-icmp success-retries 2
Done!
```

# Summary of ICMP keepalive configuration commands

For more information about these commands, see Avaya Branch Gateway G450 CLI Reference.

Root level command	Command	Description
interface fastethernet	-	Enter the FastEthernet interface configuration context
-	keepalive-icmp	Enable the ICMP keepalive mechanism on an interface in the context of the interface. Use the no form of this command to deactivate the feature.
		Includes the following parameters:
		destination ip address. The destination IP address for the keepalive packets.
		• next hop MAC address. The next hop MAC address for the keepalive packets. This parameter is only relevant for the WAN Fast Ethernet ports.

Table continues...

Root level command	Command	Description
-	keepalive-icmp failure-retries	Set the number of consecutive failed keepalive packets necessary to set the interface's keepalive status as down. The default value is 4.
-	keepalive-icmp interval	Set the interval (in seconds) between keepalive packets. The default value is 5.
-	keepalive-icmp source-address	Set the source IP address of the keepalive packets. The default value is the interface's primary IP address.
-	keepalive-icmp success-retries	Set the number of consecutive successful keepalive packets necessary to set the interface's keepalive status as up
-	keepalive-icmp timeout	Set the timeout (in seconds) for receiving the keepalive response. The default value is 1.
-	show keepalive- icmp	Display information about the extended keepalive settings

# **Dynamic CAC**

Dynamic Call Admission Control (CAC) provides enhanced control over WAN bandwidth. When Dynamic CAC is enabled on an interface, the Branch Gateway informs the MGC of the actual bandwidth of the interface and instructs the MGC to block calls when the bandwidth is exhausted.

Dynamic CAC is especially useful in situations where a primary link is down and a backup link with less bandwidth than the primary link is active in its place. Without dynamic CAC, the MGC is unaware that the interface has switched over to the backup link. Thus, the MGC is unaware of the resulting changes in network topology and bandwidth available for the interface. Consequently, the MGC might allow calls through the interface that require more than the currently available bandwidth.

### Note:

Dynamic CAC works in conjunction with the CM Call Admission Control: Bandwidth Limitation (CAC-BL) feature. A related feature is Inter-Gateway Alternate Routing (IGAR), which provides a mechanism to re-route bearer traffic from the WAN to the PSTN under certain configurable conditions. For more information on CAC-BL and IGAR, see Administrator Guide for Avaya Aura® Communication Manager.

You can enable dynamic CAC on the following interface types:

- FastEthernet
- Serial (PPP or frame relay)
- GRE Tunnel
- VLAN

# Note:

Since VLAN interfaces are always up, configuring dynamic CAC on a VLAN interface provides a means to have a default dynamic CAC bandwidth.

# **Dynamic CAC tasks**

Task	Command
Enabling dynamic CAC and setting maximum bandwidth	dynamic-cac bbl
Displaying bandwidth information	show dynamic-cac

# Note:

Dynamic CAC also requires configuration of the CM. For details, see *Administrator Guide for Avaya Aura® Communication Manager*.

For more information about these commands, see Avaya Branch Gateway G450 CLI Reference .

# **Summary of dynamic CAC configuration commands**

For more information about these commands, see the Avaya G450 CLI Reference.

Root level command	Command	Description
interface (dialer serial  loopback fastethernet  tunnel vlan)	-	Enter the Dialer, Serial, Loopback, FastEthernet, Tunnel, or VLAN interface configuration context
-	dynamic-cac-bbl	Enable dynamic CAC on the interface and set the maximum bandwidth for the interface. The dynamic-cac bbl command includes the following parameters:
		• bb1. The bearer bandwidth limit (kbps). The MGC enforces this as the maximum bandwidth for the interface. If you set the bbl to 0, the interface can only be used for signalling.
		activation priority (optional). If dynamic CAC is activated on more than one active interface, the Branch Gateway reports the bearer bandwidth limit of the interface with the highest activation priority. You can set the activation priority to any number from 1 to 255. The default activation priority is 50.

Table continues...

Root level command	Command	Description
show dynamic-cac	-	Display information about the most recent dynamic CAC event.
		The show dynamic-cac command displays the following information:
		Current RBBL. The current actual bandwidth available on the interface.
		Last event. The amount of time since the most recent update by the CAC process.
		Last event BBL. The interface's bandwidth at the time of the most recent update by the CAC process.

# Object tracking

With the Object tracking feature, you can track the state (up/down) of various objects in the system using keepalive probes, and notify registered applications when the state changes. In particular, object tracking is used to monitor Interface states and routes states, where routes can be static routes, the DHCP client default route, or PBR next hops.

The purpose of object tracking is to track the state (up/down) of various objects in the system using keepalive probes, and notify registered applications when the state changes. Configuring object tracking is a two-stage operation:

- The first stage is to define Respond Time Reports (RTRs), the basic building blocks of object tracking. RTRs actively monitor the reachability state of remote devices by generating probes at regular intervals. Each RTR, identified by a unique number, monitors one remote device, and learns the state of the device: up or down. The state of the RTR reflects the state of the device it is monitoring either up or down.
- The second stage consists of defining Object Trackers using RTRs. The definition of object
  trackers is recursive. A simple object tracker monitors a single RTR, and its state directly
  reflects the state of the RTR. A more advanced object tracker is a track list, which is
  composed of multiple simple object trackers. The state of the track list is calculated based on
  the states of the objects in the list. Because a track list is itself an object tracker, the objects
  in a track list can be previously-defined track lists.

You can view a track list as monitoring the "health" of an entire group of remote devices. You can define how to calculate the overall health of the group based on the health (up/down) state of each individual device. For example, you can specify that the overall state is up only if all remote devices are up, or if at least one device is up. Alternatively, you can base the overall state on a threshold calculation.

Using object tracking, different applications can register with the tracking process, track the same remote devices, and each take different action when the state of the remote devices changes.

# Configuring object tracking

#### **Procedure**

1. Configure RTRs to monitor remote devices and learn if their state is up or down.

Each RTR has a state:

- inactive. Not running
- · up. The remote device is considered up
- · down. The remote device is considered down
- 2. Configure object trackers to track the states of RTRs.

Each object tracker calculates its own state as either up or down based on the states of the elements it is tracking. Whenever the state of an object tracker changes, it notifies the applications registered with it.

An object tracker calculates its own state as follows:

- For an object tracker tracking a single RTR:
  - If the state of the RTR is up, the state of the object tracker is up.
  - If the state of the RTR is inactive or down, the state of the object tracker is down.

A track list applies a configurable formula (using a Boolean or a Threshold calculation) to the states of the objects comprising the list, and the result (up/down) is the state of the track list. For example, if the configured formula is the Boolean AND argument, then the state of the list is up if the state of all its objects is up, and down if the state of one or more of its objects is down.



### ■ Note:

You can register either a VPN tunnel or an interface with an object tracker. For more information see the definition of the keepalive-track command in the Avaya Branch Gateway G450 CLI Reference.

You cannot configure both DHCP Client and object tracking on the same WAN FastEthernet interface. You can however, configure tracking on the DHCP client default route.

#### Related links

**DHCP client configuration on page 178** 

### **Configuring RTR**

#### About this task

For each remote device whose state you wish to monitor:

#### **Procedure**

1. Enter rtr, followed by a number from 1 to 30, to create the RTR.

#### For example:

```
Gxxx-001(config) # rtr 5
Gxxx-001(config-rtr 5) #
```

2. Use the **type** command to specify the remote device by address, and specify the probing method to be employed by the RTR probe: ICMP Echo or TCP Connection.

If you specify a TCP Connection operation, also specify which port to probe in the remote device.

#### Examples:

```
Gxxx-001(config-rtr 5)# type echo protocol ipIcmpEcho 10.0.0.1
Gxxx-001(config-rtr icmp 5)#

Gxxx-001(config-rtr 5)# type tcpConnect dest-ipaddr 147.42.11.1 dest-port
80
Gxxx-001(config-rtr tcp 5)#
```

3. Optionally, use the **frequency** command to specify the frequency at which RTR probes are sent.

If you do not configure this parameter, the default value of five seconds is used.

### For example:

```
Gxxx-001(config-rtr icmp 5)# frequency 2 seconds
Done!
```

4. Optionally, use the **dscp** command to set the DSCP value in the IP header of the probe packet, thus setting the packets' priority.

If you do not configure this parameter, the default value of 48 is used.

### For example:

```
Gxxx-001(config-rtr icmp 5) # dscp 43
Done!
```

5. Optionally, use the **next-hop** command to specify the next-hop for the RTR probe, and bypass normal routing.

The next-hop command is disabled by default.

Use the next-hop command when the Branch Gateway is connected to a remote device via more than one interface, and you wish to monitor the state of one specific interface. When you specify the next-hop as the interface you wish to monitor, you ensure that the RTR will probe that interface.

When the RTR is used to monitor a static route, a PBR next hop, or the DHCP client default route, you must specify the same next-hop for the RTR. This ensures it will be sent over the next hop it should monitor.

If the interface is an Ethernet interface (FastEthernet not running PPPoE) or VLAN interface, specify also the interface's MAC address.

### For example:

```
Gxxx-001(config-rtr icmp 5) # next-hop interface fastethernet 10/2
mac-address 00:01:02:03:04:05
Done!
```

6. Optionally, use the **source-address** command to specify a source IP address, instead of using the output interface's address.

By default, the **source-address** command is disabled, and RTR probes use the output interface's address.

Use the **source-address** command when you are probing a device located on the Internet, and specify as the source-address the Branch Gateway public IP address.

#### For example:

```
Gxxx-001(config-rtr icmp 5) # source-address 135.64.102.5
Done!
```

7. Optionally, configure the RTR parameters that determine when the state of the remote device is considered up or down.

If you do not configure these characteristics, their default values are used:

- Use the wait-interval command to specify how long to wait for a response from the device. When the wait-interval is exceeded, the probe is considered an unanswered probe. The default value is the current value of frequency.
- Use the **fail-retries** command to specify how many consecutive unanswered probes change the state of an RTR from up to down. The default value is 5.

# Note:

When an RTR starts running, its state is considered up.

• Use the **success-retries** command to specify how many consecutive answered probes change the state of an RTR from down to up. The default value is 5.

### For example:

```
Gxxx-001(config-rtr icmp 5) # wait-interval 2 seconds
Done!
Gxxx-001(config-rtr icmp 5) # fail-retries 3
Done!
Gxxx-001(config-rtr icmp 5) # success-retries 1
Done!
```

8. Exit the RTR type context, and activate the RTR with the rtr-schedule command.

To deactivate the RTR, use the no rtr-schedule command.

### For example:

```
Gxxx-001(config-rtr icmp 5) # exit
Gxxx-001(config) # rtr-schedule 5 start-time now life forever
```

Once an RTR's probing method and remote device address are configured, you cannot change them. If you exit the RTR type context and you want to modify the configuration of the RTR, you can enter the RTR context using the rtr command and specifying the RTR

ID. From the RTR context, you can run the various modification commands described in Steps 3 to 7.

### Object tracking provisioning

### About this task

To configure object tracking, you must first configure at least one simple object tracker, that is, an object tracker that tracks a single RTR. If you wish, you can then configure a track list which contains multiple simple object trackers and specifies how to calculate the overall state of the list. Note that a track list is itself an object tracker. Therefore, you can configure track lists containing object trackers which are either simple object trackers, or other track lists.

### Configuring a simple object tracker

#### **Procedure**

1. Use the track id rtr command to specify the RTR to be tracked.

Enter a number from 1 to 50 as the unique ID for this object tracker.

#### For example:

```
Gxxx-001(config) # track 1 rtr 5
Gxxx-001(config-track rtr 1)#
```

2. Use the description command to enter a description for the object tracker.

#### For example:

```
Gxxx-001(config-track rtr 1) # description "track rtr-5"
```

### Configuring a track list

### **Procedure**

1. Use the track id list command to enter track list configuration mode, to specify the unique ID of the track list from 1 to 50, and to specify how to calculate the state of the track list.

The calculation can be either a Boolean or a Threshold calculation



### 🐯 Note:

If you do not specify how to calculate the state of the track list, it is calculated by default using the Boolean AND argument. This means that the list is up if all objects are up, and down if one or more of the objects are down.

### Examples:

```
Gxxx-001(config-track list 10) # description "track list rtr-5 and rtr-6"
Gxxx-001(config) # track 10 list boolean or
Gxxx-001(config-track list 10)#
```

- 2. Use the **description** command to enter a description for the track list.
- 3. Use the object command to add an object tracker to the list.

# Note:

The object tracker can be a simple one tracking a single RTR, or a track list.

### For example:

```
Gxxx-001(config-track list 10)# object 1
Done!
```

- 4. Repeat step 3 to add as many object trackers as you require, up to a maximum of 50.
- 5. If you specified a Threshold method of calculation in step 1, use the threshold count command to enter the threshold values.

For example, use the following command to specify that:

- The state of the object tracker will change from down to up if 2 or more hosts are up, and
- The state of the object tracker will change from up to down if 1 or less hosts are up
- Gxxx-001(config-track list 10)# threshold count up 2 down 1 Done!



#### Note:

Object trackers operate indefinitely once they are defined. To stop the operation of an object tracker, use the **no track** command to delete the object tracker.

### Object tracking configuration workflow

```
rtr
   type
      frequency
      dscp
      next-hop
      source-address
      wait-interval
      fail-retries
      success-retries
rtr-schedule
track id rtr
  description
track id list
   description
   object 1
   object n
   threshold count
```

# Tasks for maintaining object tracking

Using the **show** commands, you can display RTR and Object Tracking configuration, and enable RTR and object tracking logging to a CLI terminal.

Task	Command
Display RTR configuration values, including all defaults, for a specific RTR operation or for all RTR operations.	show rtr configuration
Display the global operational status of the RTR feature, for a specific RTR operation or for all RTR operations.	show rtr operational-state
Display tracking information.	show track

For more information about these commands, see Avaya Branch Gateway G450 CLI Reference.

#### Related links

Summary of object tracking configuration commands on page 270

# Viewing RTR and object trackers logging

### **Procedure**

1. Enter set logging session enable to enable logging to the CLI terminal.

### For example:

```
Gxxx-001# set logging session enable
Done!
CLI-Notification: write: set logging session enable
```

2. Use the set logging session condition saa to view all RTR messages of level Info and above.

#### For example:

```
Gxxx-001# set logging session condition saa Info
Done!
CLI-Notification: write: set logging session condition saa Info
```

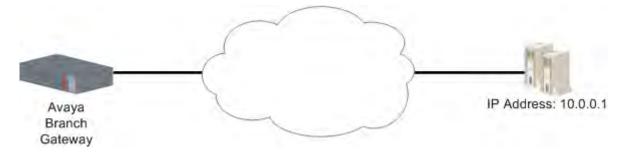
3. Use the set logging session condition tracker command to view all object tracker messages of level Info and above.

### For example:

```
Gxxx-001# set logging session condition tracker Info
Done!
CLI-Notification: write: set logging session condition tracker Info
```

### Example of tracking a single remote device

### **About this task**



### **Procedure**

1. The first step is to configure an RTR which tracks a remote device.

In this case, RTR 5 is configured to track the device at IP address 10.0.0.1. For example:

```
Gxxx-001(config) # rtr 5
Gxxx-001(config-rtr 5) # type echo protocol ipIcmpEcho 10.0.0.1
Gxxx-001(config-rtr icmp 5) # wait-interval 2 seconds
Done!
Gxxx-001(config-rtr icmp 5) # fail-retries 3
Done!
Gxxx-001(config-rtr icmp 5) # success-retries 1
Done!
Gxxx-001(config-rtr icmp 5) # exit
Gxxx-001(config) # rtr-schedule 5 start-time now life forever
```

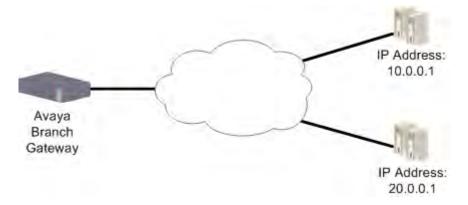
2. The second step is to configure an object tracker which tracks the state of RTR 5.

### For example:

```
Gxxx-001(config) # track 1 rtr 5
Gxxx-001(config-track rtr 1) # description "track rtr-5"
Done!
Gxxx-001(config-track rtr 1) # exit
```

# Example of tracking a group of devices

#### About this task



### **Procedure**

1. The first step is to configure several RTRs.

In this case, RTR 5 tracks the device at IP address 10.0.0.1, and RTR 6 tracks the device at IP address 20.0.0.1. For example:

```
Gxxx-001(config) # rtr 5
Gxxx-001(config-rtr 5) # type echo protocol ipIcmpEcho 10.0.0.1
Gxxx-001(config-rtr icmp 5) # wait-interval 2 seconds
Done!
Gxxx-001(config-rtr icmp 5) # fail-retries 3
Done!
Gxxx-001(config-rtr icmp 5) # success-retries 1
Done!
Gxxx-001(config-rtr icmp 5) # exit
Gxxx-001(config) # rtr-schedule 5 start-time now life forever
Gxxx-001(config) # rtr 6
```

```
Gxxx-001(config-rtr 6) # type tcpConnect dest-address 20.0.0.1 dest-port 80
Gxxx-001(config-rtr tcp 6) # frequency 500 milliseconds
Done!
Gxxx-001(config-rtr tcp 6) # dscp 34
Done!
Gxxx-001(config-rtr tcp 6) # next-hop interface fastethernet 10/2 mac-address
00:01:02:03:04:05
Done!
Gxxx-001(config) # rtr-schedule 6 start-time now life forever
Gxxx-001(config-rtr tcp 6) # exit
```

2. The second step is to configure several object trackers.

In this case, object tracker 1 tracks the state of RTR 5, and object tracker 2 tracks the state of RTR 6. For example:

```
Gxxx-001(config) # track 1 rtr 5
Gxxx-001(config-track rtr 1) # description "track rtr-5"
Done!
Gxxx-001(config-track rtr 1) # exit
Gxxx-001(config) # track 2 rtr 6
Gxxx-001(config-track rtr 2) # description "track rtr-6"
Done!
Gxxx-001(config-track rtr 2) # exit
```

3. The third step is to configure a track list object tracker which tracks the states of object trackers 1 and 2, and calculates its own state using a boolean or threshold calculation.

In this case, a Boolean OR argument is used. This means that the track list is up if *either* object tracker 1 *or* object tracker 2 is up. For example:

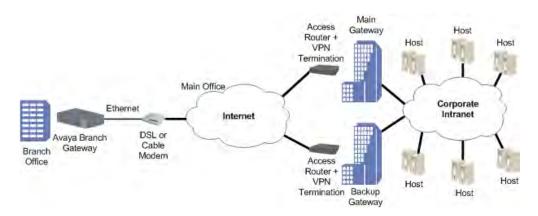
```
Gxxx-001(config) # track 10 list boolean or
Gxxx-001(config-track list 10) # description "track list rtr-5 and rtr-6"
Done!
Gxxx-001(config-track list 10) # object 1
Done!
Gxxx-001(config-track list 10) # object 2
Done!
Gxxx-001(config-track list 10) # exit
```

# Typical object tracking applications

- Trigger the failover mechanism for VPN.
- Trigger the failover mechanism for interfaces.
- Track the state of a route: a static route, a PBR next hop, or the DHCP client default route.

### Typical application – VPN failover using object tracking

In this application, Branch Gateway is connected to a remote site through an IPSec VPN tunnel. The remote site can be reached through two or more VPN gateways that can back each other up, such as a main gateway and a backup gateway. Object tracking can monitor the state of the current VPN connection, by monitoring one or more hosts that reside within the remote site's network. If the current connection is lost, Branch Gateway can failover to a backup gateway, and attempt to establish a VPN connection to it.



#### Related links

Failover using a peer-group on page 483

### Typical application – backup for the WAN FastEthernet interface

This typical application illustrates the use of object tracking as a backup mechanism for PPPoE configured on the WAN FastEthernet interface. A track list monitors the state of the connection. If the WAN FastEthernet interface is down, another connection is used.

In this application, the Branch Gateway is connected to an xDSL modem through PPPoE encapsulation configured on interface WAN FastEthernet 10/2. The Branch Gateway is connected to the Internet through the xDSL modem.

# Note:

When using a broadband modem (either xDSL or cable), it is recommended to run the VPN application.

### Configuring the backup mechanism

### **Procedure**

again.

- Define four RTRs to probe the four entrances to the main office.
   Configure each RTR to run immediately and forever.
- 2. Define four object trackers to track the four RTRs.
- 3. Define a track list consisting of all four object trackers, and configure it so that if all object trackers are up, the track list is up, and if two or less of the object trackers are up, the track list is down.
- 4. Register the WAN FastEthernet interface with the track list.
- Define Serial 3/1:1 as a backup interface for the WAN FastEthernet interface.
   Thus, when the track list is down the Serial interface will be up until the track list is up

Note that RTR packets continue to be sent over the PPPoE interface as long as the PPP-IPCP connection status is up.

```
! Define four object trackers to track the four RTRs.
track 1 rtr 1
   exit
track 2 rtr 2
   exit.
track 3 rtr 3
   exit
track 4 rtr 4
   exit.
! Define a track list consisting of the four object trackers.
! Define a threshold calculation such that if all four object trackers
! are up, the list is up, and if 2 or less are up, the list is down.
track 50 list threshold count
   threshold count up 4 down 2
   object 1
   object 2
   object 3
   object 4
   exit
! Configure PPPoE encapsulation on interface WAN FastEthernet 10/2, and
! register the interface with the track list.
interface fastethernet 10/2
   bandwidth 96
   encapsulation pppoe
   traffic-shape rate 96000
   ip address negotiated
   keepalive-track 50
   exit
! Configure the serial 3/1:1 interface
interface serial 3/1:1
encapsulation ppp
ip address 10.0.0.1
                          255.0.0.0
exit
! Assign the serial 3/1:1 interface to be the backup interface for
! interface WAN FastEthernet 10/2.
interface fastethernet 10/2
   backup interface serial 3/1:1
   backup delay 0 60
   exit
```

### Typical application - interface backup using policy-based routing

In the previous typical application, the backup interface command is used to specify a backup interface. This typical application illustrates an alternative to the backup interface command, using policy-based routing (PBR) which configures a routing scheme for specified traffic based on configured characteristics of the traffic. Thus, PBR can be used in combination with object tracking to configure a backup mechanism for interfaces.

For an example that uses policy-based routing as an alternative to the **backup interface** command, replace the last four lines of the previous typical application with the example below.

The example creates a next hop list that sends the specified traffic to the WAN FastEthernet interface that is running PPPoE encapsulation. If the WAN FastEthernet interface becomes unavailable, the next hop list routes the traffic to the Serial interface 3/1:1. PBR list 801 is created and assigned to interface VLAN 1, so that traffic defined in PBR list 801 passing through interface VLAN 1 is routed according to the next hop list.

# Note:

You can define a static route over the WAN FastEthernet interface running DHCP client. In such a case, the static route uses as the next hop the default router learned from the DHCP server. This is useful for GRE tunnels which are defined over the WAN Fast Ethernet running DHCP client. It is necessary to define static routes in order to prevent loops. Therefore, the IP route command allows configuration of static routes over WAN Fast Ethernet running DHCP client.

When the WAN Fast Ethernet is up, policy-based routing routes this traffic via the WAN FastEthernet interface. When the track list defined in the previous typical application is down, policy-based routing routes this traffic through the Serial interface 3/1:1. When the track list is up again, the traffic is again routed through the WAN FastEthernet interface.

```
! Create PBR list 801. This list routes traffic from IP address
! 149.49.42.1 to IP address 149.49.43.1 according to next hop list 10.
ip pbr-list 801
   name "list #801"
   ip-rule 10
      next-hop list 10
      source-ip host 149.49.42.1
      destination-ip host 149.49.43.1
      exit
     exit.
! Assign PBR list 801 to interface Vlan 1.
interface Vlan 1
   icc-vlan
   ip pbr-group 801
   ip address 149.49.42.254 255.255.255.0
   exit.
! Configure next hop list 10 with interface fastethernet 10/2 as the
! first next hop, and interface Serial 3/1:1 as the second next hop.
ip next-hop-list 10
   next-hop-interface 1 FastEthernet 10/2
   next-hop-interface 2 Serial 3/1:1
```

# Typical application – tracking the DHCP client default route

This typical application demonstrates a case where a user configures DHCP client on the device to enable cable modem connection to the WAN FastEthernet interface. The user wishes to know whether the DHCP client default route can be used for routing decisions – that is, whether traffic can be routed over this default route. To do so, the user activates tracking to monitor the remote HQ peer. When the object tracker is up, the DHCP default route may be used. When the object tracker is down, the DHCP default route is not used for routing and traffic is routed to alternate routes.



#### Note:

If several default routers are learned from a specific interface, the object tracker tracks only the first one.

```
! Apply DHCP client on the WAN Fast Ethernet
interface fastethernet 10/2
   ip address dhcp
   exit
! Configure the RTRs and object trackers.
! Use the next-hop command to ensure that the RTR is sent over the
! next hop it is monitoring, which is the WAN Fast Ethernet running
! DHCP client.
! 192.30.3.1 is the remote HQ peer IP address.
rtr 2
   type echo protocol ipIcmpEcho 192.30.3.1
      next-hop interface fastethernet 10/2
      exit.
track 2 rtr 2
   exit
! Apply object tracking on the DHCP client.
interface fastethernet 10/2
   ip dhcp client route track 2
   exit
```

# Summary of object tracking configuration commands

For more information about these commands, see Avaya Branch Gateway G450 CLI Reference.

Root level command	First level command	Second level command	Description
rtr	-	-	Enter Respond Time Reports (RTR) configuration mode. RTRs are the basic building blocks of object tracking.
-	type	-	Set the type of operation an RTR should employ in its probes, and specify the address of the remote device being probed
-	-	dscp	Set the DSCP value for the packets of the RTR probes
-	-	fail-retries	Set how many consecutive unanswered probes change the status of an RTR operation device from up to down
-	-	frequency	Set the frequency of the RTR probes
-	-	next-hop	Specify the next hop for the RTR probes, bypassing normal routing

Table continues...

Root level command	First level command	Second level command	Description
-	-	source-address	Set the source IP address for RTR operations
-	-	success-retries	Set how many consecutive answered probes change the status of an RTR operation device from down to up
-	-	wait-interval	Set how long to wait for a device to answer an RTR probe
rtr-schedule	-	-	Activate or stop an RTR operation
show rtr configuration	-	-	Display RTR configuration values
show rtr operational- state	-	-	Display the global operational status of the RTR feature
show track	-	-	Display tracking information
track	-	-	Configure an object tracker
-	description	-	Set a description for the object tracker
-	object	-	Add an object tracker to a track list
-	threshold count	-	Set the upper and lower thresholds for the threshold in the track list command

# Frame relay encapsulation features

The Media Gateway supports the following frame relay encapsulation features:

- Frame relay traffic shaping and FRF.12 fragmentation
- Priority DLCI



The terms PVC (Permanent Virtual Circuit) and DLCI (Data Link Connection Identifier) describe the same entity and are interchangeable.

#### Related links

Priority DLCI on page 273

Header compression configuration on page 201

# Frame relay traffic shaping and FRF.12 fragmentation

Frame relay traffic shaping regulates the outgoing traffic rate on a per-DLCI basis. Each DLCI maintains a weighted fair VoIP queue scheduler to buffer the packets.

FRF.12 fragmentation allows for link fragmentation and interleaving (LFI), which reduces the serialization delay on narrow bandwidth PVCs. This is required for VoIP traffic.

You can configure the traffic shaping and fragmentation parameters within traffic shaping templates called map classes. A map class is comprised of the following parameters:

- CIR. Default = 56,000 bps
- Committed Burst (BC) size. Default =7,000 bits
- Excess Burst (BE) size. Default = 0 bits
- Fragmentation. Fragment size, in bytes. Default = No Fragmentation.

You can configure up to 128 different map classes using different combinations of traffic shaping parameters. You then apply these map classes to a PVC.

# Note:

For a Priority DLCI group you must configure the Primary VC before associating a DLCI map class to the Priority DLCI group VCs. Removing the Primary VC after associating a DLCI map class to the Priority LCI group VCs, removes their map class configuration.

You can enable traffic shaping on a frame relay interface with the frame-relay traffic-shaping command. After you enable traffic shaping, a default map class is applied to all currently configured PVCs.

### Tasks used to configure map classes

Task	Command
Create a map class, and enter the configuration context of the map class.	map-class frame-relay
Configure the CIR, in bits per second, for the outbound direction.	cir out
Configure the BC size, in bits, for the outbound direction.	be out
Configure the BE size, in bits, for the outbound direction.	be out
Turn FRF.12 fragmentation on or off and to configure the fragment size.	fragment

For more information about these commands, see the *Avaya Branch Gateway G450 CLI Reference*.

## Task for displaying configured map classes

Task	Command
Display a table of all configured map-classes.	show map-class frame-relay

### Summary of frame relay traffic shaping commands

For more information about these commands, see Avaya Branch Gateway G450 CLI Reference.

Root level command	Command	Description
interface serial	-	Enter the Serial interface or sub interface configuration context
-	frame-relay traffic-shaping	Turn on/off traffic shaping and frame relay fragmentation
map-class frame- relay	-	Create a map class, a QoS template which can later be assigned to DLCIs, and enter the configuration context of the map class
-	bc out	Configure the committed burst size in bits, for the outbound direction
-	be out	Configure the excess burst size in bits, for the outbound direction
-	cir out	Configure the Committed Information Rate in bits per second, for the outbound direction
-	fragment	Turn FRF.12 fragmentation on or off and configure the fragment size
show map-class frame-relay	-	Display the map class table

# **Priority DLCI**

To implement new priority mechanisms, ISPs rely on new classes of service. Traffic types and users are divided into these classes and treated differently during peak periods. A premium, or first class user or traffic stream receives higher priority than a general user. This rating system ensures that the critical Internet user maintains peak performance. It also provides a means for ISPs to enhance the cost structure of network operations.

The Branch Gateway supports class-based traffic assignment (priority DLCI). Priority DLCI is a means for implementing QoS on frame relay circuits. The Branch Gateway separates traffic with different QoS levels to up to four different VCs on the same frame relay sub-interface. This feature enables you to assign unique Permanent VCs (PVC) for VoIP and non-VoIP traffic. You can set and adjust the priority using policy.

Configure Priority DLCI using the frame-relay priority-dlci-group command in the Serial sub-interface context. Specify the DLCIs in this command from the highest to lowest priority. If you specify less than four DLCIs, the last DLCI specified is automatically used for the missing priorities.

When using Priority DLCI, the primary DLCI is used to determine the state of the sub frame relay interface. When the primary DLCI is up, the sub frame relay interface is up. When the primary DLCI is down, the sub frame relay interface is down. Therefore, when using Priority DLCI, it is recommended to verify that the primary DLCI is set as the High Priority DLCI in the Priority DLCI group.

On the Branch Gateway, OSPF is mapped by default to the High Priority DLCI. For better network reliability, it is recommended to verify that the same configuration exists on the other side of the frame relay connection.

If one of the Priority DLCIs is down, its traffic is dropped.

Map the PVC control protocol on the routers at all ends of a multi-VC point-to-point link. Map this VC to the highest priority DLCI.

#### Related links

Policy lists on page 497

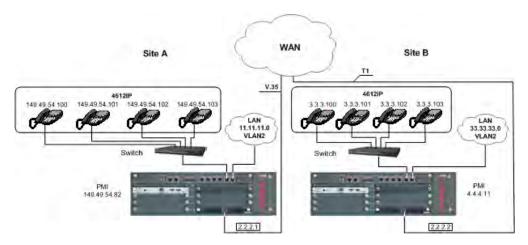
# **Summary of priority DLCI commands**

For more information about these commands, see the Avaya Branch Gateway G450 CLI Reference.

Root level command	Command	Description
interface serial	-	Enter the Serial interface or sub interface configuration context
-	frame-relay priority- dlci-group	Assign Virtual Channels to priority classifications, for the purpose of traffic separation

# **PPP VolP configuration**

The following figure illustrates a common PPP VoIP configuration between two sites connected over a WAN:



#### Site A connection details

Site A contains four IP phones and a Branch Gateway with S8300 and one MM342 media module. The MM342 media module connects the Branch Gateway to the WAN through a USP 128 Kbps V.35 interface. The following are the connection details for Site A:

• The IP phones are configured with the following DSCP tagging:

- Voice: DSCP 46

- Voice control: DSCP 34

### Note:

The policy list in the next configuration is based on the assumption that the Branch Gateway, S8300, and the IP phones send VoIP control packets with a DSCP value of 34 and voice with a DSCP value of 46. If any of the components of the topology are sending control or voice packets with other DSCP values, you must make changes in the policy list.

- The default RTP UDP port range is 2048 to 3028
- The Network IPs (24 bit subnet masks):

- IP phones: 149.49.54.0 (VLAN 1)

- Data: 11.11.11.0 (VLAN 2)

- Serial: 2.2.2.1

- S8300: 149.49.54.81

- Branch Gateway PMI: 149.49.54.82

### Site B connection details

Site B contains four IP phones and a Branch Gateway with S8300 and one MM340 media module. The MM340 media module connects the Branch Gateway to the WAN through two-timeslot (128 Kbps) T1 interface. The following are the connection details for Site B:

- IP phones are configured with DSCP tagging:
  - Voice = DSCP 46
  - Voice control = DSCP 34
- The default RTP UDP port range is 2048 to 3028
- Network IPs (24 bit subnet masks):
  - IP phones = 3.3.3.0 (VLAN 1)
  - Data = 33.33.33.0 (VLAN 2)
  - Serial = 2.2.2.2
  - S8300 = 4.4.4.10
  - Branch Gateway PMI = 4.4.4.11

### Configuration example for Site A

You can configure PPP VoIP on the Branch Gateway at Site A. Commands with footnotes are described at the end of the configuration procedure.

Loopback and PMI interfaces configuration:

```
Gxxx-001# interface loopback 1
Gxxx-001(if:Loopback 1) # ip address 149.49.54.82 24
Gxxx-001(if:Loopback 1) # pmi
The Primary management interface has changed. Please copy the running configuration
to the start-up configuration file, and reset the device.
Gxxx-001(if:Loopback 1)# exit
```

```
Gxxx-001# copy running-config startup-config
Gxxx-001# reset
```

• VLAN interface configuration:

```
Gxxx-001# interface Vlan 1
Gxxx-001(if:Vlan 1) # ip address 149.49.54.24
Gxxx-001(if:Vlan 1)# exit
Gxxx-001# interface Vlan 2
Gxxx-001(if:Vlan 2) # ip address 11.11.11.1 24
Done!
Gxxx-001(if:Vlan 2)# exit
```

Serial interface configuration:

```
Gxxx-001# interface serial 4/1
Gxxx-001(if:Serial 4/1) # ip address 2.2.2.1 24
Gxxx-001(if:Serial 4/1) # mtu 300
```

### Note:

Some LAN data applications do not support fragmented packets. In this case, do not change the MTU from its default of 1500.

```
Gxxx-001(if:Serial 4/1) # bandwidth 128
```

VoIP configuration:

```
Gxxx-001(if:Serial 4/1)# ip rtp header-compression
Gxxx-001(if:Serial 4/1)# ip rtp compression-connections 20 (4)
Gxxx-001(if:Serial 4/1) # ip rtp port-range 2048 3028
                                                            (5)
Gxxx-001(if:Serial 4/1)# exit
```

Static routes configuration:

```
Gxxx-001# ip default-gateway 4/1
```

- \* Description of footnoted commands (also applies to identical stages in configuring Site B):
- (1) At this stage you apply Priority 7 to Voice Control traffic.
- (2) At this stage you apply Priority 6 to RTP traffic.
- (3) At this stage you apply maximum trust between 802.1p priority and DSCP.
- (4) At this stage the number of connections (20) depends on the number of phones.
- (5) At this stage you are matching the RTP port range to that of the Gateway.
- (6) At this stage the default queue size is 6, and since RTP is enabled you can double the VoIP queue size.

### Configuration example for Site B

You can configure PPP VoIP on the Branch Gateway at Site B.

Loopback and PMI interfaces configuration:

```
Gxxx-001# interface loopback 1
Gxxx-001(if:Loopback1) # ip address 4.4.4.11 32
Done!
Gxxx-001(if:Loopback 1)# pmi
The Primary management interface has changed. Please copy the running configuration
to the start-up configuration file, and reset the device.
```

```
Gxxx-001(if:Loopback1)# exit
Gxxx-001# copy running-config startup-config
Gxxx-001# reset
```

### • VLAN interface configuration:

```
Gxxx-001# interface Vlan 1
Gxxx-001(if:Vlan 1)# ip address 3.3.3.1 24
Gxxx-001(if:Vlan 1)# exit
Gxxx-001# interface Vlan 2
Gxxx-001(if:Vlan 1:2)# ip address 33.33.33.1 24
Gxxx-001(if:Vlan 1:2)# exit
```

### Serial interface configuration:

```
Gxxx-001# controller t1 4/1
Gxxx-001(controller:4/1)# channel-group 1 timeslots 1-2 speed 64
Gxxx-001(controller:4/1)# exit
Gxxx-001# interface serial 4/1:1
Gxxx-001(if:Serial 4/1:1)# ip address 2.2.2.2 24
Gxxx-001(if:Serial 4/1:1)# mtu 300
```

# **₩** Note:

Some LAN data applications do not support fragmented packets. In this case, do not change the MTU from its default of 1500.

### • VoIP configuration:

```
Gxxx-001(if:Serial 4/1:1)# ip rtp header-compression

Gxxx-001(if:Serial 4/1:1)# ip rtp compression-connections 20

Gxxx-001(if:Serial 4/1:1)# ip rtp port-range 2048 3028

Gxxx-001(if:Serial 4/1:1)# exit
```

### • Static routes configuration:

```
Gxxx-001# ip route 1.1.1.0 24 serial 4/1:1
Gxxx-001# ip route 11.11.11.0 24 serial 4/1:1
```

# **Chapter 12: Emergency Transfer Relay**

The Emergency Transfer Relay (ETR) feature provides basic telephone services in the event of system failure, such as a power outage or a failed connection to the MGC. An external ETR relay panel can be used in conjunction with an analog media module (MM711, MM714, MM714B, or MM716). The ETR panel provides up to five incoming Central Office (CO) trunk loops to five selected G450 analog lines. Thus, one ETR panel supports up to five emergency lines. You can cascade a second ETR panel, providing support for up to 10 emergency analog phones. ETR is activated automatically upon system failure by closing the tip/ring contacts between the analog lines and the analog trunks. When ETR is activated, all calls are directed by the analog relays between the outside lines and the analog telephones. A current-loop detection circuit prevents ongoing calls from being disconnected when normal functioning resumes. If a call is in progress on an outside line when the problem ends, the call continues. The trunk port and analog line port passing through the ETR panel do not start to operate until the active call ends.

In addition, each MM714B media module installed in the Branch Gateway can provide identical ETR services in the event of system failure by connecting trunk port 5 to line port 4. You can install an MM714B media module in any slot. When ETR is active and the Branch Gateway has power, the ETR LED is lit.

# **ETR** state configuration

By default, ETR is set to go into effect automatically in the event of power outage or a failed connection to the MGC. You can activate and deactivate ETR manually using the CLI.

# **Activating ETR manually**

About this task

Use this command only for testing.

**Procedure** 

Enter set etr 10 manual-on

# **Deactiving ETR manually**

**Procedure** 

Enter set etr 10 manual-off.

### Result

ETR does not become active in the event of a link failure.

# Restoring ETR to automatic activation

### **Procedure**

Enter set etr 10 auto

If the system fails, the trunk and port in the MM714B, or the analog line connections and analog trunk connections passing through the ETR panel, are automatically latched.



### Note:

A call in progress is terminated when ETR is activated either automatically or manually.

# **Summary of ETR commands**

For more information about these commands, see Avaya Branch Gateway G450 CLI Reference.

Command	Description
set etr	Enable or disable ETR mode on Branch Gateway chassis or on an MM714B media module, or enable the gateway to control ETR mode automatically.
show etr	Display the status of ETR mode. This information includes the following:
	Admin state (auto, manual-off, or manual-on)
	<ul> <li>Module status (in service, out of service, or out of service waiting for off-hook)</li> </ul>
	Trunk number of the trunk connected to ETR
	Line number of the line connected to ETR
	Line status (off hook or on hook)
	ETR status on Branch Gateway chassis shows only the Admin state.

# **Chapter 13: SNMP**

SNMP uses software entities called managers and agents to manage network devices. The manager monitors and controls all other SNMP-managed devices or network nodes on the network. There must be at least one SNMP Manager in a managed network. The manager is installed on a workstation located on the network.

An agent resides in a managed device or network node. The agent receives instructions from the SNMP Manager, generates reports in response to requests from the SNMP Manager, and sends management information back to the SNMP Manager as events occur. The agent can reside on:

# Note:

SNMP is supported on IPv4 only.

- Routers
- Bridges
- Hubs
- Workstations
- Printers
- · Other network devices

There are many SNMP management applications, but all these applications perform the same basic task. They allow SNMP managers to communicate with agents to configure, get statistics and information, and receive alerts from network devices. You can use any SNMP-compatible network management system to monitor and control a Branch Gateway.

# Agent and manager communication

There are several ways that the SNMP manager and the agent communicate. The manager can:

**Retrieve a value (get):** The SNMP manager requests information from the agent, such as the number of users logged on to the agent device or the status of a critical process on that device. The agent gets the value of the requested Management Information Base (MIB) variable and sends the value back to the manager.

**Retrieve the value immediately after the variable you name (get-next):** The SNMP manager retrieves different instances of MIB variables. The SNMP manager takes the variable you name and then uses a sequential search to find the desired variable.

**Retrieve a number of values (get-bulk):** The SNMP manager retrieves the specified number of instances of the requested MIB variable. This minimizes the number of protocol exchanges required to retrieve a large amount of data.

# Note:

*Get-bulk* is not supported in SNMPv1. Keep the number of repetitions low so that the get-bulk replies are less than 1520 bytes.

**Change a configuration on the agent (set):** The SNMP manager requests the agent to change the value of the MIB variable. For example, you can run a script or an application on a remote device with a set action.

**Receive an unsolicited message (notification):** The SNMP manager receives an unsolicited message from an agent at any time if a significant, predetermined event takes place on that agent. When a notification condition occurs, the SNMP agent sends an SNMP notification to the device specified as the trap receiver or trap host. The SNMP Administrator configures the trap host, usually the SNMP management station, to perform the action needed when a trap is detected.

# Note:

For a list of traps and MIBS, see *Gateway Traps for the Avaya G450, and G700 Media Gateways*.

# **SNMP** versions

There are currently three versions of SNMP:

- SNMPv1
- SNMPv2c
- SNMPv3

The Branch Gateway supports all three versions. The implementation of SNMPv3 on the Branch Gateway is backwards compatible. That is, an agent that supports SNMPv3 will also support SNMPv1 and SNMPv2c.

## SNMPv1

SNMPv1 uses community strings to limit access rights. Each SNMP device is assigned to a read community and a write community. To communicate with a device, you must send an SNMP packet with the relevant community name.

By default, if you communicate with a device using only the read community, you are assigned the security name ReadCommN. This security name is mapped to the ReadCommG group by default. This allows you to view the agent's MIB tree, but you cannot change any of the values in the MIB tree.

If you communicate with a device using the write community, you are assigned the security name WriteCommN. This security name is mapped to the WriteCommG group by default. This allows you to view the agent's MIB tree and change any of the values in the MIB tree.

### ★ Note:

If you delete the ReadCommN or WriteCommN users, the ReadCommG or WriteCommG groups, or the snmpv1WriteView or snmpv1View, you may not be able to access the device using SNMPv1 or SNMPv2c.

In addition, traps are sent to designated trap receivers. Packets with trap information also contain a trap community string.

### SNMPv2c

SNMPv2c is very similar to SNMPv1. However, SNMPv2c adds support for the *get-bulk* action and supports a different trap format.

# SNMPv3

SNMPv3 enables the following features over SNMPv1 or v2c:

- User authentication with a username and password
- Communication encryption between the Network Management Station (NMS) and the SNMP agent at the application level
- Access control definition for specific MIB items available on the SNMP agent
- · Notification of specified network events directed toward specified users
- Definition of roles using access control, each with unique access permissions and authentication and encryption requirements

The basic components in SNMPv3 access control are users, groups, and views. In addition, SNMPv3 uses an SNMP engine ID to identify SNMP identity. An SNMP engine ID is assigned to each MAC address of each device in the network. Each SNMP engine ID should be unique in the network.

# **Users**

SNMPv3 uses the User-based Security Model (USM) for security, and the View-based Access Control Model (VACM) for access control. USM uses the HMAC-MD5-96 and HMAC-SHA-96 protocols for user authentication, and the CBC-DES56 protocol for encryption or privacy.

An unlimited number of users can access SNMPv3 at the same time.

# **SNMP** security levels

• **NoAuthNoPriv:** This is the lowest level of SNMPv3 security. No MAC is provided with the message, and no encryption is performed. This method maintains the same security level as SNMPv1, but provides a method for limiting the access rights of the user.

- AuthNoPriv: . User authentication is performed based on MD5 or SHA algorithms. The message is sent with an HMAC that is calculated with the user key. The data part is sent unencrypted.
- AuthPriv: . User authentication is performed based on MD5 or SHA algorithms. The message is sent in encrypted MAC that is calculated with the user key, and the data part is sent with DES56 encryption using the user key.

# snmp-server user command

Use the **snmp-server user** command to create a user or to change the parameters of an existing user. This command includes the following parameters:

- · A user name for the user
- The name of the SNMP group with which to associate the user
- The SNMP version functionality that the user is authorized to use. Possible values are: v1 (SNMPv1), v2c (SNMPv2c), and v3 (SNMPv3).
- For an SNMPv3 user, which authentication protocol to use, if any. Possible values are: md5 (HMAC MD5), and sha (HMAC SHA-1). If you specify an authentication protocol, you must also configure an authentication password for the user. The authentication password is transformed using the authentication protocol and the SNMP engine ID to create an authentication key.
- For an SNMPv3 user, whether or not to use the DES/AES privacy protocol, and the user's privacy password if you enable DES/AES privacy.

Use the **no** form of the **snmp-server user** command to remove a user and its mapping to a specified group. If you do not specify a group, the **no** form of the **snmp-server user** command removes the user from all groups.

# **Groups**

In SNMPv3, each user is mapped to a group. The group maps its users to defined views. These views define sets of access rights, including read, write, and trap or inform notifications the users can receive.

The group maps its users to views based on the security model and level with which the user is communicating with the Branch Gateway. Within a group, the following combinations of security model and level can be mapped to views:

- SNMPv1 security model and NoAuthNoPriv security level
- SNMPv2c security model and NoAuthNoPriv security level
- SNMPv3 security model and NoAuthNoPriv security level
- SNMPv3 security model and AuthNoPriv security level
- SNMPv3 security model and AuthPriv security level

If views are not defined for all security models and levels, a user can access the highest level view below the user's security level. For example, if the SNMPv1 and SNMPv2c views are undefined for a group, anyone logging in using SNMPv1 and SNMPv2c cannot access the device. If the

NoAuthNoPriv view is not defined for a group, SNMPv3 users with a NoAuthNoPriv security level can access the SNMPv2c view.

# **Pre-configured SNMP groups**

The Branch Gateway includes the following pre-configured groups:

Group name	Security model	Security level	Read view name	Write view name	Notify view name
initial	v3 (USM)	NoAuthNoPriv	restricted	restricted	restricted
ReadCommG	v1	NoAuthNoPriv	snmpv1View	-	snmpv1View
ReadCommG	v2c	NoAuthNoPriv	snmpv1View	-	snmpv1View
WriteCommG	v1	NoAuthNoPriv	snmpv1 WriteView	snmpv1 WriteView	snmpv1 WriteView
WriteCommG	v2c	NoAuthNoPriv	snmpv1 WriteView	snmpv1 WriteView	snmpv1 WriteView
v3ReadOnlyG	v3 (USM)	AuthNoPriv	v3configView	-	v3configView
v3AdminViewG	v3 (USM)	AuthPriv	iso	iso	iso
v3ReadWriteG	v3 (USM)	AuthNoPriv	v3configView	v3configView	v3configView

# snmp-server group command

Use the **snmp-server group** command to create an SNMPv3 group. Use the **no** form of the command to remove the specified group. You can define the following parameters with this command:

- The name of the group
- The SNMP security model
- The security level, for a group with the SNMPv3 security model
- The name of a read view to which the group maps users
- The name of a write view to which the group maps users
- The name of a notify view to which the group maps users

## **Views**

There are three types of views:

Read Views: Allow read-only access to a specified list of Object IDs (OIDs) in the MIB tree

Write Views: Allow read-write access to a specified list of OIDs in the MIB tree

Notify Views: Allow SNMP notifications from a specified list of OIDs to be sent

Each view consists of a list of OIDs in the MIB tree. This list can be created using multiple snmp-server view commands to either add OIDs to the list or exclude OIDs from a list of all of the OIDs in the Branch Gateway's MIB tree. You can use wildcards to include or exclude an entire branch of OIDs in the MIB tree, using an asterisk instead of the specific node.

#### Related links

Branch Gateway MIB files on page 566

### SNMPv3 view creation

To create an SNMPv3 view, the following information must be provided:

- ViewName: . A string of up to 32 characters representing the name of the view
- ViewType: . Indicates whether the specified OID is included or excluded from the view
- OIDs: . A list of the OIDs accessible using the view

# **SNMP** trap configuration

When SNMP traps are enabled on the device, SNMP traps are sent to all IP addresses listed in the trap receivers table. You can add and remove addresses from the trap receivers table. In addition, you can limit the traps sent to specified receivers. You can also enable and disable link up/down traps on specified Branch Gateway interfaces. Use the following commands to configure the trap receivers table:



#### Note:

You need an Admin privilege level to use the SNMP commands.

# snmp-server host command parameters

You can define the following parameters with this command:

- · The IP address of the recipient.
- Whether to send traps or informs to the recipient.
- The SNMP security model (v1, v2c, v3). For SNMPv1 and SNMPv2c, you must also specify the community name. For SNMPv3, you must specify the level of authentication and a username to use in notifications. Authentication levels are:
  - auth. Authentication without encryption
  - noauth. No authentication
  - priv. authentication with encryption
- The UDP port of the target host to use as the destination UDP port when sending a notification to this manager. Optional. The default is 162.

Notification filter groups, to modify the types of traps that are sent to the recipient. Optional. If not specified, all notification groups are sent.

# **Notification types**

Various types of SNMP traps can be sent. You can modify the type of trap by setting the notification-list parameter of the snmp-server host command to one of the following types:

- all. All traps. This is the default.
- generic. Generic traps
- hardware. Hardware faults
- rmon. RMON rising/falling alarm
- dhcp server. DHCP server error, such as a DHCP IP conflict detection or notification of no IP address left for specific network
- dhcp-clients. DHCP client error, such as a DHCP client conflict detection
- rtp-stat-faults. RTP statistics: QoS fault/clear traps
- rtp-stat-qos. RTP statistics: end-of-call QoS traps
- wan. WAN router traps
- media-gateway. Branch Gateway traps (equivalent to G700 MGP traps)
- security. Security traps, such as unAuthAccess, macSecurity, unknownHostCopy, and accountLockout
- config. Configuration change notifications
- eth-port-faults. Ethernet port fault notifications
- sw-redundancy. Software redundancy notifications
- temperature. Temperature warning notifications
- cam-change. Changes in CAM notifications
- 13-events. Duplicate IP, VLAN violations
- policy. Policy change notifications
- link-faults. ITC proprietary link down notifications
- supply. Main and backup power supply notifications

# Summary of SNMP trap configuration commands

For more information about these commands, see Avaya Branch Gateway G450 CLI Reference.

Root level command	Command	Description
interface (dialer   fastethernet   tunnel   usb-modem)	-	Enter the context of the Dialer, Fast Ethernet, Tunnel, or USB-modem interface
-	snmp trap link-status	Enable or disable Link Up and Link Down traps on an interface
set port trap	-	Enable or disable SNMP Link Up and Link Down traps notifications and traps on a port
set snmp trap enable   disable auth	-	Enable or disable authentication failure traps for all managers
set snmp trap enable   disable frame-relay	-	Enable or disable frame relay traps for all managers
show port trap	-	Display information on SNMP generic Link Up and Link Down traps sent for a specific port or for all ports
show snmp	-	Display SNMP configuration information
snmp-server enable notifications	-	Enable or disable the sending of all traps and notifications from the Branch Gateway
snmp-server host	-	Identify an SNMP management server, and specify the kind of messages it receives. Use the no form of the command to remove the specified server, or to disable a particular set of notification types.
snmp-server informs	-	Configure the SNMPv3 timeout and retries for notifications

# **Summary of SNMP access configuration commands**

For more information about these commands, see Avaya Branch Gateway G450 CLI Reference.

Command	Description
ip snmp	Enable or disable the SNMP agent for the Branch Gateway
set snmp community	Create or modify an SNMPv1 community
set snmp retries	Set the number of times to attempt to communicate with a particular node
set snmp timeout	Specify the time to wait for a response before retrying the communication
show snmp	Display SNMP configuration information, including a list of SNMP notification receivers
show snmp engineID	Display the SNMPv3 engine ID for the Branch Gateway
show snmp group	Display a list of SNMPv3 groups

Table continues...

Command	Description
show snmp retries	Display the number of retry attempts to make when attempting to communicate with a node
show snmp timeout	Display the time to wait before resending a communication
show snmp user	Display configuration information for a specified SNMP user
show snmp usertogroup	Display a table of SNMPv3 users and the groups to which they are mapped
show snmp view	Display configuration information for all SNMP views
snmp-server community	Enable or disable SNMP access to the Branch Gateway
snmp-server engineID	Specify the SNMP Engine ID for the Branch Gateway
snmp-server group	Define a new SNMPv3 group, or configure settings for the group
snmp-server remote- user	Configure settings for a remote SNMPv3 user. If the user does not exist, it is created.
snmp-server user	Configure settings for an SNMPv3 user. If the user does not exist, it is created.
snmp-server view	Configure settings for an SNMP MIB view. If the view does not exist, it is created.

# Dynamic trap manager

Dynamic trap manager is a special feature that ensures that the Branch Gateway sends traps directly to the currently active MGC. If the MGC fails, dynamic trap manager ensures that traps are sent to the backup MGC.



The dynamic trap manager is created by default and cannot be removed.

# Dynamic trap manager parameters

When you use the snmp-server dynamic-trap-manager command, you can configure the following parameters:

- Whether to send traps or informs to the recipient
- The SNMP security model (v1 or v2c)
- The SNMP community name
- The UDP port of the target host to use as the destination UDP port when sending a notification to this manager. Optional.
- The types of traps to be sent. Optional. The default is to send all types of traps.

#### Related links

Notification types on page 286

## Summary of dynamic trap manager configuration commands

For more information about these commands, see Avaya Branch Gateway G450 CLI Reference.

Command	Description
clear dynamic-trap- manager	Remove administration of the dynamic trap manager
snmp-server dynamic- trap-manager	Specify the parameters of the dynamic trap manager feature

## **SNMP** configuration examples

The following example enables link up/down traps on an Ethernet interface:

```
Gxxx-001(super)# interface fastethernet 10/3
Gxxx-001(super-if:FastEthernet 10/3)# snmp trap link-status
Done!
```

## The following example displays SNMP information:

## The following example disables Link Up and Link Down traps on an Ethernet interface:

```
Gxxx-001(super-if:FastEthernet 10/3) # no snmp trap link-status
Enter authentication password : *******

Confirm authentication password : *******
Enter privacy password : *******

Confirm privacy password : *******

Done!
```

#### The following example creates a read-only user:

```
Gxxx-001# snmp-server user joseph ReadOnlyG v3 auth md5 priv des56 ktamatan
Enter authentication password : *******

Confirm authentication password : *******
Enter privacy password : *******

Confirm privacy password : ********

Done!
```

## The following example creates a read-write user:

```
Gxxx-001# snmp-server user johnny ReadWriteG v3 auth md5 priv des56 ktamatan
Enter authentication password : *******

Confirm authentication password : *******
Enter privacy password : *******

Confirm privacy password : *******

Done!
```

### The following example creates an admin user:

```
Gxxx-001# snmp-server user johnny v3AdminG v3 auth md5 priv des56 ktamatan
Enter authentication password : *******

Confirm authentication password : *******

Enter privacy password : *******

Confirm privacy password : *******

Done!
```

## The following example sets the SNMPv1 read-only community:

```
Gxxx-001(super)# set snmp community read-only read
SNMP read-only community string set.
```

#### The following example sets the SNMPv1 read-write community:

```
Gxxx-001(super)# set snmp community read-write write
SNMP read-write community string set.
```

### The following example enables link up/down trap on a LAN port on the G250:

```
G250-001(super) # set port trap 10/3 enable
Port 10/3 up/down trap enabled
```

# The following example enables Link Up and Link Down traps on a LAN port on the Branch Gateway:

```
Gxxx-001(super) # set port trap 10/5 enable
Port 10/5 up/down trap enabled
```

## The following example disables link up/down trap on a LAN port on the G250:

```
G250-001(super)# set port trap 10/4 disable
Port 10/4 up/down trap disabled
```

# The following example disables Link Up and Link Down traps on a LAN port on the Branch Gateway:

```
Gxxx-001(super) # set port trap 10/5 disable
Port 10/5 up/down trap disabled
```

# **Chapter 14: Media encryption using AES-256**

From Communication Manager Release 7.0, the AES encryption option now includes AES-256 cipher suite. AES-256 applies to voice media streams and video media streams for the IP network region that governs the IP codec set. The feature also introduces a mechanism to define the encrypted SRTCP policy for calls governed by the IP network region.

## Screen for administering Media encryption using AES-256

Screen name	Purpose	Fields
Ip-codec-set	To select a type of media encryption.	Media encryption

## Administering Media encryption using AES-256

## Before you begin

Ensure that the **Media Encryption Over IP?** field on the system-parameters customer-options screen is set to v.

### **Procedure**

- 1. On the SAT screen, type change ip-codec-set n, where n is the number of the codec set that you want to change.
- 2. In the **Media encryption** field, type one of the following values:
  - To use encrypted and authenticated RTP with an 80-bit authentication tag, type 10srtp-aescm256-hmac80.
  - To use encrypted and authenticated RTP with a 32-bit authentication tag, type 11srtp-aescm256-hmac32.
- Save and exit.

## **Detailed description**

Advanced Encryption Standard (AES) is a widely used specification for data encryption. The AES standards describe a symmetric key algorithm. AES has a fixed block size of 128 bits and a key size of 128, 192, or 256 bits. Avaya Aura® Release 6.3 Feature Pack 4 supports AES-256 as part of TLS support over control channels. From Release 7.0, the AES-256 support extends to secure media streams.

To enable Media encryption feature, two more encryption choices are available for the **Media encryption** field on the ip-codec-set SAT screen. The choices are as follows:

- srtp-aescm256-hmac80
- srtp-aescm256-hmac32

Before Release 7.0, the **Media Encryption** field supported only three profiles. Release 7.0 onwards, the field supports five profiles.

You can add the following profiles to Media Encryption:

- 1. 10-srtp-aescm256-hmac80
- 2. 11-srtp-aescm256-hmac32
- 3. 1-srtp-aescm128-hmac80
- 4. 2-srtp-aescm128-hmac32
- 5. None

The AES-256 feature is supported on G450 Branch Gateway, G430 Branch Gateway, and Avaya Aura<sup>®</sup> Media Server (MS).

When you enable the AES-256 feature, Communication Manager determines the capability exchange with G450 Branch Gateway, G430 Branch Gateway, or Avaya Aura® Media Server (MS) and the 96x1 SIP phone. To establish call connections for media services encrypted with AES-256, an SDP media descriptor exchange occurs. During this exchange, Communication Manager functions as a back-to-back user agent. In this role, Communication Manager supports policy management over the SIP endpoints when the endpoints exercise capability negotiation.

# **Chapter 15: Encrypted SRTCP**

## **Detailed description**

With the Encrypted SRTCP feature, you can protect media control streams. To support this feature, the Encrypted SRTCP field is available on the ip-codec-set SAT screen. The following are the available policy modes:

- Force Encrypted SRTCP: To permit only encrypted SRTCP calls and to achieve high security standards. If you set the field to enforce-enc-srtcp, all the crypto profiles enforce encrypted SRTCP.
- Best Effort: To facilitate negotiation of the encrypted SRTCP parameter. If you set the field to best-effort, Communication Manager facilitates negotiation of Encrypted SRTCP capability between the endpoints. All endpoints must support negotiation to enforce the Best Effort policy mode.
- Force Unencrypted SRTCP: To support backward compatibility. If you set the field to enforce-unenc-srtcp, all the crypto profiles enforce unencrypted SRTCP. Communication Manager does not support encrypted SRTCP. This value is the default value in Communication Manager Release 10.1.

## **Encrypted SRTCP**

Use the Encrypted SRTCP feature to provide enhanced security for the media control streams associated with the RTP media stream.



#### Note:

The RTP and RTCP streams are two consecutive UDP ports. The RTCP control stream conveys usage data. An example of usage data is the identification of the two parties on a given call.

## Screen for administering Encrypted SRTCP

Screen name	Purpose	Fields
Ip-codec-set	To select a policy option to activate the encrypted SRTCP.	Encrypted SRTCP

## Administering Encrypted SRTCP

## Before you begin

Ensure that the **Media Encryption Over IP?** field on the system-parameters customer-options screen is set to y.

#### **Procedure**

- 1. On the SAT screen, type change ip-codec-set n, where n is the number corresponding to the codec set that you want to change.
- 2. In the Encrypted SRTCP field, type enforce-enc-srtcp. You can select the Best Effort option if you want Communication Manager to negotiate encrypted SRTCP capability between endpoints.



## Note:

The default value for Encrypted SRTCP is enforce-unenc-srtcp. Endpoints earlier than Release 7.0 do not support encrypted SRTCP. Therefore, enforcing unencrypted SRTCP is preferable in networks that have Communication Manager Release 7.0 with earlier endpoints.

3. Save and exit.

## Interactions for Encrypted SRTCP

This section provides information about how the Encrypted SRTCP feature interacts with other features in the system. Use this information to ensure that you receive the maximum benefits of the Encrypted SRTCP feature in any feature configuration.

## **Emergency calling**

Using the encryption options, you cannot negotiate calls with the destination party because of protocol incompatibilities. The protocol incompatibility results in the inability to pass certain types of emergency calls. Therefore, you must configure the network to ensure best routing of calls.

## Media Encryption using AES

If the RTP media encryption is set to none, the enforce-encrypted SRTCP rules do not apply to the RTP/RTCP streams.

## **Chapter 16: Contact closure**

You can use contact closure to control up to two electrical devices remotely. With contact closure, you can dial feature access codes on a telephone to activate, deactivate, or pulse electrical devices such as electrical door locks. You can also activate and deactivate contact closure using CLI commands. You can only use feature access codes if you configure the Branch Gateway to use a server with CM software.

It is recommended that you use an Avaya Partner Contact Closure Adjunct<sup>™</sup> for contact closure. For more information, see *Overview for the Avaya Branch Gateway G450*. An Avaya Partner Contact Closure Adjunct<sup>™</sup> contains two relays, one for each electrical device. You can control each relay in any of the following ways:

- When you dial the contact closure open access code, the relay opens (no contact)
- When you dial the contact closure close access code, the relay closes (contact)
- When you dial the contact closure pulse access code, the relay closes (contact) for the pulse duration and then opens (no contact)
- You can control each contact closure relay manually with CLI commands or with the Branch Gateway

## Note:

Configuration of the feature access code is performed through CM. For more information, see *Administrator Guide for Avaya Aura*® *Communication Manager*.

#### Related links

Branch Gateway Controller configuration on page 62

## Configuring contact closure hardware

## **Procedure**

Connect an Avaya Partner Contact Closure Adjunct<sup>™</sup> to the Contact Closure port on the Branch Gateway front panel, labeled CCA.

Use a telephone cable with standard RJ-11 connectors.

A qualified electrician should connect the electrical devices to the relays on the Avaya Partner Contact Closure Adjunct<sup>™</sup>.

For information on contact closure specifications, see *Overview for the Avaya Branch Gateway G450*.

## Software contact closure

## Contact closure modes

Mode	Description
mgc	The MGC controls contact closure. In mgc mode, the user dials feature access codes to activate and deactivate contact closure.
manual-trigger	Activates contact closure for the specified relay
manual-off	Deactivates contact closure for the specified relay

## **Configuring contact closure software**

### About this task

To configure the Branch Gateway to activate contact closure when the feature access code is dialed:

#### **Procedure**

1. Enter the set contact-closure admin command.

In the following example, the command sets contact closure to work in relay 1 of the Avaya Partner Contact Closure Adjunct  $^{\text{TM}}$  when activated by the call controller.

```
set contact-closure admin 10/1:1 mgc
```

2. Use the set contact-closure pulse-duration command to set the length of time for the relay to return to normal after the call controller triggers it.

In the following example, the command sets relay 2 of the Avaya Partner Contact Closure  $Adjunct^{TM}$  to return to normal five seconds after the call controller triggers contact closure in the relay.

set contact-closure pulse-duration 10/1:2 5

## Activating a contact closure manually

#### **Procedure**

Use the set contact-closure admin command with the parameter manual-trigger.

In the following example, the command activates contact closure in relay 1 of the Avaya Partner Contact Closure Adjunct<sup>™</sup>. Contact closure remains active until you deactivate it by using the set contact-closure admin command with the parameter manual-off or mgc.

set contact-closure admin 10/1:1 manual-trigger

## Deactivating a contact closure manually

#### **Procedure**

Use the set contact-closure admin command with the parameter manual-off.

In the following example, the command deactivates contact closure in relay 2 of the Avaya Partner Contact Closure Adjunct<sup>™</sup>. Contact closure will not operate, even automatically, until you use the set contact-closure admin command to change the status of contact closure to mgc or manual-trigger.

set contact-closure admin 10/1:2 manual-off

## **Showing contact closure status**

## **Procedure**

Use the **show contact-closure** command to display the status of one or more contact closure relays.

The following example displays the contact closure status of relay 1 of the Avaya Partner Contact Closure Adjunct<sup>™</sup> box.

Gxxx-001	(super)	# show o	contact-closure		
MODULE	PORT	RELAY	ADMIN	PULSE DURATION (secs)	STATUS
10	2	1	mgc	5 secs	off
10	2	2	mqc	3 secs	off

## **Summary of contact closure commands**

For more information about these commands, see Avaya Branch Gateway G450 CLI Reference.

Command	Description
set contact-closure admin	Specify how the contact closure relay is controlled
set contact-closure pulse-duration	Set the length of time for the relay to return to normal after the call controller triggers the relay
show contact-closure	Display the status of one or all contact closure relays

# **Chapter 17: Announcement files**

The Branch Gateway stores announcement files in an internal announcement directory. The Branch Gateway supports up to 256 announcement files, totalling up to 45 minutes of audio for announcements and music on hold. If a compact flash is installed with increased RAM, the Branch Gateway supports up to 1024 announcement files, for a total of 240 minutes. A total of 63 announcements can be played simultaneously, and one port may be used for recording. Recording, storing, and playing announcement files is controlled by CM.

## Note:

For information about installing and using a compact flash and increased RAM, refer to Job Aid: Installing the upgrade memory kit in the G450 / G430 Branch Gateway.

Avaya Voice Announcement Manager (VAM) can be used to centrally manage announcement files for multiple voice systems, including Branch Gateways. VAM is designed to be installed on a customer-provided platform at a remote location. For information about VAM, see Avaya Voice Announcement Manager Reference.

The Branch Gateway supports:

- Secure transfer of announcement files to and from VAM using SCP
- Simple management operations for the announcement files stored in the announcement directory
- Dynamic allocation of announcement time slots for 64 announcement ports on an as-needed basis

## Uploading announcement files to a remote SCP server **Procedure**

Upload an announcement file to a remote SCP server, using the copy announcement-file scp command.

Specify the file name of the announcement file in the Branch Gateway announcement directory, followed by the IP address of the remote SCP server, and, optionally, a destination file name, including the full path.

### For example:

Gxxx-001(super) # copy announcement-file scp local announcement2.wav 192.168.49.10 remote announcement2.wav

## Downloading announcement files from a remote SCP server

## **Procedure**

Download an announcement file from a remote SCP server to the Branch Gateway announcement directory, using the copy scp announcement-file command.

Specify the file name of the announcement file on the remote SCP server, followed by the IP address of the remote SCP server, and, optionally, a destination file name, including the full path.

### For example:

```
Gxxx-001(super) \# copy scp announcement-file announcement_file1.wav 192.168.49.10
```

# Uploading announcement files to a remote FTP server

Upload an announcement file to a remote FTP server, using the copy announcement-file ftp command.

Specify the file name of the announcement file in the Branch Gateway announcement directory, followed by the IP address of the remote FTP server, and, optionally, a destination file name, including the full path.

### **Example**

```
Gxxx-001(super)# copy announcement-file ftp local_announcement2.wav 192.168.49.10 remote announcement2.wav
```

# Downloading announcement files from an FTP server

Download an announcement file from an FTP server to the Branch Gateway announcement directory, using the copy ftp announcement-file command.

Specify the file name of the announcement file on the FTP server, followed by the IP address of the FTP server, and, optionally, a destination file name, including the full path.

#### For example:

```
Gxxx-001(super) \# copy ftp announcement-file announcement_file1.wav 192.168.49.10
```

# Uploading an announcement file to a USB mass storage device

#### **Procedure**

Upload an announcement file to a USB mass storage device, using the copy announcement-file usb command.

Specify the file name of the announcement file in the Branch Gateway announcement directory, followed by the name of the USB device, and, optionally, a destination file name, including the full path.

#### **Example**

Gxxx-001(super)# copy announcement-file usb local\_announcement2.wav
usb-device0 remote\_announcement2.wav

# Downloading an announcement file from a USB mass storage device

#### **Procedure**

Download an announcement file from a USB mass storage device to the Branch Gateway announcement directory, using the copy usb announcement-file command.

Specify the name of the USB device, followed by the file name of the announcement file on the USB device, and, optionally, a destination file name, including the full path.

#### For example:

Gxxx-001(super)# copy usb announcement-file usb-device0 \temp\
announcement\_file1.wav local\_announcement\_file2.wav

# Uploading announcement files to a remote HTTP or HTTPS server

#### **Procedure**

Upload an announcement file to a remote HTTP or HTTPS server, using the copy announcement-file https command.

Specify the file name of the announcement file in the Branch Gateway announcement directory, followed by the URL of the remote HTTP or HTTPS server, the transfer type, and optionally, the destination filename.

### **Example**

Gxxx-001(super)# copy announcement-file https local\_announcement2.wav
192.168.49.10 c:\remote announcement2.wav unsecure

# Downloading announcement files from an HTTP or HTTPS server

#### **Procedure**

Download an announcement file from an HTTP or HTTPS server to the Branch Gateway announcement directory, using the copy https announcement-file command.

Specify the URL of the announcement file on the HTTPS server followed by the optional transfer type, and, optionally, a destination file name, including the full path.

#### For example:

Gxxx-001cp(super) # copy http announcement-file http://www.example.com/files/ann123.wav Username: dan Password:

# Uploading announcement files to a remote SCP server via Avaya SBCE tunnel

### **Procedure**

Uploads an announcement file from the Branch Gateway announcement directory to a remote SCP server using SCP via Avaya SBCE tunnel, using the copyedge announcement-file scp command.

Specify the file name of the announcement file in the Branch Gateway announcement directory, followed by the file directory path and file server IP address of the remote SCP server.

#### For example:

 $Gxxx-001(super) \# copyedge announcement-file scp local_announcement2.wav 192.168.49.10$ 

# Downloading announcement files from a remote SCP server via Avaya SBCE tunnel

## **Procedure**

Downloads an announcement file from the Voice Announcements Manager or an SCP server via Avaya SBCE tunnel to the Branch Gateway announcement directory, using the **copyedge** scp announcement-file command.

Specify the file name of the announcement file in the Branch Gateway announcement directory, followed by the file directory path and file server IP address of the remote SCP server.

#### For example:

Gxxx-001(super)# copyedge scp announcement-file c:\temp\announcement\_file2.wav
192.168.49.10

## Erasing an announcement file from the directory

#### **Procedure**

Erase an announcement file from the Branch Gateway announcement directory, using the erase announcement-file command.

Specify the name of the file.

#### For example:

Gxxx-001# erase announcement-file local announcement1.wav

## Renaming an announcement file in the directory

### **Procedure**

Rename an announcement file in the Branch Gateway announcement directory, using the **rename announcement-file** command.

Specify the current name of the file followed by the new name.

#### For example:

Gxxx-001# rename announcement-file from\_local\_announcement1.wav
to local announcement1.wav

# Displaying the announcement files stored in the directory Procedure

Display the announcements files stored in the Branch Gateway announcement directory, using the show announcements-files command.

Optionally add the keyword brief to display less detail.

#### For example:

## Displaying the status of a download process

#### **Procedure**

Display the status of a download process of announcement files, using the **show download** announcement-file status command.

#### For example:

## Displaying the status of an upload process

#### **Procedure**

Display the status of an upload process of announcement files, using the **show upload** announcement-file status command.

## For example:

Gxxx-001(super) # show upload announcement-file status

Module #9

Module : 9
Source file : hellosource.wav

Destination file : d:\hellodestination.wav

Host : 135.64.102.64
Running state : Idle
Failure display : (null)
Last warning : No-warning

## Summary of announcement files commands

For more information about these commands, see Avaya Branch Gateway G450 CLI Reference.

Command	Description
copy announcement-file ftp	Upload an announcement file to a remote FTP server
copy announcement-file scp	Upload an announcement file to a remote SCP server
copy announcement-file usb	Upload an announcement file to a USB mass storage device
copy ftp announcement-file	Download an announcement file from an FTP server to Branch Gateway announcement directory
copy scp announcement-file	Download an announcement file from a remote SCP server to Branch Gateway announcement directory
copy usb announcement-file	Download an announcement file from a USB mass storage device to Branch Gateway announcement directory
copy https announcement-file	Download an announcement file from a remote HTTP or HTTPS server to Branch Gateway announcement directory
copyedge scp announcement-file	Download an announcement file from a remote SCP server via Avaya SBCE tunnel to Branch Gateway announcement directory
erase announcement-file	Erase an announcement file from Branch Gateway announcement directory
rename announcement-file	Rename an announcement file in Branch Gateway announcement directory
show announcements files	Display the announcements files stored in Branch Gateway announcement directory
show download announcement-file status	Display the status of a download process of announcement files from the remote SCP server
show upload announcement-file status	Display the status of an upload process of announcement files to the remote SCP server

## **Dynamic time slots allocation**

Branch Gateway dynamically allocates announcement time slots for announcement ports on an as-needed basis. This flexibility provides greater assurance of having time slots available for voice calls. However, Branch Gateway can also potentially run out of time slots for voice calls. To protect Branch Gateway from running out of time slots, use the set fault-threshold timeslot command, which determines at what level of time slots occupancy an SNMP trap is sent to the CM. If you see that Branch Gateway is often at 100% time slot capacity, you may need to add another Branch Gateway to your system.

## Summary of dynamic time slots allocation commands

For more information about these commands, see Avaya Branch Gateway G450 CLI Reference.

Command	Description
	Set time slot occupancy notification, by specifying the occupancy rate at which an SNMP trap is generated
show fault-thresholds timeslot	Display time slot occupancy

## Chapter 18: Advanced switching

You can configure advanced switching on the switch ports of the Branch Gateway. The switch ports consist of the ETH LAN ports located on the front panel.

## **VLAN** configuration

A VLAN is made up of a group of devices on one or more LANs that are configured so the devices operate as if they form an independent LAN. These devices can, in fact, be located on several different LAN segments. VLANs can be used to group together departments and other logical groups, thereby reducing network traffic flow and increasing security within the VLAN.

## **VLAN Tagging**

VLAN Tagging is a method of controlling the distribution of information on the network. The ports on devices supporting VLAN Tagging are configured with the Port VLAN ID and Tagging Mode parameters.

The Port VLAN ID is the number of the VLAN to which the port is assigned.

## Note:

You need to create a VLAN with the set vlan command before you can assign it to a port. You can also create a VLAN by using the interface vlan command, followed by the number of the VLAN (in other words., enter interface vlan 2 to create VLAN 2).

Untagged frames and frames tagged with VLAN 0 entering the port are assigned the port's VLAN ID. Tagged frames are unaffected by the port's VLAN ID.

The Tagging Mode determines the behavior of the port that processes outgoing frames:

- If Tagging Mode is set to clear, the port transmits frames that belong to the port's VLAN table. These frames leave the device untagged.
- If Tagging Mode is set to IEEE-802.1Q, all frames keep their tags when they leave the
  device. Frames that enter the switch without a VLAN tag are tagged with the VLAN ID of the
  port through which they entered.

## Multi VLAN binding

Multi VLAN binding, also known as Multiple VLANs per port, allows access to shared resources by stations that belong to different VLANs through the same port. This is useful in applications such as multi-tenant networks, where each user has a personal VLAN for privacy. The whole building has a shared high-speed connection to the ISP.

In order to accomplish this, Branch Gateway enables multiple VLANs per port. The available Port Multi-VLAN binding modes are:

**Bound to Configured:** The port supports all the VLANs configured in the switch

Statically Bound: The port supports VLANs manually configured on the port

The following figure shows these binding modes.



## Bind to Configured

- The VLAN table of the port supports all the Static VLAN entries and all the ports' VLAN IDs (PVIDs) present in the switch
- VLANs 1, 3, 5, 9, 10 coming from the bus are allowed access through this port
- All the ports in Bound to Configured mode support the same list of VLANs

#### Static Binding

- The user manually specifies the list of VLAN IDs to be bound to the port, up to 64 VLANs
- · Default mode for all ports
- Only VLAN 9, and any other VLANs statically configured on the port will be allowed to access this port

## Gateway VLAN table

The Branch Gateway VLAN table lists all VLANs configured on the Branch Gateway. You can configure up to 64 VLANs. To display a list of VLANs, use the **show vlan** command.

When the VLAN table reaches its maximum capacity, you cannot configure any more VLANs. If this occurs, use the clear vlan command, followed by the name or number of the VLAN you

want to delete, to free space in the VLAN table. Any new VLANs configured by you are made known to all the modules in the system.

## **Ingress VLAN Security**

Ingress VLAN Security enables easy implementation of security, and is always active. A port that is assigned to a VLAN allows packets tagged for that VLAN only to enter through that port. Unassigned packets receive the PVID of the port and are therefore allowed to enter.

## **ICC-VLAN**

When the Branch Gateway includes an ICC, the ICC connects to the Branch Gateway through an internal switch. By default, the ICC is connected on Vlan 1. The VLAN to which the ICC connects is called the ICC-VLAN.

You can use the icc-vlan command to attach the ICC to a different VLAN. Enter the context of the VLAN interface to which you want to attach the ICC switch, and enter icc-vlan.

You can use the **show icc-vlan** command from the general context to show the current ICC-VLAN.

## **Configuring ICC-VLAN**

#### About this task

You must enter the VLAN interface context to configure the ICC VLAN.

#### **Procedure**

- 1. Enter the VLAN interface context by using the interface vlan CLI command
- 2. Enter icc-vlan.

#### **Example**

The following example sets Vlan 2 as the ICC-VLAN:

```
Gxxx-001(super)# interface vlan 2
Gxxx-001(super-if:Vlan 2)# icc-vlan
Done!
Gxxx-001(super-if:Vlan 2)# exit
Gxxx-001(super)# show icc-vlan
VLAN 2
Gxxx-001(super)#
```

## VLAN configuration examples

The following example deletes a statically bound VLAN from a port:

```
Gxxx-001(super)# clear port static-vlan 10/3 34
VLAN 34 is unbound from port 10/3
```

The following example deletes a VLAN and its interface:

```
Gxxx-001(super)# clear vlan 34
This command will assign all ports on VLAN 34 to their default in
```

```
the entire management domain - do you want to continue (Y/N)? y All ports on VLAN-id assigned to default VLAN. VLAN 34 was deleted successfully.
```

## The following example sets the current VLAN as the ICC-VLAN:

```
Gxxx-001(super)# interface Vlan 66
Gxxx-001(super-if:Vlan 66)# icc-vlan
Done!
```

### The following example enters configuration mode for a VLAN interface:

```
Gxxx-001(super) # interface Vlan 66
Gxxx-001(super-if:Vlan 66) #
```

### The following example deletes a VLAN interface:

```
Gxxx-001(super) # no interface vlan 66
Done!
```

### The following example statically binds a VLAN to a port:

```
Gxxx-001(super)# set port vlan-binding-mode 10/3 static
Set Port vlan binding method:10/3
```

## The following example sets a port's VLAN ID:

```
Gxxx-001(super) # set port vlan 54 10/3
Port 10/3 added to VLAN 54
```

#### The following example sets a port's VLAN binding mode:

```
Gxxx-001(super)# set port vlan-binding-mode 10/3 bind-to-configured
Set Port vlan binding method:10/3
```

## The following example configures the VLAN tagging mode of a port:

```
Gxxx-001(super)# set trunk 10/3 dot1q
Dot1Q VLAN tagging set on port 10/3.
```

#### The following example creates a VLAN:

```
Gxxx-001(super)# set vlan 2121 name Training VLAN id 2121, vlan-name Training created.
```

## The following example displays a list of the MAC addresses in the CAM of a VLAN:

```
Gxxx-001(super) # show cam vlan 54

Total Matching CAM Entries Displayed = 3

Dest MAC/Route Dest VLAN Destination Ports
------
00:01:02:dd:2f:9f 54 6/13

00:02:2d:47:00:6f 54 10/3

00:02:4b:5b:28:40 54 6/13
```

#### The following example displays the ICC-VLAN:

```
Gxxx-001(super) # show icc-vlan
VLAN 1
```

## The following example displays interface configuration and statistics for a VLAN:

```
Gxxx-001(super) # show interfaces Vlan 1
VLAN 1 is up, line protocol is up
Physical address is 00.04.0d.29.c6.bd.
MTU 1500 bytes. Bandwidth 100000 kbit.
Reliability 255/255 txLoad 1/255 rxLoad 1/255
```

```
Encapsulation ARPA, ICC-VLAN
Link status trap disabled
Full-duplex, 100Mb/s
ARP type: ARPA, ARP Timeout 04:00:00
Last input never, Last output never
Last clearing of 'show interface' counters never.
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
0 input drops, 0 output drops, 0 unknown protocols
0 packets input, 0 bytes
0 broadcasts received, 0 giants
0 input errors, 0 CRC
0 packets output, 0 bytes
0 output errors, 0 collisions
```

### The following example displays port VLAN binding information:

```
Gxxx-001(super) # show port vlan-binding-mode 10 port 10/3 is bind to all configured VLANs
```

### The following example displays VLAN tagging information:

## The following example displays the VLANs configured on the device:

```
Gxxx-001(super) # show vlan
VLAN ID VLAN-name
------
1    V1
54    Marketing
66    V66
2121    Training
Total number of VLANs: 4
```

## **Summary of VLAN commands**

For more information about these commands, see Avaya Branch Gateway G450 CLI Reference.

Root level command	First level Command	Description
clear port static- vlan	-	Delete statically configured VLANs from the port
clear vlan	-	Delete an existing VLAN and its interface, remove the entry from the VLAN table, and return ports from this VLAN to the default VLAN 1
interface vlan	-	Create a VLAN interface, enter interface VLAN configuration mode, or delete a VLAN interface
-	icc-vlan	Set the current VLAN as the ICC-VLAN
set port static-vlan	-	Assign a static VLAN to a port
set port vlan	-	Set the port VLAN ID (PVID)
set port vlan-binding-mode	-	Define the binding method used by ports

Table continues...

Root level command	First level Command	Description
set trunk	- Configure the VLAN tagging mode of a port	
set vlan	-	Create or modify a VLAN
show cam vlan	-	Display all MAC entries in the CAM table for a specific VLAN
show icc-vlan	-	Display the current ICC VLAN
show interfaces	-	Display interface configuration and statistics for a particular interface or all interfaces
show port vlan-binding- mode	-	Display port VLAN binding mode information
show trunk	-	Display VLAN tagging information for all or some ports
show vlan	-	Display the VLANs configured in the Branch Gateway

## Port redundancy

Redundancy involves the duplication of devices, services, or connections, so that in the event of a failure, the redundant duplicate can take over for the one that failed.

Since computer networks are critical for business operations, it is vital to ensure that the network continues to function even if a piece of equipment fails. Even the most reliable equipment might fail on occasion, but a redundant component can ensure that the network continues to operate despite such failure.

To achieve port redundancy, you can define a redundancy relationship between any two ports in a switch. One port is defined as the primary port and the other as the secondary port. If the primary port fails, the secondary port takes over.

#### Note:

When port redundancy is activated on Branch Gateway, manually disabling the primary port will also disable the secondary port. To prevent the disabling of the secondary port, you must disable port redundancy before disabling the primary port.

## Secondary port activation

The secondary port takes over within one second and is activated when the primary port link stops functioning. Subsequent switchovers take place after the minimum time between switchovers has elapsed. To set the minimum time between switchovers, use the set port redundancyintervals command.

## **Switchback**

If switchback is enabled and the primary port recovers, a switchback takes place. Use the set port redundancy-intervals command to set the following switchback parameters:

- min-time-between-switchovers. The minimum time that is allowed to elapse before a primary-backup switchover.
- switchback-interval. The minimum time the primary port link has to be up before a switchback to the primary port takes place. If you set this to none, there is no switchback to the primary port when it recovers. In this case, switchback to the primary port only takes place if the secondary port fails.

## Port redundancy configuration commands

The following commands are used to configure port redundancy. For more information about these commands, see *Avaya Branch Gateway G450 CLI Reference*.

## **Enabling and disabling redundancy pairs**

#### **Procedure**

To globally enable or disable the redundancy pairs you have defined, use the set port redundancy enable/disable command.

This command does not delete existing redundancy entries.

## Defining or removing redundancy pairs

- 1. To define or remove redundancy pairs, see the set port redundancy command.
- 2. To ensure that there is no redundancy scheme already defined on any of the links, enter show port redundancy.

## **Configuring time constants**

#### **Procedure**

To configure the two time constants that determine redundancy switchover parameters, use the set port redundancy-intervals command.

## Displaying port redundancy schemes

#### **Procedure**

To display information about software port redundancy schemes defined for the switch, enter **show port redundancy**.

## Port redundancy configuration examples

The following example creates a port redundancy pair:

```
G450-001(super)# set port redundancy 10/5 10/6 on 1
Monitor: Port 10/6 is redundant to port 10/5.
Port redundancy is active - entry is effective immediately
```

### The following example deletes a port redundancy pair:

```
G450-001 (super)# set port redundancy 10/5 10/6 off Entry Monitor removed: Port 10/6 is not redundant to port 10/5
```

## The following example enables all configured port redundancies:

```
Gxxx-001(super) # set port redundancy enable
All redundancy schemes are now enabled
```

## The following example disables all configured port redundancies:

```
Gxxx-001(super)# set port redundancy disable
All redundancy schemes are disabled but not removed
```

## The following example configures the switchback interval for all configured port redundancies:

```
Gxxx-001(super) # set port redundancy-intervals 60 30 Done!
```

### The following example displays port redundancy information:

## **Summary of port redundancy commands**

For more information about these commands, see Avaya Branch Gateway G450 CLI Reference.

Command	Description
set port redundancy	Define or remove redundancy pairs
set port redundancy enable  disable	Globally enable or disable port redundancy pairs defined on the Branch Gateway
set port redundancy-intervals	Configure the two time constants that determine redundancy switchover parameters
show port redundancy	Display information about software port redundancy pairs defined on the Branch Gateway

## **Port mirroring**

Port mirroring copies all received and transmitted packets (including local traffic) from a source port to a predefined destination port, in addition to the normal destination port of the packets. Port mirroring, also known as "sniffing," is useful in debugging network problems.

Port mirroring allows you to define a source port and a destination port, regardless of port type. For example, a 10 Mbps and a 100 Mbps port can form a valid source/destination pair. You

cannot, however, define the port mirroring source and destination ports as the same source and destination ports.

You can define one source port and one destination port on each Branch Gateway for received (Rx), transmitted (Tx), or transmitted and received (both) traffic.

## Port mirroring configuration examples

The following example creates a port mirroring pair in the Branch Gateway:

```
G450-001(super) # set port mirror source-port 10/5 mirror-port 10/6 sampling always direction rx Mirroring rx packets from port 10/5 to port 10/6 is enabled
```

The following example displays port mirroring information for the Branch Gateway:

```
G450-001(super)# show port mirror port mirroring
Mirroring both Rx and Tx packets from port 10/5 to port 10/6 is enabled
```

The following example disables port mirroring:

```
Gxxx-001(super) # clear port mirror
```

## Summary of port mirroring commands

For more information about these commands, see Avaya Branch Gateway G450 CLI Reference.

Command	Description
clear port mirror	Delete a port mirroring pair
set port mirror	Define a port mirroring source-destination pair
show port mirror	Display mirroring information for a specified port or for all ports

<sup>•</sup> auto. Attempts to automatically detect the port's connection type.

## **Spanning tree**

Branch Gateways support the enhanced Rapid Spanning Tree Protocol (802.1w). The 802.1w standard is a faster and more sophisticated version of the 802.1d (STP) standard, and includes backward compatibility with 802.1d. Spanning tree makes it possible to recover connectivity after an outage within approximately a minute. RSTP, with its "rapid" algorithm, can usually restore connectivity to a network where a backbone link has failed in much less time.

## Spanning tree protocol

The spanning tree algorithm ensures the existence of a loop-free topology in networks that contain parallel bridges. A loop occurs when there are alternate routes between hosts. If there is a loop in an extended network, bridges may forward traffic indefinitely, which can result in increased traffic and degradation in network performance.

The spanning tree algorithm produces a logical tree topology out of any arrangement of bridges. The result is a single path between any two end stations on an extended network. In addition, the spanning tree algorithm provides a high degree of fault tolerance. It allows the network to automatically reconfigure the spanning tree topology if there is a bridge or data-path failure.

The spanning tree algorithm requires five values to derive the spanning tree topology. These are:

- A multicast address specifying all bridges on the extended network. This address is mediadependent and is automatically determined by the software.
- A network-unique identifier for each bridge on the extended network
- A unique identifier for each bridge/LAN interface (a port)
- The relative priority of each port
- The cost of each port

After these values are assigned, bridges multicast and process the formatted frames (called Bridge Protocol Data Units, or BPDUs) to derive a single, loop-free topology throughout the extended network. The bridges exchange BPDU frames quickly, minimizing the time that service is unavailable between hosts.

## Spanning tree per port

Spanning tree can take up to 30 seconds to open traffic on a port. This delay can cause problems on ports carrying time-sensitive traffic. You can, therefore, enable or disable spanning tree in the Branch Gateway on a per-port basis to minimize this effect.

## Rapid Spanning Tree Protocol (RSTP)

The enhanced feature set of the 802.1w standard includes:

- Bridge Protocol Data Unit (BPDU) type 2
- New port roles: Alternate port, Backup port
- Direct handshaking between adjacent bridges regarding a desired topology change (TC). This eliminates the need to wait for the timer to expire.
- Improvement in the time it takes to propagate TC information. Specifically, TC information does not have to be propagated all the way back to the Root Bridge (and back) to be changed.
- Origination of BPDUs on a port-by-port basis

## Port roles

At the center of RSTP – specifically as an improvement over STP (802.1d) – are the roles that are assigned to the ports. There are four port roles:

**Root port:** The port closest to the root bridge

**Designated port:** The corresponding port on the remote bridge of the local root port

**Alternate port:** An alternate route to the root

**Backup port:** An alternate route to the network segment

The RSTP algorithm usually makes it possible to change port roles rapidly through its fast topology change propagation mechanism. For example, a port in the blocking state can be assigned the role of alternate port. When the backbone of the network fails, the port can rapidly be changed to forwarding.

Whereas the STA *passively* waited for the network to converge before turning a port into the forwarding state, RSTP *actively* confirms that a port can safely transition to forwarding without relying on any specific, programmed timer configuration.

## **RSTP** port types

RSTP provides a means of fast network convergence after a topology change. It does this by assigning different treatments to different port types.

**Edge ports:** Setting a port to edge-port admin state indicates that this port is connected directly to end stations that cannot create bridging loops in the network. These ports transition quickly to forwarding state. However, if BPDUs are received on an edge port, its operational state will be changed to non-edge-port and bridging loops will be avoided by the RSTP algorithm. The default admin state of 10/100 M ports is edge-port.

Enter set port edge admin state, followed by the module and port number – or a range of port numbers – to specify whether or not a port is considered an edge port.

The following command specifies that port 10/5 is not an edge port:

```
Gxxx-001(super) # set port edge admin state 10/5 non-edge-port
```

Enter show port edge state, followed by the module and port number, to display the edge state of the specified port. Use this command without specifying a module number or port to display the edge state of all ports.

**Non-edge ports:** You must manually configure uplink and backbone ports to be non-edge ports, using the set port edge admin state command.

**Point-to-point link ports:** This port type applies only to ports interconnecting RSTP compliant switches and is used to define whether the devices are interconnected using shared Ethernet segment or point-to-point Ethernet link. RSTP convergence may be faster when switches are connected using point-to-point links. The default setting for all ports – automatic detection of point-to-point link – is sufficient for most networks.

Enter set port point-to-point admin status, followed by the module and port number or a range of port numbers, and an admin status parameter, to specify the port's connection type. Admin status parameter values are:

- · force-true. Treats the port as if it is connected point-to-point
- force-false. Treats the port as if it is connected to shared media
- auto. Attempts to automatically detect the port's connection type

For example, the following command specifies that ports 10/5 and 10/6 are treated as if they were connected point-to-point:

Gxxx-001(super)# set port point-to-point admin status 10/5-6 force-true

**All ports:** Enter **show port point-to-point status**, followed by the module and port number, to display the point-to-point status of the specified point-to-point status of all ports

## Spanning tree configuration examples

The following example enables spanning tree on a port:

```
Gxxx-001(super) # set port spantree enable 10/5 port 10/5 was enabled on spantree
```

The following example disables spanning tree on a port:

```
Gxxx-001(super) # set port spantree disable 10/5 port 10/5 was disabled on spantree
```

The following example sets the spanning tree cost of port 10/5 to 4096:

```
Gxxx-001(super) # set port spantree cost 10/5 4096 port 10/5 spantree cost is 4096
```

The following example configures the version of the spanning tree default path cost used by this bridge:

```
Gxxx-001(super) # set spantree default-path-cost common-spanning-tree Spanning tree default path costs is set to common spanning tree.
```

The following example configures the time used when transferring the port to the forwarding state:

```
Gxxx-001(super)# set spantree forward-delay 16 bridge forward delay is set to 16.
```

The following example configures the time interval between the generation of configuration BPDUs by the root:

```
Gxxx-001(super)# set spantree hello-time 2
bridge hello time is set to 2.
```

The following example configures the amount of time an information message is kept before being discarded:

```
Gxxx-001(super) # set spantree max-age 21 bridge max age is set to 21.
```

The following example configures the bridge priority for spanning tree:

```
Gxxx-001(super)# set spantree priority 36864
Bridge priority set to 36864.
```

The following example sets the value in packets used by spanning tree in order to limit the maximum number of BPDUs transmitted during a hello-time period:

```
Gxxx-001(super)# set spantree tx-hold-count 4
tx hold count is set to 4.
```

The following example configures the version of spanning tree to use on the device:

```
Gxxx-001(super)# set spantree version rapid-spanning-tree Spanning tree version is set to rapid spanning tree.
```

The following example displays spanning tree information:

```
Spanning tree state is enabled
Designated Root: 00-04-0d-ea-b0-2d
```

## **Summary of spanning tree commands**

For more information about these commands, see Avaya Branch Gateway G450 CLI Reference.

Command	Description		
set port edge admin state	Assign or de-assign RSTP edge-port admin state to a port for Rapid Spanning Tree Protocol (RSTP) treatment		
set port point-to-point admin status	Specify a port's connection type		
set port spantree	Enable or disable spanning tree for specific ports		
set port spantree cost	Set the spanning tree cost of a port		
set port spantree force- protocol-migration	Force the port to send a rapid spanning tree hello packet (Bridge Protocol Data Unit)		
set port spantree priority	Set the spanning tree priority level of a port		
set spantree default-path- cost	Set the version of the spanning tree default path cost used by the current bridge		
set spantree enable disable	Enable or disable the spanning-tree algorithm for Branch Gateway		
set spantree forward-delay	Specify the time used when transferring the state of a port to the forwarding state		
set spantree hello-time	Specify the time interval between the generation of configuration BPDUs by the root		
set spantree max-age	Specify the time to keep an information message before it is discarded		
set spantree priority	Set the bridge priority for the spanning tree		
set spantree tx-hold-count	Set the value in packets used by the spanning tree in order to limit the maximum number of BPDUs transmitted during a hello-time period		
set spantree version	Set the version of the spanning tree protocol used by the device		
show port edge state	Display the edge state of a specified port		

Table continues...

Command	Description
show port point-to-point status	Display the point-to-point status of a specific port or all ports
show spantree	Display spanning-tree information

## Port classification

With the Branch Gateway, you can classify any port as either regular or valuable. Classifying a port as valuable means that a link fault trap is sent in the event of a link failure. The trap is sent even when the port is disabled. This feature is particularly useful for the port redundancy application, where you need to be informed about a link failure on the dormant port.



The 1 GB ports are classified as valuable by default.

## Port classification configuration examples

The following example classifies a port as a valuable port:

```
Gxxx-001(super) # set port classification 10/5 valuable
Port 10/5 classification has been changed.
```

The following example displays the port classification of all ports:

```
G450-001(super) # show port classification
Port Port Classification
10/5 valuable 10/6 regular
          valuable
```

## Summary of port classification commands

For more information about these commands, see Avaya Branch Gateway G450 CLI Reference.

Command	Description		
set port classification	Set the port classification to either regular or valuable (any change in the spanning tree state from forwarding for a valuable port will erase all learned MAC addresses in the switch)		
show port classification	Display port classification for a specified port or all ports		

## **Chapter 19: Monitoring applications**

The Branch Gateway provides several software tools for monitoring and diagnosing your network. Use these tools to monitor the status of your network operations, and to analyze the flow of information.

## **RMON**

Remote Monitoring (RMON), the internationally recognized network monitoring standard, is a network management protocol that allows network information to be gathered at a single workstation. You can use RMON probes to monitor and analyze a single segment only. When you deploy a switch on the network, there are additional components in the network that cannot be monitored using RMON. These components include the switch fabric, VLAN, and statistics for all ports.

RMON is the internationally recognized and approved standard for detailed analysis of shared Ethernet media. It ensures consistency in the monitoring and display of statistics between different vendors.

RMON's advanced remote networking capabilities provide the tools needed to monitor and analyze the behavior of segments on a network. In conjunction with an RMON agent, RMON gathers details and logical information about network status, performance, and users running applications on the network.

An RMON agent is a probe that collects information about segments, hosts, and traffic, and sends the information to a management station. You use specific software tools to view the information collected by the RMON agent on the management station.

You can configure RMON for switching on the Branch Gateway. The Branch Gateway uses RMON I, which analyzes the MAC layer (Layer 2 in the OSI seven-layer model). You can also configure a port to raise an SNMP trap whenever the port fails.

## **RMON** configuration examples

The following example creates an RMON alarm entry:

Gxxx-001(super)# rmon alarm 1 1.3.6.1.2.1.16.1.1.1.5.16777216 20 delta rising-threshold 10000 32 falling-threshold 1000 32 risingOrFalling root alarm 1 was created successfully

### The following example creates an RMON event entry:

```
Gxxx-001(super)# rmon event 32 log description "Change of device"
  owner root
  event 32 was created successfully
```

The following example creates an RMON history entry with an index of 80 on port 10/3, recording activity over 60 intervals (buckets) of 20 seconds each.

```
Gxxx-001(super)# rmon history 80 10/3 interval 20 buckets 60 owner root history index 80 was created successfully
```

#### The following example displays information about an RMON alarm entry:

```
Gxxx-001(super) # show rmon alarm 1
alarm
alarm 1 is active, owned by root
Monitors ifEntry.1.16777216 every 20 seconds
Taking delta samples, last value was 0
Rising threshold is 10000, assigned to event # 32
Falling threshold is 1000, assigned to event # 32
On startup enable rising or_falling alarms
```

## The following example displays information about an RMON event entry:

```
Gxxx-001(super) # show rmon event 32
event
Event 32 is active, owned by root
Description is Change of device
Event firing causes log, last fired 12:36:04
```

### The following example displays information about an RMON history entry:

```
Gxxx-001(super) # show rmon history 80
history
Entry 80 is active, owned by root
Monitors the port 10/3 every 20 seconds
Requested # of time intervals, ie buckets, is 60
Granted # of time intervals, ie buckets, is 60
Sample # 2 began measuring at 0:21:16
Received 4081 octets, 41 packets,
0 broadcast and 10 multicast packets,
0 undersize and 0 oversize packets,
0 fragments and 0 jabbers,
0 CRC alignment errors and 0 collisions,
# of dropped packet events (due to a lack of resources): 0
Network utilization is estimated at 0
```

#### The following example displays RMON statistics for a port:

```
Gxxx-001(super) # show rmon statistics 10/3
Statistics for port 10/3 is active, owned by Monitor
Received 6952909 octets, 78136 packets,
26 broadcast and 257 multicast packets,
0 undersize and 0 oversize packets,
0 fragments and 0 jabbers,
0 CRC alignment errors and 0 collisions,
# of dropped packet events (due to a lack of resources): 0
# of packets received of length (in octets):
64:18965, 65-127:295657, 128-255:4033,
256-511:137, 512-1023:156, 1024-1518:0,
```

## **Summary of RMON commands**

For more information about these commands, see Avaya Branch Gateway G450 CLI Reference.

Command	Description		
clear rmon statistics	Clear RMON statistics		
rmon alarm	Create or delete an RMON alarm entry		
rmon event	Create or delete an RMON event entry		
rmon history	Create or delete an RMON history entry		
show rmon alarm	Display information about a specific RMON alarm entry or all existing RMON alarm entries		
show rmon event	Display a specific RMON event entry or all RMON event entries		
show rmon history	Display a specific RMON history entry or all RMON history entries		
show rmon statistics	Display RMON statistics for a specific interface or for all interfaces		

## **RTP statistics**

The RTP statistics application collects data and statistics for RTP sessions (streams) from Branch Gateway VoIP engine. You can view the data and configure SNMP traps to be generated when the QoS level falls below a configured level. RTP statistics support IPv4 and IPv6 addresses.

Insert content for the first section.



#### Note:

An alternative tool available from Avaya for debugging QoS problems is VMON. VMON is an RTCP QoS reports collector, VMON support, available in all Avava devices, is the capability of a VoIP device to send a copy of an RTCP message to the IP address of a VMON server. VMON can collect RTCP reports, store them on its host hard disk, and analyze and generate graphic reports. However, VMON requires a dedicated Windows server. The RTP statistics, application runs on Branch Gateway firmware, and does not require any dedicated hardware. For information about configuring VMON in CM, see Administrator Guide for Avaya Aura® Communication Manager.

Branch Gateway performs traceroutes whenever RTP statistics is enabled.

The RTP statistics application provides the following functionality:

1. Collects QoS data from Branch Gateway VoIP engines, including Real-Time Control Protocol (RTCP) data, traceroute reports, and information from the DSP regarding jitter buffer, internal delays, and so on.



## ■ Note:

RTCP is a standard QoS report companion protocol to RTP. RTP endpoints periodically send RTCP report packets to their remote peer (or peers in multicast). RTCP reports include QoS data such as delay, jitter, and loss.

- 2. Collects call data from Branch Gateway, such as duration, start-time, and end-time.
- 3. Displays the RTP statistics in CLI and MIB formats.

- 4. Displays summary reports for the VoIP engines.
- 5. Assesses QoS status based on configurable thresholds on an extensive set of QoS metrics.
- 6. Generates QoS traps.

QoS traps are notifications sent via SNMP upon termination of an RTP stream that suffers from bad QoS. These notifications include extensive data about the session that enables offline troubleshooting of QoS problems. The trap rate is controlled by a configurable trap rate limiter.

## ■ Note:

QoS trap generation is an especially convenient troubleshooting tool for large installations, since all devices that support the RTP statistics application can be configured to send traps to a single SNMP trap manager.

7. Generates QoS fault and clear traps.

QoS fault traps are notifications that are sent when more than a configurable number of active sessions have QoS indicators over the configured thresholds. A QoS clear trap is a notification that is sent after a QoS fault trap when the number of active RTP sessions with QoS indicators over the configured thresholds reduces to a specified number.

## Configuring the RTP statistics application

#### About this task

To configure the RTP statistics application, work through a set of procedures.

#### **Procedure**

- 1. View RTP statistics thresholds.
- 2. Set up RTP statistics thresholds on page 325.
- 3. Set up the RTP statistics application on page 326.
- 4. View the application configuration on page 326.
- 5. Set up QoS traps on page 328.
- 6. Set up QoS fault and clear traps on page 329.
- 7. Set up the trap rate limiter on page 330.

## Viewing RTP statistics thresholds

The RTP statistics application uses a system of thresholds to evaluate levels of QoS during RTP sessions. The thresholds are configured on several QoS metrics. Your configuration of the thresholds determines when the application evaluates a session as having bad QoS conditions.

This section describes the thresholds that you can configure, how you can view the thresholds that are currently configured, and the metrics on which you can configure them.

The RTP statistics application samples the VoIP engine every RTCP interval, which is configured in CM, where it is called "RTCP Report Period". The RTCP interval is typically 5 to 8 seconds. For information about configuring the RTCP interval (RTCP report period), see *Administrator Guide for Avaya Aura*<sup>®</sup> *Communication Manager*.

## Thresholds types

### About this task

**A threshold on a metric:** For example, you can configure a threshold on the metric 'packet loss'. The application samples the metric every RTP interval and increments a counter (event counter) if the sampled value is over the threshold. Hence, the 'event-counter' represents the number of times the metric was sampled over its threshold.

An event threshold: An event threshold is a threshold on an event counter. If QoS traps are configured, the application generates a QoS trap when, at the end of a session, one or more event counters are over their event thresholds. For example, if the event threshold for packet loss is 2, the application generates a QoS trap if packet loss is sampled over its threshold two or more times.

**Thresholds on metric averages:** The application calculates averages of some of the metrics. When an RTP session terminates, the application evaluates the average metrics and generates a QoS trap (if QoS traps are configured) if one of them is over its corresponding threshold.



All CLI commands described in this section are available in the general context of the CLI.

## Viewing the configured thresholds

1. Enter show rtp-stat thresholds. For example:

<pre>Gxxx-001(super)# show Item</pre>	-	holds Event Threshold
Codec Loss	6.0%	1
Average Codec Loss	3.0%	N/A
Codec RTT	700mS	2
Echo Return Loss	0dB	1
Loss	6.0%	2
Average Loss	3.0%	N/A
Remote Loss	6.0%	2
Average Remote Loss	3.0%	N/A
RTT	500mS	2
Local Jitter	50mS	2
Remote Jitter	50mS	2
SSRC Changes	N/A	2

#### **QoS** metrics

The following table describes the QoS metrics on which thresholds are configured, and the time when each metric is evaluated.

Metric	Description	Evaluation time
Codec Loss	The percentage of time the codec plays fill frames due to lack of valid RTP frames. Possible causes include jitter and packet loss.	Every RTCP interval
Average Codec Loss	The average codec loss measurement since the beginning of the RTP stream	At the end of the session

Table continues...

Metric	Description	Evaluation time
Codec RTT	An estimation of the overall Round Trip Time (RTT) on the voice-channel, including the network delay and internal delays.	Each time an RTCP packet is received
	RTT is the time taken for a message to get to the remote peer and back to the local receiver.	
Echo Return Loss	The echo cancellation loss on the TDM bus	Every RTCP interval
Loss	The estimated network RTP packet loss.	Every RTCP interval
	The VoIP engine evaluates the current received packet loss every RTCP interval – usually 5 to 8 seconds. The VoIP engine postpones loss estimation until the next interval if the number of packets received is less than the minimum statistic window. The minimum statistic window is configured with the CLI command rtp-stat min-stat-win.	
Average Loss	The average packet loss evaluation since the beginning of the RTP stream	At the end of the session
Remote Loss	The network loss according to the remote RTP receiver. The device learns of the remote packet loss from received RTCP messages.	Each time an RTCP packet is received
Average Remote Loss	The average remote network loss measurement since the beginning of the RTP stream	At the end of the session
RTT	The network RTT. This metric does not include internal delay. The device learns of the RTT from RTCP messages.	Each time an RTCP packet is received
Local Jitter	Variation in delay of packet delivery to the local peer	Every RTCP interval
Remote Jitter	Variation in delay of packet delivery to the remote peer. The device learns of the remote jitter from RTCP messages.	Each time an RTCP packet is received
SSRC Changes	The number of times the RTP SSRC field in received RTP packets has changed	Every RTCP interval

# **Configuring RTP statistics thresholds**

### About this task

Configure RTP statistics thresholds so that incrementation of QoS event counters coincides with real detectable bad QoS in your network. Optimal values are different for each network.

The Codec metrics, Codec loss and Codec RTT are useful for evaluating the actual user experience. The other metrics are useful for identifying network problems that contribute to QoS problems experienced by the user.

### **Procedure**

1. Run the rtp-stat thresholds command to set thresholds on QoS indicators.

#### For example:

```
Gxxx-001(super) # rtp-stat thresholds echo-return-loss 5
```

With this example configuration, if echo-return-loss is sampled higher than 5 dB during an RTP session, the echo-return-loss event counter increments.

2. Run the rtp-stat event-threshold command to set thresholds on QoS events.

#### For example:

```
Gxxx-001(super) # rtp-stat event-threshold echo-return-loss 2
Done!
```

With this example configuration, if echo-return-loss is sampled over its threshold more than twice during an RTP session, the application considers the session to have QoS faults.

#### Related links

Viewing RTP statistics thresholds on page 323

# Setting up the RTP statistics application

#### About this task

When you enable the RTP statistics application on Branch Gateway, the application starts to collect QoS data from the VoIP engines and stores the data in Branch Gateway RAM, which holds a limited history of RTP session entries. The VoIP engine also starts to perform and report UDP traceroutes.

You can view session data and automatic session traceroute results using the CLI.

#### Procedure

1. To enable the RTP statistics application, type rtp-stat-service.



# Note:

Admin level access is required in order to use the rtp-stat-service command.

#### For example:

```
Gxxx-001# rtp-stat-service
The RTP statistics service is enabled (default: disabled)
```

2. To reset the RTP statistics application, type rtp-stat clear.

All counters are reset and the RTP statistics history is erased.

# Viewing application configuration

### About this task

View the application configuration to see if the application is enabled, which types of traps are enabled, and how the trap rate limiter and minimum statistics window are configured. The minimum statistics window is the minimum number of observed RTP sequence increments for which the application evaluates packet loss.

### **Procedure**

### Type show rtp-stat config.

```
Gxxx-001(super) # show rtp-stat config
RTP Statistic: Enabled
QoS Trap: Enabled
QoS Fault Trap: Enabled
    Fault: 2
    Clear: 0
QoS Trap Rate Limiter:
    Token Interval: 10.00 seconds
    Bucket Size: 5
Session Table:
    Size: 128
    Reserved: 64
Min Stat Win: 50
```

# RTP statistics application outputs

The following table describes the output of the show rtp-stat config command.

Name	Description
RTP Statistic	Status of the RTP statistics application. Possible values:
	Enabled. The application is enabled.
	Disabled. The application is disabled.
QoS Trap	QoS trap status. Possible values:
	Enabled. The RTP statistics application is configured to generate QoS traps.
	Disabled. The RTP statistics application is not configured to generate QoS traps.
QoS Fault Trap	QoS fault trap status. Possible values:
	Enabled. The RTP statistics application is configured to generate QoS fault and clear traps.
	Disabled. The RTP statistics application is not configured to generate QoS fault and clear traps.
Fault	The QoS fault trap boundary. That is, the minimum number of active sessions with QoS faults that triggers a QoS fault trap.
Clear	The QoS clear trap boundary. That is, the reduced number of active sessions with QoS faults that triggers a QoS clear trap to be sent after a QoS fault trap was sent.
QoS Trap Rate Limiter:	
Token Interval	The displayed token interval is in seconds. The maximum long term trap rate, expressed as an interval in seconds. In the example shown, the maximum long term trap rate is one trap every 10 seconds.
Bucket Size	The maximum number of tokens stored in the token bucket of the trap rate limiter. This item limits the size of a QoS trap burst.
Session Table:	

Name	Description
Size	The maximum number of RTP session entries held in the session table in the gateway RAM
Reserved	The number of rows in the session table that are reserved for sessions with QoS problems. In the example shown, the table size is 128 and the reserved number is 64. If, from 1000 sessions only 300 had QoS problems, the session table will hold at least the last 64 sessions that had QoS problems. Note that if the last 128 sessions all had QoS problems, all rows in the session table will be filled with sessions that had QoS problems.
Min Stat Win	The minimum statistic window configured for the RTP statistics application. That is, the minimum number of observed RTP sequence increments for which the application evaluates packet loss.

# **Enabling QoS traps**

#### About this task

You can configure the application to automatically generate QoS traps using SNMP at the termination of RTP sessions that have QoS problems. SNMP traps are automatically sent to the SNMP trap manager on the active Media Gateway Controller (MGC). You can also configure SNMP traps to be sent to an external trap manager. The application generates a QoS trap when, at the end of an RTP session, one or more event counters are over their event thresholds.



### Caution:

If the thresholds for trap generation are set too low, a significant amount of trap traffic will be generated and negatively impact network performance.

#### **Procedure**

- View the RTP statistic thresholds and modify their configurations as necessary.
- 2. If you need to modify the minimum statistic window, run the rtp-stat min-stat-win command.

```
Gxxx-001(super) # rtp-stat min-stat-win 50
```

The minimum statistic window is the minimum number of observed RTP sequence increments for which the application evaluates packet loss. The VoIP engine evaluates the current received packet loss every RTCP interval. The VoIP engine postpones loss estimation to the next interval if the number of received packets is less than the minimum statistic window. By modifying the minimum statistic window, you can prevent the application from generating loss-events based on too few packets and safely configure a low packet loss threshold.

3. To configure an additional trap destination, such as an external trap manager, use the command snmp-server host.

```
Gxxx-001(super) # snmp-server host 136.9.71.47 traps v1 public
```

# Note:

When using the snmp-server host command, you can specify only to send certain types of traps to the specified trap manager. For example, snmp-server host 1.1.1.1 traps v1 public rtp-stat-qos rtp-stats-faults configures only QoS traps and QoS fault and clear traps to be sent to host 1.1.1.1.

To check your current SNMP configurations, enter **show snmp**. Traps are automatically sent to the active MGC by the dynamic trap manager feature. To configure the dynamic trap manager, use the command **snmp-server dynamic-trap-manager**.

4. Type rtp-stat gos-trap to enable the traps, if not already enabled.

```
Gxxx-001# rtp-stat qos-trap
The RTP statistics QoS trap is enabled
```

QoS traps are now enabled.

#### Related links

Configuring RTP statistics thresholds on page 325
Viewing RTP statistics thresholds on page 323
Dynamic trap manager on page 288

# QoS fault and clear traps

### About this task

You can configure the RTP statistics application to send QoS fault and clear traps. A QoS fault trap is sent when a specified number of active RTP sessions have QoS indicators over the configured thresholds. A QoS clear trap is sent after a QoS fault trap when the number of active RTP sessions with QoS indicators over the configured thresholds reduces to a specified number. Since some RTP sessions can be very long, and QoS traps are sent only after the termination of the stream, QoS fault and clear traps are important for providing timely information about QoS problems.

# Note:

QoS fault traps appear in the Network Management Console Event Log Browser, indicating to the user that there are QoS problems in a specific network device. See the *Avaya Network Management Console User Guide*.

# Configuring QoS fault and clear traps

### **Procedure**

Use the rtp-stat fault command.

#### For example:

```
Gxxx-001(super)# rtp-stat fault 1 0
The fault trap boundary was set to 1 (default: 3)
The clear trap boundary was set to 0
```

With this example configuration, a QoS fault trap is sent if and when one active RTP session has QoS problems. A QoS clear trap is then sent if and when the number of active RTP sessions with QoS problems reaches 0.

# The trap rate limiter

The application features a trap rate limiter. The trap rate limiter limits the rate at which QoS traps are sent. The rate limiter protects against overloading the trap manager with bursts of traps when a single event causes multiple RTP sessions to terminate simultaneously.

The trap rate limiter uses a token bucket scheme, in which traps are sent only if there are tokens in a virtual bucket. Tokens are added to the bucket every 'token interval,' which sets the maximum long term trap rate. Each time a trap is sent, the number of tokens in the bucket decrements. The 'bucket size' is the maximum number of tokens that the bucket can hold. The bucket size limits the trap burst size.

# Configuring the trap rate limiter

#### **Procedure**

Use the rtp-stat qos-trap-rate-limit command.

For example:

```
Gxxx-001# rtp-stat qos-trap-rate-limit 2000 10
```

In this example configuration, the token-interval is 2000 and the bucket-size is 10. This means that a token is added to the bucket every 2000 hundredths of a second (20 seconds) and the bucket is limited to a maximum size of 10 tokens.

# RTP statistics output

### About this task

This section describes the reports, statistics, and traps you can view, how to view them, and how to understand the output.

# Viewing RTP statistics summary reports

RTP statistics summary reports display QoS trap statistics for the VoIP engine(s).

1. Enter show rtp-stat summary. For example:

# RTP statistics summary reports output

### About this task

The following table describes the fields in the summary report.

Field	Description
Total QoS traps	The total number of QoS traps sent since the RTP statistics application was enabled or since the last use of the rtp-stat clear command
QoS traps Drop	The number of QoS traps dropped by the rate limiter since the RTP statistics application was enabled or since the last use of the rtp-stat clear command
Qos Fault/QoS Clear	General QoS state: QoS Fault means that the number of active RTP sessions with QoS faults is currently higher than the QoS fault boundary. QoS Clear means that the number of active RTP sessions with QoS faults is currently less than or equal to the QoS clear boundary. You can configure the QoS fault and clear boundaries using the rtp-stat fault command. See QoS fault and clear traps on page 329.
Engine ID	The ID of the VoIP engine. Since the Aura Media Gateway has one VoIP engine, one line appears in the table.
Description	Description of the VoIP engine
Uptime	The uptime of the RTP statistics application. This is the time since the RTP statistics application was enabled or since the last use of the rtp-stat clear command.
Active Session	The number of active sessions / number of active sessions with QoS problems
Total Session	The total number of sessions / number of sessions that had QoS problems
Mean Duration	The mean RTP session duration (calculated only for terminated calls)
Tx TTL	The IP Time To Live (TTL) field for transmitted RTP packets

# **Viewing RTP session statistics**

# **About this task**

Using the CLI, you can view a summary of active and terminated sessions and you can view RTP statistics for a given RTP session.

#### **Procedure**

1. Use the **show rtp-stat sessions** command to display a summary of the active and/or terminated RTP sessions in the session table.

### For example:

An asterisk (\*) in the QoS column indicates that the session had QoS problems.

2. Use the **show rtp-stat detailed** command to display detailed information about a specified active or terminated RTP session, including the QoS metrics reported by the RTP statistics application.

### For example:

```
Gxxx-001(super) # show rtp-stat detailed 35
Session-ID: 351
Status: Terminated<sup>2</sup>
, QOS: Faulted<sup>3</sup>
, EngineId: 0<sup>4</sup>
Start-Time: 2015-08-23<sup>5</sup>
,11:09:07<sup>6</sup>
 , End-Time: 2015-08-23,11:13:40<sup>7</sup>
Duration: 00:04:338
CName: gwp@135.8.118.2529
Phone: 69:2011<sup>10</sup>
Local-Address: 135.8.118.252:2061<sup>11</sup>
SSRC 154611212<sup>12</sup>
Remote-Address: 135.8.76.107:2061<sup>13</sup>
SSRC 2989801899 (0)<sup>14</sup>
Samples: 54^{15} (5 sec) ^{16}
Codec:
G723<sup>17</sup>
62B<sup>18</sup>
 30mS<sup>19</sup>
Off^{20}
 Silence-suppression(Tx/Rx) Disabled<sup>21</sup>
/Not-Supported<sup>22</sup>
Play-Time 272.610 sec^{23}
, Loss 0.0%<sup>24</sup>
 #1<sup>25</sup>
, Avg-Loss 0.1%<sup>26</sup>
, RTT 741mS<sup>27</sup>
#38<sup>28</sup>
Avg-RTT 570mS<sup>29</sup>
, JBuf-under/overruns 0.1%30
/0.0%31
, Jbuf-Delay 22mS<sup>32</sup>
Max-Jbuf-Delay 60mS<sup>33</sup>
Received-RTP:
Packets 9236<sup>34</sup>
, Loss 0.0\%^{35}
#0<sup>36</sup>
, Avg-Loss 0.0%<sup>37</sup>
, RTT 604mS<sup>38</sup> #38<sup>39</sup>
, Avg-RTT
376mS<sup>40</sup>
, Jitter 0 \, \text{mS}^{41}
#0<sup>42</sup>
, Avg-Jitter OmS<sup>43</sup>
, TTL(last/min/max) 63/63/63<sup>44</sup>
Duplicates 045
, Seq-Fall 0<sup>46</sup>
, DSCP 46<sup>47</sup>
, L2Pri 12<sup>48</sup>
, RTCP 54<sup>49</sup>
Transmitted-RTP:
VLAN 1<sup>50</sup>
, DSCP 184<sup>51</sup>
, L2Pri 6<sup>52</sup>
, RTCP 62<sup>53</sup>
Remote-Statistics:
```

```
Loss 0.0\%^{54} \#0^{55}, Avg-Loss 0.0\%^{56}, Jitter 0mS^{57} \#0^{58}, Avg-Jitter 0mS^{59} Echo-Cancellation:
Loss 45dB^{60} \#1^{61}, Len 32mS^{62} RSVP:
Status Disabled<sup>63</sup>, Failures 0^{64}
```

# **Detailed CLI output per RTP session**

The following table describes the fields in the **show rtp-stat detailed** command output according to the numbered labels in the example.

Field	Label	Description	From the CLI example
Session-ID	1	An arbitrary index number for the session in the session table	Session-ID: 35
Status	2	The status of the session. Possible values:  • Active. The session is still open.  • Terminated. The session is finished.	Status: Terminated
QOS	3	The QoS status of the session. Possible values:	QOS: Faulted
		OK. There are no QoS problems in the session.	
		Faulted. There are QoS problems in the session.	
EngineId	4	The ID of the VoIP engine. The Branch Gateway has one VoIP engine.	Engineld: 0
Start-Time	5	The date of the RTP session	2015-08-23
	6	The start time of the RTP session	Start-Time: 2015-08-23,11:09:07
End-Time	7	The end time of the RTP session	End-Time: 2015-08-23,11:13:40
Duration	8	The duration of the RTP session	Duration: 00:04:33
CName	9	format: gwt@ <mgp-address></mgp-address>	CName: gwp@135.8.118.252

Field	Label	Description	From the CLI example
Phone	10	The local extension number and conference ID in format <conference id="">:<extension number="">.</extension></conference>	Phone: 69:2011
		Conference calls can involve more than one entry in the session table. Multiple sessions belonging to the same conference call can usually be identified by a common conference ID.	
		Notes:	
		Phone data is received from CM only if VMON is configured.	
		If you are not running VMON, you can cause CM to send the phone data by configuring a dummy RTCP-server for the region, with a 'localhost' IP address (127.x.x.x).	
Local-Address	11	The PMI. The number after the colon is the UDP port number.	Local-Address: 135.8.118.252:2061
Remote-Address	13	The remote VoIP engine, gateway PMI, or IP phone address. The number after the colon is the UDP port number.	Remote-Address: 135.8.76.107:2061
	12, 14	SSRC ID. The number in parentheses is the number of observed SSRC changes during the session.	SSRC 2989801899 (0)
Samples	15	The number of times the application has sampled the VoIP engine (RTP receiver) statistics.	Samples: 54 <sup>15</sup> (5 sec)
	16	The sampling interval	Samples: 54 (5 sec) <sup>16</sup>
Codec:	17	The codec used for the session	G723
	18	The RTP packet size, in bytes	62B
	19	The RTP packet interval, in ms	30mS
	20	The encryption method	Off
Silence suppression (Tx/Rx)	21	The received silence suppression method	Silence- suppression(Tx/Rx) Disabled <sup>21</sup> /Not- Supported
	22	The transmitted silence suppression method	Silence- suppression(Tx/Rx) Disabled/Not- Supported <sup>22</sup>

Field	Label	Description	From the CLI example
Play-Time	23	The overall time the codec played valid received frames	Play-Time 272.610sec
Codec Loss codec-loss%	24	The last value of codec loss sampled. Codec loss is the percentage of time the codec played fill frames due to lack of valid RTP frames. Possible causes include jitter and packet loss.	Loss 0.0% <sup>24</sup> #1
#codec-loss-events	25	The codec loss event counter	Loss 0.0% #1 <sup>25</sup>
Avg-Loss	26	The average of all codec loss values sampled during the session	Avg-Loss 0.1%
RTT rtt ms	27	The last sampling of codec round trip time (RTT), in ms. Codec RTT is the round-trip delay experienced by the user, including internal delay. This value is not entirely accurate since remote internal delays are not always known.	RTT 741mS <sup>27</sup> #38
#rtt-events	28	The codec RTT event counter	RTT 741mS #38 <sup>28</sup>
Avg-RTT	29	The average of all codec RTT values sampled during the session	Avg-RTT 570mS
Jbuf-under/ overruns	30	The estimated percentage contribution of jitter-buffer underruns to the average codec loss	JBuf-under/overruns 0.1% <sup>30</sup> /0.0%
	31	The estimated percentage contribution of jitter-buffer overruns to the average codec loss	JBuf-under/overruns 0.1%/0.0% <sup>31</sup>
Jbuf-delay	32	The last jitter buffer delay	Jbuf-Delay 22mS
Max-Jbuf-Delay	33	The maximum jitter buffer delay during the session	Max-Jbuf-Delay 60mS
Received RTP:			
Packets	34	The total number of received packets	Packets 9236
Loss	35	The last sampled value of network RTP packet loss	Loss 0.0% <sup>35</sup> #0
loss%		·	
#loss-events	36	The network RTP packet loss event counter	Loss 0.0% #0 <sup>36</sup>
Avg-loss	37	The average of all network RTP packet loss values during the session	Avg-Loss 0.0%
RTT rtt ms	38	The network RTT. The RTT is calculated upon RTCP packet reception.	RTT 604mS <sup>38</sup> #38
#rtt-events	39	The network RTT event counter	RTT 604mS #38 <sup>39</sup>
Avg-RTT	40	The average of all network RTT values during the session	Avg-RTT 376mS
			Table continues

Field	Label	Description	From the CLI example
Jitter	41	The network jitter at the RTP receiver.	Jitter 0mS <sup>41</sup> #0
jitter ms		Combined with long RTT, a large jitter value may indicate WAN congestion.	
#jitter-event	42	The RTP receiver network jitter event counter	Jitter 0mS #0 <sup>42</sup>
Avg-Jitter	43	The average of all network jitter values during the session	Avg-Jitter 0mS
TTL (last/min/max)	44	The last value of TTL, minimum value of TTL, and maximum value of TTL sampled during the session. TTL changes during a session may indicate route flaps in the IP network.	TTL(last/min/max) 63/63/63
Duplicates	45	This counter increments each time two consecutive RTP packets with the sample RTP sequence number are received. A large number of duplicates may indicate problems in the Layer 2/Ethernet topology (for example, loops).	Duplicates 0
Seq-Fall	46	This counter increments each time an RTP packet with a sequence number less than the last known sequence is received. Packet resequencing may be caused by switching to a backup WAN interface or route flaps.	Seq-Fall 0
DSCP	47	The last received DSCP value of the RTP packets	DSCP 46
L2Pri	48	The last received Layer 2 priority value of an RTP packet (usually IEEE802.1p)	L2Pri 12
RTCP	49	The total number of received RTCP packets	RTCP 54
Transmitted-RTP:			
VLAN	50	The VLAN-ID on which the RTP packets are transmitted	VLAN 1
DSCP	51	The DSCP of RTP packets	DSCP 184
L2Pri	52	The Layer 2 priority of transmitted RTP packets (usually 802.1p)	L2Pri 6
RTCP	53	The total number of transmitted RTCP packets	RTCP 62
Remote-Statistics:	•		
(Remote-Statistics ite	ms are cald	culated and evaluated upon reception of RTCP n	nessages)

Field	Label	Description	From the CLI example
Loss rem-loss%	54	The network loss experienced by the remote RTP receiver. The local RTP receiver learns about its remote peer statistics from RTCP packets.	Loss 0.0% <sup>54</sup> #0
#rem-loss-ev	55	The number of samples that were over the rem-loss threshold	Loss 0.0% #0 <sup>55</sup>
Avg-Loss	56	The average network loss experienced by the remote RTP receiver	Avg-Loss 0.0%
Jitter rem-jitter	57	The network jitter experienced by the remote RTP receiver	Jitter 0mS <sup>57</sup> #0
#rem-jitter-ev	58	The number of samples that were over the remote jitter threshold	Jitter 0mS #0 <sup>58</sup>
Avg-jitter	59	The average remote jitter	Avg-Jitter 0mS
Echo Cancellation:			
Loss loss dbm	60	The echo cancellation loss on the TDM bus. A high value (that is, a low absolute value) may indicate impairment of DCP terminals.	Loss 45dB <sup>60</sup> #1
#loss-ev	61	A counter that increments each time the echo-cancellation loss is sampled below its threshold	Loss 45dB #1 <sup>61</sup>
Len	62	The last echo-cancellation tail length used for this session	Len 32mS
RSVP:			
Status	63	The current (last) RSVP reservation state at the end of the session	Status Disabled
Failures	64	The total number of reservation failures during the session	Failures 0

# Viewing QoS traps, QoS fault traps, and QoS clear traps

### About this task

QoS traps, QoS fault traps, and QoS clear traps sent to the active MGC by the dynamic trap manager are converted to syslog messages by the SNMP Trap manager on the MGC.

The syslog messages are stored in the messages file on the MGC hard disk. You can view the syslog messages through the Avaya Maintenance Web Interface to debug the QoS problems.

### **Procedure**

- 1. In the Avaya Maintenance Web Interface, enter the Setup log viewing screen.
- 2. In the **Select Log Types** list, select Linux syslog.
- 3. Under **Select Event Range**, select the date range over which you want to view traps.
- 4. In the **Match Pattern** field, enter the string avrtp.

- 5. In the **Number of Lines** field, enter the maximum number of traps you want to view.
- Click View Log.

Each line on the View System Logs screen contains one message.

# **Example of QoS trap output**

The following is an example of the syslog message for the QoS trap sent upon termination of RTP session 35 (see the session ID in bold) that terminated at 11:13:40 on Oct. 20:

```
Oct 20<sup>1</sup>
11:13:40<sup>2</sup>
LZ-SIT-SR1 snmptrapd[9407]: 135.8.118.252<sup>3</sup>
[135.8.118.252]: Trap
sysUpTime.0 = Timeticks: (43147723) 4 days, 23:51:17.234
, snmpTrapOID.0 = OID: av
RtpQoSTrap<sup>5</sup>
, avRtpSessionLocAddrV4.0 = IpAddress: 135.8.118.2526
avRtpSessionRemAddrV4.0 = IpAddress: 135.8.76.1077
, avRtpSessionDuration.0 =
INTEGER: 2738
, avRtpSessionCname.0 = STRING: gwp@135.8.118.2529
avRtpSessionPhone.0 = STRING: 69:2011<sup>10</sup>
, avRtpSessionSeverity.0 = INTEGER:
warning(4), avRtpSessionDebugStr.0 = STRING: Id{35
} 11
Traps{24<sup>12</sup>
/0^{13}
};Stats{S 54<sup>14</sup>
RTCP 54<sup>15</sup>
RX 9236<sup>16</sup>
};Codec{g723<sup>17</sup>
 encryptionOff^{19}
SSup disabled<sup>20</sup>
/disabled<sup>21</sup>
Loss 0.1%<sup>22</sup>
 #1^{23}
RTT 570mS<sup>24</sup>
#38<sup>25</sup>
Jbuf
0.1%26
/0.0%<sup>27</sup>
};Net{Loss 0.0%28
#0<sup>29</sup>
 RTT 376mS<sup>30</sup> #38<sup>31</sup>
 Jtr #0<sup>32</sup>
 TTL 63-63^{33}
 Dup 0<sup>34</sup>
Fall 0^{35}
};Rem{Loss 0.0%36
#0<sup>37</sup>
Jtr #0^{38}
} EC{Loss 45dB<sup>39</sup>
```

# **QoS Trap output fields**

The following table describes the fields in the QoS trap according to the numbered labels in the example.

Label	Description	From the trap example
1	The date on which the trap was received	Oct 20
2	The time at which the trap was received	11:13:40
3	The IP address of the local MGP	135.8.118.252
4	The Branch Gateway up time	sysUpTime.0 = Timeticks: (43147723) 4 days, 23:51:17.23
5	The trap name, which indicates that this is a QoS trap	snmpTrapOID.0 = OID: av
		RtpQoSTrap
6	The local gateway PMI	avRtpSessionLocAddrV4.0 = IpAddress: 135.8.118.252
7	The remote VoIP engine, gateway PMI, or IP phone address	avRtpSessionRemAddrV4.0 = IpAddress: 135.8.76.107
8	The duration of the RTP session	Duration: 00:04:33
9	Format: gwt@ <mgp-address></mgp-address>	avRtpSessionCname.0 = STRING: gwp@135.8.118.252
10	The local extension number and conference ID in format <pre><conference id="">:<extension number="">.</extension></conference></pre>	avRtpSessionPhone.0 = STRING: 69:2011
	Conference calls can involve more than one entry in the session table. Multiple sessions belonging to the same conference call can usually be identified by a common conference ID.	
	Notes:	
	The phone string data is received from CM if VMON is configured.	
	If you are not running VMON, you can cause CM to send the phone string data by configuring a dummy RTCP-server for the region, with a 'localhost' IP address (127.x.x.x).	
11	An arbitrary index number for the session in the session table	avRtpSessionDebugStr.0 = STRING: Id{35}
12	The total number of sent traps since the application was enabled	Traps{24 <sup>11</sup> /0}

Label	Description	From the trap example
13	The number of traps that were dropped by the trap rate limiter since the application was enabled. This item can be used, when analyzing received traps logs, to identify missing traps (due to network conditions or the rate limiter). This is also displayed by the show rtp-stat summary command.	Traps{24/0 <sup>12</sup> }
14	The number of times the application sampled the VoIP engine (RTP receiver) statistics	Stats{S 54}
15	The total number of received RTCP packets	Stats{S 54 RTCP 54 <sup>14</sup> RX 9236}
16	The total number of received RTP packets	Stats{S 54 RTCP 54 RX 9236 <sup>15</sup> }
17	The codec used for the session	g723
18	The codec packet size, in bytes	62B
19	The encryption method	encryptionOff
20	The received silence suppression method	SSup disabled <sup>19</sup> /disabled
21	The transmitted silence suppression method	SSup disabled/disabled <sup>20</sup>
22	The average of all codec loss values sampled during the session	Loss 0.1% <sup>21</sup> #1
23	The codec loss event counter	Loss 0.1% #1 <sup>22</sup>
24	The average of all codec round trip time values sampled during the session	RTT 570mS <sup>23</sup> #38
25	The codec round trip time event counter	RTT 570mS #38 <sup>24</sup>
26	The percentage contribution of jitter-buffer underruns to the average codec loss	Jbuf 0.1% <sup>25</sup> /0.0%
27	The percentage contribution of jitter-buffer overruns to the average codec loss	Jbuf 0.1%/0.0% <sup>26</sup>
28	The average of all network RTP packet loss values sampled during the session	Loss 0.0% <sup>27</sup> #0
29	The network RTP packet loss event counter	Loss 0.0% #0 <sup>28</sup>
30	The average of all network RTT values during the session	RTT 376mS <sup>29</sup> #38
31	The network RTT event counter	RTT 376mS #38 <sup>30</sup>
32	The network jitter at the RTP receiver	Jtr #0
33	The minimum and maximum TTL values sampled in the session	TTL 63-63
34	A counter that increments each time two consecutive RTP packets with the sample RTP sequence number are received	Dup 0
35	A counter that increments each time an RTP packet with a sequence number less than the last known sequence is received	Fall 0

Label	Description	From the trap example
36	The average network loss experienced by the remote RTP receiver	Rem{Loss 0.0% <sup>36</sup> #0 Jtr #0}
37	A counter that increments each time the remote loss is sampled over its threshold	Rem{Loss 0.0% #0 <sup>37</sup> Jtr #0}
38	A counter that increments each time the network jitter experienced by the remote RTP receiver is sampled over its threshold	Rem{Loss 0.0% #0 Jtr #0 <sup>38</sup> }
39	The echo cancellation loss on the TDM bus. A high value (that is, a low absolute value) may indicate impairment of DCP terminals.	EC{Loss 45dB}

# **Example of QoS fault and clear trap output**

The following is an example of the syslog message for the QoS fault and clear traps sent during RTP session 35, which terminated at 11:13:40 on October 20:

```
Oct 20^{1}
11:10:54<sup>2</sup>
 LZ-SIT-SR1 snmptrapd[9407]: 135.8.118.252
[135.8.118.252]: TrapsysUpTime.0 = Timeticks: (43131114) 4 days,
23:48:31.14<sup>3</sup>
, snmpTrapOID.0 = OID: avRtpQoSFault4
, avRtpQoSFaultTh.0 =
INTEGER: 15
, avRtpQoSClearTh.0 = INTEGER: 0^6
Oct 20^{1}
11:13:40<sup>2</sup>
LZ-SIT-SR1 snmptrapd[9407]: 135.8.118.252
[135.8.118.252]: TrapsysUpTime.0 = Timeticks: (43147723) 4 days,
23:51:17.23<sup>3</sup>
, snmpTrapOID.0 = OID: avRtpQoSClear4
, avRtpQoSFaultTh.0 =
INTEGER: 15
, avRtpQoSClearTh.0 = INTEGER: 0^6
```

# QoS fault and clear trap output fields

The following table describes the fields in the QoS fault and clear traps according to the numbered labels on the example above.

Label	Description	From the QoS fault trap example	From the QoS clear trap example
1	The date on which the trap was received	Oct 20	Oct 20
2	The time at which the trap was received	11:10:54	11:13:40
3	The Branch Gateway uptime	sysUpTime.0 = Timeticks: (43131114) 4 days, 23:48:31.14	sysUpTime.0 = Timeticks: (43147723) 4 days, 23:51:17.23

Label	Description	From the QoS fault trap example	From the QoS clear trap example
4	The trap name. Indicates that this is a QoS fault trap or a QoS clear trap.	snmpTrapOID.0 = OID: avRtpQoSFault	snmpTrapOID.0 = OID: avRtpQoSClear
5	The QoS fault trap boundary. That is, the number of active sessions with QoS faults that causes a QoS fault trap to be sent.	avRtpQoSFaultTh.0 = INTEGER: 1	avRtpQoSFaultTh.0 = INTEGER: 1
6	The QoS clear trap boundary. That is, the reduced number of active sessions with QoS faults that causes a QoS clear trap to be sent after a QoS fault trap was sent.	avRtpQoSClearTh.0 = INTEGER: 0	avRtpQoSClearTh.0 = INTEGER: 0

# Viewing automatic traceroute results

#### About this task

The VoIP engine automatically performs UDP traceroutes whenever the RTP statistics application is enabled.

A traceroute is performed per RTP session, 10 seconds after the session begins. A traceroute is not performed if there is another active session to the same destination for which a traceroute was already performed within the last five seconds.

#### **Procedure**

Use the show rtp-stat traceroute command.

You can filter the results according to subnet address by adding **destination-ip** and specifying the remote subnet address and subnet mask, or by specifying the rtp-statistics session index.

The traceroute results are displayed with the most recent first.

### For example:

# RTP traceroute results output

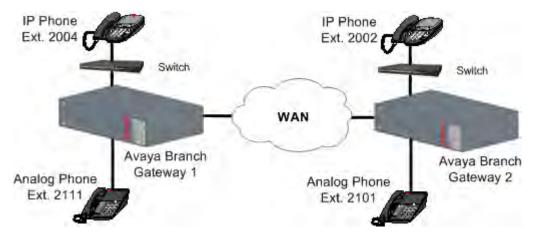
Name	Description
Session ID	The RTP statistics index for the RTP session
From	The IP address of the Branch Gateway
То	The IP address of the session destination (in this case, a destination within the specified subnet)
At	The time the traceroute is performed
TTL	The hop count and TTL field value of probe packets
HOP ADDRESS	The hop IP address
DELAY	The round trip time per probe packet. Three probe packets are sent per hop address, and the displayed value is the average of the three round-trip times. An asterisk (*) indicates that the probe packet timed out.

# RTP statistics examples

This section includes an example of configuring the RTP statistics application for a sample network. In addition, there are some example calls between various types of phones.

# Four telephones in a sample network

The following figure shows the locations of four telephone extensions in an example network. Telephones with extensions 2004 and 2111 are connected to the local Branch Gateway 1. Extensions 2002 and 2101 are connected to the remote Branch Gateway 2.



At the site of local Branch Gateway 1 – the administrator enabled and configured the RTP-MIB application as follows:

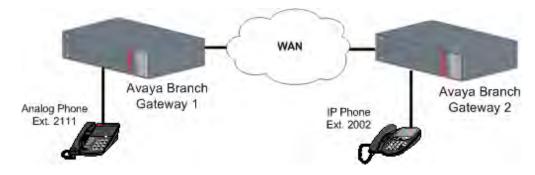
```
//to enable the RTP statistics application:
Gxxx-001(super)# rtp-stat-service
//to view the configuration of the application:
Gxxx-001(super)# show rtp-stat config
RTP Statistic: Enabled
```

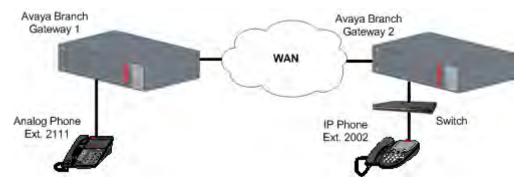
```
QoS Trap: Disabled
QoS Fault Trap: Disabled
   Fault: 0
    Clear: 0
QoS Trap Rate Limiter:
   Token Interval: 10.00 seconds
   Bucket Size: 5
Session Table:
   Size: 128
   Reserved: 64
Min Stat Win: 1
//to view the thresholds:
Gxxx-001(super) # show rtp-stat thresholds
        Threshold
                                                   Event Threshold
Codec Loss
                              0.0%
                                                         1
                               1.0%
Average Codec Loss
                                                        N/A
Codec RTT
Echo Return Loss
                               5 mS
1 dB
                                                         1
                                                         1
                               1.0%
Loss
Average Loss
LOSS
                               1.0%
                                                        N/A
Remote Loss
                               1.0%
                                                         1
Average Remote Loss
                               1.0%
                                                         N/A
                                13mS
                               1mS
Local Jitter
                                                         1
Remote Jitter
                               1mS
SSRC Changes
                               N/A
//to change the thresholds appropriately for the network:
Gxxx-001(super) # rtp-stat thresholds codec-loss 6.0
Gxxx-001(super) # rtp-stat thresholds average-codec-loss 0.0
Gxxx-001(super) # rtp-stat thresholds codec-rtt 700
Gxxx-001(super)# rtp-stat thresholds echo-return-loss 5
Gxxx-001(super) # rtp-stat thresholds loss 6.0
Gxxx-001(super)# rtp-stat thresholds remote-loss 6.0
Gxxx-001(super)# rtp-stat thresholds average-loss 0.0
Gxxx-001(super) # rtp-stat thresholds average-remote-loss 0.0
Gxxx-001(super)# rtp-stat thresholds jitter 70
Gxxx-001(super) # rtp-stat thresholds remote-jitter 70
Gxxx-001(super) # rtp-stat thresholds rtt 500
Gxxx-001(super) # rtp-stat event-threshold echo-return-loss 0
Gxxx-001(super) # rtp-stat event-threshold loss 1
Gxxx-001(super) # rtp-stat event-threshold remote-loss 0
Gxxx-001(super)# rtp-stat event-threshold jitter 0
Gxxx-001(super)# rtp-stat event-threshold remote-jitter 0
Gxxx-001(super) # rtp-stat event-threshold rtt 0
Gxxx-001(super) # rtp-stat event-threshold ssrc-change 0
//to review the threshold configuration again:
Gxxx-001(super) # show rtp-stat thresholds
Item Threshold Event Threshold
                                                   _____
                            6.0%
0.0%
700mS
                                                         1
Codec Loss
Average Codec Loss
                                                        N/A
Codec RTT
                                                         1
Echo Return Loss
                                5dB
                                                         0
Loss
                                6.0%
Loss
Average Loss
                               0.0%
                                                         N/A
Remote Loss
                               6.0%
Average Remote Loss
                               0.0%
                                                         N/A
RTT
                                500mS
                                 70mS
Local Jitter
                                70mS
Remote Jitter
SSRC Changes
                               N/A
//to configure the minimum statistics window for evaluating packet loss:
Gxxx-001(super)# rtp-stat min-stat-win 50
//to configure an external trap manager as a trap destination in addition to the active
```

```
MGC:
Gxxx-001(super) # snmp-server host 136.9.71.47 traps v1 public
//to check SNMP configuration
Gxxx-001(super) # show snmp
Authentication trap enabled
Community-Access Community-String
read-only ****
read-write ****
SNMPv3 Notifications Status
Traps: Enabled
Informs: Enabled Retries: 3 Timeout: 3 seconds
SNMP-Rec-Address Model Level Notification Trap/Inform User name
135.9.77.47 v1 noauth all trap ReadCommN UDP port: 162 DM
136.9.71.47 v1 noauth all trap WriteCommN
UDP port: 162
//to enable the sending of QoS traps:
Gxxx-001(super) # rtp-stat qos-trap
//to enable and configure the sending of fault and clear traps:
Gxxx-001(super) # rtp-stat fault 2 0
//to view RTP statistics configuration again:
Gxxx-001(super) # show rtp-stat config
RTP Statistic: Enabled
QoS Trap: Enabled
QoS Fault Trap: Enabled
   Fault: 2
   Clear: 0
QoS Trap Rate Limiter:
   Token Interval: 10.00 seconds
   Bucket Size: 5
Session Table:
   Size: 128
    Reserved: 64
Min Stat Win: 50
```

# Remote calls from analog to IP telephone

At 00:39 on August 23, 2015, an analog phone with an extension 2111 establishes a call with an IP phone with an extension 2002 in the network described in <u>Four telephones in a sample network</u> on page 343.





You must configure the RTP statistics application as described in <u>Four telephones in a sample</u> <u>network</u> on page 343. Following complaints related to QoS problems during the call, the administrator performs a check as follows:

```
//to see if the RTP statistics application registered QoS problems for the call:
Gxxx-001 (super) # show rtp sessions
   QoS Start date and time End Time Type
                                                     Destination
00001 *1
 2015-08-23,00:39:26 00:41:01 G711U
                                            20.20.20.2
//to display more details on the session:
Gxxx-001 (super) # show rtp-stat detailed 1
Session-ID: 1
Status: Terminated, QOS: Faulted<sup>2</sup>
, EngineId: 0
Start-Time: 2015-08-23,00:39:26, End-Time: 2015-08-23,00:41:01
Duration: 00:01:35
CName: gwp@30.30.30.1
Phone: 199:2111
Local-Address: 30.30.30.1:2329 SSRC 2764463979
Remote-Address: 20.20.20.2:2329 SSRC 1260226 (0)
Samples: 19 (5 sec)
Codec:
G711U 200B 20mS Off, Silence-suppression(Tx/Rx) Disabled/Disabled, Play-Time 63.
916sec, Loss 11.0% #15<sup>3</sup>
, Avg-Loss 8.6%, RTT 201mS #0, Avg-RTT 210mS, JBuf-under/o
verruns 9.4%/0.0%, Jbuf-Delay 2mS, Max-Jbuf-Delay 35mS
Received-RTP:
Packets 3225, Loss 0.0% #9^4
, Avg-Loss 8.4%, RTT 124mS #0, Avg-RTT 96mS, Jitter 11
mS #0, Avg-Jitter 9mS, TTL(last/min/max) 63/63/63, Duplicates 0, Seq-Fall 0, DSC
P 46, L2Pri 12, RTCP 9
Transmitted-RTP:
VLAN 1, DSCP 46, L2Pri 6, RTCP 17
Remote-Statistics:
Loss 11.6% #14<sup>5</sup>
, Avg-Loss 8.9%, Jitter 33mS #0, Avg-Jitter 26mS
Echo-Cancellation:
Loss 49dB #0, Len 32mS
RSVP:
Status Disabled, Failures 0
```

### A few points to note:

- The asterisk in the show rtp sessions output indicates that session 1 has QoS faults [1]
- The QoS is described as Faulted because of QoS faults [2]

- QoS faults that can be seen in the output are:
  - The codec loss event counter indicates that the codec loss exceeded the threshold 15 times [3]
  - The received-RTP packet loss event counter indicates that packet loss exceeded the threshold nine times [4]
  - The remote packet loss event counter indicates that remote packet loss exceeded the threshold 14 times [5]

# Local calls between an IP and an analog telephone

At 00:57, a local call is placed between an IP telephone with an extension 2004 and an analog telephone with an extension 2111 in the network described in <u>Four telephones in a sample network</u> on page 343. The call ends at 00:59:19.





# After the call ends, the administrator uses the CLI to view the QoS statistics:

```
//to see if there were QoS problems registered during the session
Gxxx-001 (super) # show rtp sessions last 1
    QoS<sup>1</sup>
Start date and time End Time Type
                                           Destination
00001 2015-08-23,00:57:13 00:59:19 G711U
                                                     30.30.30.2
//To display details of the session:
Gxxx-001 (super) # show rtp-stat detailed 1
Session-ID: 1
Status: Terminated, QOS: Ok2
, EngineId: 0
Start-Time: 2015-08-23,00:57:13, End-Time: 2015-08-23,00:59:19
Duration: 00:02:06
CName: gwp@30.30.30.1
Phone: 200:2111
Local-Address: 30.30.30.1:2165 SSRC 2533871380
Remote-Address: 30.30.30.2:2165 SSRC 93269 (0) ip phone or another medi proc
Samples: 25 (5 sec)
G711U 200B 20mS Off, Silence-suppression(Tx/Rx) Disabled/Disabled, Play-Time 130
.080sec, Loss 0.0\% #0<sup>3</sup>
, Avg-Loss 0.0\%^4
, RTT 83mS #0<sup>5</sup>
, Avg-RTT 108mS<sup>6</sup>
JBuf-under/overruns 0.0%/0.0%, Jbuf-Delay 5mS, Max-Jbuf-Delay 27mS
Received-RTP:
Packets 6503, Loss 0.0% #0^7
, Avg-Loss 0.0%8
, RTT 0mS #09
, Avg-RTT 0mS<sup>10</sup>
, Jitter 0mS \#0^{11}
, Avg-Jitter 0mS<sup>12</sup>
, TTL(last/min/max) 64/64/64, Duplicates 0, Seq-Fall 0, DSCP
46, L2Pri 12, RTCP 26
Transmitted-RTP:
VLAN 1, DSCP 46, L2Pri 6, RTCP 31
```

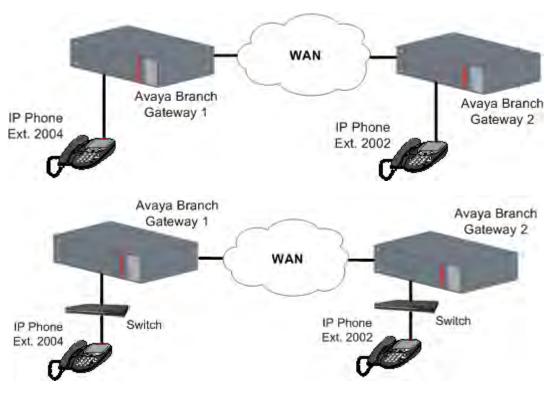
```
Remote-Statistics:
Loss 0.0\% \#0^{13}
, Avg-Loss 0.0\%^{14}
, Jitter 10\text{mS} \#0^{15}
, Avg-Jitter 10\text{mS}^{16}
Echo-Cancellation:
Loss 49\text{dB} \#0^{17}
, Len 32\text{mS}
RSVP:
Status Disabled, Failures 0
```

### A few points to note:

- The QoS column in the show rtp sessions output has no asterisk (\*), indicating that no metrics exceeded their event thresholds or average thresholds during the session [1].
- The QoS is described as Ok because there were no QoS problems [2]
- All average metric values are below the average thresholds [4] [5] [6] [8] [10] [12] [14] [16]
- All event counters are zero [3] [5] [7] [9] [11] [13] [15] [17]

# Remote calls from IP telephone to IP telephone

An IP telephone with an extension 2004 establishes an unshuffled call to another IP telephone with an extension 2002 in the network described in <u>Four telephones in a sample network</u> on page 343.



### The following commands are run after call termination:

```
00011 2015-08-23,00:57:13 00:59:19 G711U 30.30.30.2

00012 * 2015-08-23,00:39:26 00:41:01 G711U 20.20.20.2

00013 * 2015-08-23,01:02:45 01:05:15 G711U 20.20.20.2

00014 2015-08-23,01:02:50 01:05:15 G711U 30.30.30.3
```

Both sessions 13 and 14 are part of the call. The call architecture follows this pattern because an unshuffled call between two IP telephones use two VoIP channels: one channel between each telephone and the Branch GatewayVoIP engine.

### Session 13 has QoS problems.

```
//to display details of session 13:
Gxxx-001 (super) # show rtp-stat detailed 13
Session-ID: 13
Status: Terminated, QOS: Faulted, EngineId: 0
Start-Time: 2015-08-23,01:02:45, End-Time: 2015-08-23,01:05:15
Duration: 00:02:30
CName: gwp@30.30.30.1
Phone: 202:2004
Local-Address: 30.30.30.1:2329 SSRC 3510756141
Remote-Address: 20.20.20.2:2329 SSRC 1372162 (0)
Samples: 30 (5 sec)
G711U 200B 20mS Off, Silence-suppression(Tx/Rx) Disabled/Disabled, Play-Time 144
.540sec, Loss 0.0% #17, Avg-Loss 6.9%, RTT 99mS #0, Avg-RTT 208mS, JBuf-under/ov
erruns 7.4%/0.0%, Jbuf-Delay 9mS, Max-Jbuf-Delay 73mS
Received-RTP:
Packets 7279, Loss 0.0% #17 , Avg-Loss 6.8%, RTT 8mS #0, Avg-RTT 68mS, Jitter 0mS
#0, Avg-Jitter 6mS, TTL(last/min/max) 63/63/63, Duplicates 0, Seq-Fall 0, DSCP
46, L2Pri 12, RTCP 23
Transmitted-RTP:
VLAN 1, DSCP 46, L2Pri 6, RTCP 27
Remote-Statistics:
Loss 0.4% #17 , Avg-Loss 6.5%, Jitter 3mS #0, Avg-Jitter 22mS
Echo-Cancellation:
Loss 49dB #0, Len 32mS
RSVP:
Status Disabled, Failures 0
```

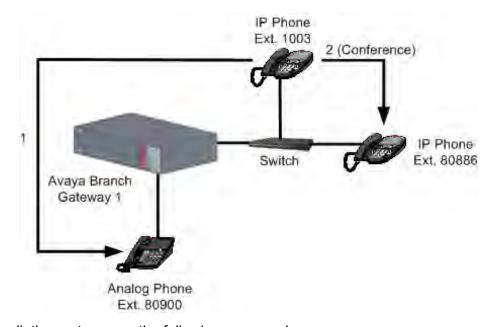
#### Session 14 is free of QoS problems:

```
//to display details of session 14:
Gxxx-001 (super) # show rtp-stat detailed 14
Session-ID: 14
Status: Terminated, QOS: Ok, EngineId: 0
Start-Time: 2015-08-23,01:02:50, End-Time: 2015-08-23,01:05:15
Duration: 00:02:25
CName: gwp@30.30.30.1
Phone: 202:2002
Local-Address: 30.30.30.1:2165 SSRC 247950253
Remote-Address: 30.30.30.2:2165 SSRC 120077 (0)
Samples: 29 (5 sec)
Codec:
G711U 200B 20mS Off, Silence-suppression(Tx/Rx) Disabled/Disabled, Play-Time 151
.140sec, Loss 0.0% #0, Avg-Loss 0.0%, RTT 95mS #0, Avg-RTT 106mS, JBuf-under/ove
rruns 0.0%/0.0%, Jbuf-Delay 11mS, Max-Jbuf-Delay 27mS
Received-RTP:
Packets 7556, Loss 0.0% #0, Avg-Loss 0.0%, RTT 0mS #0, Avg-RTT 0mS, Jitter 0mS #
0, Avg-Jitter 0mS, TTL(last/min/max) 64/64/64, Duplicates 0, Seq-Fall 0, DSCP 46
, L2Pri 12, RTCP 31
Transmitted-RTP:
VLAN 1, DSCP 46, L2Pri 6, RTCP 25
--type q to quit or space key to continue--
Remote-Statistics:
```

```
Loss 0.0% #0, Avg-Loss 0.0%, Jitter 7mS #0, Avg-Jitter 7mS
Echo-Cancellation:
Loss 49dB #0, Len 32mS
RSVP:
Status Disabled, Failures 0
```

### **Conference Calls**

A conference call is placed between two IP phones with extensions 1003 and 80886, and an analog phone with an extension 80900. The IP phone with extension 1003 connects to the analog phone with an extension 80900. The conference function of the IP phone with an extension 1003 is used to add the IP phone with an extension 80886 to the conference.



### During the call, the system runs the following commands:

```
//to display the RTP sessions:
Gxxx-001(super) # show rtp sessions
ID QoS Start date and time End Time Type
                                                       Destination
                ._____ ._...
00001 2015-08-23,09:55:17 - 00002 2015-08-23,09:55:20 -
                                         G729 16.16.16.101
                                                G711U 149.49.41.50
//to display details of session 1:
Gxxx-001(super) # show rtp detailed 1
Session-ID: 1
Status: Active, QOS: Ok, EngineId: 0
Start-Time: 2015-08-23,09:55:17, End-Time: -
Duration: 00:00:48
CName: gwp@33.33.33.33
Phone: 140<sup>1</sup>
:80900:1003
Local-Address: 33.33.33.33:61999 SSRC 3585271811
Remote-Address: 16.16.16.101:61999 SSRC 1369159108 (0)
Samples: 9 (5 sec)
Codec:
G729 40B 0mS Off, Silence-suppression(Tx/Rx) No-RTP/No-RTP, Play-Time 4.760sec,
Loss 0.0% #0, Avg-Loss 0.8%, RTT 137mS #0, Avg-RTT 141mS, JBuf-under/overruns 0.
8%/0.0%, Jbuf-Delay 20mS, Max-Jbuf-Delay 30mS
Received-RTP:
```

```
Packets 238, Loss 0.0% #0, Avg-Loss 0.0%, RTT 24mS #0, Avg-RTT 21mS, Jitter 0mS
#0, Avg-Jitter OmS, TTL(last/min/max) 0/61/61, Duplicates 0, Seq-Fall 0, DSCP 0,
L2Pri 6, RTCP 26
Transmitted-RTP:
VLAN 400, DSCP 46, L2Pri 6, RTCP 34
Remote-Statistics:
Loss 0.0% #0, Avg-Loss 0.0%, Jitter 2mS #0, Avg-Jitter 1mS
Echo-Cancellation:
Loss 49dB #0, Len 0mS
RSVP:
Status Reserved, Failures 0
//to display details of session 2:
Gxxx-001(super) # show rtp detailed 2
Session-ID: 2
Status: Active, QOS: Ok, EngineId: 0
Start-Time: 2015-08-23,09:55:20, End-Time: -
Duration: 00:00:50
CName: qwp@33.33.33.33
Phone: 140^2
:80886:1003
Local-Address: 33.33.33.33:61175 SSRC 3702564610
Remote-Address: 149.49.41.50:61175 SSRC 15161893 (0)
Samples: 10 (5 sec)
Codec:
G711U 40B 0mS Off, Silence-suppression(Tx/Rx) Disabled/Disabled, Play-Time 161.9
00sec, Loss 0.0% #0, Avg-Loss 0.0%, RTT 103mS #0, Avg-RTT 105mS, JBuf-under/over
runs 0.0%/0.0%, Jbuf-Delay 11mS, Max-Jbuf-Delay 13mS
Received-RTP:
Packets 8094, Loss 0.0% #0, Avg-Loss 0.0%, RTT 8mS #0, Avg-RTT 9mS, Jitter 0mS #
0, Avg-Jitter 0mS, TTL(last/min/max) 0/64/64, Duplicates 0, Seq-Fall 0, DSCP 0,
L2Pri 6, RTCP 30
Transmitted-RTP:
VLAN 400, DSCP 46, L2Pri 6, RTCP 30
Remote-Statistics:
Loss 0.0% #0, Avg-Loss 0.0%, Jitter 1mS #0, Avg-Jitter 0mS
Echo-Cancellation:
Loss 49dB #0, Len 0mS
RSVP:
Status Reserved, Failures 0
```

For clarity, suggest: The conference ID that appears in the Phone string for session 1 and for session 2 is identical and indicates that the two sessions belong to the same conference call [1] [2].

# **Summary of RTP statistics commands**

For more information about these commands, see Avaya Branch Gateway G450 CLI Reference.

Command	Description
rtp-stat clear	Reset the RTP statistics application
rtp-stat event-threshold	Set a QoS event-threshold for RTP streams
rtp-stat fault	Configure the RTP statistics application to send QoS fault and/or clear traps
rtp-stat min-stat-win	Set the RTP statistics minimum statistic window

Command	Description	
rtp-stat qos-trap	Configure the RTP statistics application to automatically send a QoS trap upon the termination of an RTP stream in which one or more QoS event counters exceeded their configured threshold	
rtp-stat qos-trap-rate-limit	Configure the QoS trap rate limiter	
rtp-stat-service	Enable the RTP statistics application	
rtp-stat thresholds	Set thresholds for the RTP statistics applications	
show rtp-stat config	Display the RTP statistics application configuration	
show rtp-stat detailed	Display a detailed QoS log for a specific RTP session	
show rtp-stat sessions	Display RTP sessions QoS statistics	
show rtp-stat summary	Display a summary of the RTP statistics	
show rtp-stat thresholds	Display the configured RTP statistic thresholds	
show rtp-stat traceroute	Display the results of UDP traceroutes issued by the Branch Gateway VoIP engine per active RTP session	

# **Packet sniffing**

The Branch Gateway packet sniffing service allows you to analyze packets that pass through the Branch Gateway's interfaces. Packets are captured to a buffer based on criteria that you specify. The buffer is then uploaded via FTP to a file that can be analyzed using the Ethereal analysis tool.

The packet sniffing service on the Branch Gateway offers several advantages to the network administrator. Since the capture file is saved in the libpcap format, which is the industry standard, it is readable both by the S8300's Tethereal software, and by standard versions of Ethereal for Unix, Windows, and Linux (see <a href="http://www.ethereal.com">http://www.ethereal.com</a>).

# Note:

Ethereal is an open source application.

In addition, the Branch Gateway's packet sniffing service is capable of capturing non-Ethernet packets, such as frame-relay and PPP. Non-Ethernet packets are wrapped in a dummy Ethernet header to allow them to be viewed in a libpcap format. Thus, the Branch Gateway allows you to analyze packets on all the interfaces of the device.

The Branch Gateway's packet sniffing service gives you full control over the memory usage of the sniffer. You can set a maximum limit for the capture buffer size, configure a circular buffer so that older information is overwritten when the buffer fills up, and specify a maximum number of bytes to capture for each packet.

# What can be captured

The Branch Gateway packet sniffing service captures only the packets handled by the Branch Gateway and delivered to the device CPU ("non-promiscuous" mode). This is unlike regular sniffer applications that pick up all traffic on the network.

See Roadmap for configuring packet sniffing on page 354 for a description of how to configure packet sniffing and analyze the resulting capture file.

# Streams that can always be captured

- H.248 registration
- · RTP from the Branch Gateway
- ARP on the LAN (broadcast)
- All packets that traverse the WAN
- All traffic to/from the Branch Gateway

# Streams that can never be captured

The following streams can never be captured because they are switched by the internal Ethernet switch and not by the CPU:

- H.323 Signaling from an IP phone on the LAN to an ICC on the LAN
- RTP stream between IP phones on the LAN

# Streams that can sometimes be captured

If the Branch Gateway is the WAN router of the following streams, they can be captured:

- H.323 Signaling from IP phones on the LAN to an ECC over the WAN
- DHCP when the DHCP server is behind the WAN (using the Branch Gateway DHCP relay capability)
- RTP stream on an IP phone on the LAN to a remote IP phone

# Roadmap for configuring packet sniffing

#### About this task

Packet sniffing configuration consists of the following steps:

#### **Procedure**

- 1. Enabling packet sniffing on page 355.
- 2. Limiting packet sniffing to specific interfaces on page 355 (if necessary).
- 3. Applying a capture list on page 362 that specifies which packets to capture.
- 4. Rule criteria for a capture list on page 356.
- 5. Viewing the capture list on page 362.

- 6. Applying a capture list on page 362.
- 7. Configuring packet sniffing settings on page 362.
- 8. Starting the packet sniffing service on page 364.

# **Enabling and disabling packet sniffing**

#### About this task

Since the packet sniffing service presents a potential security breach, the administrator must first enable the service on the Branch Gateway before a user can start capturing packets.

#### **Procedure**

1. Enter capture-service to enable the packet sniffing service.



# Note:

The packet sniffing service can only be enabled by an administrator connecting with a serial cable to the Branch Gateway Console port or the Services port.

2. To disable packet sniffing, enter no capture-service.

# Limiting packet sniffing to specific interfaces

#### About this task

By default, the packet sniffing service captures packets and Ethernet frames from all the router's interfaces. You can use the capture interface command to limit packet sniffing to a specific interface

For example, the following command limits packet sniffing to the FastEthernet Interface:

```
Gxxx-001(super) # capture interface fastethernet 10/3
Done!
Gxxx-001(super)#
```

The following command enables packet sniffing on all available interfaces:

```
Gxxx-001(super) # capture interface any
Done!
Gxxx-001(super)#
```

# Capture lists

By default, the packet sniffing service captures all packets passing through the interfaces on which it is enabled. Use a capture list to selectively filter the packets that are captured by the service.

A capture list contains an ordered list of rules and actions. A rule specifies criteria against which packets are tested. The action tells the Branch Gateway whether to capture or not capture packets matching the rule criteria. Only packets that match the specified criteria and have an action of capture are captured to the capture file. The rules are evaluated one by one, according to their number. If none of the rules match the packet, the default action is executed. You can set the default action as desired. Use the command ip-rule default to set the default action.

#### Note:

ARP frames are not IP packets and therefore cannot be filtered by capture lists. However, in a healthy network, the ARP frames rate is relatively low.

# **Configuring capture lists**

### **Procedure**

Use the ip capture-list command, followed by the list number, to enter the context of a capture list (and to create the capture list if it does not exist).

Capture lists are numbered from 501 to 599.

#### For example:

```
Gxxx-001(super) # ip capture-list 510
Gxxx-001(super-Capture 510)#
```

### **Example**

You can use the following commands to set the parameters of the capture list:

- Use the name command to assign a name to the capture list.
- Use the owner command to record the name of the person that created the list.
- Use the ip-rule command to define rule criteria for the capture list.

# Note:

You can use the cookie command to set the list cookie for the capture list. However, capture list cookies are not currently used by any application.

# Rule criteria for a capture list

Once in the capture list context, use the ip-rule command, followed by a number from 1 to 9999, to define a set of criteria against which to test packets. In addition to the rule criteria, each rule must include a composite operation. The composite operation determines the action the rule takes with respect to packets that match the rule criteria, and can be one of the following:

- capture
- no-capture

# Configuring rule criteria for a capture list

### **Procedure**

Use the composite-operation command to include a composite operation in a rule for a capture list.

For example, the following commands create a rule (rule 10 in capture list 510) that determines that TCP packets are not captured:

```
Gxxx-001(super) # ip capture-list 510
Gxxx-001(super-Capture 510) # ip-rule 10
Gxxx-001(super-Capture 510/ip rule 10) # composite-operation no-capture
Done!
Gxxx-001(super-Capture 510/ip rule 10)# ip-protocol tcp
```

```
Done!

Gxxx-001(super-Capture 510/ip rule 10)# composite-operation no-capture

Done!

Gxxx-001(super-Capture 510/ip rule 10)# ip-protocol tcp

Done!

Gxxx-001(super-Capture 510/ip rule 10)#
```

# **Rule applications**

Rules work in the following ways, depending on the type of information in the packet, and the number of criteria in the rule:

- L4 rules with a *Permit* operation are applied to non-initial fragments
- L4 rules with a *Deny* operation are not applied to non-initial fragments, and the device continues checking the next IP rule. This is to prevent cases in which fragments that belong to other L4 sessions may be blocked by the other L4 session which is blocked.
- L3 rules apply to non-initial fragments
- L3 rules that include the fragment criteria do not apply to initial fragments or non-fragment packets
- L3 rules that do not include the fragment criteria apply to initial fragments and non-fragment packets
- L4 rules apply to initial fragments and non-fragment packets

#### Rule criteria commands

You can use the following rule criteria commands. These commands are described in more detail below.

- dscp
- ip protocol
- source ip address
- · destination ip address
- tcp source-port
- tcp destination-port
- udp source-port
- udp destination-port
- icmp
- fragment

# Note:

You can also use the **description** command in the rule context to add a description of the rule.

# Applying rules to packets with DSCP values Procedure

Use the **dscp** command, followed by a DSCP value (from 0 to 63) to apply the rule to all packets with the specified DSCP value.

For example, the following rule is defined to capture all VoIP Bearer packets (DSCP = 46):

```
Gxxx-001(super)# ip capture-list 520
Gxxx-001(super-Capture 520)# ip-rule 20
Gxxx-001(super-Capture 520/ip rule 20)# composite-operation capture
Done!
Gxxx-001(super-Capture 520/ip rule 20)# dscp 46
Done!
Gxxx-001(super-Capture 520/ip rule 20)#
```

# Applying rules to packets with IP protocols

### **Procedure**

- 1. Use the ip-protocol command, followed by the name of an IP protocol, to apply the rule to all packets with the specified IP protocol.
- 2. If you want the rule to apply to all protocols, use any after the command (ip-protocol any).

For example, the following rule is defined to capture all TCP packets:

```
Gxxx-001(super)# ip capture-list 520
Gxxx-001(super-Capture 520)# ip-rule 20
Gxxx-001(super-Capture 520/ip rule 20)# composite-operation capture
Done!
Gxxx-001(super-Capture 520/ip rule 20)# ip-protocol tcp
Done!
Gxxx-001(super-Capture 520/ip rule 20)#
```

3. To apply the rule to all protocols except the specified protocol, use the no form of this command.

#### For example:

```
Gxxx-001(super-Capture 520/ip rule 20)# no ip-protocol tcp
Done!
Gxxx-001(super-Capture 520/ip rule 20)#
```

# Applying rules to source or destination IP address

### **Procedure**

- 1. Use the **source-ip** command to apply the rule to packets from the specified IP address or range of addresses.
- 2. Use the **destination-ip** command to apply the rule to packets going to the specified IP address or range of addresses.

# IP range criteria

**Range:** Type two IP addresses to set a range of IP addresses to which the rule applies. You can use wildcards in setting the range. For example:

```
Gxxx-001(super-Capture 520/ip rule 20) # source-ip 135.64.102.0 0.0.255.255
Done!
Gxxx-001(super-Capture 520/ip rule 20) #
```

**Single address:** Type host, by an IP address, to set a single IP address to which the rule applies. For example:

```
Gxxx-001(super-Capture 520/ip rule 20) # destination-ip host 135.64.104.102
Done!
Gxxx-001(super-Capture 520/ip rule 20) #
```

**Wildcard:** Type host, followed by an IP address using wildcards, to set a range of IP addresses to which the rule applies. For example:

```
Gxxx-001(super-Capture 520/ip rule 20)# source-ip host 135.0.0.0
Done!
Gxxx-001(super-Capture 520/ip rule 20)#
```

**Any:** Type **any** to apply the rule to all IP addresses. For example:

```
Gxxx-001(super-Capture 520/ip rule 20) # destination-ip any
Done!
Gxxx-001(super-Capture 520/ip rule 20) #
```

To apply the rule to all source or destination IP addresses except the specified address or range of addresses, use the **not** form of the applicable command. For example:

```
Gxxx-001(super-Capture 520/ip rule 20) # not destination-ip 135.64.102.0 0.0.255.255 Done!
Gxxx-001(super-Capture 520/ip rule 20) #
```

# Commands used to specify a range of source and destination ports

To specify a range of source and destination ports to which the rule applies, use the following commands, followed by either port name or port number range criteria:

- tcp source-port. The rule applies to TCP packets from ports that match the defined criteria
- tcp destination-port. The rule applies to TCP packets to ports that match the defined criteria
- udp source-port. The rule applies to UDP packets from ports that match the defined criteria
- udp destination-port. The rule applies to UDP packets to ports that match the defined criteria

For information about parameters and default settings, see *Avaya Branch Gateway G450 CLI Reference*.

# Port name or number range criteria

The port name or number range criteria can be any of the following:

**Range:** Type range, followed by two port numbers, to set a range of port numbers to which the rule applies. For example:

```
Gxxx-001(super-Capture 520/ip rule 20)# tcp destination-port range 1 3
Done!
Gxxx-001(super-Capture 520/ip rule 20)#
```

**Equal:** Type **eq**, followed by a port name or number, to set a port name or port number to which the rule applies. For example:

```
Gxxx-001(super-Capture 520/ip rule 20)# tcp source-port eq ftp
Done!
Gxxx-001(super-Capture 520/ip rule 20)#
```

**Greater than:** Type gt, followed by a port name or port number, to apply the rule to all ports with a name or number greater than the specified name or number. For example:

```
Gxxx-001(super-Capture 520/ip rule 20) # udp destination-port gt 10
Done!
Gxxx-001(super-Capture 520/ip rule 20) #
```

**Less than:** Type 1t, followed by a port name or port number, to apply the rule to all ports with a name or number less than the specified name or number. For example:

```
Gxxx-001(super-Capture 520/ip rule 20)# udp source-port lt 10
Done!
Gxxx-001(super-Capture 520/ip rule 20)#
```

**Any:** Type **any** to apply the rule to all port names and port numbers. For example:

```
Gxxx-001(super-Capture 520/ip rule 20)# tcp source-port any
Done!
Gxxx-001(super-Capture 520/ip rule 20)#
```

To apply the rule to all protocols except the specified protocol, use the **not** form of the applicable command. For example:

```
Gxxx-001(super-Capture 520/ip rule 20) # not udp source-port lt 10
Done!
Gxxx-001(super-Capture 520/ip rule 20) #
```

### Applying rules to ICMP

#### **Procedure**

1. To apply the rule to a specific type of ICMP packet, use the icmp command.

This command specifies an ICMP type and code to which the rule applies. You can specify the ICMP type and code by integer or text string.

For example:

```
Gxxx-001(super-Capture 520/ip rule 20) # icmp Echo-Reply
Done!
Gxxx-001(super-Capture 520/ip rule 20) #
```

2. To apply the rule to all ICMP packets except the specified type and code, use the not form of this command.

#### For example:

```
Gxxx-001(super-Capture 520/ip rule 20) # not icmp 1 2
Done!
Gxxx-001(super-Capture 520/ip rule 20) #
```

### Fragment command

To apply the rule to non-initial fragments, enter **fragment**. You cannot use the **fragment** command in a rule that includes UDP or TCP source or destination ports.

### Capture list example

The following commands create a capture list that captures all traffic from subnet 135.122.50.149 255.255.254 to an ECC at address 135.122.50.171, except telnet:

```
Gxxx-001(super) # ip capture-list 511
Gxxx-001(super-Capture 511) # name "list #511"
Done!
! Rules 10 and 15 provide that telnet packets are not captured.
Gxxx-001(super-Capture 511) # ip-rule 10
Gxxx-001(super-Capture 511/ip rule 10)# composite-operation no-capture
Done!
Gxxx-001(super-Capture 511/ip rule 10)# ip-protocol tcp
Done!
! You can use a port number instead of "telenet"
(23).
Gxxx-001(super-Capture 511/ip rule 10)# tcp destination-port eq telnet
Gxxx-001(super-Capture 511/ip rule 10)# exit
Gxxx-001 (super-Capture 511) #
Gxxx-001(super-Capture 511) # ip-rule 15
Gxxx-001(super-Capture 511/ip rule 15)# composite-operation no-capture
Gxxx-001(super-Capture 511/ip rule 15)# ip-protocol tcp
Done!
! You can use a port number instead of "telenet"
(23).
Gxxx-001(super-Capture 511/ip rule 15)# tcp source-port eq telnet
Gxxx-001(super-Capture 511/ip rule 15)# exit
! Rule 20 provides for capturing any packet coming from the host IP address
! 135.122.50.171 and going to the subnet 135.122.50.128, including packets going
! to any of the 30 possible hosts in that subnet.
Gxxx-001(super-Capture 511) # ip-rule 20
Gxxx-001(super-Capture 511/ip rule 20)# ip-protocol tcp
Gxxx-001(super-Capture 511/ip rule 20) # source-ip host 135.122.50.171
Done!
Gxxx-001(super-Capture 511/ip rule 20)# destination-ip 135.122.50.128 0.0.0.31
Done!
Gxxx-001(super-Capture 511/ip rule 20)# exit
! Rule 30 provides for capturing any packet coming from the subnet
! 135.122.50.128 and going to the host IP address 135.122.50.171, including
! packets from any of the 30 possible hosts in that subnet.
Gxxx-001(super-Capture 511) # ip-rule 30
Gxxx-001(super-Capture 511/ip rule 30) # source-ip 135.122.50.128 0.0.0.31
Done!
Gxxx-001(super-Capture 511/ip rule 30)# destination-ip host 135.122.50.171
Gxxx-001(super-Capture 511/ip rule 30) # exit
Gxxx-001(super-Capture 511) # ip-rule default
Gxxx-001(super-Capture 511/ip rule default)# composite-operation no-capture
Done!
```

```
Gxxx-001(super-Capture 511/ip rule default)# exit
Gxxx-001(super-Capture 511)# exit
Gxxx-001(super)#
```

### Viewing the capture list

#### **Procedure**

Use the **show** ip **capture-list** command to display the capture list in an easy-to-read format.

#### For example:

Gxxx-		ip o	capture-list 511	Owner		
	list #513 Protocol DSCP		IP	other Wildcard	Port	Operation
10	tcp Any		Any Any		Any eq Telnet	No-Capture
15	tcp	Src	Any Any		-	No-Capture
20	tcp Any		135.122.50.171 135.122.50.128		Any Any	Capture
30	Any Any		135.122.50.128 135.122.50.171		Any Any	
Deflt	-		Any Any		Any Any	No-Capture
Index	Name		Trust			
0	Capture No-Captur	re	No No			

### Applying a capture list

### **Procedure**

To apply a capture list, use the capture filter-group command from the general context.

For example, to set the Branch Gateway to use capture list 511 on interfaces in which packet sniffing is enabled, specify the following command:

```
Gxxx-001(super)# capture filter-group 511
Done!
Gxxx-001(super)#
```

#### Result

If no capture list is applied, the packet sniffing service captures all packets.

# **Configuring packet sniffing settings**

#### About this task

The packet sniffing service provides several administrative settings you can use to control the capture functionality. Use the following commands to configure packet sniffing settings. These commands are all used from general context, and require read/write access.

#### **Procedure**

1. Use the capture buffer-mode command to specify the type of buffer to use.

The available parameters are:

- cyclic. Circular buffer that overwrites the oldest records when it is filled up. Use a cyclic buffer to store the most recent history of packet activity.
- non-cyclic. Linear buffer that is used until it is filled up

#### For example:

```
Gxxx-001(super) # capture buffer-mode cyclic
Done!
Gxxx-001(super)#
```

2. Use the capture buffer-size command to specify the maximum size of the capture buffer.

Available values are 56 to 10000 kb. The default value is 1000. To activate the change in buffer size, enter copy running-config startup-config, and reboot the Branch Gateway.

#### For example:

```
Gxxx-001(super) # capture buffer-size 2000
To change capture buffer size, copy the running
configuration to the start-up configuration file, and reset the device.
Gxxx-001(super)# copy running-config startup-config
Beginning copy operation ...... Done!
Gxxx-001(super)#
```

3. Use the capture max-frame-size command to specify the maximum number of bytes captured for each packet.

This is useful, since in most cases, the packet headers contain the relevant information. Available values are 14 to 4096. The default value is 128.

### For example:

```
Gxxx-001(super) # capture max-frame-size 4000
This command will clear the capture buffer
- do you want to continue (Y/N)? y
Gxxx-001 (super) #
```



### ☑ Note:

When you change the maximum frame size, the Branch Gateway clears the capture buffer

4. Enter clear capture-buffer to clear the capture buffer.



To reduce the size of the capture file, use any combination of the following methods:

- Use the capture interface command to capture only from a specific interface.
- Use the capture max-frame-size to capture only the first N octets of each frame. This is valuable since it is usually the packets headers that contain the interesting information.

Use capture lists to select specific traffic.

### Starting the packet sniffing service

#### About this task

Use this procedure to enable the packet sniffing service.

You must apply a capture list using the capture filter-group command in order for the capture list to be active. If you do not use the capture filter-group command, the packet sniffing service captures all packets.



#### Note:

The capture start command resets the buffer before starting the sniffer.

#### **Procedure**

Once you have defined and applied the packet capture lists, use the capture start command in general context to instruct the packet sniffing service to start capturing packets.

#### Result

If packet sniffing has been enabled by the administrator, the following appears:

```
Gxxx-001(super) # capture start
Starting the packet sniffing process
Gxxx-001(super)#
```

If packet sniffing has not been enabled by the administrator, the following appears:

```
Gxxx-001(super) # capture start
Capture service is disable
To enable, use the `capture-service` command in supervisor mode.
Gxxx-001(super)#
```

### **Decrypted IPSec VPN packets**

IPSec VPN packets are encrypted packets. The contents of encrypted packets cannot be viewed when captured. However, you can use the capture ipsec command to specify that IPSec VPN packets, handled by the internal VPN Branch Gateway process, should be captured in plain text format.

# **Analyzing captured packets**

#### **Procedure**

Analyze the captured packets by stopping the packet sniffing service, uploading the capture file, and analyzing the capture file.

# Stopping the packet sniffing service

#### **Procedure**

Enter capture stop to stop the packet sniffing service.

Stop the service in order to upload a capture file.

### Note:

The capture stop command is not saved in the startup configuration file.

### Viewing packet sniffing information

### **Procedure**

1. You can enter show capture to view information about the packet sniffing configuration and the capture state.

#### For example:

```
Gxxx-001> show capture
Capture service is enabled and inactive
Capture start time 23/08/2015-13:57:40
Capture stop time 23/08/2015-13:58:23
Current buffer size is 1024 KB
Buffer mode is cyclic
Maximum number of bytes captured from each frame: 1515
Capture list 527 on interface "FastEthernet 10/3"
Number of captured frames in file: 3596 (out of 3596 total captured frames)
Size of capture file: 266 KB (26.6 %)
```

### Note:

The number of captured frames can be larger than the number of the frames in the buffer because the capture file may be in cyclic mode.

2. You can use the show capture-buffer hex command to view a hex dump of the captured packets.

However, for a proper analysis of the captured packets, you should upload the capture file and analyze it using a sniffer application, as described in the following sections.

### Example

The following is an example of the show capture-buffer hex command:

```
Gxxx-001> show capture-buffer hex
Frame number: 1
Time relative to first frame (D H:M:S:Micro-S): 0, 0:0:0.0
Packet time: 14/01/1970-13:24:55.583598
Frame length: 60 bytes
Capture Length: 60 bytes
00000000:ffff ffff ffff 0040 0da9 4201 0806 0001
                                               00000010:0800 0604 0001 0040 0da9 4201 9531 4e7a
                                                 ......@..B..1Nz
00000020:0000 0000 0000 9531 4e7a 0000 0000 0000
00000030:0000 0000 0000 0000 0000
Frame number: 2
Time relative to first frame (D H:M:S:Micro-S): 0, 0:0:0.76838
Packet time: 14/01/1970-13:24:55.660436
Frame length: 60 bytes
Capture Length: 60 bytes
00000000:ffff ffff ffff 0040 0d8a 5455 0806 0001
                                                 00000010:0800 0604 0001 0040 0d8a 5455 9531 4e6a
                                                 .......@...TU.1Nj
00000020:0000 0000 0000 9531 4e6a 0000 0000 0000
                                                 .....1Nj.....
00000030:0000 0000 0000 0000 0000 0000
```

### Uploading the capture file

#### **Procedure**

Once the packet sniffing service is stopped, upload the capture file to a server for viewing and analysis.



### Note:

The capture file may contain sensitive information, such as usernames and passwords of non-encrypted protocols. It is therefore advisable to upload the capture file over a secure channel - via VPN or using SCP (Secure Copy).

In most cases, you can upload the capture file to a remote server. However, in cases where the capture file is very large, or you encounter a WAN problem, you can upload the capture file to an S8300 Server and view it using Tethereal, which is a command-line version of Ethereal.

### Uploading the capture file to a remote server or USB mass storage device **Procedure**

Use one of the following commands to upload the capture file:

- · copy capture-file ftp
- · copy capture-file tftp
- copy capture-file scp
- copy capture-file usb
- copy capture-file https
- copyedge capture-file scp

#### Result



### Note:

The use of the copy capture-file scp command is limited to uploading files of 1 MB or less.

### For example:

```
Gxxx-001(super) # copy capture-file ftp myCature.cap 135.64.103.66
This command will stop the capture if capturing is started
Confirmation - do you want to continue (Y/N)? y
Username: xxxx
Password: xxxx
Beginning upload operation ...
This operation may take up to 20 seconds.
Please refrain from any other operation during this time.
For more information , use 'show upload status 10' command
Gxxx-001(super)#
```

### Uploading the capture file to an S8300 Server **Procedure**

1. Telnet into the S8300 Server, for example by entering session mgc.

2. Open the Avaya Maintenance Web Interface.

For instructions on accessing the Avaya Maintenance Web Interface, see *Installing and Upgrading the Avaya Branch Gateway G450*.

- 3. In the Avaya Maintenance Web Interface, select FTP under Security in the main menu.
- 4. Click Start Server.
- 5. Log into the Branch Gateway.
- 6. Use the copy capture file ftp command to upload the capture file.

Specify that the capture file should be placed in the ftp /pub subdirectory.

For example:

```
Gxxx-001(super) # copy capture-file ftp pub/capfile.cap 149.49.43.96
```

- 7. At the FTP login prompt, enter anonymous.
- 8. At the FTP password prompt, enter your e-mail address.
- 9. Optionally, enter show upload status 10 to view upload status.

### For example:

```
Gxxx-001(super) # show upload status 10

Module #10
========

Module : 10

Source file : sniffer

Destination file : pub/capfile.cap

Host : 149.49.43.96

Running state : Executing

Failure display : (null)

Last warning : No-warning
```

### Capture file analysis

The uploaded capture file is in libpcap format and can therefore be viewed by most sniffer applications, including topdump, Ethereal and Tethereal.

If you uploaded the capture file to an S3800 server, view the file using Tethereal, a command-line version of Ethereal available on the S3800. See the Tethereal man pages for more information about the Tethereal application.

If you uploaded the capture file to a remote server, you can view the file using the industry standard Ethereal application. The latest version of Ethereal for Windows, Linux, UNIX, and other platforms can be downloaded from <a href="http://www.ethereal.com">http://www.ethereal.com</a>.

### Note:

Ethereal allows you to create filter expressions to filter the packets in the capture file and display desired files only. For example, you can display only packets with a specific source address, or only those received from a specific interface. See <a href="Interface identification">Interface identification</a> on page 368.

#### Interface identification

The Branch Gateway's packet sniffing service can capture also non-Ethernet packets, such as frame-relay and PPP, into the capture file. This is achieved by wrapping non-Ethernet packets in a dummy Ethernet header to allow the packets to be stored in a libpcap format. This enables you to analyze packets on all the device interfaces.

The dummy Ethernet headers are allocated according to the original packet type. Dummy Ethernet headers start with 00:00. Therefore, if the source or destination address of a packet you are viewing in Ethereal starts with 00:00, this indicates the packet is a non-Ethernet packet.

The dummy Ethernet header is identified by special MAC addresses. Packets sent from a non-Ethernet interface are identified with an SA address in the format 00:01:00:00:xx and a DA address which holds the interface index. Packets received over a non-Ethernet interface are identified with DA address in the format 00:01:00:00:xx and an SA address which holds the interface index. The show capture-dummy-headers command displays the dummy header addresses and their meaning according to the current configuration.

### Note:

Ethernet packets received on a VLAN interface are identified by their VLAN tag. However, decrypted IPSec packets received on a VLAN interface are stored with a dummy header.

```
Gxxx-001> show capture-dummy-headers

MAC

Description

00:00:01:00:00:00

Src/dst address of Packet to/from frame-relay or PPP

00:00:01:00:00:01

Decrypted IPSec packet

00:00:0a:00:0a:02

interface fastethernet 10/3

00:00:0c:a0:b0:01

interface vlan 1

00:00:21:20:10:01

interface serial 3/1:1

00:00:21:40:10:02

interface serial 4/1:2

00:00:31:00:00:01

interface dialer 1
```

# **About simulating packets**

Capture lists support the IP simulate command. Refer to Simulating packets on page 515.

# Summary of packet sniffing commands

For more information about these commands, see Avaya Branch Gateway G450 CLI Reference.

Root level command	First level command	Second level command	Description
capture buffer- mode			Set the capture buffer to cyclic mode
capture buffer- size			Change the size of the capture file
capture filter- group			Activate a capture list

Table continues...

Root level command	First level command	Second level command	Description
capture interface			Specify a capture interface (by default, the service captures from all interfaces simultaneously)
capture ipsec			Set whether to capture IPSec VPN packets, handled by the internal VPN process, decrypted (plaintext) or encrypted (cyphertext)
capture max- frame-size			Set the maximum octets that are captured from each frame
capture start			Start capturing packets
capture stop			Stop capturing packets
capture-service			Enable or disable the capture service
clear capture- buffer			Clear the capture buffer (useful in case it holds sensitive information)
copy capture- file ftp			Upload the packet sniffing buffer to a file on a remote FTP server
copy capture- file scp			Upload the packet sniffing buffer to a file on a remote SCP server
copy capture- file tftp			Upload the packet sniffing buffer to a file on a remote TFTP server
copy capture- file usb			Upload the capture file to a USB mass storage device
copy capture- file https			Upload the packet sniffing buffer to a file on a remote HTTP server
copyedge capture-file scp			Upload the packet sniffing buffer to a file on a remote SCP server via Avaya SBCE tunnel
ip capture-list			Enter the capture list configuration context, create a capture list, or delete a capture list
	cookie		Set a number to identify a list (used by the rule-manager application)
	ip-rule		Enter an ip-rule context or erase an ip-rule
			Create or edit a composite operation
		destination-ip	Define an equation on the destination IP
		dscp	Specify the DSCP value to be set by the current IP rule

Table continues...

Root level command	First level command	Second level command	Description
		fragment	Apply the current rule to non-initial fragments only
		icmp	Set 'ip-protocol' to ICMP and an equation on the types of ICMP messages
		ip-protocol	Set the IP protocol
		source-ip	Set the current rule to apply to packets from the specified source IP address
		tcp destination- port	Set 'ip-protocol' to TCP and an equation on the destination port
		tcp source-port	Set 'ip-protocol' to TCP and an equation on the source port
		udp destination- port	Set 'ip-protocol' to UDP and an equation on the destination port
		udp source-port	Set 'ip-protocol' to UDP and an equation on the source port
	name		Name a capture list
	owner		Set the name of the person or application that has created the list
show capture			Show the sniffer status
show capture- buffer hex			Show a hex-dump of the captured frames
show ip capture- list			Show capture list(s)
show upload status			View capture file upload status

# Interface status reports

You report on the status of an interface using the **show interfaces** command. The command reports on the administrative status of the interface, its operational status, and its extended operational status (the ICMP keepalive status). For information about ICMP keepalive status, refer to <a href="ICMP keepalive">ICMP keepalive</a> on page 253.

For example, if an interface is enabled but normal keepalive packets are failing, show interfaces displays:

FastEthernet 10/3 is up, line protocol is down

However, if normal keepalive reports that the connection is up but ICMP keepalive fails, the following is displayed:

FastEthernet 10/3 is up, line protocol is down (no KeepAlive)

# Reporting of interface status

Port status	Keepalive status	Show interfaces output	Administrative state	Operational state	Extended operational state
Up	No Keepalive	FastEthernet 10/3 is up, line protocol is up	Up	Up	Up
Up	Keepalive Up	FastEthernet 10/3 is up, line protocol is up	Up	Up	Up
Up	Keepalive down	FastEthernet 10/3 is up, line protocol is down (no keepalive)	Up	Up	KeepAlive-Down
Down	N/A	FastEthernet 10/3 is up, line protocol is down	Up	Down	FaultDown
Standby	N/A	FastEthernet 10/3 is in standby mode, line protocol is down	Up	Dormant	DormantDown
Shutdown	N/A	FastEthernet 10/3 is administratively down, line protocol is down	Down	Down	AdminDown

For more information about these commands, see Avaya Branch Gateway G450 CLI Reference.

# **Summary of interface status commands**

For more information about these commands, see Avaya Branch Gateway G450 CLI Reference.

Command	Description
show interfaces	Display interface information

# **Echo cancellation**

Echo canceller control is intended to improve voice quality on a call by call basis.

The Branch Gateway has multiple echo cancellers of various capabilities. For best echo cancellation performance, the general rule is to enable only one echo canceller in any direction -- the one with the greater capacity in terms of echo tail control in the steady state. Tandeming echo cancellers in the same direction in a media path results in poorer performance in terms of

echo control, double-talk performance, noise, etc. In addition, if a smaller tail echo canceller is in the echo path of a longer tail canceller, audible echo can result when echo exists partly in one canceler's window and partly in the other.

For cases where there is no echo to cancel, it is usually best to disable any echo canceller in the path. Echo cancellers are not totally transparent and sometimes introduce undesirable artifacts.

However, the best echo cancellation policy varies depending on each specific call configuration. The Branch Gateway has an internal table for determining which VoIP engine and analog card echo cancellers to enable on a case-by-case basis. This table is consulted when the default auto mode is specified in the echo cancellation CLI commands. The CLI commands also offer the option of overriding the default automatic mode, but those alternative modes are intended for debugging and diagnostics purposes only.

#### Note:

DS1 echo cancellation can only be administered via the CM SAT, and these settings are always honored by the Branch Gateway. Therefore, the Branch Gateway CLI controls only the operation of the VoIP engine and analog trunk/line echo cancellers in relation to the DS1 echo canceller and between themselves.

# **Summary of echo cancellation commands**

For more information about these commands, see Avaya Branch Gateway G450 CLI Reference.

Command	Description
set echo-cancellation analog	Control echo cancellation on analog lines and trunks.
	The recommended setting for all analog trunks and lines is the default auto mode. In this mode, the Media Gateway controller consults internal rules to determine when to employ the analog echo canceller for each call.
set_echo-cancellation config	Configure echo cancellation on analog lines and trunks
analog	The recommended setting for all analog trunks and lines is the default configuration. The rest of the configuration options are intended for debugging or diagnosing issues in the field.
set echo-cancellation config voip	Configure echo cancellation on the VoIP engine
	The recommended setting is the default configuration. The rest of the configuration options are meant for debugging or diagnosing issues in the field.
set echo-cancellation voip	Control echo cancellation on the VoIP engine
	The recommended setting is the default auto mode. In this mode, the Media Gateway controller consults internal rules to determine when to employ the VoIP echo canceller for each call.
show echo-cancellation	Display echo cancellation settings and configuration information

# Integrated analog testing – Test and Heal

The analog trunk ports of the Branch Gateway are designed to meet certain standards. However, loop characteristics such as signal loss, noise, and crosstalk can cause deviation from those standards.

External testing of the loop typically involves removing the line from the Branch Gateway and connecting it to measurement equipment, dialing into the Local Exchange Carrier's test facility, and taking measurements locally. Alternatively, a technician can dial into a remote location that terminates in additional measurement equipment.

The Branch Gateway's integrated analog testing feature provides a simpler procedure in which the necessary testing is integrated into the Branch Gateway's analog ports, and the Branch Gateway plays the role of the measurement equipment. Using CLI commands, you can:

- Dial out on a specific trunk port to measure noise, receive-loss, crosstalk, trans-hybrid loss, or hybrid balance match
- Display the results of the measurements
- Take corrective action by manually setting a port's balance, receive-gain, or transmit-gain

The integrated analog testing feature enables quick and accurate testing of the loops at installation, and custom modifications to the analog ports that require correction for the actual loop characteristics. After installation, you can run additional tests whenever needed and correct each port that requires tuning.

# Hardware support for integrated analog testing

- The MM711 hardware vintage 30 and above
- The MM714 hardware vintage 10 and above, and the MM716

For detailed information about accepted values and recommended corrections, see *Analog Test* and *Heal User Guide*.

# Types of tests

Tests typically make a series of measurements in frequencies between 100Hz and 3400Hz in 100Hz increments. You can run the following tests:

**Noise test:** Noise is the measure of unwanted signals in the transmission path. After the call is established and while the far end is silent, the Branch Gateway collects the noise level.

**Receive-loss test:** After the call is established and while the tone (or tones) specific to the responder sequence is being received, the Branch Gateway collects the signal level at the reference frequency and compares it with the reference level. The difference in decibel between the level sent and the level received is the loss.

**Crosstalk test:** While the analog port under test is in a call and both ends of the call are silent, the crosstalk port establishes another call and plays a sequence of tones. The Branch Gateway collects during that time the tone level for different frequencies on the port under test.

**Balance test:** This test measures trans-hybrid loss. After the call is established and while the far end is silent, the Branch Gateway transmits a tone and measures the reflected signal level. The transmitted tone level minus the reflected tone level is the trans-hybrid loss at that frequency.

**Match test:** This test matches hybrid balance. Stored in the integrated analog testing firmware is a group of hybrid balance coefficient sets. Each entry in the group balances the hybrid against a different loop impedance. The match test executes a balance test for each set of coefficients and determines which set best matches the loop.

# Types of test lines

The measurements performed by the analog trunk ports in the Branch Gateway are based on some of the more common Centralized Automatic Reporting On Trunks (CAROT) test lines: Test 100, Test 102, and Test 105.

- The Test 100 line answers an incoming call, sends a 1004 Hz tone at 0 dBm for 5.5 seconds, and then remains quiet until it is disconnected.
- The Test 102 line answers an incoming call, sends a 1004 Hz tone at 0 dBm for 9 seconds, and then remains quiet for 1 second. The line repeats the 1004Hz/quiet sequence until disconnected.
- The Test 105 line answers an incoming call, then:
  - Sends a 1004 Hz tone at -16 dBm for 9 seconds
  - Remains quiet for 1 second
  - Sends a 404 Hz tone at -16 dBm for 9 seconds
  - Remains quiet for 1 second
  - Sends a 2804 Hz tone at -16 dBm for 9 seconds
  - Remains quiet for 30 second
  - Sends a 2225 Hz tone (progress tone) at -16 dBm for half a second
  - Forces disconnect

### Setting up a test profile

#### About this task

A test profile is a set of definitions for running a particular test. In essence, it specifies what measurements to run on which port. Once you set up a test profile, you can run it whenever necessary using the single launch command. You can define up to 30 profiles.

#### **Procedure**

- 1. Enter analog-test to enter the analog-test context.
- 2. Use the **profile** command to enter the analog-test-profile context, for configuring a specific test profile.

- 3. In the analog-test-profile context, setup the test profile:
  - Use the **set type** command to specify what type of test to run, that is, what type of measurements to run.
  - Use the **set port** command to specify which port to test. Note that only analog trunk ports are accepted.
  - Use the **set destination** command to set the Local Exchange Carrier (LEC) number destination of the measurement call. This number is called by the port being tested.

### Note:

If you enter set destination none, the port does not attempt to make a call toward any destination but makes the measurement on the current call. The test is performed while the port is in use. Remember to start the call before launching the test.

4. Use the **set responder** command to specify a responder port.

A responder is an analog trunk port that answers an incoming call and then plays a sequence of tones. The analog media module or the LEC collect the measurements while the responder plays its specific sequence. The responder can be a port in the media module, or the Local Exchange Carrier (LEC).

5. Use the **set responder-type** command to specify the responder type.

The different types send different sequences of tones, as explained in <u>Types of test lines</u> on page 374.

- 6. If the type of the current profile is crosstalk, use the following commands:
  - Use the set crosstalk-port command to specify the crosstalk port. The port must be on the same board as the port being tested, but it must be a different port from the port being tested.
  - Use the set crosstalk-destination command to set the Local Exchange Carrier number destination of the call from the crosstalk port.



If you enter set crosstalk-destination none, this indicates that the crosstalk port does not attempt to make a call toward any destination but expects an incoming call. Remember to start the call before launching the test.

• Use the set crosstalk-responder command to specify the responder port for the crosstalk port.

# Displaying and clearing profiles

#### **Procedure**

Use any of the following commands to display or clear profiles:

• In the analog-test-profile context, use the **show** command to display the test profile.

- In the analog-test context, use the **show profile** command to display a particular profile or all profiles.
- In the analog-test context, use the clear profile command to delete a particular test profile or all profiles.

# Launching and cancelling a test

### About this task

Once you created a test profile, you can launch it when desired. However, due to memory constraints on the analog media modules, only one test can be run at a time.

### Note:

A test fails if the port specified for the test is in use for a call, unless you specify set destination none for this test profile.

#### **Procedure**

- 1. Enter analog-test to enter the analog-test context.
- 2. Use the launch command to launch a specific test.

The port specified in the test profile must be busied out from CM before the test is launched.

As soon as **launch** is issued, the results of previous measurements on the port are cleared.

3. **(Optional)** To abort a currently running analog test, use the cancel command.

# Displaying test results

#### **Procedure**

Use any of the following commands to display test results:

- In the analog-test context, use the **show result** command to display the result of the latest measurements performed for a particular profile.
- In the analog-test-profile context, use the **show result** command to display the results of the latest measurements performed by the test profile.

#### Result

If a test did not succeed, the output indicates the reason for the test failure.

# **Healing trunks**

#### About this task

You can manually tune three parameters on each analog trunk port: balance, receive-gain, and transmit gain.

#### **Procedure**

- 1. Enter analog-test to enter the analog-test context.
- 2. Correct the balance, receive-gain, or transmit-gain of a port using the following commands:
  - Use the set balance command to set the balance on a specific port.
  - Use the set receive-gain command to set the receive-gain on a specific port.
  - Use the set transmit-gain command to set the transmit-gain on a specific port.

# **Displaying corrections**

#### About this task

After correcting the balance, receive-gain or transmit-gain, you can view the corrections applied to each port.

#### **Procedure**

- 1. Enter analog-test to enter the analog-test context.
- 2. Use the **show correction** command to display the balance, receive-gain, and transmit-gain corrections applied to each port.

# Summary of integrated analog testing commands

For more information about these commands, see Avaya Branch Gateway G450 CLI Reference.

Root Level Commands	First level command	Second level command	Description
analog-test			Enter the analog-test context
	cancel		Abort an analog test if it is already running
	clear profile		Delete a test profile
	launch		Launch a specific test
	profile		Enter the analog-test-profile context to setup or edit a test profile
		set crosstalk- destination	Set the Local Exchange Carrier number destination of the call from the crosstalk port
		set crosstalk-port	Specify the crosstalk port
		set crosstalk- responder	Specify the responder port for the crosstalk port
		set destination	Set the Local Exchange Carrier number destination of the measurement call

Table continues...

Root Level Commands	First level command	Second level command	Description
		set port	Specify the port to test
		set responder	Specify the responder port
		set responder-type	Specify the responder type
		set type	Specify what type of test to run
		show	Display a test profile
		show result	Display the results of the latest measurement obtained by this test profile
	set balance		Set the balance on a specific port
	set receive-gain		Set the receive-gain on a specific port
	set transmit- gain		Set the transmit-gain on a specific port
	show correction		Display the balance, receivegain, and transmit-gain corrections applied to each port
	show profile		Display the details of a test profile
	show result		Display the result of the last measurement performed for a particular profile

# **Service Level Agreement Monitor Agent**

The Service Level Agreement (SLA) Monitor is a diagnostic and monitoring system for the converged network. It employs the use of a web-based server application to communicate with agents embedded in the components of IP telephony as well as other sources to reveal how the network contributes to the performance of audio and video applications.

The SLA Monitor performs analysis on the following network elements:

- Correct Differentiated Services (DiffServ) issues.
- · Handle rogue applications.
- Provide real-time visibility to live sessions.

For more information on the SLA Monitor server and agent, see *Operations Intelligence Suite Advanced Implementation Guide for SLA Mon*.

Root Level Commands	First level command	Second level command	Description
	copy scp root-ca sla		Copy and install a trusted CA certificate to be used for the TLS connection to the SLA server.
	copy usb root-ca sla		Copy and install a trusted CA certificate to be used for the TLS connection to the SLA server.
	set sla-monitor		Enables or disables the SLA Monitor Agent.
	show root-ca sla		Display the trusted CA certificates to be used for the SLA TLS connection.
	show sla-monitor		Displays the state of the SLA Monitor Agent for example, enabled or disabled. The command also displays all gateway parameters pertaining to the SLA Monitor Agent.

# **Chapter 20: Router**

The Branch Gateway has an internal router. You can configure the following routing features on the router:



WAN features are supported on IPv4 only.

- Interfaces
- Unnumbered IP interfaces
- · Routing table
- GRE tunneling
- DHCP and BOOTP relay
- DHCP server
- · Broadcast relay
- ARP table
- ICMP errors
- RIP
- OSPF
- · Route redistribution
- VRRP
- Fragmentation

You can configure multiple routing schemes on the Branch Gateway. See <u>Routing sources</u> on page 386 for an explanation of the priority considerations employed by the Branch Gateway to determine the next hop source.

# **Enabling and disabling the router**

#### **Procedure**

1. Use the ip routing command to enable the router.

2. Use the no ip routing command to disable the router.

# Interface configuration

You can use the CLI to configure interfaces on the router.

# **Router interface concepts**

The router in the Branch Gateway includes the following interface categories:

- Physical
- · Layer 2 virtual
- · Layer 3 routing

# Physical router interfaces

The physical interfaces of the Branch Gateway router include:

**WAN Interfaces:** When you add a WAN media module to the Branch Gateway, the media module provides a WAN interface. You can add one of the following types of WAN media modules:

- The Avaya MM340 media module provides an E1/T1 WAN interface
- The Avaya MM342 media module provides a USP WAN interface

**FastEthernet Interface:** The 10/3 and 10/4 Fast Ethernet ports on the front panel of the Branch Gateway provide a FastEthernet interface. This interface is an autosensing 10/100 Mbps Fast Ethernet port. It can be used to connect to a LAN, an external firewall, an external Virtual Private Network (VPN), or a DeMilitarized Zone (DMZ). This interface can also be used as a WAN interface when configured for PPPoE. For more information, see Configuring PPPoE on page 227.

**Switching Interface:** An internal 100 Mbps connection to the Branch Gateway internal switch provides a switching interface. The switching interface supports VLANs. By default, the switching interface is associated with the first VLAN (Vlan 1).

When you configure the Branch Gateway without an external VPN or firewall, Vlan 1 is used to connect the internal Branch Gateway router to the internal Branch Gateway switch. If an external firewall or VPN is connected to the Fast Ethernet port, it is important to disable Vlan 1 to prevent a direct flow of packets from the WAN to the LAN.

# Layer 2 virtual interfaces

**Loopback:** The Loopback interface is a virtual Layer 2 interface over which loopback IP addresses are configured. The Loopback interface represents the router by an IP address that is always available, a feature necessary mainly for network troubleshooting.

Since the Loopback interface is not connected to any physical interface, an entry in the routing table can not have the Loopback interface's subnet as its next hop.

**GRE tunnel:** A GRE tunnel is a virtual point-to-point link using two routers at two ends of an Internet cloud as its endpoints. GRE tunneling encapsulates packets and sends them over a GRE tunnel. At the end of the GRE tunnel, the encapsulation is removed and the packet is sent to its destination in the network at the far end of the GRE tunnel. For more information, see <u>GRE tunneling</u> on page 391.

### Layer 2 logical interfaces

**VLAN (on the Switching Interface):** The Branch Gateway switch can have multiple VLANs defined within its switching fabric. The Branch Gateway router supports up to 64 VLANs that can be configured over their internal switching interface connections.

**Serial Interface:** The Serial interface is a virtual interface that is created over a portion of an E1/T1 or USP port. Serial interfaces support PPP and frame relay encapsulation protocols. For more information about configuring Serial interfaces for a WAN, see <u>Configuring the initial WAN</u> on page 217.

**Dialer Interface:** The Dialer interface is used for the modem dial-backup feature. Refer to Modem dial backup on page 236.



One or more IP interfaces can be defined over each Serial, FastEthernet, switching, and Loopback interface.

# Configuring an IP interface

#### **Procedure**

1. To create an interface, enter **interface** followed by the type of interface you want to create.

Some types of interfaces require an identifier as a parameter. Other types of interfaces require the interface's module and port number as a parameter.

### For example:

```
interface vlan 1 interface serial 3/1 interface fastethernet 10/2
```

2. Enter ip address, followed by an IP address and subnet mask, to assign an IP address to the interface.

Use the **no** form of this command to delete the IP interface.

# Interface configuration examples

Use the following commands to configure the fixed router port with IP address 10.20.30.40 and subnet mask 255.255.0.0:

```
Gxxx-001# interface fastethernet 10/3
Gxxx-001(if:FastEthernet 10/3)# ip address 10.20.30.40 255.255.0.0
Done!
```

Use the following commands to create VLAN 2 on the switching interface and configure it with IP address 10.30.50.70 and subnet mask 255.255.0.0:

```
Gxxx-001# interface Vlan 2
Gxxx-001(if:Vlan 2)# ip address 10.30.50.70 255.255.0.0
Done!
```

# Summary of basic interface configuration commands

For more information about these commands, see Avaya Branch Gateway G450 CLI Reference.

Root level command	Command	Description
interface console		Enter the Console interface configuration context, create the interface if it does not exist, or delete the Console interface
	ip address	Assign an IP address and mask to an interface or delete an interface
interface dialer		Enter the Dialer interface context, create the Dialer interface if it does not exist, or delete the Dialer interface
	ip address	Assign an IP address and mask to an interface or delete an interface
	ip admin-state	Set the administrative state of an IP interface
	ip broadcast- address	Update the interface broadcast address
interface fastethernet		Enter FastEthernet interface configuration context, create a FastEthernet interface if it does not exist, or delete a FastEthernet interface
	ip address	Assign an IP address and mask to an interface or delete an interface
	ip admin-state	Set the administrative state of an IP interface
	ip broadcast- address	Update the interface broadcast address
interface loopback		Enter loopback interface configuration context, create a Loopback interface if it does not exist, or delete a Loopback interface or sub-interface
	ip address	Assign an IP address and mask to an interface or delete an interface
	ip admin-state	Set the administrative state of an IP interface
interface serial		Enter Serial interface or sub-interface configuration context, create a serial interface if it does not exist, or delete a serial interface or sub-interface
	ip address	Assign an IP address and mask to an interface or delete an interface

Table continues...

Root level command	Command	Description
	ip admin-state	Set the administrative state of an IP interface
	ip broadcast-address	Update the interface broadcast address
interface tunnel		Enter tunnel interface configuration context, create a tunnel interface if it does not exist, or delete a tunnel interface or sub-interface
	ip address	Assign an IP address and mask to an interface or delete an interface
	ip admin-state	Set the administrative state of an IP interface
interface usb-modem		Enter the USB-modem interface configuration context, reset the USB-modem interface settings to their factory defaults
	ip address	Assign an IP address and mask to an interface or delete an interface
interface vlan		Enter VLAN interface configuration context, create a VLAN interface if it does not exist, or delete a VLAN interface
	ip address	Assign an IP address and mask to an interface or delete an interface
	ip admin-state	Set the administrative state of an IP interface
	ip broadcast-address	Update the interface broadcast address
show ip interface brief		Display a summary of the interface configuration information for a specific interface or for all of the interfaces

# **Unnumbered IP interfaces**

Unnumbered IP is a feature that enables you to configure a point-to-point interface to borrow an IP address from another interface. Unnumbered IP enables IP processing on a point-to-point interface without assigning an explicit IP address to the interface.

Although unnumbered IP is supported on all point-to-point interfaces, the main use of the feature is to enable dynamic routing on the Dialer interface. The Dialer interface is used for the modem dial-backup feature. Refer to <a href="Modem dial backup">Modem dial backup</a> on page 236. Modem dial-backup is a feature that sets up a backup dialing destination for a Branch Gateway. Modem dial-backup requires unnumbered IP to be configured on the Dialer interface of the Branch Gateway and at both the default and the backup dialing destinations.

#### **Related links**

Modem dial backup on page 236

# Unnumbered IP on an interface configuration

To configure unnumbered IP on an interface, you must specify the interface from which to borrow the IP address. The borrowed interface must already exist and have an IP address configured on it.

The status of an unnumbered IP interface is down whenever the borrowed interface is down. Therefore, it is recommended to borrow the IP address from an interface that is always up, such as the Loopback interface.

Routes discovered on an unnumbered interface by the RIP and OSPF routing protocols are displayed as via routes in the routing table. The next hop is listed as via the IP unnumbered interface instead of the source address of the routing update.

# Configuring IP on an interface configuration

#### **Procedure**

- 1. Decide which interface from which to borrow the IP address.
  - If necessary, configure the interface. You can use the **show interfaces** command to display existing interface configuration.
- 2. Enter the context of the interface on which you want to configure an unnumbered IP address (usually the Dialer interface).
- 3. Use the ip unnumbered command, specifying the interface from which to borrow the IP address.

# **Unnumbered IP examples**

In the following example, a VLAN interface is configured, and then the Dialer interface is configured with an unnumbered IP address, borrowing the IP address from the VLAN interface.

```
//enter the context of vlan interface 1:
Gxxx-001(super) # interface Vlan 1
//to configure the IP address of the vlan interface:
Gxxx-001(super-if:Vlan 1)# ip address 180.0.0.1 255.255.255.0
Gxxx-001(super-if:Vlan 1) # exit
Gxxx-001# !
//enter the context of the Dialer interface:
Gxxx-001(super) # interface dialer 1
Gxxx-001(super-if:Dialer 1) # dialer string 1 3001
Gxxx-001(super-if:Dialer 1) # dialer persistent delay 1
Gxxx-001(super-if:Dialer 1) # dialer modem-interface USB-modem
//to configure IP unnumbered on the Dialer interface, borrowing the IP address from
vlan interface 1, configured above:
Gxxx-001(super-if:Dialer 1) # ip unnumbered 1 Vlan 1
Gxxx-001(super-if:Dialer 1)# exit
Gxxx-001(super)#!
```

The following sample routing table shows how routes discovered on unnumbered interfaces by routing protocols are listed as via routes in the Next-Hop column:

Network	Mask	Interface	Next-Hop	Cost	TTL	Source
0.0.0.0	0	FastEth10/3	149.49.54.1	1	n/a	STAT-HI
2.2.2.0	24	Vlan15	2.2.2.1	1	n/a	LOCAL
10.0.0.0	8	Vlan1	0.0.0.40	1	n/a	LOCAL
3.0.0.0	8	Tunnel1	Via Dia.1	2	172	RIP
4.0.0.0	8	Tunnel 1	Via Dia.1	2	172	RIP
20.0.0.0	8	Tunnel 1	Via Dia.1	11112	n/a	OSPF
20.0.0.1	32	Tunnel 1	Via Dia.1	22222	n/a	OSPF
26.0.0.0	8	Vlan 15	2.2.2.2	3	n/a	STAT-LO
31.0.0.0	8	Serial 3/1:1.1	31.0.0.1	1	n/a	LOCAL
32.0.0.0	8	Serial 3/1:1.2	32.0.0.1	1	n/a	LOCAL
33.0.0.0	8	Serial 3/1:1.3	33.0.0.1	1	n/a	LOCAL
99.0.0.0	8	Vlan 99	99.1.1.1	1	n/a	LOCAL
135.64.0.0	16	FastEth 10/3	149.49.54.1	1	n/a	STAT-HI
138.0.0.0	8	Serial 3/1:1.1	Via Ser.3/1:1.1	2	n/a	STAT-LO
139.0.0.0	8	Serial 3/1:1.1	Via Ser.3/1:1.1	1	n/a	STAT-LO
149.49.54.0	24	FastEth 10/3	149.49.54.112	1	n/a	LOCAL
180.0.0.0	8	Loopback 1	180.0.0.1	1	n/a	LOCAL

# Summary of unnumbered IP interface configuration commands

For more information about these commands, see Avaya Branch Gateway G450 CLI Reference.

Root level command	Command	Description
<pre>interface (dialer  fastethernet  serial tunnel)</pre>		Enter the Dialer, FastEthernet, Serial, or Tunnel interface context
	ip unnumbered	Configure an interface to borrow an IP address from another interface or remove an unnumbered IP configuration from an interface

# **Routing sources**

The Branch Gateway router supports both static and dynamic routing per interface. You can configure static routes with two levels of priority, high and low, and you can enable and configure Open Shortest Path First (OSPF) and Routing Information Protocol (RIP) dynamic routing protocols. Additionally, when DHCP client is configured on an interface, you can configure DHCP client to request a default router address from the DHCP server (DHCP option 3).

The actual source from which the router learns the next hop for any given interface is determined as follows: The router seeks the best match to a packet's destination IP address from all enabled routing sources. If there is no best match, the next hop source is determined according to the following priority order:

1. High priority static route (highest)

If a high priority static route is configured on the interface, this route overrides all other sources.

#### 2. OSPF

If no high priority static route is configured on the interface, but OSPF is enabled, then OSPF determines the next hop.

3. RIP

If no high priority static router is configured on a given interface, and OSPF is not enabled, but RIP is enabled, RIP determines the next hop.

- 4. EXT OSPF
- 5. DHCP

If no high priority static router is configured on a given interface, and neither OSPF nor RIP are enabled, and DHCP client is configured on the interface with a default router requested from the DHCP server (DHCP option 3), then the default router provided by DHCP is used.

6. Low priority static route (lowest)

When more than one next hop is learned from the same source, the router uses an equal cost multi path algorithm that performs load balancing between routes.

- For information about configuring static routes, see Routing table configuration on page 387.
- For information about configuring OSPF, see OSPF on page 419.
- For information about configuring RIP, see RIP on page 414.
- For information about configuring DHCP client, see <a href="DHCP client configuration">DHCP client configuration</a> on page 178.

# Routing table configuration

When you configure the routing table, you can:

- View information about the routing table
- · Add entries to the routing table
- Delete entries from the routing table

### Note:

To change an entry in the routing table, delete the entry and then add it as a new entry.

The routes in the routing table are static routes. They are never timed-out, and can only be removed manually. If you delete the interface, all static routes on the interface are also deleted.

A static route becomes inactive whenever the underlying Layer 2 interface is down, except for permanent static routes. You can disable the interface manually using the <code>ip</code> <code>admin-state</code> down command. For more information, see Permanent static route on page 389. When the underlying Layer 2 interface becomes active, the static route enters the routing table again.

You can monitor the status of non-permanent static routes by applying object tracking to the route. Thus, if the track state is changed to down then the static route state is changed to inactive, and if the track state is changed to up then the static route state is changed to active. For more information on object tracking, see Object tracking on page 258.

Static routes can be advertised by routing protocols, such as RIP and OSPF. For more information, see <u>Route redistribution</u> on page 422. Static routes also support load-balancing similar to OSPF.

# **Next hops**

Static routes can be configured with the following as next hops:

**Via-interface route:** Specifies a Serial interface as the next hop, without a specific next hop IP address.

**Next-hop IP address:** Specifies the IP address of a router as a next hop. The next hop router must belong to one of the directly attached networks for which the Branch Gateway has an IP interface.

# Static route types

Two kinds of static routes can be configured:

High Preference static routes: Preferred to routes learned from any routing protocol

Low Preference static routes: Used temporarily until the route is learned from a routing protocol

By default, a static route has low preference.

# Configuring multiple next hops

#### **Procedure**

You can configure up to three next hops for each static route in one of the following manners:

- Enter all of the next hops using a single ip route command. To add a new next hop to an existing static route, enter the new next hop individually, as in the following option.
- Enter each next hop individually with its own ip route command

### Note:

If you apply tracking to a static route, you can only configure one next hop for the route.

Metrics are used to choose between routes of the same protocol. Preferences are used to choose between routes of different protocols.

# Deleting a route and its next hops

#### **Procedure**

Use the no ip route command to delete the route including all of its next-hops.

This deletes all of the next-hops, whether entered individually or with a single command. For example, to specify next hops 149.49.54.1 and 149.49.75.1 as a static route to the network 10.1.1.0, do one of the following:

- Enter ip route 10.1.1.0 24 149.49.54.1 149.49.75.1, specifying all next hops together
- Enter both ip route 10.1.1.0 24 149.49.54.1 and ip route 10.1.1.0 24 149.49.75.1

### Via-interface static route

PPP and frame relay allow for a Layer 3 interface to be established without knowing in advance the next-hop on the other side of a serial link. In this case, you can specify a Serial Layer 2 interface or a GRE tunnel as a next-hop instead of providing a specific next hop IP address. This is equivalent to specifying the node on the other side of the serial link as the next hop when its IP address is unknown. The via interface option is configured by specifying the type and the number of the Serial interface using the ip route command.

### Note:

The interface used in the via route must have an IP address attached to it.

For example, the command ip route 193.168.10.0 24 serial 3/1:1 creates a static route to the network 193.168.10.0 24 via the Serial 3/1:1 interface.

A static route can have both via interface and IP addressed next hops, with a maximum of three next-hops. If such a combination is required, separate ip route commands should be used for the via interface static route and the IP addressed next hop routes. Also, if more than one via interface next hop is required, each must be configured by separate ip route commands.

### Note:

You cannot define a static route through the FastEthernet Interface unless the interface was previously configured to use PPPoE encapsulation or was configured as a DHCP Client. See Configuring PPPoE on page 227 and DHCP client configuration on page 178.

### Permanent static route

The Branch Gateway enables you to configure a static route as a permanent route. Configuring this option prevents the static route from becoming inactive when the underlying Layer 2 interface is down. This prevents routing table updates from being sent each time an interface goes up or

down when there is a fluctuating Layer 2 interface on the static route. Configure the permanent option using the ip route command.

For example, the command ip route 193.168.10.0 24 serial 3/1:1 permanent creates a permanent static route to the network 193.168.10.0 24 via the serial 3/1:1 interface.

The command ip route 132.55.0.0 255.255.0.0 132.55.4.45 3 high creates a high static route to the network 132.55.0.0/255.255.0.0 using next-hop ip address 132.55.4.45 and with cost 3.

Permanent static routes should not be configured over Serial Layer 2 interfaces that participate in a Primary-Backup pair.

For more information on Backup interfaces, see <u>Backup interfaces</u> on page 234.



You cannot configure tracking on a permanent static route.

### **Discard routes**

### About this task

Discard route enables you to prevent forwarding traffic to specific networks. You can configure a static route that drops all packets destined to the route. This is called a discard route, indicated by the null0 parameter.

#### **Procedure**

Use the ip route<network><mask>nullo CLI command.



You cannot configure tracking on a discard route.

#### **Example**

For example, the command ip route 134.66.0.0 16 Nullo configures the network 134.66.0.0 16 as a discard route

### Summary of routing table commands

For more information about these commands, see Avaya Branch Gateway G450 CLI Reference.

Command	Description		
clear ip route	Delete all the dynamic routing entries from the routing table		
ip default-gateway	Define a default gateway for the router		
no ip default-gateway	Removes a default gateway for the router		
ip netmask-format	Specify the format of subnet masks in the output of show commands		
ip redirects	Enable the sending of redirect messages on the current interface		
no ip redirects	Disable the sending of redirect messages on the current interface		

Table continues...

Command	Description
ip route	Establish a static route
no ip route	Removes a static route
ip routing	Enable IP routing
show ip route	Display information about the IP routing table
show ip route best- match	Display a routing table for a destination address
show ip route static	Display static routes
show ip route summary	Display the number of routes known to the device
show ip route track- table	Display all routes with configured object trackers
traceroute	Trace the route packets are taking to a particular IP address by displaying the hops along the path
	The Branch Gateway traces the route by launching UDP probe packets with a small TTL, then listening for an ICMP time exceeded reply from a gateway.
	You can also trace the route inside a locally-terminated tunnel (GRE, VPN)

# **GRE tunneling**

Generic Routing Encapsulation (GRE) is a multi-carrier protocol that encapsulates packets with an IP header and enables them to pass through the Internet via a GRE tunnel. A GRE tunnel is a virtual interface in which two routers serve as endpoints. The first router encapsulates the packet and sends it over the Internet to a router at the far end of the GRE tunnel. The second router removes the encapsulation and sends the packet towards its destination.

A GRE tunnel is set up as an IP interface, which allows you to use the GRE tunnel as a routing destination. A GRE tunnel can transport multicast packets, which allows it to work with routing protocols such as RIP and OSPF.

To set up a GRE tunnel, you must create the interface and assign it an IP address, a tunnel source address, and a tunnel destination address. GRE tunnels can be configured as next hops on static routes and policy-based routing next hop lists. Packets can also be routed to GRE tunnels dynamically.

### Note:

There may be cases in which the GRE tunnel is not used for routing. In such cases, it may not be necessary to assign an IP address to the tunnel.

The main application for GRE tunneling is to allow packets that use protocols not supported on the Internet, or packets that use private IP addresses that cannot be routed on the Internet, to travel across the Internet. The following are examples of situations in which this can be useful:

- · Providing multiprotocol local networks over a single-protocol backbone
- Providing workarounds for networks containing protocols that have limited hop counts, such as AppleTalk
- Connecting discontinuous subnetworks
- Enabling virtual private networks (VPNs) over a WAN

You can also configure a GRE tunnel to serve as a backup interface. For information on configuring backup interfaces, see Backup interfaces on page 234.

For an example of a GRE tunneling application, see <u>GRE tunnel application example</u> on page 397.

# Packet routing to a GRE tunnel

Packets can be routed to a GRE tunnel in the following ways:

- The Tunnel interface is configured as the next hop in a static route. See <u>Routing table</u> configuration on page 387.
- The packet is routed to the Tunnel interface dynamically by a routing protocol (RIP or OSPF)
- The packet is routed to the Tunnel interface via policy-based routing. See Policy-based routing section.

# Prevention of nested tunneling in GRE tunnels

Nested tunneling occurs when the tunnel's next hop for its destination is another tunnel, or the tunnel itself. When the next hop is the tunnel itself, a tunnel loop occurs. This is also known as recursive routing.

When the Branch Gateway recognizes nested tunneling, it brings down the Tunnel interface and produces a message that the interface is temporarily disabled due to nested tunneling. The tunnel remains down until the tunnel is re-configured to eliminate the nested tunneling.

In addition to checking for nested tunneling, the Branch Gateway prevents loops in connection with GRE tunnels by preventing the same packet from being encapsulated more than once in the Branch Gateway.

### Reasons for nested tunneling in a GRE tunnel

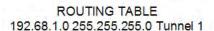
- A static route exists on the source tunnel endpoint that tells the tunnel to route packets addressed to the receiving tunnel endpoint via the tunnel itself
- The local endpoint of the tunnel learns the tunnel as a route to the tunnel's remote endpoint via OSPF or RIP

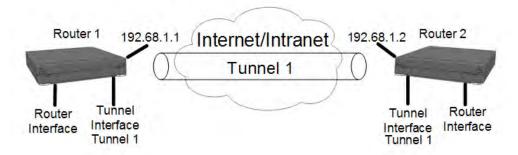
• A combination of static routes via parallel tunnels lead to a situation in which each tunnel is routing packets via another tunnel. For example:

```
Gxxx-001(super) # interface tunnel 1
Gxxx-001(super-if:Tunnel 1) # tunnel source x.x.x.x
Gxxx-001(super-if:Tunnel 1)# tunnel destination 1.0.0.1
Done!
Gxxx-001(super-if:Tunnel 1) # exit
Gxxx-001(super) # interface tunnel 2
Gxxx-001(super-if:Tunnel 2) # tunnel source x.x.x.x
Gxxx-001(super-if:Tunnel 2) # tunnel destination 2.0.0.1
Gxxx-001(super-if:Tunnel 2) # exit
Gxxx-001(super) # interface tunnel 3
Gxxx-001(super-if:Tunnel 3) # tunnel source x.x.x.x
Gxxx-001(super-if:Tunnel 3)# tunnel destination 3.0.0.1
Gxxx-001(super-if:Tunnel 3)# exit
Gxxx-001(super) # ip route 1.0.0.1 tunnel 2
Gxxx-001(super) # ip route 2.0.0.1 tunnel 3
Gxxx-001(super) # ip route 3.0.0.1 tunnel 1
Done!
```

Using the network shown in <u>Nested tunneling example</u> on page 393 as an illustration, if Router 1 has an entry in its routing table regarding the tunnel's receiving endpoint, this will cause an internal route in which all packets exiting the tunnel will be redirected back into the tunnel itself.

### **Nested tunneling example**





### Recommendations on avoiding nested tunneling

**Announce policy:** Configure a policy rule on the receiving tunnel endpoint (router 2) that causes the receiving endpoint to block advertisements of the source network (192.68.1.0) in its routing updates. This prevents the source endpoint (router 1) from learning the route. This solution is for nested tunneling caused by RIP. For example, using the network shown in <a href="Figure">Figure</a> on page 393 as an illustration, configure the following policy rule on router 2 and activate it on the router RIP with the matching interface:

```
Gxxx-001(super)# ip distribution access-list-name 1 "list #1"
Done!
Gxxx-001(super)# ip distribution access-default-action 1 default-action-permit
```

```
Done!
Gxxx-001(super)# ip distribution access-list 1 10 "deny"
   192.68.1.0 0.0.0.255
Done!
Gxxx-001(super)# router rip
Gxxx-001(super router:rip)# distribution-list 1 out FastEthernet 10/3
Done!
Gxxx-001(super router:rip)# exit
Gxxx-001(super)#
```

**Accept policy:** Configure a policy rule on the source tunnel endpoint (router 1) that will cause the source endpoint to not accept routing updates that include the source network (192.68.1.0). This solution is for nested tunneling caused by RIP. For example, using the network shown in <a href="Nested tunneling example">Nested tunneling example</a> on page 393 as an illustration, you would configure the following policy rule on router 1 and activate it on the router RIP with the matching interface:

```
Gxxx-001(super)# ip distribution access-list-name 1 "list #1"
Done!
Gxxx-001(super)# ip distribution access-default-action 1 default-action-permit
Done!
Gxxx-001(super)# ip distribution access-list 1 10 "deny"
    192.68.1.0 0.0.0.255
Done!
Gxxx-001(super)# router rip
Gxxx-001(super router:rip)# distribution-list 1 in FastEthernet 10/3
Done!
Gxxx-001(super router:rip)# exit
Gxxx-001(super)#
```

**Static route:** Configure a static rule on router 1 telling it the route for packets destined to the tunnel's receiving endpoint (192.68.1.2). This route should be configured with a high route preference. For example:

```
Gxxx-001(super) # ip route 192.68.1.2 255.255.0.0 192.68.1.3 high permanent Done!
Gxxx-001(super) #
```

# **Optional GRE tunnel features**

You can configure optional features in GRE tunnels. The tunnel keepalive feature enables periodic checking to determine if the tunnel is up or down. The dynamic MTU discovery feature determines and updates the lowest MTU on the current route through the tunnel.

# Keepalive feature

The tunnel keepalive feature sends keepalive packets through the Tunnel interface to determine whether the tunnel is up or down. This feature enables the tunnel's source interface to inform the host if the tunnel is down. When the tunnel keepalive feature is not active, if the tunnel is down, the tunnel's local endpoint continues to attempt to send packets over the tunnel without informing the host that the packets are failing to reach their destination.

# **Enabling the keepalive feature**

### **Procedure**

Use the **keepalive** command in the GRE Tunnel interface context to enable the tunnel keepalive feature.

### Note:

You do not have to configure tunnel keepalive on both sides of the tunnel.

Use the **no** form of this command to deactivate the feature.

### Example

The following example configures Tunnel 1 to send keepalive packets every 20 seconds. If the tunnel's destination interface fails to respond to three consecutive packets, the tunnel's source interface concludes that the tunnel is down. The source interface continues to send keepalive packets, but until it receives a response from the tunnel's destination interface, the tunnel informs hosts that send packets to the tunnel that the tunnel is down.

```
Gxxx-001# interface tunnel 1
Gxxx-001(if:Tunnel 1)# keepalive 20 3
Done!
```

### **Keepalive command parameters**

The **keepalive** command includes the following parameters:

**seconds:** The length, in seconds, of the interval at which the source interface sends keepalive packets. The default value is 10.

retries: The number of retries after which the source interface declares that the tunnel is down. The default value is 3.

### **Dynamic MTU discovery**

The size of packets that can travel through a GRE tunnel is limited by the lowest MTU of any router along the route through the tunnel. When dynamic MTU discovery is enabled, the tunnel maintains an MTU limit.

When a large packet is sent from the host with the DF bit on, and a router in the tunnel path has an MTU that is smaller than the size of the packet, since the DF bit is set, the router sends an ICMP unreachable message back in the originator (in this case, the GRE router). The GRE router then updates the tunnel's MTU limit accordingly. When a packet larger than the MTU arrives at the tunnel, if the packet is marked "do not fragment", the tunnel's source interface sends the packet back to the host requesting the host to fragment the packet. When dynamic MTU discovery is disabled, the tunnel's source interface marks each packet as *may be fragmented*, even if the packet's original setting is *do not fragment*. For more information on MTU and fragmentation, refer to <u>Fragmentation</u> on page 426.

### Enabling and deactivating dynamic MTU discovery Procedure

- 1. Use the tunnel path-mtu-discovery command in the GRE Tunnel interface context to enable dynamic MTU discovery by the tunnel.
- 2. To deactivate the feature, use the no tunnel path-mtu-discovery command.

### tunnel path-mtu-discovery parameters

The tunnel path-mtu-discovery command includes the following parameters:

age-timer: How long until the local tunnel endpoint returns the tunnel MTU to its default. The default value of this parameter is 10 minutes.

infinite: The tunnel does not update the MTU, and its value remains permanent

### Setting up a GRE tunnel

### **Procedure**

1. Enter interface tunnel, followed by a number identifying the tunnel, to create the new Tunnel interface.

If you are changing the parameters of an existing tunnel, enter interface tunnel, followed by a number identifying the tunnel, to enter the Tunnel context.

### For example:

```
Gxxx-001(super) # interface tunnel 2
Gxxx-001(super-if:Tunnel 2) #
```

2. In the Tunnel interface context, enter tunnel source, followed by the public IP address of the local tunnel endpoint, to set the source address of the tunnel.

#### For example:

```
Gxxx-001(super-if:Tunnel 2) # tunnel source 70.70.70.2
Done!
Gxxx-001(super-if:Tunnel 2) #
```

3. In the Tunnel interface context, enter tunnel destination, followed by the IP address of the remote tunnel endpoint, to set the destination address of the tunnel.

#### For example:

```
Gxxx-001(super-if:Tunnel 2) # tunnel destination 20.0.1.1
Done!
Gxxx-001(super-if:Tunnel 2) #
```



### Note:

The Branch Gateway does not check whether the configured tunnel source IP address is an existing IP address registered with the Branch Gateway router.

4. In most cases, it is recommended to configure keepalive in the tunnel so that the tunnel's source interface can determine and inform the host if the tunnel is down.

For more information on keepalive, see Keepalive feature on page 394.

To configure keepalive for a Tunnel interface, enter **keepalive** in the Tunnel interface context, followed by the length (in seconds) of the interval at which the source interface sends keepalive packets, and the number of retries necessary in order to declare the tunnel down.

The following example configures the tunnel to send a keepalive packet every 20 seconds, and to declare the tunnel down if the source interface sends three consecutive keepalive packets without a response.

```
Gxxx-001(super-if:Tunnel 2) # keepalive 20 3
Done!
Gxxx-001(super-if:Tunnel 2) #
```

5. In most cases, it is recommended to configure dynamic MTU discovery in the tunnel.

This prevents fragmentation of packets larger than the tunnel's MTU. When dynamic MTU discovery is not enabled, the tunnel fragments packets larger than the tunnel's MTU, even when the packet is marked *do not fragment*. For more information on dynamic MTU discovery, see <a href="Dynamic MTU discovery">Dynamic MTU discovery</a> on page 395.

The following example configures dynamic MTU discovery, with an age timer of 15 minutes.

```
Gxxx-001(super-if:Tunnel 2)# tunnel path-mtu-discovery age-timer 15
Done!
Gxxx-001(super-if:Tunnel 2)#
```

6. Enter copy running-config startup-config.

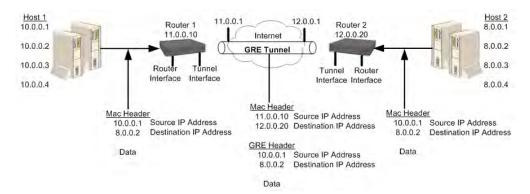
This saves the new Tunnel interface configuration in the startup configuration file.

### Result

For a list of optional GRE tunnel features, refer to <u>Optional GRE tunnel features</u> on page 394. For a list of additional GRE tunnel CLI commands, refer to <u>Summary of GRE tunneling commands</u> on page 398.

# **GRE tunnel application example**

This section provides an example of a GRE tunnel application and its configuration.



In the example shown in this figure, Host 1 and Host 2 are private networks using a GRE tunnel to connect them via the Internet. 11.0.0.10 and 12.0.0.20 are public IP addresses used by the GRE tunnel for the tunnel encapsulation.

A packet originating from 10.0.0.1 on Host 1 is sent to the destination 8.0.0.2 on Host 2. Since the destination IP address is a private IP address, the packet cannot be routed as is over the Internet. Instead, Router 1 receives the packet from host 1, looks up the packet's destination address in its

routing table, and determines that the next hop to the destination address is the remote end of the GRE tunnel.

Router 1 encapsulates the packet with a GRE header and a new IP header that assigns the IP address of Router 2 (12.0.0.20) as the destination IP address and the IP address of Router 1 (11.0.0.10) as the source IP address. When the packet arrives at Router 2, which is the end point of the GRE tunnel, Router 2 removes the outer IP header and the GRE header and sends the packet to its original destination at IP address (8.0.0.2).

You can use the following commands to configure GRE tunneling (with OSPF) in this example:

### **Example**

### Router 1 configuration

```
Gxxx-001(super) # interface fastethernet 10/3
Gxxx-001(super-if:FastEthernet 10/3)# ip address 11.0.0.10 255.255.255.0
Gxxx-001(super-if:FastEthernet 10/3)# exit
Gxxx-001(super) # interface tunnel 1
Gxxx-001(super-if:Tunnel 1) # keepalive 10 3
Gxxx-001(super-if:Tunnel 1) # tunnel source 11.0.0.10
Done!
Gxxx-001(super-if:Tunnel 1) # tunnel destination 12.0.0.20
Gxxx-001(super-if:Tunnel 1)# ip address 1.1.1.1 255.255.255.0
Done!
Gxxx-001(super-if:Tunnel 1)# exit
Gxxx-001(super) # ip route 12.0.0.0 255.255.255.0 11.0.0.1 1 high
Gxxx-001(super) # router ospf
Gxxx-001(super router:ospf)# network 1.1.1.0 0.0.0.255 area 0.0.0.0
Gxxx-001(super router:ospf)# exit
Gxxx-001(super)#
```

### **Example**

### Router 2 configuration

```
Gxxx-001(super)# interface vlan 1
Gxxx-001(super-if:Vlan 1)# ip address 12.0.0.10 255.255.255.0
Gxxx-001(super-if:Vlan 1)# exit
Gxxx-001(super)# interface tunnel 1
Gxxx-001(super-if:Tunnel 1)# tunnel source 12.0.0.20
Done!
Gxxx-001(super-if:Tunnel 1)# tunnel destination 11.0.0.10
Done!
Gxxx-001(super-if:Tunnel 1)# ip address 1.1.1.2 255.255.255.0
Gxxx-001(super-if:Tunnel 1)# exit
Gxxx-001(super)# ip route 11.0.0.0 255.255.255.0 12.0.0.1 1 high
Gxxx-001(super)# router ospf
Gxxx-001(super router:ospf)# network 1.1.1.0 0.0.0.255 area 0.0.0.0
Done!
Gxxx-001(super router:ospf)# exit
Gxxx-001(super)#
```

# Summary of GRE tunneling commands

For more information about these commands, see Avaya Branch Gateway G450 CLI Reference.

Root level command	Command	Description
interface tunnel		Enter tunnel interface configuration context, create a Tunnel interface if it does not exist, or delete a Tunnel interface or sub-interface
	keepalive	Enable the tunnel keepalive feature
	tunnel checksum	Add a checksum to the GRE header of packets traveling through the tunnel
		When a checksum is included on one endpoint, the receiving tunnel endpoint performs checksum validation on incoming packets and packets without a valid checksum are discarded.
	no tunnel checksum	Disables checksums
	tunnel destination	Set the destination address of the tunnel
	tunnel dscp	Assign a DSCP value to packets traveling through the tunnel
		The DSCP value is placed in the packet's Carrier IP header. You can assign a DSCP value of from 0 to 63. If you do not assign a DSCP value, the DSCP value is copied from the packet's original IP header.
		Note:
		The Carrier IP header identifies the source and destination IP address of the tunnel.
	tunnel key	Enable and set an ID key for the tunnel
		Tunnel ID keys are used as a security device. The key must be set to the same value on the tunnel endpoints. Packets without the configured key must be discarded.
	no tunnel key	Disables key checking
	tunnel path- mtu- discovery	Enable dynamic MTU discovery by the tunnel
	tunnel source	Set the source address of the tunnel
	tunnel ttl	Assign a TTL value to packets traveling through the tunnel
		The TTL value is placed in the packet's Carrier IP header. You can assign a TTL value of from 1 to 255. The default tunnel TTL value is 255.

Root level command	Command	Description
show interfaces tunnel		Show interface configuration and statistics for a particular tunnel or all GRE tunnels
		If the Tunnel interface is down, this command displays the MTU value as not available.

# **DHCP and BOOTP relay**

You can configure the router to relay Dynamic Host Configuration Protocol (DHCP) and BOOTstrap Protocol (BOOTP) client broadcasts to a server on a different segment of the network. When you configure DHCP and BOOTP relay, you can control how the router relays DHCP and BOOTP packets. The router also relays replies from the server back to the client. The Branch Gateway can alternatively function as a DHCP server, providing DHCP service to local devices. For information about configuring DHCP server on the Branch Gateway, see <a href="DHCP server">DHCP server</a> on page 402. For information about configuring DHCP client on the Branch Gateway, see <a href="DHCP server">DHCP server</a> on page 178.

### **DHCP**

DHCP assigns dynamic IP addresses to devices on a network. With dynamic addressing, a device can have a different IP address whenever the device connects to the network. In some systems, the device's IP address can even change while it is still connected. DHCP also supports a mix of static and dynamic IP addresses.

Dynamic addressing simplifies network administration because the software keeps track of IP addresses rather than requiring an administrator to manage the task. This means you can add a new computer to a network without needing to manually assign a unique IP address. Many ISPs use dynamic IP addressing for dial-up users. However, dynamic addressing may not be desirable for a network server.

# **BOOTP**

BOOTP is an Internet protocol that allows a diskless workstation to discover the following:

- · Its own IP address
- The IP address of a BOOTP server on the network
- A file to be loaded into memory to boot the workstation

BOOTP allows the workstation to boot without requiring a hard disk or floppy disk drive. It is used when the user or station location changes frequently. The protocol is defined by RFC 951.

# **DHCP/BOOTP** relay

The Branch Gateway supports the DHCP/BOOTP relay agent function. This is an application that accepts DHCP/BOOTP requests that are broadcast on one VLAN. The application sends them to

a DHCP/BOOTP server. That server connects to another VLAN or a server that might be located across one or more routers that might otherwise not get the broadcast request. The relay agent handles the DHCP/BOOTP replies as well. The relay agent transmits the replies to the client directly or as broadcast, according to a flag in the reply message.

### Note:

The same DHCP/BOOTP relay agent serves both the BOOTP and DHCP protocols.

When there is more than one IP interface on a VLAN, the Branch Gateway chooses the lowest IP address on this VLAN when relaying DHCP/BOOTP requests. The DHCP/BOOTP server then uses this address to decide the network from which to allocate the address. When there are multiple networks configured, the Branch Gateway performs a round-robin selection process.

When the DHCP/BOOTP server is configured to allocate addresses only from a single subnetwork among the different subnetworks defined on the VLAN, you might need to configure the Branch Gateway with the relay address on that subnet so the DHCP/BOOTP server can accept the request.

DHCP/BOOTP Relay in the Branch Gateway is configurable per VLAN and allows for two DHCP/ BOOTP servers to be specified. In this case, the Branch Gateway duplicates each request, and sends it to both servers. This duplication provides redundancy and prevents the failure of a single server from blocking hosts from loading. You can enable or disable DHCP/BOOTP Relay in the Branch Gateway.

# Summary of DHCP and BOOTP relay commands

For more information about these commands, see Avaya Branch Gateway G450 CLI Reference.

Root level command	Command	Description
interface (fastethernet  VLAN)		Enter the FastEthernet or VLAN interface configuration context
	ip bootp-dhcp network	Select the network from which the BOOTP/DHCP server should allocate an address
		This command is required only when there are multiple IP interfaces over the VLAN. You must be in an interface context to use this command
	no ip bootp-dhcp network	Restores the default value.
	ip bootp-dhcp server	Add or remove a BOOTP/DHCP server to handle BOOTP/DHCP requests received by the current interface
		A maximum of two servers can be added to a single interface. You must be in an interface context to use this command

Root level command	Command	Description
	no ip bootp-dhcp server	Removes a server.
ip bootp-dhcp relay		Enable or disable relaying of BOOTP and DHCP requests to the BOOTP/DHCP server
		You must be in general context to use this command.
no ip bootp-dhcp relay		Disables the relaying of BOOTP and DHCP requests.

## **DHCP** server

The Branch Gateway supports DHCP server. DHCP server is a protocol for automatically assigning IP addresses and other configuration parameters to clients on a TCP/IP network. DHCP server minimizes the maintenance of a network of, among other things, IP telephones and PCs, by removing the need to assign and maintain IP addresses and other parameters for each device on the network individually.

Since a DHCP server can be configured on the Branch Gateway, local branch devices are not dependant on receiving configuration parameters over the WAN from a remote DHCP server and, therefore, can be assigned IP configuration parameters in case of WAN failure.

The Branch Gateway supports the following DHCP server features:

- Up to 32 DHCP pools
- Up to 120 users
- Up to 1024 IP addresses for all DHCP pools together
- · Automatic and reservation pools
- Standard DHCP options and IP phone and wireless special options
- Vendor specific information option
- · DHCP relay packets
- · Global statistics
- Syslog/traps for special events

The Branch Gateway can function as a DHCP server, as a DHCP relay, or both simultaneously, with each interface configured in either DHCP server mode or DHCP relay mode. For example, you can configure the Branch Gateway to provide DHCP service to voice devices while DHCP requests by data devices are routed to a central remote DHCP server using DHCP relay.

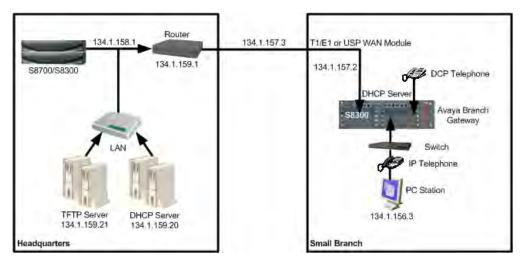
The Branch Gateway can function as a DHCP server or as a DHCP client, or both simultaneously. For information about configuring DHCP client on the Branch Gateway, see <a href="DHCP client">DHCP client</a> configuration on page 178.

### Related links

**DHCP client configuration on page 178** 

# Typical DHCP server application

In the typical application shown in the following table, the Branch Gateway is configured as a local DHCP server and router for IP phones and PCs in the branch office. The remote DHCP server allocates IP addresses for headquarters users. The local DHCP server allocates IP addresses in the branch offices. If there is a local ICC or LSP, calls can still be made. If there is no ICC or LSP to control calls, the DHCP server can allocate IP addresses to all devices, but, since no calls can be made, the IP address allocation effectively applies to PCs only.



The branch DHCP server does not depend on the headquarters' DHCP server. There is no backup mechanism between the servers. The branch DHCP server operates continually regardless of the status of the centralized DHCP server or the WAN link.

By default, the DHCP server is inactive. Before activating DHCP server, you configure DHCP pools to define ranges of IP addresses and other network configuration information to be assigned to clients. Create a minimum of two dynamic pools: at least one pool for data devices (PCs) and at least one pool for voice devices (IP phones). The Branch Gateway also supports reservation pools, which map hardware addresses/client identifiers to specific IP addresses. Reservation pools may be required for security issues or servers.

Overlap between pools is not allowed. You cannot configure a reservation pool on an IP address that falls within the range of another pool.

# **Configuring the DHCP server**

### **Procedure**

- 1. Enter ip dhcp pool, followed by a number from 1 to 32, to create a DHCP pool.
- 2. Use the name command to configure the pool's name.

3. Configure a range of available IP addresses that the DHCP server may assign to clients, using start-ip-addr to set the start IP address of the range and end-ip-addr to set the end IP address of the range.

Consider the following:

- For a manual/reservation pool, set identical IP addresses for the start and end IP addresses
- The start IP address and end IP address must be on the same network according to the subnet mask
- The start IP address must be lower than the end IP address
- The combined number of IP addresses in all pools must not exceed 256 addresses
- Both the start IP address and end IP address can be up to 223.255.255.255
- The start IP address and end IP address may not be network/broadcast addresses according to the subnet mask
- 4. Use the subnet-mask command to configure the subnet mask of the pool.
- 5. Use the lease command to configure the lease period for IP address assignment. By default, the lease is eight days.
- 6. For a manual/reservation pool, use the client identifier command to reserve the pool's IP address for assignment to a specific client.
  - To configure a reservation, the start IP address and end IP address must be identical. You cannot configure more than one reservation on a single pool.
- 7. Configure DHCP options for the pool, if required.
  - See Configuring options on page 405 and, for vendor specific options, Configuring vendorspecific options on page 406.
- 8. Repeat steps 1 to 7 to configure as many DHCP pools as you require.
  - You can configure up to 32 DHCP pools. By default, all pools are inactive until you activate them. This enables you to modify each pool's configuration without affecting network devices.
- 9. Activate each of the DHCP pools you configured using the ip dhcp activate pool command in general context, followed by the pool number.
- 10. Enter ip dhcp-server to activate DHCP server.
  - DHCP server is now active. If you change the pool configuration, it is recommended to do so while the pool is active.



### Note:

If you try to configure a new start and end IP address that is not part of the current network and beyond the allowed maximum of 256 IP addresses, first use the no

start ip address and no end ip address commands before configuring the new start and end IP addresses.

# **Configuring options**

### About this task

DHCP options are various types of network configuration information that the DHCP client can receive from the DHCP server. The Branch Gateway supports all DHCP options. The most common options used for IP phones are listed in Common user-configurable DHCP options on page 405. Some options are configured with specific CLI commands that are also listed in Common user-configurable DHCP options on page 405. Options 0, 50, 51, 52, 53, 54, 55, 56, and 255 are not configurable.

### **Procedure**

1. Use the option command to specify the option code and enter the context for the option.



### ☑ Note:

To configure an option that is listed in Common user-configurable DHCP options on page 405 with an entry in the "Specific command" column, use the specific command instead of the option command.

- 2. Use the name command to set the name of the DHCP option (optional).
- 3. Use the value command to enter the option data type and the option data.

### Common user-configurable DHCP options

Option	Description	Specific command
1	Subnet Mask	subnet-mask
3	Router	default-router
6	Domain name server	dns_server
7	Log Server	
15	Domain Name	domain-name
43	vendor-specific information	vendor-specific-option
44	Wins/NBNS server	
46	Wins/NBT Node Type	
51	IP Address Lease Time	lease
66	TFTP server name	
69	SMTP server	
176	Avaya IP phone private	

### **Configuring vendor-specific options**

### About this task

You can configure an option unique to an individual vendor class. This is called a vendor-specific option (option 43).

### **Procedure**

- 1. Use the **vendor-specific-option** command to create a vendor-specific option with a unique index.
- 2. Use the name command to name the option (optional).
- 3. Use the class-identifier command to set a vendor-specific identifier.
- 4. Use the value command to set the data type and value of the vendor-specific option.

# Deleting an IP address binding

### About this task

When the DHCP server detects an IP address conflict after attempting to allocate an IP address that is already in use, the server locks the IP address for half an hour by marking the IP address with client identifier 00:00:00:00:00:00:00. If you have solved the conflict within half an hour, you can use this command to free the IP address for reallocation

### **Procedure**

To delete an IP address binding, use the clear ip dhcp-server binding command.

# **DHCP** pool configuration examples

The following example defines a dynamic pool for voice devices:

```
Gxxx-001(super) # ip dhcp pool 1
Gxxx-001(super-DHCP 1) # name "IP phone Pool"
Done!
Gxxx-001(super-DHCP 1) # start-ip-addr 135.64.20.2
Gxxx-001(super-DHCP 1) # end-ip-addr 135.64.20.30
Gxxx-001(super-DHCP 1) # subnet-mask 255.255.255.0
Done!
Gxxx-001(super-DHCP 1) # default-router 135.64.20.1
Done!
Gxxx-001(super-DHCP 1)# option 176
Gxxx-001(super-DHCP 1/option 176) # name "Avaya IP phone option"
Gxxx-001(super-DHCP 1/option 176) # value ascii "MCIPADD=10.10.2.140,
MCPORT=1719, TFTPSRVR=10.10.5.188"
Gxxx-001(super-DHCP 1/option 176) # exit
Gxxx-001(super-DHCP 1) # exit
Gxxx-001(super) # ip dhcp activate pool 1
Done!
Gxxx-001(super) # ip dhcp-server
Done!
Gxxx-001(super)#
```

### The following example defines a dynamic pool for data devices:

```
Gxxx-001(super)# ip dhcp pool 2
Gxxx-001(super-DHCP 2) # name "Data Pool"
Done!
Gxxx-001(super-DHCP 2) # start-ip-addr 135.64.20.34
Done!
Gxxx-001(super-DHCP 2) # end-ip-addr 135.64.20.60
Gxxx-001(super-DHCP 2) # subnet-mask 255.255.255.0
Gxxx-001(super-DHCP 2) # default-router 135.64.20.33
Done!
Gxxx-001 (super-DHCP 2) # dns-server 10.10.1.1
Done!
Gxxx-001(super-DHCP 2) # domain-name my.domain.com
Gxxx-001(super-DHCP 2)# option 176
Gxxx-001(super-DHCP 2/option 176)# value ascii "MCIPADD=192.168.50.17,
192.168.50.15, MCPORT=1719, TFTPSRVR=192.168.50.1, TFTPDIR=/phonedir/"
Gxxx-001(super-DHCP 2/option 176)# exit
Gxxx-001(super-DHCP 2) # exit
Gxxx-001(super) # ip dhcp activate pool 2
Done!
Gxxx-001(super) # ip dhcp-server
Done!
Gxxx-001(super)#
```

### The following example configures a vendor-specific option for DHCP pool 5:

```
Gxxx-001(super-DHCP 5) # vendor-specific-option 1
Gxxx-001(super-DHCP 5/vendor specific 1) # class-identifier"ccp.avaya.com"
Done!
Gxxx-001(super-DHCP 5/vendor specific 1) # value raw ascii "gfdgfd"
Done!
Gxxx-001(super-DHCP 5/vendor specific 1) # exit
Gxxx-001(super-DHCP 5) #
```

### The following example defines a reservation pool for data devices:

```
Gxxx-001(super) # ip dhcp pool 3
Gxxx-001(super-DHCP 3) # name "Data 1 Server"
Gxxx-001(super-DHCP 3) # start-ip-addr 135.64.20.61
Done!
Gxxx-001(super-DHCP 3) # end-ip-addr 135.64.20.61
Done!
Gxxx-001(super-DHCP 3) # subnet-mask 27
Gxxx-001(super-DHCP 3) # client identifier 01:11:22:33:44:55:66
Done!
Gxxx-001(super-DHCP 3) # default-router 135.64.20.33
Done!
Gxxx-001(super-DHCP 3) # dns-server 10.10.1.1
Done!
Gxxx-001(super-DHCP 3)# exit
Gxxx-001(super) # ip dhcp activate pool 3
Done!
Gxxx-001(super)#
```

# Commands for displaying DHCP server information

• show ip dhcp-pool

- show ip dhcp-server bindings
- show ip dhcp-server statistics

For more information about these commands, see <u>Summary of DHCP Server commands</u> on page 408 or the *Avaya Branch Gateway G450 CLI Reference*.

# **Summary of DHCP Server commands**

For more information about these commands, see Avaya Branch Gateway G450 CLI Reference.

Root level command	First level command	Second level command	Description
clear ip dhcp- server binding			Delete IP address binding
clear ip dhcp-server statistics			Clear the statistics of the DHCP server
ip dhcp activate pool			Activate configured DHCP pools
ip dhcp ping packets			Enable the sending of a ping packet by the DHCP server to check if the IP address it is about to allocate is already in use by another client
ip dhcp ping timeout			Set the time the DHCP server waits for a reply to a sent ping packet before allocating an IP address to a DHCP client
ip dhcp pool			Create a DHCP pool
	bootfile		Provide startup parameters for the DHCP client device
	client- identifier		Reserve the pool's IP address for assignment to a specific client
	default- router		Set up to eight default router IP addresses in order of preference
	dns-server		Set up to eight Domain Name Server (DNS) IP addresses
	domain-name		Set a domain name string for the client
	end-ip-addr		Set the end IP address of the range of available IP addresses that the DHCP server may assign to clients

Root level command	First level command	Second level command	Description
	lease		Configure the lease period for IP address assignment
	name		Configure the pool's name
	next-server		Specify the IP address of the next server in the boot process of a DHCP client
	option		Enter the context of a DHCP option
		name	Configure a name for the DHCP option
		value	Enter the option data type and the option data
	server-name		Specify the optional server name in the boot process of a DHCP client
	show ip dhcp- pool		Display DHCP pool configurations
	start-ip-addr		Set the start IP address of the range of available IP addresses that the DHCP server may assign to clients
	subnet-mask		Configure the subnet mask of the pool
	vendor- specific- option		Create a vendor-specific option with a unique index
		name	Name the vendor-specific option
		class-identifier	Set a vendor-specific identifier
		value	Set the data type and value of the vendor-specific option
ip dhcp-server			Activate DHCP server
show ip dhcp- server bindings			Display bindings
show ip dhcp-server statistics			Display DHCP server statistic

# **Broadcast relay**

When you configure broadcast relay, the router forwards broadcast packets across interfaces. You can configure broadcast relay types including directed broadcast forwarding, NetBIOS rebroadcast, DHCP, and BOOTP client broadcast.

For more information about DHCP and BOOTP client broadcast, see <u>DHCP and BOOTP relay</u> on page 400.

# **Directed broadcast forwarding**

### About this task

A directed broadcast is an IP packet whose destination address is the broadcast address of a network or subnet. A directed broadcast causes every host on the network to respond. You can use directed broadcasts to obtain a list of all active hosts on the network. A hostile user can exploit directed broadcasts to launch a denial-of-service attack on the network. For each interface on the Branch Gateway, you can configure whether the Branch Gateway forwards directed broadcast packets to the network address or subnet mask address of the interface.

#### **Procedure**

Enter ip directed-broadcast to enable directed broadcast forwarding on an interface. Use the no form of this command to disable directed broadcast forwarding on an interface.

### **NetBIOS** rebroadcast

Network Basic Input Output System (NetBIOS) is a protocol for sharing resources among desktop computers on a LAN. You can configure the Branch Gateway to relay NetBIOS UDP broadcast packets. This feature is used for applications such as WINS that use broadcast but might need to communicate with stations on other subnetworks or VLANs.

Configuration is performed on a per-interface basis. A NetBIOS broadcast packet arrives from an interface on which NetBIOS rebroadcast is enabled. The packet is distributed to all other interfaces configured to rebroadcast NetBIOS.

- If the NetBIOS packet is a net-directed broadcast, for example, 149.49.255.255, the packet is relayed to all other interfaces on the list, and the IP destination of the packet is replaced by the appropriate interface broadcast address.
- If the NetBIOS broadcast packet is a limited broadcast, for example, 255.255.255.255, it
  is relayed to all VLANs on which there are NetBIOS-enabled interfaces. In that case, the
  destination IP address remains the limited broadcast address.

# Summary of broadcast relay commands

For more information about these commands, see Avaya Branch Gateway G450 CLI Reference.

Root level command	Command	Description
<pre>interface (dialer  fastethernet  tunnel  vlan)</pre>		Enter the Dialer, FastEthernet, Tunnel, or VLAN interface context
	ip directed- broadcast	Enable or disable directed broadcast forwarding on the interface
	ip netbios- rebroadcast	Enable or disable NetBIOS rebroadcasts on the interface

### ARP table

When you configure the Address Resolution Protocol (ARP) table, you can:

- View information about the ARP table
- · Add entries to the ARP table
- Delete entries from the ARP table
- Configure the ARP timeout

### Overview of ARP

IP logical network addresses are independent of physical addresses. The physical address must be used to convey data in the form of a frame from one device to another. Therefore, a mechanism is required to acquire a destination device hardware address from its IP address. This mechanism is called ARP.

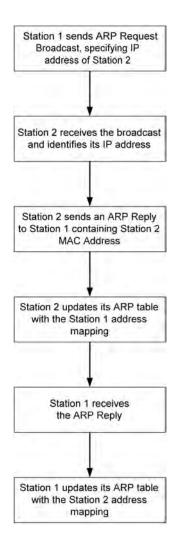
# Static and dynamic table entries

The ARP table stores pairs of IP and MAC addresses. This storage saves time and communication costs, since the host looks in the ARP table first when transmitting a packet. If the information is not there, then the host sends an ARP Request.

There are two types of entries in the ARP table:

Static ARP table entries: Static ARP table entries do not expire.

**Dynamic ARP table entries:** Dynamic ARP table entries are mappings between IP addresses and MAC addresses that the switch used recently. Dynamic ARP table entries expire after a configurable amount of time. The following diagram shows how a switch adds dynamic ARP table entries:



# Adding static ARP table entries

### **Procedure**

To add static ARP table entries manually, use the arp command.

For example, to add a static ARP table entry for station 192.168.7.8 with MAC address 00:40:0d:8c:2a:01, use the following command:

Gxxx-001# arp 192.168.7.8 00:40:0d:8c:2a:01

# Removing static and dynamic entries

### **Procedure**

To remove static and dynamic entries from the ARP table, use the no arp command.

For example, to remove the ARP table entry for the station 192.168.13.76:

Gxxx-001# no arp 192.168.13.76

# Changing an entry in the ARP table

### **Procedure**

To change an entry in the ARP table, delete the entry and reinsert it with revised parameters.

# **Summary of ARP table commands**

For more information about these commands, see Avaya Branch Gateway G450 CLI Reference.

Command	Description
arp	Add a permanent entry to the ARP table
no arp	Remove either a static entry or a dynamically-learned entry from the ARP table
arp timeout	Configure the amount of time, in seconds, that an entry remains in the ARP table
	Entering this command without a time parameter displays the current timeout value.
no arp timeout	Restore the default value (four hours)
clear arp-cache	Delete all dynamic entries from the ARP table and the IP route cache
ip max-arp-entries	Specify the maximum number of ARP table entries allowed in the ARP table
no ip max-arp- entrie	Restore the maximum number of ARP table entries allowed in the ARP table to default value
show ip arp	Display a list of the ARP resolved MAC to IP addresses in the ARP table
show ip reverse-	Display the IP address of a host, based on a known MAC address

# **Proxy ARP**

The Branch Gateway supports proxy ARP. Proxy ARP is a technique by which a router provides a false identity when answering ARP requests intended for another device. By falsifying its identify, the router accepts responsibility for routing packets to their true destination.

Proxy ARP can help devices on a subnet to reach remote subnets without the need to configure routing or a default gateway.

# **Summary of Proxy ARP commands**

For more information about these commands, see Avaya Branch Gateway G450 CLI Reference.

Root level command	Command	Description
interface (fastethernet		Enter the FastEthernet or VLAN interface context
vlan)		

Root level command	Command	Description
	ip proxy-arp	Enable proxy ARP on an Branch Gateway interface
	no ip proxy-arp	Disable proxy ARP on an interface

# **ICMP** errors

You can control whether the router sends Internet Control Message Protocol (ICMP) error messages. The router sends an ICMP error message to the source of a packet if the router rejects the packet.

# **Summary of ICMP errors commands**

For more information about these commands, see Avaya Branch Gateway G450 CLI Reference.

Command	Description
ip icmp-errors	Set ICMP error messages to ON or OFF
show ip icmp	Display the status (enabled or disabled) of ICMP error messages

# **RIP**

The Routing Information Protocol (RIP) enables routers to compute the path that an IP packet should follow. Routers exchange routing information using RIP to determine routes that other routers are connected to. OSPF is a newer protocol that serves a similar purpose. For more information about OSPF, see <a href="OSPF">OSPF</a> on page 419.

You can configure route redistribution between OSPF, RIP, and static routes. With route redistribution, you can configure the Branch Gateway to redistribute routes learned from one protocol into the domain of the other routing protocol. For more information, see <a href="Route redistribution">Route Route redistribution</a> on page 422.

RIP is a distance vector protocol. The router decides which path to use on distance or the number of intermediate hops. In order for this protocol to work correctly, all the routers, and possibly the nodes, need to gather information on how to reach each destination in the Internet. However the very simplicity of RIP has a disadvantage. This protocol does not take into account network bandwidth, physical cost, and data priority. The Branch Gateway supports two versions of RIP:

- RIPv1 on page 415
- RIPv2 on page 415

### RIPv1

RIPv1 is the original version of the RIP protocol. The RIPv1 protocol imposes some limitations on the network design with regard to subnetting. When operating RIPv1, you must not configure variable length subnetwork masks (VLMS). Each IP network must have a single mask, implying that all subnetworks in a given IP network are of the same size. Also, when operating RIPv1, you must not configure supernets. RIPv1 is defined in RFC 1058.

### RIPv2

RIPv2 is a newer version of the RIP routing protocol. RIPv2 solves some of the problems associated with RIPv1. The most important change in RIPv2 is the addition of a **subnetwork mask** field which allows RIPv2 to support variable length subnetworks. RIPv2 also includes an authentication mechanism similar to the one used in OSPF. RIPv2 is defined in RFC 2453. For more information, see RIPv1 vs. RIPv2 on page 415.

### RIPv1 vs. RIPv2

RIPv1	RIPv2
Broadcast addressing	Multicast addressing
Timer-based – updated every 30 seconds	Timer-based – updated every 30 seconds
Fixed subnetwork masks	VLSM support – subnet information transmitted
No security	Security (authentication)
No provision for external protocols	Provision for EGP/BGP (Route tag)

# Prevention of routing loops in RIP

You can use the following features in RIP to help avoid routing loops:

- Split-horizon: The split-horizon technique prevents information about routes from exiting the router interface through which the information was received. This prevents small routing loops.
- Poison-reverse: Poison-reverse updates explicitly indicate that a network or subnet is unreachable. Poison-reverse updates are sent to defeat large routing loops.

For information on the CLI commands, see <u>Commands used to prevent routing loops in RIP</u> on page 415

# Commands used to prevent routing loops in RIP

### Split-horizon technique

- Enter ip rip split-horizon to enable the split-horizon mechanism.
- Use the **no** form of this command to disable the split-horizon mechanism. By default, split-horizon is enabled.

### Poison-reverse updates

- Enter ip rip poison-reverse to enable split-horizon with poison-reverse on an interface.
- Use the no form of this command to disable the poison-reverse mechanism.

### RIP distribution access lists

RIP distribution access lists consist of rules that specify how a router distributes and accepts RIP routing information from other routers. Before sending an update, the router consults an access list to determine if it should include specific routes in the update. When receiving an update, the router first checks a set of rules which apply to incoming updates to determine if it should insert those routes into its routing table. You can assign the rules per interface and per direction.

You can configure up to 99 RIP distribution access lists on the Branch Gateway.

# Configuring a distribution access list example

### About this task

For example, to configure RIP distribution access list number 10 permitting distribution and learning of network 10.10.0.0, do the following:

#### **Procedure**

1. Enter the command: ip distribution access-list 10 1 permit 10.10.0.0 0.0.255.255

The default action of the access list is deny and can be changed using the ip distribution access-default-action command.



### Note:

Whenever at least one permit rule exists, distributing and learning of all the remaining networks is denied, unless specifically permitted by another rule.

- 2. Apply the distribution access list created in Step 1 by performing the following procedure within the Router RIP context:
  - a. Enter the distribution-list 10 in command to apply list number 10 created in Step 1 on all updates received on all interfaces.
  - b. Enter the distribution-list 10 in FastEthernet 10/3 command to apply Access List 10 on updates received on interface 'FastEthernet 10/3'.
  - c. Enter the distribution-list 10 out command to apply Access List 10 to all advertised updates.
  - d. Enter the distribution-list 10 out ospf command to apply Access List 10 to all advertised updates that were learned from OSPF (redistributed from OSPF into RIP).

### Result

If no distribution access list is defined, learning and advertising is allowed for all of the routing information. This is the default.

### **RIP limitations**

Configuration of RIPv1 and RIPv2 is per IP interface. Configuration must be homogeneous on all routers on each subnetwork. That is, RIPv1 and RIPv2 routers should not be configured on the same subnetwork. However, you can configure different IP interfaces of the Branch Gateway with different RIP versions. This configuration is valid as long as all routers on the subnet are configured with the same version.

RIPv2 and RIPv1 are considered the same protocol with regard to redistribution to and from OSPF and static route preferences.

# **Summary of RIP commands**

For more information about these commands, see Avaya Branch Gateway G450 CLI Reference.

Root level command	Command	Description
ip distribution access- default-action		Set the default action for a specific RIP distribution access list
ip distribution access-		Create a RIP distribution access list
ip distribution access- list-cookie		Set the access list cookie
ip distribution access- list-copy		Copy the distribution access list
ip distribution access- list-name		Set the name of the distribution list
ip distribution access- list-owner		Set the owner of the distribution list
<pre>interface (dialer  fastethernet loopback  serial vlan tunnel)</pre>		Enter the Dialer, FastEthernet, Loopback, Serial, Tunnel, or VLAN interface context
	ip rip authentication key	Set the authentication string used on the interface
	no ip rip authentication key	Clear the password
	ip rip authentication mode	Specify the type of authentication used in RIP v2 packets
	no ip rip authentication mode	Restore the default value, none

Root level command	Command	Description
	ip rip default- route-mode	Enable learning of the default route received by the RIP protocol. The default state is talk-listen.
		The default state is talk-listen.
	no ip rip default- route-mode	Disable listening to default routes.
	ip rip poison- reverse	Enable or disable split-horizon with poison-reverse on an interface
	no ip rip poison- reverse	Disable the poison-reverse mechanism
	ip rip rip-version	Specify the RIP version running on the interface
	ip rip send-receive- mode	Set the RIP send and receive modes on an interface
	no ip rip send- receive-mode	Set the RIP to talk, that is, to send reports
	ip rip split-horizon	Enable or disable the split-horizon mechanism
	no ip rip split- horizon	Disable the split-horizon mechanism. By default split-horizon is enabled.
router rip		Enable the RIP and enter the router configuration context or disable the RIP
no router rip		Restore the default value by disabling RIP
	default-metric	Set or reset the interface RIP route metric value
	no default-metric	restore the interface RIP route metric default value.
	distribution-list	Apply a distribution access list for incoming or outgoing routing information in route updates or deactivate the list
	no distribution-list	Deactivate the distribution access list
	network	Specify a list of networks on which the RIP is running
	no network	Remove an entry from the list of networks
	redistribute	Redistribute routing information from other protocols into RIP
	no redistribute	Restore the default value, disable redistribution by RIP

Root level command	Command	Description
	timers basic	Set RIP timers
	no timers basic	Set the RIP timers to their default value
show ip distribution access-lists		Display the contents of all current distribution lists or of a specific list
show ip protocols		Display parameters and statistics of a given IP routing protocol

### **OSPF**

The Open Shortest Path First (OSPF) protocol enables routers to compute the path that an IP packet should follow. Routers exchange routing information with OSPF to determine where to send each IP packet on its next hop. RIP is an older protocol that serves a similar purpose. For more information about RIP, see RIP on page 414.

OSPF is based on the shortest-path-first or link-state algorithm. It was introduced to overcome the limitations of RIP in increasingly complex network designs. OSPF uses the cost of a path as the criterion for comparing paths. In contrast, RIP uses the number of hops as the criterion for comparing paths. Also, updates are sent when there is a topological change in the network, rather than every 30 seconds as with RIP.

The advantage of shortest-path-first algorithms is that under stable conditions, there are less frequent updates (thereby saving bandwidth). They converge quickly, thus preventing such problems as routing loops and Count-to-Infinity, when routers continuously increment the hop count to a particular network. These algorithms make a stable network. The disadvantage of shortest-path-first algorithms is that they require a lot of CPU power and memory.

In OSPF, routers use link-state updates to send routing information to all nodes in a network by calculating the shortest path to each node. This calculation is based on a topography of the network constructed by each node. Each router sends that portion of the routing table that describes the state of its own links, and it also sends the complete routing structure (topography).

You can configure route redistribution between OSPF, RIP, and static routes. With route redistribution, you can configure the Branch Gateway to redistribute routes learned from one protocol into the domain of the other routing protocol. For more information, see <a href="Route redistribution">Route Route redistribution</a> on page 422.

# **OSPF** dynamic Cost

An OSPF interface on the Branch Gateway can dynamically set a Cost. The Cost represents the price assigned to each interface for purposes of determining the shortest path.

By default the OSPF interface Cost is calculated based on the interface bandwidth, according to the following formula: Cost = 100,000 / bandwidth (in kbps)

The result is that the higher the bandwidth, the lower the Cost.

When manually configuring the Cost of an OSPF interface (ip ospf cost command), dynamic bandwidth updates do not change the Cost.

When manually adjusting the interface's bandwidth, (bandwidth command), if Cost is being determined dynamically, it is this configured bandwidth and not the actual interface bandwidth that is used to calculate Cost.

### **OSPF** limitations

You can configure the Branch Gateway as an OSPF Autonomous System Boundary Router (ASBR) using route redistribution. The Branch Gateway can be installed in the OSPF backbone area (area 0.0.0.0) or in any OSPF area that is part of a multiple areas network. However, the Branch Gateway cannot be configured to be an OSPF area border router itself.

The Branch Gateway supports the ECMP equal-cost multipath (ECMP) feature which allows load balancing by splitting traffic between several equivalent paths.

While you can activate OSPF with default values for each interface using a single command, you can configure many of the OSPF parameters.

# **Summary of OSPF commands**

For more information about these commands, see Avaya Branch Gateway G450 CLI Reference.

Root level command	Command	Description
<pre>interface (dialer fastethernet  loopback  serial  tunnel vlan)</pre>		Enter the Dialer, FastEthernet, Loopback, Serial, Tunnel, or VLAN interface context
	bandwidth	Set the bandwidth parameter manually for this interface
	ip ospf authentication	Specify the authentication type for an interface
	no ip ospf authentication	Remove the authentication type for an interface.
	ip ospf authentication-key	Configure the interface authentication password
	no ip ospf authentication-key	Remove the OSPF password
	ip ospf cost	Configure the Cost of an OSPF interface, for the purpose of determining the shortest path
	no ip ospf cost	Set the cost to its default value
	ip ospf dead-interval	Configure the interval before declaring the neighbor as dead
	no ip ospf dead- interval	Set the dead-interval to its default value

	ip ospf hello-interval no ip ospf hello- interval ip ospf message- digest-key	Specify the time interval between hello packets sent by the router  Set the hello-interval to its default value  Specify the message-digest key for
	interval ip ospf message-	
		Specify the message-digest key for
		the interface and enable OSPF MD5 authentication
	no ip ospf message- digest-key	Return the interface to its default value
	ip ospf network point- to-multipoint	Specify the network type for the interface
	ip ospf network point- to-multipoint	Return the interface to its default value
	ip ospf priority	Configure interface priority used in Designated Router election
	no ip ospf priority	Set the OSPF priority to its default value
ip ospf router-id		Configure the router ID
no ip ospf router-id		Return the router ID to its default value
router ospf		Enable OSPF protocol on the system and to enter the router configuration context
no router ospf		Restore the default value and disable OSPF globally
	area	Configure the OSPF area ID of the router
	no area	Delete the OSPF area id
	default-metric	Set the interface OSPF route metric value
	network	Enable OSPF in a network
	no network	Disable OSPF in a network. The default value is disabled.
	passive-interface	Suppress OSPF routing updates on an interface. Used to allow interfaces to be flooded into the OSPF domain as OSPF routes rather than external routes.
		Note:
		Use the network command with this command to make the network passive.

Root level command	Command	Description
	redistribute	Redistribute routing information from other protocols into OSPF
	no redistribute	Disable resistribution by OSPF
	timers spf	Configure the delay between runs of OSPFs (SPF) calculation
	no timers spf	Restore the default value
show ip ospf		Display general information about OSPF routing
show ip ospf database		Display lists of information related to the OSPF database for a specific router
show ip ospf interface		Display the OSPF-related interface information
show ip ospf neighbor		Display OSPF neighbor information on a per-interface basis
show ip protocols		Display OSPF parameters and statistics

## **Route redistribution**

Route redistribution is the interaction of multiple routing protocols. OSPF and RIP can be operated concurrently in the Branch Gateway. In this case, you can configure the Branch Gateway to redistribute routes learned from one protocol into the domain of the other routing protocol. Similarly, static routes can be redistributed to RIP and OSPF.

### Note:

Take care when you configure route redistribution. It involves metric changes and might cause routing loops in the presence of other routes with incompatible schemes for route redistribution and route preferences.

The Branch Gateway scheme for metric translation in route redistribution is as follows:

- Static to RIP metric configurable (default 1)
- OSPF internal metric N to RIP metric (default 1)
- OSPF external type 1 metric N to RIP metric (default 1)
- OSPF external type 2 metric N to RIP metric (default 1)
- Static to OSPF external type 2, metric configurable (default 20)
- RIP metric N to OSPF external type 2, metric (default 20)
- Direct to OSPF external type 2, metric (default 20)

By default, the Branch Gateway does not redistribute routes between OSPF and RIP. Redistribution from one protocol to the other can be configured. Static routes are, by default, redistributed to RIP and OSPF. The Branch Gateway allows the user to globally disable

redistribution of static routes to RIP, and separately to globally disable redistribution of static routes to OSPF. In addition you can configure, on a per static route basis, whether the route is to be redistributed to RIP and OSPF, and what metric to use (in the range of 1-15). The default state is to allow the route to be redistributed at metric 1. When static routes are redistributed to OSPF, they are always redistributed as external type 2.

# **Export default metric**

The Branch Gateway enables you to configure the metric to be used in updates that are redistributed from one routing protocol to another.

In RIP, the default is 1 and the maximum value is 16. In OSPF, the default is 20.

Set the default metric value before redistribution, using the default-metric command from within the Router RIP or Router OSPF contexts. This value is used for all types of redistributed routes, regardless of the protocol from which the route was learned.

# **Summary of route redistribution commands**

For more information about these commands, see Avaya Branch Gateway G450 CLI Reference.

Root level command	Command	Description
router ospf		Enable OSPF and enter the router configuration context
	redistribute	Redistribute routing information from other protocols into OSPF
		Use in the Router RIP context to configure route redistribution into RIP.
		Use in the Router OSPF context to configure route redistribution into OSPF.
	default-metric	Configure the metric to be used in updates that are redistributed from one routing protocol to another
router rip		Enable RIP and enter the router configuration context
	redistribute	Redistribute routing information from other protocols into RIP
	default-metric	Configure the metric to be used in updates that are redistributed from one routing protocol to another

# **VRRP**

Virtual Router Redundancy Protocol (VRRP) is an IETF protocol designed to support redundancy of routers on the LAN and load balancing of traffic. VRRP is open to host stations, making it an ideal option when redundancy, load balancing, and ease of configuration are required.

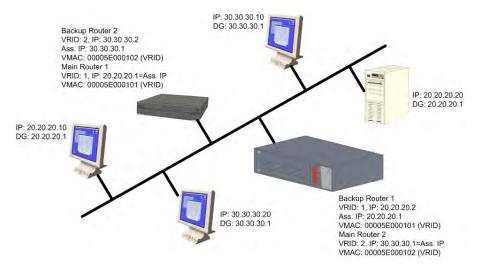
The concept underlying VRRP is that a router can back up other routers, in addition to performing its primary routing functions. This redundancy is achieved by introducing the concept of a virtual router. A virtual router is a routing entity associated with multiple physical routers. One of the physical routers with which the virtual router is associated performs the routing functions. This router is known as the master router. For each virtual router, VRRP selects a master router. If the selected master router fails, another router is selected as master router.

In VRRP, two or more physical routers can be associated with a virtual router, thus achieving extreme reliability. In a VRRP environment, host stations interact with the virtual router. The stations are not aware that this router is a virtual router, and are not affected when a new router takes over the role of master router. Thus, VRRP is fully interoperable with any host station.

You can activate VRRP on an interface using a single command while allowing for the necessary fine-tuning of the many VRRP parameters. For a detailed description of VRRP, see VRRP standards and published literature.

# VRRP configuration example

The following diagram illustrates an example of a VRRP configuration:



There is one main router on IP subnet 20.20.20.0, such as a Branch Gateway, switch, or any router that supports VRRP, and a backup router. You can configure more backup routers.

- The Branch Gateway itself must have an interface on the IP subnetwork, for example, 20.20.20.2
- Configure all the routers under the same VRID, for example, 1. You must configure the routers per VLAN.
- An assigned VRID must not be used in the network, even in a different VLAN
- When router configuration is complete and the network is up, the main router for each virtual router is selected according to the following order of preference:
  - The virtual router IP address is also the router's interface IP address

- It has the highest priority (you can configure this parameter)
- It has the highest IP address if the previous conditions do not apply
- The virtual router IP address needs to be configured as the default gateway on the stations
- The Main router advertises a six-byte Virtual MAC address, in the format 00.00.5E.00.01.02 VRID, as a response to the stations' ARP requests
- The redundant router uses a VRRP polling protocol to check the Main router integrity at one-second intervals (default). Otherwise, it is idle.
- If the Main router fails, the redundant router that does not receive a response from four consecutive polling requests (default) takes over and starts to advertise the same Virtual MAC for ARP requests. Therefore, the stations will not detect any change either in the configured default gateway or at the MAC level.
- VRRP has no provisions for routing database synchronization among the redundant routers. You must perform this manually, if needed.

# **Summary of VRRP commands**

For more information about these commands, see Avaya Branch Gateway G450 CLI Reference.

Root level command	Command	Description
<pre>interface (fastethernet  vlan)</pre>		Enter the FastEthernet or VLAN interface configuration context
	ip vrrp	Create a virtual router on an interface
	no ip vrrp	Delete a virtual router
	ip vrrp address	Assign an IP address to a virtual router
	no ip vrrp address	Remove an IP address from a virtual router
	ip vrrp auth-key	Set the virtual router simple password authentication key for the virtual router ID
	no ip vrrp auth- key	Disable simple password authentication for the virtual router instance
	ip vrrp override addr owner	Accept packets addressed to the IP addresses associated with the virtual router, such as ICMP, SNMP, and telnet (if it is not the IP address owner)
	no ip vrrp override addr owner	Discard the packets
	ip vrrp preempt	Configure a router to preempt a lower priority master for the virtual router ID
	no ip vrrp preempt	Disable preemption for a virtual router instance. By default, preemption is enabled.

Root level command	Command	Description
	ip vrrp primary	Set the primary address used as the source address of VRRP packets for the virtual router ID
	no ip vrrp primary	Restore the default primary address for a virtual router instance. By default, the primary address is selected automatically by the device.
	ip vrrp priority	Set the virtual router priority value used when selecting a master router
	ip vrrp timer	Set the virtual router advertisement timer value for the virtual router ID
router vrrp		Enable or disable VRRP routing globally
show ip vrrp		Display VRRP information

# **Fragmentation**

Branch Gateway supports IP fragmentation and reassembly. The Branch Gateway router can fragment and reassemble IP packets according to RFC 791. This feature allows the router to send and receive large IP packets where the underlying data link protocol constrains the Maximum Transport Unit (MTU).

IP fragmentation involves breaking a datagram into a number of pieces that can be reassembled later. The IP source, destination, identification, total length, and fragment offset fields, along with the more fragment and don't fragment flags in the IP header, are used for IP fragmentation and reassembly.

IP fragmentation works as follows:

- Each IP packet is divided into fragments
- Each fragment becomes its own IP packet
- Each packet has same identifier, source, and destination address

Fragments are usually not reassembled until final destination. The Branch Gateway supports fragmentation of IP packets according to RFC 791, and reassembly of IP packets destined only to its interfaces.

# **Summary of fragmentation commands**

For more information about these commands, see Avaya Branch Gateway G450 CLI Reference.

Command	Description
clear fragment	Clear the fragment database and restore its default values
fragment chain	Set the maximum number of fragments that can comprise a single IP packet destined to the router

Command	Description
no fragment chain	Set the fragment chain to its default value
fragment size	Set the maximum number of fragmented IP packets destined to the router to reassemble at any given time
no fragment size	Set the fragment size to its default value
fragment timeout	Set the maximum number of seconds to reassemble a fragmented IP packet destined to the router
no fragment timeout	Set the fragment timeout to its default value.
show fragment	Display information regarding fragmented IP packets that are destined to a router

# **Chapter 21: IPSec VPN**

VPN (Virtual Private Network) defines a private secure connection between two nodes on a public network such as the Internet. VPN at the IP level is deployed using IP Security (IPSec). IPSec is a standards-based set of protocols defined by the IETF that provide privacy, integrity, and authenticity to information transferred across IP networks.

The standard key exchange method employed by IPSec uses the Internet Key Exchange (IKE) protocol to exchange key information between the two nodes (referred to as peers). Each peer maintains Security Associations (SAs) to maintain the private secure connection. IKE operates in two phases:

- The Phase-1 exchange negotiates an IKE SA
- The IKE SA created in Phase-1 secures the subsequent Phase-2 exchanges, which in turn generate IPSec SAs

IPSec SAs secure the actual traffic between the protected networks behind the peers, while the IKE SA only secures the key exchanges that generate the IPSec SAs between the peers.

The Branch Gateway IPSec VPN feature is designed to support site-to-site topologies, in which the two peers are gateways.



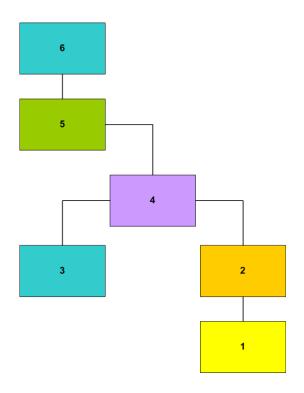
To configure IPSec VPN, you need at least a basic knowledge of IPSec. Refer to the following guide for a suitable introduction:

http://www.tcpipguide.com/free/t IPSecurityIPSecProtocols.htm

# Overview of IPSec VPN configuration

# **IPSec VPN configuration model**

The following figure summarizes the components you need to define and the order in which you need to define them.



### Table 4: Figure notes:

- 1. ISAKMP Policy
- 2. IPSEC Transform-set
- 3. ISAKMP Peer or Peer Group
- 4. Crypto Map
- 5. Crypto List
- 6. Interface

# **Overview of IPSec VPN components**

The basic IPSec VPN building blocks define how to secure packets, as follows:

**ISAKMP policies:** Define parameters for IKE phase 1 negotiation

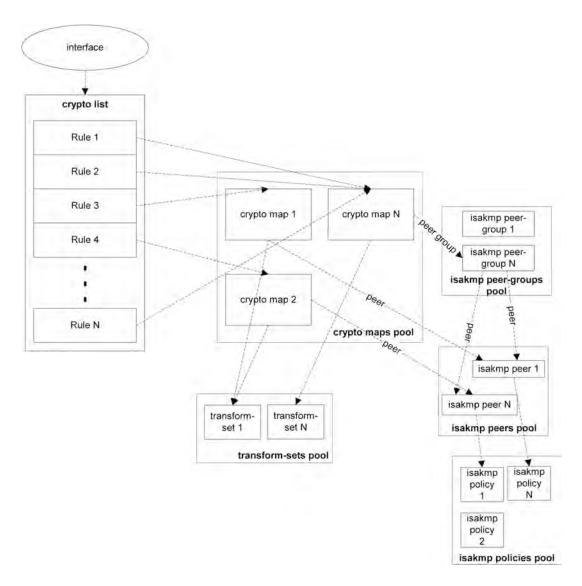
**Transform-sets:** Define parameters for IKE phase 2 negotiation

Once the building blocks are defined, IPSec VPN is implemented using a crypto list. The crypto list defines, for the interface to which it applies, which packets should be secured and how, as follows:

Each rule in the crypto list points to a crypto-map. A crypto-map points to a transform-set, and to a peer or peer-group. The peer or peer-group, in turn, point to an ISAKMP policy.

# **IPSec VPN components**

The following figure describes the relationships among the various VPN components.



# **Summary of configuration commands**

The commands required to configure a VPN are listed below. For a step-by-step description of the VPN procedures, see <u>Site-to-site IPSec VPN</u> on page 432.

# Note:

You must configure VPN in the order shown in the summary. Commands appearing in bold are mandatory.

- ISAKMP policy <u>crypto isakmp policy</u> on page 433
  - description
  - authentication pre-share
  - encryption

- hash
- group
- lifetime
- IPSEC transform-set <u>crypto ipsec transform-set</u> on page 434
  - set pfs
  - set security-association lifetime seconds
  - set security-association lifetime kilobytes
  - mode (tunnel/transport)
- ISAKMP peer <u>crypto isakmp peer</u> on page 435
  - description
  - isakmp-policy
  - pre-shared-key
  - initiate mode
  - self-identity
  - keepalive
  - keepalive-track
  - continuous-channel
- (Optional) ISAKMP peer group <u>crypto isakmp peer-group</u> on page 438
  - description
  - set peer
- Crypto map crypto map on page 439
  - description
  - set transform-set
  - set peer Or set peer-group
  - set dscp
  - continuous-channel
- IP crypto list ip crypto-list on page 441
  - local-address
  - ip-rule
    - · description
    - source-ip
    - destination-ip

- protect crypto map
- ip-protocol
- tcp
- udp
- icmp
- dscp
- fragment
- Access control list <u>ip access-control-list</u> on page 444
- global parameters on page 444
  - crypto isakmp invalid-spi-recovery
  - crypto ipsec nat-transparency udp-encapsulation
  - crypto isakmp nat keepalive
- assigning a crypto-list to an interface on page 446
  - crypto ipsec df-bit
  - crypto ipsec minimal-pmtu
  - ip crypto-group

### Site-to-site IPSec VPN

This section describes the concepts and procedures for VPN configuration.

To configure a site-to-site IPSec VPN, two devices (the Branch Gateway and a peer Gateway) must be configured symmetrically.

In some cases, you may wish to configure global VPN parameters (see <u>Configuring global</u> parameters on page 444).



In the following sections, all IPSec VPN parameters that you must configure are indicated as mandatory parameters. Non-mandatory VPN parameters have default values that are used unless otherwise set. Thus for example, although it is mandatory to define at least one ISAKMP policy, it is not mandatory to set the values for that ISAKMP policy since the Branch Gateway contains default ISAKMP policy settings.

# **VPN** peer coordination

Before commencing IPSec VPN configuration, you must resolve jointly with your VPN peer the basic parameters so that IPSec VPN can be set up symmetrically in the two peers. If the IPSec VPN configuration in the two peers does not match, no VPN is created.

If you will be defining a peer-group which maintains a list of redundant peers, each of the peers in the group must be configured to match the Branch Gateway.

The basic parameters include:

- The IKE phase 1 parameters (as defined in the ISAKMP policy, see <a href="Configuring ISAKMP">Configuring ISAKMP</a> policies on page 433)
- The IKE phase 2 parameters (as defined in the transform-set, see <u>Configuring transform-sets</u> on page 434)
- The ISAKMP peer parameters (see <a href="Configuring ISAKMP peer information">Configuring ISAKMP peer information</a> on page 435)
- Which packets should be secured (as defined in the crypto list, see <u>Configuring crypto lists</u> on page 441)
- The peer addresses. For each peer, the local address entered in the crypto list (see
   <u>Configuring crypto lists</u> on page 441) should match the ISAKMP peer address in the other
   peer (see <u>Configuring ISAKMP</u> peer information on page 435).
- NAT Traversal, if your installation includes one or more NAT devices between the local and remote VPN peers. See Configuring global parameters on page 444.

See <u>Configuring IPSec VPN logging</u> on page 448 for information on how to view IPSec VPN configuration in both peers so as to pinpoint the problem in case of a mismatch between the two peers.

### Configuring ISAKMP policies

### **About this task**

An ISAKMP policy defines the IKE phase 1 parameters.

Note:

You can configure up to 40 ISAKMP policies.

Important:

Define at least one ISAKMP policy.

#### **Procedure**

1. Enter crypto isakmp policy, followed by an index number from 1 to 20, to enter the context of an ISAKMP policy list and to create the list if it does not exist.

For example:

```
Gxxx-001# crypto isakmp policy 1
Gxxx-001(config-isakmp:1)#
```

- 2. You can use the following commands to set the parameters of the ISAKMP policy:
  - Use the description command to assign a description to the ISAKMP policy.
  - Use the authentication pre-share command to set the authentication of ISAKMP policy to pre-shared secret.

- Use the **encryption** command to set the encryption algorithm for the ISAKMP policy. Possible values are des (default), 3des, aes, aes-192 and aes-256.
- Use the hash command to set the hash (authentication) algorithm for the ISAKMP policy. Possible values are md5 and sha (default).
- Use the group command to set the Diffie-Hellman group for the ISAKMP policy. Possible values are 1 (default), 2, 5 and 14.
- Use the lifetime command to set the lifetime of the ISAKMP SA, in seconds. The range of values is 60 to 86,400 seconds (default is 86,400). For example:

```
Gxxx-001(config-isakmp:1) # description "lincroft ike"
Done!
Gxxx-001(config-isakmp:1) # authentication pre-share
Done!
Gxxx-001(config-isakmp:1) # encryption des
Done!
Gxxx-001(config-isakmp:1) # hash md5
Done!
Gxxx-001(config-isakmp:1) # group 1
Done!
Gxxx-001(config-isakmp:1) # lifetime 60000
Done!
```

3. Exit the ISAKMP policy context with the exit command.

### For example:

```
Gxxx-001(config-isakmp:1)# exit
Gxxx-001#
```

### **Configuring transform-sets**

### About this task

A transform-set defines the IKE phase 2 parameters. It specifies the encryption and authentication algorithms to be used, sets a security association lifetime, and specifies whether PFS is enabled and which DH group it uses. In addition, it specifies the IPSec VPN mode (tunnel or transport).

### Note:

You can define up to 40 transform-sets.

# Important:

Define at least one transform-set.

#### **Procedure**

1. Use the **crypto ipsec transform-set** command to enter the context of a transform-set (and to create the transform-set if it does not exist).

The command variables include:

- · The name of the transform-set
- The encryption algorithm used by the transform-set. Possible values are esp-des, esp-3des, esp-aes, esp-aes-192, esp-aes-256 and esp-null (no encryption).

- The authentication algorithm used by the transform-set. Possible values are esp-md5-hmac and esp-sha-hmac.
- The IP compression algorithm used by the transform-set. The only possible value is comp-lzs.

### For example:

```
Gxxx-001# crypto ipsec transform-set ts1 esp-3des esp-md5-hmac comp-lzs
Gxxx-001(config-transform:ts1)#
```

- 2. You can use the following commands to set the parameters of the transform-set:
  - Use the set pfs command to specify whether each IKE phase 2 negotiation employs
    Perfect Forward Secrecy (PFS), and if yes, which Diffie-Hellman group to employ. PFS
    ensures that even if someone were to discover the long-term secret(s), the attacker
    would not be able to recover the session keys, both past and present. In addition, the
    discovery of a session key compromises neither the long-term secrets nor the other
    session keys. The default setting is no set pfs.
  - Use the set security-association lifetime seconds command to set the security association lifetime in seconds.
  - Use the set security-association lifetime kilobytes command to set the security association lifetime in kilobytes.
  - Use the mode command to set the IPSec mode (tunnel or transport). Transport mode does not add an additional IP header (i.e., a tunnel header), but rather uses the original packet's header. However, it can be used only when the VPN tunnel endpoints are equivalent to the original packet's source and destination IP addresses. This is generally the case when using GRE over IPSec. Note that transport mode cannot be used unless the remote VPN peer supports that mode and was configured to use it.

```
Gxxx-001001(config-transform:ts1ts1) # set pfs group2
Done!
Gxxx-001(config-transform:ts1) # set security-association lifetime seconds
7200
Done!
Gxxx-001(config-transform:ts1) # set security-association lifetime
kilobytes 268435456
Gxxx-001(config-transform:ts1) # mode tunnel
Done!
```

3. Exit the crypto transform-set context with the exit command.

```
Gxxx-001(config-transform:ts1)# exit
Gxxx-001#
```

# Configuring ISAKMP peer information

### About this task

ISAKMP peer information defines the remote peer identification, the pre-shared key used for peer authentication, and the ISAKMP policy to be used for IKE phase 1 negotiations between the peers.

You can define up to 100 ISAKMP peers.

Important:

Define at least one ISAKMP peer.

#### **Procedure**

1. Enter crypto isakmp peer, followed by the address of the ISAKMP peer or its Fully Qualified Domain Name (FQDN), to enter the context of an ISAKMP peer and to create the peer if it does not exist.



If you want to specify the ISAKMP peer by its FQDN name, configure the Branch Gateway as a DNS client. and verify that the peer's name is listed in a DNS server. See <u>DNS resolver</u> on page 70.

Note:

Do not specify an ambiguous ISAKMP peer. In other words, do not configure an FQDN that translates to an IP address which is already associated with another ISAKMP peer.

### For example:

```
Gxxx-001# crypto isakmp peer address 149.49.70.1
Gxxx-001(config-peer:149.49.70.1)#

Gxxx-001# crypto isakmp peer fqdn vpn.lnd.ny.avaya.com
Gxxx-001(config-peer:vpn.lnd.ny.avaya.com)#
```

2. Use the **description** command to enter a description for the peer.

### For example:

```
Gxxx-001(config-peer:149.49.70.1)# description "New York office" Done!
```

3. Specify an ISAKMP policy to be used with the peer, using the isakmp policy command.



isakmp policy is a mandatory command.

#### For example:

```
Gxxx-001(config-peer:149.49.70.1)# isakmp-policy 1
Done!
```

4. Enter the preshared key for peer authentication using the pre-shared-key command.

# **!** Important:

pre-shared-key is a mandatory command.

#### For example:

```
Gxxx-001(config-peer:149.49.70.1) # pre-shared-key GNpi1odGNBrB5z4GJL
```

Alternatively, you can obtain a cryptographic-grade random key from the Branch Gateway with the suggest-key command, and then enter it using the pre-shared-key command. The suggested key-length can vary from 8 to 127 alphanumeric characters, or from 8 to 64 bytes represented in hexadecimal notation. The default length is 32 characters.

#### For example:

```
Gxxx-001(config-peer:149.49.70.1) # suggest-key 24
The suggest key: yjsYIz9ikcwaq0FUPTF3CIrw
Gxxx-001(config-peer:149.49.70.1) pre-shared-key yjsYIz9ikcwaq0FUPTF3CIrw
```

5. If you wish to work in IKE aggressive mode, use the initiate mode aggressive command.



### Note:

Aggressive mode is one of the prerequisites for working with dynamic local peer IP addresses. For more information about working with dynamic local peer IP addresses, see Dynamic local peer IP on page 453.

### For example:

```
Gxxx-001(config-peer:149.49.70.1) # initiate mode aggressive
```

6. If you want to listen in to communication from a remote peer that has a dynamic IP address, use the initiate mode none command.

In this mode, the device can only accept inbound IKE Aggressive Mode connections from the peer, and is not able to initiate IKE phase-1 (Main Mode or Aggressive Mode) to the peer, nor is the peer able to participate as part of a peer-group. In addition, specifying the continuous-channel command when configuring the crypto ISAKMP peer information has no effect in this mode. For more information on continuous-channel, see Continuous channel on page 456.

7. Specify the branch device (Branch Gateway) by its address or by the FQDN name that identifies the Branch Gateway in the remote peer, using the self-identity command.



#### Note:

Specifying self-identity as a name is one of the prerequisites for working with dynamic local peer IP addresses. For more information about working with dynamic local peer IP addresses, see Dynamic local peer IP on page 453.

#### For example:

```
Gxxx-001(config-peer:149.49.70.1) # self-identity address
Gxxx-001(config-peer:149.49.70.1) # self-identity fqdn vpn.avaya.com
Done!
```

8. Enable Dead Peer Detection (DPD) keepalives that check whether the remote peer is up using the keepalive command, followed by the number of seconds between DPD keepalive probes, and the number of seconds between retries if keepalive fails.

The following example sets DPD keepalive to send probes every 10 seconds, and to send retries every two seconds if DPD keepalive fails.

```
Gxxx-001(config-peer:149.49.70.1) # keepalive 10 retry 2
```

9. Bind peer status to an object tracker that can monitor hosts inside the remote peer's protected network.

To do so, use the keepalive-track command. For more information on object trackers, see Object tracking on page 258.

### For example:

```
Gxxx-001(config-peer:149.49.70.1)# keepalive-track 5
```



### Note:

DPD and object tracking can coexist and augment each other. However, object tracking does not impose any requirements on the remote peer. You can, therefore, use object tracking rather than DPD keepalives if the remote peer does not support DPD.

10. Specify whether to enable continuous-channel IKE phase 1, with the continuouschannel command.

The default setting is no continuous-channel that disables continuous-channel IKE phase 1. For more information on continuous-channel see Continuous channel on page 456.

#### For example:

```
Gxxx-001(config-peer:149.49.70.1)# continuous-channel
Done!
```

11. Exit the peer context with the exit command.

#### For example:

```
Gxxx-001(config-peer:149.49.70.1) # exit
Gxxx-001#
```

# Configuring an ISAKMP peer-group

### About this task

An ISAKMP peer-group maintains an ordered list of redundant peers. The purpose of the peergroup is to provide a backup in the case of remote peer failure. At any point in time, only one peer is active and acting as the remote peer. If the active peer is presumed dead, the next peer in the peer-group becomes the active remote peer. For a full explanation of the redundancy mechanism see Introduction to the failover mechanism on page 471.

You can define up to 50 peer-groups.

Note:

A peer configured as initiate mode none cannot be a member of a peer-group.

#### **Procedure**

1. Use the crypto isakmp peer-group command, followed by the name of a peer-group (a string of up to 110 characters), to enter the context of an ISAKMP peer-group (and to create the peer-group if it does not exist).

#### For example:

```
Gxxx-001# crypto isakmp peer-group NY-VPN-group
Gxxx-001(config-peer-grp:NY-VPN-group)#
```

2. Use the description command to enter a description for the ISAKMP peer-group.

### For example:

```
Gxxx-001(config-peer-grp:NY-VPN-group) # description "Avaya peer group"
Done!
```

3. Add a peer to the list of peers in the group, using the set peer command:

Specify the peer's name or address.

Note:

You can define up to a maximum of five peers in a peer-group.

**!** Important:

Each of the peers listed in the peer-group must be configured as an ISAKMP peer (see Configuring ISAKMP peer information on page 435).

Optionally enter an index number, specifying the relative position of the peer within the peer-group. If you do not enter an index number, the peer is added at the end of the peer-group list, and is assigned an index following the last peer's index.

#### For example:

```
Gxxx-001(config-peer-grp:NY-VPN-group) # set peer 149.49.52.135 1
Done!
```

4. Repeat Step 3 on page 439 for every peer you want to add to the list.

# **Configuring crypto maps**

#### About this task

A crypto map points to a transform-set and to a peer that in turn points to an ISAKMP policy. If you defined a peer-group, the crypto map can point to the peer-group. The transform-set and ISAKMP policy define how to secure the traffic that matches the ip-rule that points to this crypto map.

### Important:

It is mandatory to create at least one crypto map.

### Note:

You can configure up to 100 crypto maps.

### **Procedure**

1. Use the crypto map command, followed by an index number from 1 to 50, to enter the context of a crypto map and to create the crypto map if it does not exist.

### For example:

```
Gxxx-001# crypto map 1
Gxxx-001(config-crypto:1)#
```

2. Use the **description** command to enter a description for the crypto map.

### For example:

```
Gxxx-001(config-crypto:1)# description "vpn lincroft branch"
Done!
```

- 3. Do one of the following commands:
  - Specify the remote peer, using the **set peer** command. For example:

```
Gxxx-001(config-crypto:1) # set peer 149.49.60.60
Done!
```

• Specify a peer-group, using the set peer-group command. For example:

```
Gxxx-001(config-crypto:1)# set peer-group NY-VPN-group
Done!
```

# Important:

Specify either set peer or set peer-group, but not both.

- 4. Specify the specific transform-set to which this crypto map points, using the set transform-set command.
  - Important:

set transform-set is a mandatory command.

### For example:

```
Gxxx-001(config-crypto:1)# set transform-set ts1
Done!
```

5. Set the static DSCP value in the DS field of the tunneled packet by using the set dscp command, followed by a value from 0 to 63.

The default setting is **no set dscp** that specifies that the DSCP is copied from the DS field of the original packet.

### For example:

```
Gxxx-001(config-crypto:1)# set dscp 38
Done!
```

6. Specify whether to enable continuous-channel IPSec (IKE phase 2) with the continuous-channel command.

The default setting is **no continuous-channel** that disables continuous-channel IPSec. For more information on continuous-channel see <u>Continuous channel</u> on page 456.

### For example:

```
Gxxx-001(config-crypto:1) # continuous-channel
Done!
```

7. Exit crypto map context with the exit command.

### For example:

```
Gxxx-001(config-crypto:1)# exit
Gxxx-001#
```

# **Configuring crypto lists**

### About this task

A crypto list is an ordered list of ip-rules that control which traffic requires IPSec protection and which does not, based on IP groups (source and destination IP addresses and wildcard). A crypto list is activated on an interface. The Branch Gateway can have multiple crypto lists activated on different interfaces.

# Important:

It is mandatory to create at least one crypto list.

# Note:

You can configure up to 100 crypto lists.

#### **Procedure**

1. Use the ip crypto-list command, followed by an index number from 901 to 999, to enter the context of a crypto list (and to create the list if it does not exist).

### For example:

```
Gxxx-001# ip crypto-list 901
Gxxx-001(Crypto 901)#
```

2. Specify the local IP address for the IPSec tunnels derived from this crypto list, using the local-address command.

The local address can be either the IP address or the name of an IP interface of the device.

# Important:

local-address is a mandatory command.

### Examples:

```
Gxxx-001 (Crypto 901) # local-address 192.168.49.1
Gxxx-001(Crypto 901)# local-address FastEthernet 10/3
Done!
```



#### Note:

Specifying the interface as a name is one of the prerequisites for working with dynamic local peer IP addresses. For more information about working with dynamic local peer IP addresses, see Dynamic local peer IP on page 453.

3. Specify the name of the crypto list using the name command.

#### For example:

```
Gxxx-001(Crypto 901) # name "Public Network via ADSL"
```

4. Use the ip-rule command, followed by an index number from 1 to 1000, to enter the context of an ip-rule and to create the ip-rule if it does not exist.



### **!** Important:

It is mandatory to create at least one ip-rule.

### For example:

```
Gxxx-001(Crypto 901) # ip-rule 10
Gxxx-001(Crypto 901/ip rule 10)#
```

- 5. Configure ip-rule parameters as follows:
  - Use the **description** command to assign a description to the ip-rule.
  - To specify a range of source and destination IP addresses to which the rule applies, use the source-ip and destination-ip commands, followed by the IP range criteria. The IP range criteria can be one of the following:
    - single address: . Type host, followed by an IP address, to set a single IP address to which the rule applies.
    - wildcard: Type host, followed by an IP address using wildcards, to set a range of IP addresses to which the rule applies.
    - All addresses: . Type any to apply the rule to all IP addresses.
  - Use the no form of the appropriate command to return to the default value, any.
  - Define the action by specifying whether to protect traffic that matches the source and destination addresses, using one of the following commands:
    - no protect. Do not protect traffic that matches the source and destination addresses.
    - protect crypto map crypto-map-id. Protect traffic that matches the source and destination addresses. The specified crypto map specifies how to secure the

traffic. For instructions on configuring crypto maps, see <u>Configuring crypto maps</u> on page 439.

### For example:

```
Gxxx-001(Crypto 901/ip rule 10) # description "vpn tunnel to uk main office"
Done!
Gxxx-001(Crypto 901/ip rule 10) # source-ip 10.1.0.0 0.0.255.255
Done!
Gxxx-001(Crypto 901/ip rule 10) # destination-ip any
Done!
Gxxx-001(Crypto 901/ip rule 10) # protect crypto map 1
Done!
```

- For rules whose action is no protect, you can fine-tune the definition of packets that match this rule by using the following commands. For a full description of the commands see *Avaya CLI Reference*. Note that this fine-tuning is not applicable for rules whose action is protect crypto map.
  - ip-protocol. Specify the IP protocol to match.
  - tcp. Specify the TCP settings to match.
  - udp. Specify the UDP settings to match.
  - icmp. Specify the ICMP protocol settings to match.
  - dscp. Specify the DSCP to match.
  - fragment. Specify whether this rule applies to non-initial fragments only.
- Exit ip-rule context with the exit command.

#### For example:

```
Gxxx-001(Crypto 901/ip rule 10)# exit
Gxxx-001(Crypto 901)#
```

- 7. Repeat Steps 4 to 6 for every ip-rule you wish to define in the crypto list.
- 8. Exit crypto list context with the exit command.

### For example:

```
Gxxx-001(Crypto 901)# exit
Gxxx-001#
```

### Deactivating crypto lists to modify IPSec VPN parameters

#### About this task

Most IPSec VPN parameters cannot be modified if they are linked to an active crypto list.

#### **Procedure**

1. To modify a parameter linked to an active crypto list, you must first deactivate the list using the no ip crypto-group command in the context of the interface on which the crypto list is activated.



### 🐯 Note:

If the crypto list is activated on more than one interface, deactivate the crypto list for each of the interfaces on which it is activated.

#### For example:

```
Gxxx-001# interface serial 3/1
Gxxx-001(if:serial 3/1)# no ip crypto-group
```

2. After modifying IPSec VPN parameters as desired, re-activate the crypto list on the interface using the ip crypto-group crypto-list-id command.

### For example:

```
Gxxx-001# interface serial 3/1
Gxxx-001(if:serial 3/1)# ip crypto-group 901
```

### Changing parameters of a crypto list.

#### **Procedure**

- 1. Use the ip policy-list-copyold listnew list command
- 2. Edit the new list
- Activate it on the interface.

Note that activating the new list causes all the current IPSec tunnels to close.

### **Access control lists**

Since VPN is intended for a public network such as the Internet, it is recommended to define an access control list using the ip access-control-list command, to avoid traffic that should not enter the device. You should, therefore, define an ingress access control list that allows only IKE, ESP, and ICMP traffic to enter the device from the public interface. For a configuration example see the access control list in Simple VPN topology – VPN hub and spokes on page 449.

# Configuring global parameters

### **Enabling invalid SPI recovery**

### About this task

Invalid SPI Recovery enables an IKE SA to be established when an invalid security parameter index error occurs during packet processing. A notification of the invalid SPI error is sent to the originating peer so that the SA databases can be re-synchronized, and successful packet processing can be resumed.



#### Note:

Invalid SPI recovery is enabled by default. Configure invalid SPI recovery only if you wish to re-enable it after it was disabled.

### **Procedure**

1. Enable invalid SPI recovery with the crypto isakmp invalid-spi-recovery command.

#### For example:

```
Gxxx-001# crypto isakmp invalid-spi-recovery
Done!
```

2. Configure NAT Traversal global parameters as described in NAT Traversal on page 445

### **NAT Traversal**

Network Address Translation (NAT) is a solution to the problem of the scarcity and cost of public IP addresses. An organization with a single public IP address can use a NAT device to connect multiple computers to the Internet sharing a single public IP address. However, NAT causes compatibility problems for many types of network applications, including VPN.

NAT Traversal enables detecting the presence of NAT devices along the path of the VPN tunnel. Once detected, the two peers tunnel IKE and IPSEC traffic through an agreed-upon UDP port, allowing the NAT device to work seamlessly with VPN. The standard UDP port used is port 4500; to find out the port number, use the show crypto ipsec sa command.

The Branch Gateway IPSec VPN feature supports NAT Traversal. If your installation includes one or more NAT devices between the local and remote VPN peers, NAT Traversal should be enabled, although in some rare cases it may not be required.

### Note:

NAT Traversal is enabled by default. Configure NAT Traversal only if you need to reenable it after it was disabled, using the no crypto ipsec nat-transparency udp-encapsulation command. NAT Traversal keepalive is also enabled by default (with a default value of 20 seconds). Configure NAT Traversal keepalive only if you need to re-enable it after it was disabled, using the no crypto isakmp nat keepalive command.

### Configuring NAT Traversal

#### **Procedure**

1. Enable NAT Traversal by entering crypto ipsec nat-transparency udp-encapsulation.

#### For example:

```
Gxxx-001\# crypto ipsec nat-transparency udp-encapsulation Done!
```

2. Enable NAT Traversal keepalives and configure the keepalive interval in seconds by entering crypto isakmp nat keepalive, followed by a number from 5 to 3600.

NAT Traversal keepalives are empty UDP packets that the device sends on a periodic basis at times of inactivity when a dynamic NAT is detected along the way. These keepalives are intended to maintain the NAT translation alive in the NAT device, and not

let it age-out due to periods of inactivity. Set the NAT Traversal keepalive interval on the Branch Gateway to be less than the NAT translation aging time on the NAT device.

For example:

```
Gxxx-001# crypto isakmp nat keepalive 60
Done!
```

# Assigning a crypto list to an interface

### **About this task**

A crypto list is activated on an interface. You can assign multiple crypto lists to different interfaces on the Branch Gateway.

### **Procedure**

1. Enter interface context using the interface command.

### For example:

```
Gxxx-001# interface fastethernet 10/3
Gxxx-001(config-if:FastEthernet 10/3)#
```

2. Configure the IP address of the interface.

You can configure either a static or a dynamic IP address.

- To configure a static IP address:
  - Be sure to specify an IP address (not an interface name) as the local-address in the crypto list (see Configuring crypto lists on page 441)
  - Within the interface context, specify the IP address and mask using the ip address command

### For example:

```
Gxxx-001(config-if:FastEthernet 10/3)# ip address 192.168.49.1 25.255.255.0
```

- To configure a dynamic IP address, see <a href="Dynamic local peer IP">Dynamic local peer IP</a> on page 453
- 3. Use the ip crypto-group command, followed by the index of the crypto-group, to assign a crypto-group to the interface.

# Important:

ip crypto-group is a mandatory command.

- 4. Optionally, you can set the following parameters:
  - The crypto ipsec minimal-pmtu command is intended for advanced users only. It sets the minimal PMTU value which can be applied to an SA when the Branch Gateway participates in Path MTU Discovery (PMTUD) for the tunnel pertaining to that SA.
  - The crypto ipsec df-bit command is intended for advanced users only. It sets the Do Not Fragment (DF) bit to either clear or copy mode:
    - copy. The DF bit of the encapsulated packet is copied from the original packet, and PMTUD is maintained for the IPSec tunnel.

 clear. The DF bit of the encapsulated packet is never set, and PMTUD is not maintained for the IPSec tunnel. Packets traversing an IPSec tunnel are prefragmented according to the MTU of the SA, regardless of their DF bit. In case packets are fragmented, the DF bit is copied to every fragment of the original packet.

### For example:

```
Gxxx-001(config-if:FastEthernet 10/3) # ip crypto-group 901
Done!
Gxxx-001(config-if:FastEthernet 10/3) # crypto ipsec minimal pmtu 500
Done!
Gxxx-001(config-if:FastEthernet 10/3) # crypto ipsec df-bit copy
Done!
```

5. Exit the interface context with the exit command.

### For example:

```
Gxxx-001(config-if:FastEthernet 10/3) # exit
Gxxx-001#
```

### **IPSec VPN maintenance**

You can display IPSec VPN configuration and status, and clear IPSec VPN data, using certain show and clear commands. In addition, you can display the IPSec VPN log to verify the success or failure of IPSec VPN operations, and to view the actual configuration of both peers for a successful debug in case of a problem.

For a description of these commands, see <u>Summary of VPN commands</u> on page 492 or *Avaya Branch Gateway G450 CLI Reference*.

# Commands used to display an IPSec VPN configuration

```
• show crypto ipsec transform-set
```

```
    show crypto isakmp policy
```

- show crypto isakmp peer
- show crypto isakmp peer-group
- show crypto map
- show ip crypto-list list#
- show ip crypto-list
- show ip active-lists

For a description of these commands, see Summary of VPN commands on page 492

For a full description of the commands and their output fields, see *Avaya Branch Gateway G450 CLI Reference*.

### Commands used to display IPSec VPN status

The following show commands show runtime IPSec VPN database status and statistics, and clear runtime statistics.

- show crypto isakmp sa
- show crypto ipsec sa
- show crypto ipsec sa address
- · show crypto ipsec sa list



### Tip:

The detail option in the various show crypto ipsec sa commands, provides detailed counters information on each IPSec SA. To pinpoint the source of a problem, check for a counter whose value grows with time.

· clear crypto sa counters

For a description of these commands, see Summary of VPN commands on page 492.

For a full description of the commands and their output fields, see Avaya Branch Gateway G450 CLI Reference.

# Clearing both ISAKMP connection and IPSec SAs

### **Procedure**

- 1. Clear the IPSec SAs with the clear crypto sa all command.
- 2. Clear the ISAKMP SA with the clear crypto isakmp command.

# Configuring IPSec VPN logging

#### About this task

IPSec VPN logging allows you to view the start and finish of IKE phase 1 and IKE phase 2 negotiations. Most importantly, it displays the configuration of both peers, so that you can pinpoint the problem in case of a mismatch between the IPSec VPN configuration of the peers.



#### Note:

For more information about logging, see <a href="System logging">System logging</a> on page 186.

#### **Procedure**

1. Use the set logging session enable command to enable session logging.

```
Gxxx-001# set logging session enable
Done!
CLI-Notification: write: set logging session enable
```

2. Use the set logging session condition ISAKMP command to view all ISAKMP messages of Info level and above.

#### For example:

```
Gxxx-001# set logging session condition ISAKMP Info
Done!
CLI-Notification: write: set logging session condition ISAKMP Info
```

3. Use the set logging session condition IPSEC command to view all IPSec messages of Info level and above.

### For example:

```
Gxxx-001# set logging session condition IPSEC Info
Done!
CLI-Notification: write: set logging session condition IPSEC Info
```

4. Initiate a session by pinging the peer device.

#### For example.

```
Gxxx-001# ping 135.64.102.109
```

### Result

The logging information details the IKE negotiations, including the ISAKMP SA and IPSec SA configuration of the peers.

### **Example**

```
IPSEC-Informational: Call IKE negotiation for outgoing SPD entry 901 20:
   Peers 149.49.77.202<->135.64.102.109
ISAKMP-Informational: Initiating IKE phase 1 negotiation:
   Peers 149.49.77.202<->135.64.102.109
ISAKMP-Informational: Finished IKE phase 1 negotiation, creating ISAKMP
   Peers 149.49.77.202<->135.64.102.109
   Icookie - 0e2fb5ac12ec04b2, Rcookie - 541b912b0a30085d
esp-des, esp-sha-hmac, DH group 1, Lifetime 86400 seconds ISAKMP-Informational: Initiating IKE phase 2 negotiation:
   Peers 149.49.77.202<->135.64.102.109
ISAKMP-Informational: Finished IKE phase 2, creating outbound IPSEC SA:
   SPI 0x4d706e3, Peers 149.49.77.202<->135.64.102.109
   Identities: 149.49.77.0/255.255.255.0->135.64.102.0/255.255.255.0
   esp-des, esp-md5-hmac, 3600 seconds, 4608000 KB
ISAKMP-Informational: Finished IKE phase 2, creating inbound IPSEC SA:
   SPI 0x6798, Peers 135.64.102.109<->149.49.77.202
   Identities: 135.64.102.0/255.255.255.0->149.49.77.0/255.255.255.0
   esp-des, esp-md5-hmac, 3600 seconds, 4608000 KB
```

# Typical installations for IPSec VPN

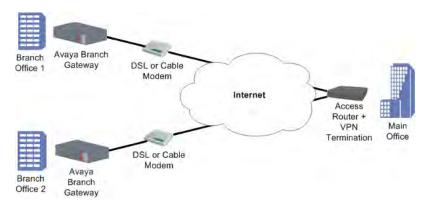
Included in the typical installations, are examples of installing VPN hub and spokes, full or partial mesh, and a hub-and-spoke with VPN for data and VoIP control backup.

# Simple VPN topology - VPN hub and spokes

The simple VPN topology consists of several VPN spokes (branch offices) connected via the Internet to the VPN hub (Main Office).

### In this topology:

- The Broadband Internet connection uses cable or DSL modem, with a static public IP address
- There is a VPN tunnel from each spoke to the VPN hub over the Internet
- Only VPN traffic is allowed via the Internet connection



# Configuring the simple VPN topology Procedure

- 1. Configure each branch as follows:
  - · The default gateway is the Internet interface
  - VPN policy is configured on the Internet interface egress as follows:
    - Traffic from the local subnets to any IP address is encrypted, using tunnel mode IPSec
    - The remote peer is the Main Office (the VPN Hub)
  - An access control list (ACL) is configured on the Internet interface to allow only the VPN / ICMP traffic. See <u>Simple VPN topology</u> on page 451 for configuration settings.
- 2. Configure the VPN Hub (Main Office) as follows:
  - Static routing: Branch subnets > Internet interface
  - The VPN policy portion for the branch is configured as a mirror image of the branch, as follows:
    - Traffic from any to branch local subnets > encrypt, using tunnel mode IPSec
    - The remote peer is the VPN spoke (Branch Internet address)

# W Note:

For information about using access control lists, see Policy lists on page 497.

### Simple VPN topology

Traffic direction	ACL parameter	ACL value	Description
Ingress	IKE	Permit	-
Ingress	ESP	Permit	-
Ingress	ICMP	Permit	This enables the PMTUD application to work
Ingress	All allowed services from any IP address to any local subnet	Permit	Due to the definition of the VPN Policy, this will be allowed only if traffic comes over ESP
Ingress	Default VPN policy	Deny	-
Egress	IKE	Permit	-
Egress	ESP	Permit	-
Egress	ICMP	Permit	This enables the PMTUD application to work
Egress	All allowed services from any IP address to any local subnet	Permit	This traffic is tunnelled using VPN
Egress	Default	Deny	-

### Simple VPN topology example

```
crypto isakmp policy 1
        encryption aes
        hash sha
        group 2
        exit
crypto isakmp peer address <Main Office Public Internet Static IP Address>
        pre-shared-key <secret key>
        isakmp-policy 1
        exit
crypto ipsec transform-set ts1 esp-3des esp-sha-hmac
        set pfs 2
        exit
crypto map 1
        set peer <Main OfficeMain Office Public Internet Static IP
        set transform-set ts1
        exit
ip crypto-list 901
      local-address <Branch Office Public Internet Static IP Address>
      ip-rule 10
               source-ip <Branch Subnet1> <Branch Subnet1 Mask>
               destination-ip any
               protect crypto map 1
               exit
     ip-rule 20
               source-ip <Branch Subnet2> <Branch Subnet2 Mask>
               destination-ip any
               protect crypto map 1
               exit
    exit
ip access-control-list 301
     ip-rule 10
             source-ip any
```

```
destination-ip any
            ip-protocol udp
            udp destination-port eq Ike
            composite-operation Permit
             exit
   ip-rule 11
             source-ip any
             destination-ip any
             ip-protocol
                           udp
             udp destination-port eq Ike-nat-t
             composite-operation permit
             exit
   ip-rule 12
             source-ip any
             destination-ip any
             ip-protocol
                          udp
             udp destination-port eq Ike-nat-t-vsu
             composite-operation permit
   ip-rule 20
             source-ip any
            destination-ip any
            ip-protocol esp
            composite-operation Permit
            exit
   ip-rule 30
            source-ip any
            destination-ip any
             ip-protocol icmp
            composite-operation Permit
            exit
   ip-rule 40
             source-ip any
            destination-ip host <Branch Subnet1> <Branch Subnet1 Mask>
            composite-operation Permit
            exit
   ip-rule 50
            source-ip any
            destination-ip host <Branch Subnet2> <Branch Subnet2 Mask>
            composite-operation Permit
            exit
   ip-rule default
            composite-operation deny
            exit
   exit
ip access-control-list 302
   ip-rule 10
            source-ip any
            destination-ip any
             ip-protocol udp
            udp destination-port eq Ike
            composite-operation Permit
            exit
   ip-rule 11
             source-ip any
             destination-ip any
             ip-protocol
                           udp
             udp destination-port eq Ike-nat-t
             composite-operation permit
             exit
   ip-rule 12
             source-ip any
             destination-ip any
             ip-protocol
                            udp
             udp destination-port eq Ike-nat-t-vsu
```

```
composite-operation permit
      ip-rule 20
               source-ip any
               destination-ip any
               ip-protocol esp
               composite-operation Permit
               exit
      ip-rule 30
               source-ip any
               destination-ip any
               ip-protocol icmp
               composite-operation Permit
               exit
      ip-rule 40
               desintation-ip any
               source-ip host <Branch Subnet1> <Branch Subnet1 Mask>
               composite-operation Permit
      ip-rule 50
               destination-ip any
               source-ip host <Branch Subnet2> <Branch Subnet2 Mask>
               composite-operation Permit
               exit.
      ip-rule default
               composite-operation deny
      exit
interface vlan 1.1
        ip-address <Branch Subnet1> <Branch Subnet1 Mask>
       pmi
     icc-vlan
    exit
interface vlan 1.2
       ip-address <Branch Subnet2> <Branch Subnet2 Mask>
       exit
interface FastEthernet 10/3
        encapsulation PPPoE
       traffic-shape rate 256000
        ip Address <Branch Office Public Internet Static IP Address>
                                                  <Branch Office Public Internet network mask>
        ip crypto-group
ip access-group
ip access-group
301 in
302 out
         exit
ip default-gateway FastEthernet 10/3 high
```

### Dynamic local peer IP

When the number of static IP addresses in an organization is limited, the ISP allocates temporary IP addresses to computers wishing to communicate over IP. These temporary addresses are called dynamic IP addresses.

The Branch Gateway IPSec VPN feature provides dynamic local peer IP address support. To work with dynamic local peer IP, you must first configure some prerequisites and then instruct the Branch Gateway to learn the IP address dynamically using either PPPoE or DHCP client.

# Note:

When working with dynamic local peer IP, you must verify that it is the Branch Gateway that initiates the VPN connection. The VPN peer cannot initiate the connection since it does not

know the Branch Gateway's IP address. To maintain the Branch Gateway as the initiator, do one of the following:

- Specify continuous channel in the context of the VPN peer, to maintain the IKE phase 1 connection even when no traffic is sent (see Continuous channel on page 456).
- Maintain a steady transmission of traffic by sending GRE keepalives or employing object tracking.

### Prerequisites for dynamic local peer IP

• Specify IKE aggressive mode with the initiate mode aggressive command when entering the ISAKMP peer information (see <u>Configuring ISAKMP peer information</u> on page 435).

```
Gxxx-001(config-peer:149.49.70.1) # initiate mode aggressive
Done!
```

 Specify the local device by its FQDN name, using the self-identity command, when entering the ISAKMP peer information (see <u>Configuring ISAKMP peer information</u> on page 435). For example:

```
Gxxx-001(config-peer:149.49.70.1) # self-identity fqdn vpn.avaya.com
Done!
```

• Specify the local address by name in the ip crypto lists, using the local-address command (see <u>Configuring crypto lists</u> on page 441). You must specify the local address by interface name. For example:

```
Gxxx-001(Crypto 901) # local-address FastEthernet 10/3
Done!
```

### Configuring dynamic local peer IP on a PPPoE interface

### **Procedure**

1. Enter the context of the FastEthernet interface.

### For example:

```
Gxxx-001(config) # interface fastethernet 10/3
Gxxx-001(config-if:FastEthernet 10/3) #
```

2. Enter the following commands in the context of the interface: no ip address, encapsulation pppoe, and ip address negotiated.

```
Gxxx-001(config-if:FastEthernet 10/3) # no ip address
Done!
Gxxx-001(config-if:FastEthernet 10/3) # encapsulation pppoe
Done!
Gxxx-001(config-if:FastEthernet 10/3) # ip address negotiated
Done!
```

3. Exit the context of the interface, and set the interface name as the next hop.

#### For example:

```
Gxxx-001(config-if:FastEthernet 10/3) # exit
Gxxx-001(config) # ip default-gateway FastEthernet 10/3
Done!
```

PPP over Ethernet (PPPoE) is a client-server protocol used for carrying PPP-encapsulated data over Ethernet frames. You can configure PPPoE on the Branch Gateway's ETH WAN Fast Ethernet port. For more information about PPPoE on the Branch Gateway, see <u>Configuring PPPoE</u> on page 227.

# Configuring dynamic local peer IP for a DHCP Client Procedure

- 1. Permit DHCP packets in the ingress access control list (ACL) and the egress ACL.
  - To do so, perform the following:
    - a. Use the no ip access-group command to deactivate both the ingress ACL and the egress ACL on the FastEthernet interface.
    - Add a rule to the ingress ACL and to the egress ACL, permitting DHCP packets to pass (for information on defining ACL policy rules, see <u>Policy rule configuration</u> on page 505).
    - c. Use the ip access-group command to activate the ingress ACL and the egress ACL on the FastEthernet interface.

### For example:

```
! Deactivate the Ingress and Egress ACLs on the FastEthernet Interface
Gxxx-001(config) # interface fastethernet 10/3
Gxxx-001(config-if:FastEthernet 10/3) # no ip access-group in
Done!
Gxxx-001(config-if:FastEthernet 10/3)# no ip access-group out
Gxxx-001(config-if:FastEthernet 10/3)# exit
! Add a Permit rule to the Ingress ACL for DHCP
Gxxx-001(config) # ip access-control-list 301
Gxxx-001(config-ACL 301) # ip-rule 25
Gxxx-001(config-ACL 301/ip rule 25) # source-ip any
Gxxx-001(config-ACL 301/ip rule 25) # destination-ip any
Gxxx-001(config-ACL 301/ip rule 25) # ip-protocol udp
Gxxx-001(config-ACL 301/ip rule 25) # udp source-port eq bootps
Done!
Gxxx-001(config-ACL 301/ip rule 25)# udp destination-port eq bootpc
Gxxx-001(config-ACL 301/ip rule 25)# composite-operation permit
Gxxx-001(config-ACL 301/ip rule 25)# exit
Gxxx-001(config-ACL 301) # exit
! Add a Permit rule to the Egress ACL for DHCP
Gxxx-001(config) # ip access-control-list 302
Gxxx-001(config-ACL 302)# ip-rule 25
Gxxx-001(config-ACL 302/ip rule 25)# source-ip any
Done!
Gxxx-001(config-ACL 302/ip rule 25) # destination-ip any
```

```
Done!
Gxxx-001(config-ACL 302/ip rule 25) # ip-protocol udp
Gxxx-001(config-ACL 302/ip rule 25) # udp source-port eq bootpc
Gxxx-001(config-ACL 302/ip rule 25)# udp destination-port eq bootps
Done!
Gxxx-001(config-ACL 302/ip rule 25)# composite-operation permit
Gxxx-001(config-ACL 302/ip rule 25)# exit
Gxxx-001(config-ACL 302)# exit
! Activate the Ingress and Egress ACLs on the FastEthernet Interface
Gxxx-001(config) # interface fastethernet 10/3
Gxxx-001(config-if:FastEthernet 10/3)# ip access-group 301 in
Done!
Gxxx-001(config-if:FastEthernet 10/3) # ip access-group 302 out
```

2. Specify no ip address and then ip address dhcp in the context of the FastEthernet Interface.

### For example:

```
Gxxx-001(config-if:FastEthernet 10/3) # no ip address
no ip address defined on this interface
Gxxx-001(config-if:FastEthernet 10/3)# ip address dhcp
```

3. Exit the context of the interface, and set the interface name as the next hop.

### For example:

```
Gxxx-001(config-if:FastEthernet 10/3)#exit
Gxxx-001(config) # ip route 5.0.0.0 255.0.0.0 FastEthernet 10/3
Done!
```



### Note:

For more information on DHCP client in the Branch Gateway, see DHCP client configuration on page 178.

### Continuous channel

An IPSec VPN connection exists as long as traffic is traversing the connection, or the timeouts have not expired. However, there are advantages to keeping the connection continuously alive. such as eliminating the waiting time necessary to construct a new IPSec VPN connection.

The Branch Gateway IPSec VPN feature supports continuous channel, which maintains a continuous IPSec VPN connection. That means that when you activate the ip crypto-group command on the defined interface, the IPSec VPN tunnel is immediately started, even if no traffic is traversing the interface and the timeouts have expired.

### Enabling continuous channel

### About this task

You can set continuous channel for either or both IKE phase 1 and IKE phase 2, as follows:

### **Procedure**

 To set continuous channel for IKE phase 1, enter continuous-channel when configuring the crypto ISAKMP peer information (see <u>Configuring ISAKMP peer</u> <u>information</u> on page 435).

#### For example:

```
Gxxx-001# crypto isakmp peer address 149.49.70.1
Gxxx-001(config-peer:149.49.70.1)# continuous-channel
Done!
```

2. To set continuous channel for IKE phase 2, enter continuous-channel when configuring the crypto map.

See Configuring crypto maps on page 439.

### For example:

```
Gxxx-001# crypto map 1
Gxxx-001(config-crypto:1)# continuous-channel
Done!
```

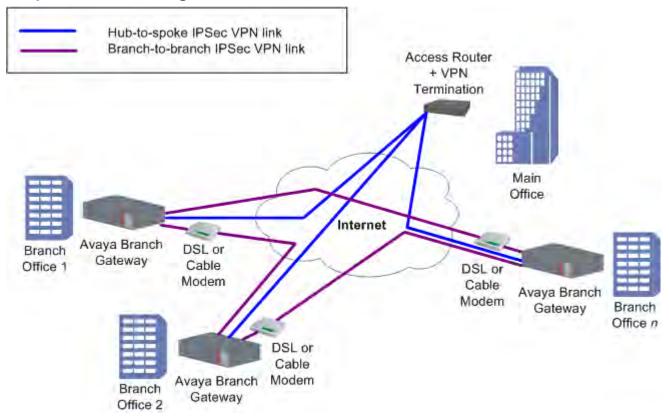
### Full or partial mesh

This installation is very similar to the simple hub and spokes installation, but instead of connecting to a single central site, the branch is also connected to several other branch sites by direct IPSec VPN tunnels. The configuration is therefore very similar to the previous one, duplicated several times.

In this topology:

- The Broadband Internet connection uses cable or DSL modem, with a static public IP address
- There is a VPN tunnel from each spoke to the VPN hub over the Internet
- There is a VPN tunnel from one spoke to another spoke
- Only VPN traffic is allowed via the Internet connection

# Full or partial mesh diagram



# Configuring the mesh VPN topology Procedure

- 1. Configure Branch Office 1 as follows:
  - The default gateway is the Internet interface
  - VPN policy is configured on the Internet interface egress as follows:
    - Traffic from the local subnets to the second spoke subnets -> encrypt, using tunnel mode IPSec, with the remote peer being the second spoke
    - Traffic from the local subnets to any IP address -> encrypt, using tunnel mode IPSec, with the remote peer being the main office (VPN hub)
  - An access control list (ACL) is configured on the Internet interface to allow only the VPN / ICMP traffic. See step 2 for configuration settings.

# Note:

For information about using access control lists, see Policy lists on page 497.

- 2. Configure Branch Office 2 as follows:
  - The default gateway is the Internet interface

- VPN policy is configured on the Internet interface egress as follows:
  - Traffic from the local subnets to the First Spoke subnets -> encrypt, using tunnel mode IPSec, with the remote peer being the First Spoke
  - Traffic from the local subnets to any IP address -> encrypt, using tunnel mode IPSec, with the remote peer being the Main Office (VPN hub)
- An ACL is configured on the Internet interface to allow only the VPN / ICMP traffic. See <u>Mesh VPN topology – Branch Office 2</u> on page 460 for configuration settings.

For information about using access control lists, see Policy lists on page 497.

- 3. Configure the VPN Hub (Main Office) as follows:
  - Static routing: Branch subnets -> Internet interface
  - The VPN policy portion for the branch is configured as a mirror image of the branch, as follows:
    - Traffic from any IP address to branch local subnets -> encrypt, using tunnel mode IPSec
    - The remote peer is the VPN Spoke (Branch Internet address)

### Mesh VPN topology - Branch Office 1

Traffic direction	ACL parameter	ACL value	Description
Ingress	IKE from Main Office IP to Branch IP	Permit	-
Ingress	ESP from Main Office IP to Branch IP	Permit	-
Ingress	IKE from Second Branch IP to Branch IP	Permit	-
Ingress	ESP from Second Branch IP to Branch IP	Permit	-
Ingress	ICMP from any IP address to local tunnel endpoint	Permit	This enables the PMTUD application to work
Ingress	All allowed services from any IP address to any local subnet	Permit	Due to the definition of the VPN Policy, this will be allowed only if traffic comes over ESP
Ingress	Default	Deny	-
Egress	IKE from Branch IP to Main Office IP	Permit	-
Egress	ESP from Branch IP to Main Office IP	Permit	-

Table continues...

Traffic direction	ACL parameter	ACL value	Description
Egress	IKE from Branch IP to Second Branch IP	Permit	This enables the PMTUD application to work
Egress	ESP from Branch IP to Second Branch IP	Permit	This traffic is tunnelled using VPN
Egress	ICMP from local tunnel endpoint to any IP address	Permit	This enables the PMTUD application to work
Egress	All allowed services from any local subnet to any IP address	Permit	This traffic is tunnelled using VPN
Egress	Default	Deny	-

### Mesh VPN topology - Branch Office 2

Traffic direction	ACL parameter	ACL value	Description
Ingress	IKE from Main Office IP to Branch IP	Permit	-
Ingress	ESP from Main Office IP to Branch IP	Permit	-
Ingress	IKE from First Branch IP to Branch IP	Permit	-
Ingress	ESP from First Branch IP to Branch IP	Permit	-
Ingress	ICMP from any IP address to local tunnel endpoint	Permit	This enables the PMTUD application to work
Ingress	All allowed services from any IP address to any local subnet	Permit	Due to the definition of the VPN Policy, this will be allowed only if traffic comes over ESP
Ingress	Default	Deny	-
Egress	IKE from Branch IP to Main Office IP	Permit	-
Egress	ESP from Branch IP to Main Office IP	Permit	-
Egress	IKE from Branch IP to First Branch IP	Permit	This enables the PMTUD application to work
Egress	ESP from Branch IP to First Branch IP	Permit	This traffic is tunnelled using VPN
Egress	ICMP from local tunnel endpoint to any IP address	Permit	This enables the PMTUD application to work
Egress	All allowed services from any local subnet to any IP address	Permit	This traffic is tunnelled using VPN
Egress	Default	Deny	-

# Mesh VPN topology example

# **Branch Office 1 configuration**

```
crypto isakmp policy 1
encryption aes
hash sha
group 2
exit
```

```
crypto isakmp peer address <Main Office Public Internet Static IP
        pre-shared-key <secret key>
         isakmp-policy 1
         exit
crypto isakmp peer address < Second Branch Office Public Internet Static
        pre-shared-key <secret key 2>
        isakmp-policy 1
        exit
crypto ipsec transform-set ts1 esp-3des esp-sha-hmac
        set pfs 2
        exit
crypto map 1
        set peer <Main Office Public Internet Static IP Address>
        set transform-set ts1
        exit
crypto map 2
         set peer <Second Branch Office Public Internet Static IP Address>
        set transform-set ts1
        exit
ip crypto-list 901
      local-address <Branch Office Public Internet Static IP Address>
     ip-rule 1
               source-ip <Branch Subnet1> <Branch Subnet1 Mask>
               destination-ip
                               <Second Branch Subnet1> <Second Branch</pre>
               protect crypto map 2
               exit
     ip-rule 2
               source-ip <Branch Subnet2> <Branch Subnet2 Mask>
               destination-ip <Second Branch Subnet1> <Second Branch
               protect crypto map 2
               exit
     ip-rule 3
               source-ip <Branch Subnet1> <Branch Subnet1 Mask>
               destination-ip <Second Branch Subnet2> <Second Branch
               protect crypto map 2
               exit
     ip-rule 4
               source-ip <Branch Subnet2> <Branch Subnet2 Mask>
               destination-ip <Second Branch Subnet2> <Second Branch
               protect crypto map 2
       ip-rule 10
               source-ip <Branch Subnet1> <Branch Subnet1 Mask>
               destination-ip any
               protect crypto map 1
               exit
     ip-rule 20
              source-ip <Branch Subnet2> <Branch Subnet2 Mask>
               destination-ip any
               protect crypto map 1
               exit
     exit
ip access-control-list 301
     ip-rule 10
              source-ip any
              destination-ip any
```

Subne

Subne

Subne

Subne

```
ip-protocol udp
               udp destination-port eq Ike
               composite-operation Permit
               exit
     ip-rule 11
                source-ip any
                destination-ip any
                ip-protocol
                              udp
                udp destination-port eq Ike-nat-t
                composite-operation permit
      ip-rule 12
                source-ip any
                destination-ip any
                ip-protocol
                               udp
                udp destination-port eq Ike-nat-t-vsu
                composite-operation permit
                exit
      ip-rule 20
               source-ip any
               destination-ip any
               ip-protocol esp
               composite-operation Permit
               exit
     ip-rule 30
              source-ip any
              destination-ip any
               ip-protocol icmp
               composite-operation Permit
               exit
     ip-rule 40
               source-ip any
               destination-ip host <Branch Subnet1> <Branch Subnet1 Mask>
               composite-operation Permit
               exit
     ip-rule 50
               source-ip any
               destination-ip host <Branch Subnet2> <Branch Subnet2 Mask>
               composite-operation Permit
               exit
     ip-rule default
              composite-operation deny
              exit
     exit
ip access-control-list 302
     ip-rule 10
               source-ip any
               destination-ip any
               ip-protocol udp
               udp destination-port eq Ike
               composite-operation Permit
               exit
      ip-rule 11
                source-ip any
                destination-ip any
                ip-protocol
                               udp
                udp destination-port eq Ike-nat-t
                composite-operation permit
                exit
     ip-rule 12
                source-ip any
                destination-ip any
                ip-protocol
                               udp
                udp destination-port eq Ike-nat-t-vsu
                composite-operation permit
```

```
exit
     ip-rule 20
               source-ip any
               destination-ip any
               ip-protocol esp
               composite-operation Permit
               exit
      ip-rule 30
               source-ip any
               destination-ip any
               ip-protocol icmp
               composite-operation Permit
               exit
     ip-rule 40
               desintation-ip any
               source-ip host <Branch Subnet1> <Branch Subnet1 Mask>
               composite-operation Permit
     ip-rule 50
               destination-ip any
               source-ip host <Branch Subnet2> <Branch Subnet2 Mask>
               composite-operation Permit
               exit
     ip-rule default
               composite-operation deny
     exit.
interface vlan 1.1
        ip-address <Branch Subnet1> <Branch Subnet1 Mask>
       pmi
       icc-vlan
       exit
interface vlan 1.2
       ip-address <Branch Subnet2> <Branch Subnet2 Mask>
       exit
interface fastethernet 10/3
        encapsulation PPPoE
traffic-shape rate 256000
        ip Address <Branch Office Public Internet Static IP Address>
                                     <Branch Office Public Internet network mask>
                                901
        ip crypto-group
        ip access-group
                              301 in
                              302 out
        ip access-group
         exit
ip default-gateway FastEthernet 10/3 high
```

The highlighted commands are the CLI commands that add the mesh capabilities to the simple hub and spokes configuration.

### **Branch Office 2 configuration**

```
crypto isakmp policy 1
        encryption aes
        hash sha
        group 2
        exit
crypto isakmp peer address <Main Office Public Internet Static IP

    pre-shared-key <secret key>
    isakmp-policy 1
    exit
```

```
crypto isakmp peer address <First Branch Office Public Internet Static IP
        pre-shared-key <secret key 2>
         isakmp-policy 1
        exit
crypto ipsec transform-set ts1 esp-3des esp-sha-hmac
        set pfs 2
        exit
crypto map 1
        set peer <Main Office Public Internet Static IP Address>
        set transform-set ts1
        exit
crypto map 2
        set peer <First Branch Office Public Internet Static IP Address>
        set transform-set ts1
        exit
ip crypto-list 901
      local-address <Branch Office Public Internet Static IP Address>
               source-ip <Branch Subnet1> <Branch Subnet1 Mask>
               destination-ip <First Branch Subnet1> <Second Branch
               protect crypto map 2
               exit
     ip-rule 2
               source-ip <Branch Subnet2> <Branch Subnet2 Mask>
               destination-ip <First Branch Subnet1> <Second Branch
               protect crypto map 2
               exit
     ip-rule 3
               source-ip <Branch Subnet1> <Branch Subnet1 Mask>
               destination-ip <First Branch Subnet2> <Second Branch
               protect crypto map 2
               exit
     ip-rule 4
               source-ip <Branch Subnet2> <Branch Subnet2 Mask>
               destination-ip <First Branch Subnet2> <Second Branch
               protect crypto map 2
               exit
     ip-rule 10
               source-ip <Branch Subnet1> <Branch Subnet1 Mask>
               destination-ip any
               protect crypto map 1
               exit
     ip-rule 20
               source-ip <Branch Subnet2> <Branch Subnet2 Mask>
               destination-ip any
               protect crypto map 1
               exit
    exit
ip access-control-list 301
     ip-rule 10
               source-ip any
               destination-ip any
               ip-protocol udp
               udp destination-port eq Ike
               composite-operation Permit
     ip-rule 11
               source-ip any
```

Administering Avaya G450 Branch Gateway Comments on this document? infodev@avaya.com Subr

Subr

Subr

Subr

```
destination-ip any
              ip-protocol
                            udp
              udp destination-port eq Ike-nat-t
              composite-operation permit
              exit
    ip-rule 12
              source-ip any
              destination-ip any
              ip-protocol
                            udp
              udp destination-port eq Ike-nat-t-vsu
              composite-operation permit
              exit
     ip-rule 20
             source-ip any
             destination-ip any
             ip-protocol esp
             composite-operation Permit
   ip-rule 30
             source-ip any
             destination-ip any
             ip-protocol icmp
             composite-operation Permit
             exit
   ip-rule 40
             source-ip any
             destination-ip host <Branch Subnet1> <Branch Subnet1 Mask>
             composite-operation Permit
             exit
   ip-rule 50
             source-ip any
             destination-ip host <Branch Subnet2> <Branch Subnet2 Mask>
             composite-operation Permit
             exit
   ip-rule default
            composite-operation deny
   exit
ip access-control-list 302
    ip-rule 10
             source-ip any
             destination-ip any
             ip-protocol udp
             udp destination-port eq Ike
             composite-operation Permit
             exit
    ip-rule 11
              source-ip any
              destination-ip any
              ip-protocol udp
              udp destination-port eq Ike-nat-t
              composite-operation permit
              exit
   ip-rule 12
              source-ip any
              destination-ip any
              ip-protocol
                            udp
              udp destination-port eq Ike-nat-t-vsu
              composite-operation permit
              exit
    ip-rule 20
             source-ip any
             destination-ip any
             ip-protocol esp
```

```
composite-operation Permit
              exit.
     ip-rule 30
             source-ip any
             destination-ip any
             ip-protocol icmp
             composite-operation Permit
              exit
     ip-rule 40
             desintation-ip any
             source-ip host <Branch Subnet1> <Branch Subnet1 Mask>
              composite-operation Permit
              exit
     ip-rule 50
             destination-ip any
             source-ip host <Branch Subnet2> <Branch Subnet2 Mask>
              composite-operation Permit
     ip-rule default
             composite-operation deny
             exit
     exit
interface vlan 1.1
       ip-address <Branch Subnet1> <Branch Subnet1 Mask>
       pmi
       icc-vlan
       exit.
interface vlan 1.2
       ip-address <Branch Subnet2> <Branch Subnet2 Mask>
       exit
interface fastethernet 10/3
       encapsulation PPPoE
traffic-shape rate 256000
        <Branch Office Public Internet network mask>
        ip crypto-group
                            901
                           301 in
        ip access-group
        ip access-group
                          302 out
ip default-gateway FastEthernet 10/3 high
```

The highlighted commands are the CLI commands that add the mesh capabilities to the simple hub and spokes configuration.

# Full solution: hub and spoke with VPN

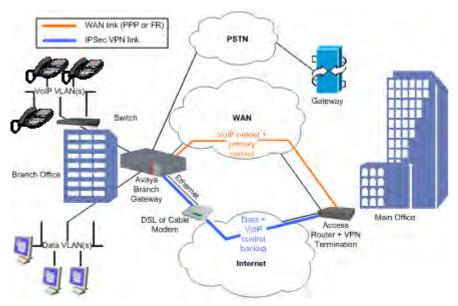
The full solution consists of a hub-and-spoke with VPN for data and VoIP control backup.

In this topology:

- There is a direct WAN connection to the Main Office for VoIP bearer and as primary VoIP control connection.
- The Broadband Internet connection uses cable or DSL modem, with a static public IP address
- There is a VPN tunnel to the hub over the Internet for intranet data, and as backup connection for VoIP control

- The local hosts access the Internet directly through the local broadband connection
- The PSTN connection backs up the voice bearer

# Full solution: hub-and-spoke with VPN for data and VoIP control backup



# Configuring hub-and-spoke with VPN for data and VoIP control backup Procedure

- 1. Configure the Branch Office as follows:
  - The default gateway is the Internet interface.
  - VPN policy is configured on the Internet interface egress as follows: Traffic from the local GRE tunnel endpoint to the remote GRE tunnel endpoint > encrypt, using IPSec tunnel mode, with the remote peer being the Main Office.
  - An access control list (ACL) is configured on the Internet interface to allow only the VPN tunnel and ICMP traffic. See <u>Configuring hub-and-spoke with VPN for data and VoIP</u> <u>control backup</u> on page 467 for configuration settings.

# **Note:**

For information about using access control lists, see Policy lists on page 497.

- Policy Based Routing (PBR) is configured as follows on VoIP VLAN and loopback interfaces:
  - Destination IP = local subnets > Route: DBR
  - DSCP = bearer > Route: WAN
  - DSCP = control > Route: 1. WAN 2. DBR

For information about PBR, see Policy-based routing section.

- 2. Configure the VPN Hub (Main Office) as follows:
  - The VPN policy portion for the branch is configured as a mirror image of the branch
  - The ACL portion for the branch is a mirror image of the branch, with some minor modifications
  - Static routing is configured as follows:

Branch subnets > Internet interface

- The PBR portion for the branch is configured as follows, on most interfaces:
  - Destination IP = branch VoIP subnets or GW address (PMI), DSCP = bearer > Route:
     WAN
  - Destination IP = branch VoIP subnets or GW address (PMI), DSCP = control > Route:
     1. WAN 2. DBR
- ACM is configured to route voice calls through PSTN when the main VoIP trunk is down.

### **Hub-and-spoke with VPN**

Traffic direction	ACL parameter	ACL value
Ingress	IKE (UDP/500) from remote tunnel endpoint to local tunnel endpoint	Permit
Ingress	ESP/AH from remote tunnel endpoint to local tunnel endpoint	Permit
Ingress	Remote GRE tunnel endpoint to local GRE tunnel endpoint	Permit
Ingress	Allowed ICMP from any IP address to local tunnel endpoint	Permit
Ingress	Default	Deny
Egress	IKE (UDP/500) from local tunnel endpoint to remote tunnel endpoint	Permit
Egress	Local GRE tunnel endpoint to remote GRE tunnel endpoint	Permit
Egress	All allowed services from any local subnet to any IP address	Permit
Egress	Allowed ICMP from local tunnel endpoint to any IP address	Permit
Egress	Default	Deny

### **Hub-and-spoke with VPN example**

```
crypto isakmp policy 1
    encryption aes
    hash sha
    group 2
    authentication pre-share
    exit
crypto isakmp peer address <Main Office Internet public Static IP

pre-shared-key <key1>
    isakmp-policy 1
    exit
crypto ipsec transform-set ts1 esp-3des esp-sha-hmac
    exit
crypto map 1
```

```
set peer <Main Office Internet public Static IP Address>
   set transform-set ts1
   exit
ip crypto-list 901
     local-address <Branch Office Public Internet Static IP Address>
     ip-rule 10
               source-ip <Branch data Subnet> <Branch data Subnet Mask>
               destination-ip any
               protect crypto map 1
               exit
     ip-rule 20
               source-ip <Branch voice Subnet> <Branch voice Subnet Mask>
               destination-ip any
               protect crypto map 1
               exit
     exit
ip access-control-list 301
     ip-rule 10
               source-ip any
               destination-ip any
               ip-protocol udp
               udp destination-port eq Ike
               composite-operation Permit
               exit
     ip-rule 11
              source-ip any
             destination-ip any
              ip-protocol
                            udp
              udp destination-port eq Ike-nat-t
              composite-operation permit
              exit.
      ip-rule 12
               source-ip any
               destination-ip any
               ip-protocol
                              udp
               udp destination-port eq Ike-nat-t-vsu
               composite-operation permit
               exit
     ip-rule 20
               source-ip any
               destination-ip any
               ip-protocol esp
               composite-operation Permit
               exit
     ip-rule 30
               source-ip any
              destination-ip any
               ip-protocol icmp
               composite-operation Permit
               exit
     ip-rule 40
               source-ip any
               destination-ip <Branch data Subnet> <Branch data Subnet
               composite-operation Permit
               exit
     ip-rule 50
               source-ip any
               destination-ip <Branch voice Subnet> <Branch voice Subnet
               composite-operation Permit
               exit
     ip-rule default
              composite-operation deny
```

```
exit
ip access-control-list 302
     ip-rule 10
               source-ip any
               destination-ip any
               ip-protocol udp
               udp destination-port eq Ike
               composite-operation Permit
               exit
    ip-rule 11
              source-ip any
              destination-ip any
              ip-protocol
                            udp
              udp destination-port eq Ike-nat-t
              composite-operation permit
              exit
      ip-rule 12
               source-ip any
               destination-ip any
               ip-protocol
                            udp
               udp destination-port eq Ike-nat-t-vsu
               composite-operation permit
               exit
     ip-rule 20
               source-ip any
               destination-ip any
               ip-protocol esp
               composite-operation Permit
               exit
      ip-rule 30
               source-ip any
               destination-ip any
               ip-protocol icmp
               exit
      ip-rule 40
               source-ip <Branch data Subnet> <Branch data Subnet Mask>
               destination-ip
                                     any
               composite-operation Permit
               exit
      ip-rule 50
               source-ip <Branch voice Subnet> <Branch voice Subnet Mask>
               destination-ip
                                    any
               composite-operation Permit
               exit
     ip-rule default
               composite-operation deny
     exit
interface vlan 1
   description "VoIP_VLAN"
   ip address <branch voice subnet IP address> <branch voice subnet mask>
   icc-vlan
   pmi
   exit
interface vlan 2
  description "DATA VLAN"
   ip address <branch data subnet IP address> <branch data subnet mask>
       interface fastethernet 10/3
    encapsulation pppoe
traffic-shape rate 256000
    ip address <Branch Office Internet public Static IP Address> <Branch
                                                                  Office Internet public net mask>
ip crypto-group 901
                          301 in
ip access-group
```

```
ip access-group 302 out
    exit
interface serial 3/1 ip address <Branch Office serial IP address> <Branch Office
serial
   exit
ip next-hop-list 2
   next-hop-interface 1 FastEthernet 10/3 next-hop-interface 2 serial 3/1
ip pbr-list 801
 ip-rule 10
! The following command specifies the Voice bearer
     dscp 46
    next-hop list 1
     exit
 ip-rule 20
 The following command specifies the Voice Control
    dscp 34
    next-hop list 2
    exit
 ip-rule default
    next-hop PBR
    exit.
```

## Typical failover applications

### Introduction to the failover mechanism

The failover mechanism provides switchover to backup peers in case of remote peer failure. To enable the failover mechanism, you must:

- Configure VPN keepalives, which check the remote peer periodically and announce when the remote peer is dead
- Provide backup peers and a mechanism for switching to a backup in case of remote peer failure

In addition to the GRE failover mechanism (see <u>Failover using GRE</u> on page 472), the Branch Gateway supports several additional failover mechanisms which are described in the following sections.

## **VPN** keepalives

VPN keepalives can improve the speed with which the Branch Gateway detects loss of connectivity with the remote VPN peer. Two types of VPN keepalives are available. You can use either or both methods:

- Enable DPD keepalives, a standard VPN keepalive, that check whether the remote peer is up. This type of detection can be used only if it is supported also by the remote peer.
- Bind peer status to an object tracker. Object trackers track the state (up/down) of remote devices using keepalive probes, and notify registered applications such as VPN when the state changes. Object tracking allows monitoring of hosts inside the remote peer's protected network, not just of the remote peer itself as in DPD.

## Backup peer mechanism

You can use any one of these alternate backup peer mechanisms:

- DNS server (see <u>Failover using DNS</u> on page 478). This method uses the Branch Gateway's DNS resolver capability for dynamically resolving a remote peer's IP address via a DNS query.
  - Use this feature when your DNS server supports failover through health-checking of redundant hosts. On your DNS server, configure a hostname to translate to two or more redundant hosts, which act as redundant VPN peers. On the Branch Gateway, configure that hostname as your remote peer. The Branch Gateway will perform a DNS query in order to resolve the hostname to an IP address before establishing an IKE connection. Your DNS server should be able to provide an IP address of a living host. The Branch Gateway will perform a new DNS query and try to re-establish the VPN connection to the newly provided IP address whenever it senses that the currently active remote peer stops responding. The Branch Gateway can sense that a peer is dead when IKE negotiation times-out, through DPD keepalives, and through object tracking.
- Using the Branch Gateway's peer-group entity (see <u>Failover using a peer-group</u> on page 483):
  - Define a peer-group. A peer-group is an ordered list of redundant remote peers, only one of which is active at any time. When the active peer is considered dead, the next peer in the list becomes the active remote peer.
  - When configuring a crypto map, point to the peer-group instead of to a single peer

## Failover using GRE

A branch with a Branch Gateway can connect to two or more VPN hub sites, in a way that will provide either redundancy or load sharing.

In this topology, the Branch Gateway is connected through its 10/100 WAN Ethernet port to a DSL modem.

- · Define two GRE Tunnel interfaces:
  - GRE1 that leads to a Primary Main Office GRE End Point behind the VPN Hub Gateway
  - GRE2 that leads to a Backup Main Office GRE End Point behind the VPN Hub Gateway
- Define two VPNs
- Connectivity to the networks in Primary/Backup Main Office is determined through GRE keepalives. If network connectivity is lost due to failures in the WAN, in the Primary Main Office, the GRE keep-alive will fail and the GRE interface will transition to a "down" state.

## Redundancy and load sharing modes

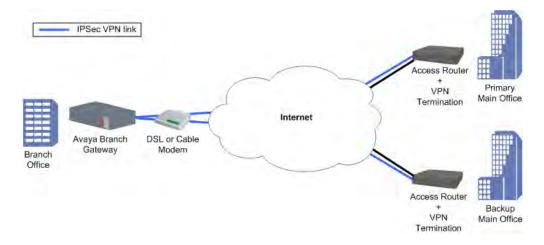
The two GRE tunnels can then be used for branch to Primary/Backup Main Office in either Redundancy or Load sharing mode:

**Redundancy:** GRE2 is configured as a backup interface for GRE1, and is activated only when GRE1 is down

**Load sharing:** Both Tunnel interfaces are active. Routing protocols (RIP or OSPF) route traffic to destinations based on route cost and availability, as follows:

For two routes of equal cost to the same destination, one through the Primary Main Office and one through the Backup Main Office, OSPF will automatically distribute traffic through both routes, effectively sharing the load between routes.

## Hub and spoke with hub redundancy/load sharing using GRE



# Configuring VPN hub redundancy and load sharing topologies using GRE

### **Procedure**

- 1. Configure the Branch Office as follows:
  - a. VPN policy is configured on the Internet interface egress as follows:
    - GRE Traffic from the local tunnel endpoint to remote tunnel endpoint 1 -> encrypt, using IPSec tunnel mode, with the remote peer being tunnel endpoint 1
    - GRE Traffic from the local tunnel endpoint to remote tunnel endpoint 2 -> encrypt, using IPSec tunnel mode, with the remote peer being tunnel endpoint 2
  - b. An access control list (ACL) is configured on the Internet interface to allow only the VPN / ICMP traffic. See <a href="VPN hub redundancy and load sharing topologies">VPN hub redundancy and load sharing topologies</a> on page 474 for configuration settings.
    - For information about using access control lists, see Policy lists on page 497.
  - c. Configure dynamic routing (OSPF or RIP) to run over local data interfaces (data VLANs) and on the GRE interfaces
- 2. Configure the VPN Hubs (Main Offices) as follows:
  - a. The VPN policy portion for the branch is configured as a mirror image of the branch
  - b. The ACL portion for the branch is a mirror image of the branch, with some minor modifications
  - c. The GRE Tunnel interface is configured for the branch
  - d. Dynamic routing (OSPF or RIP) is configured to run over the GRE interface to the branch

## VPN hub redundancy and load sharing topologies

Traffic direction	ACL parameter	ACL value
Ingress	IKE (UDP/500) from remote tunnel endpoint to local tunnel endpoint	Permit
Ingress	ESP/AH from remote tunnel endpoint to local tunnel endpoint	Permit
Ingress	Allowed ICMP from any IP address to local tunnel endpoint	Permit
Ingress	Default	Deny
Egress	IKE (UDP/500) from local tunnel endpoint to remote tunnel endpoint	Permit
Egress	All allowed services from any local subnet to any IP address	Permit
Egress	Allowed ICMP from local tunnel endpoint to any IP address	Permit
Egress	Default	Deny

## VPN hub redundancy and load sharing topologies example

```
crypto isakmp policy 1
   encryption aes
   hash sha
   group 2
   authentication pre-share
crypto isakmp peer address <Primary Main Office Internet public Static IP
  pre-shared-key <key1>
  isakmp-policy 1
  exit
crypto isakmp peer address <Backup Main Office Internet public Static
  pre-shared-key <key2>
  isakmp-policy 1
  exit
crypto ipsec transform-set ts1 esp-3des esp-sha-hmac
  exit
   set peer <Primary Main Office Internet public Static IP Address>
   set transform-set ts1
   exit
crypto map 2
   set peer <Backup Main Office Internet public Static IP Address>
   set transform-set ts1
   exit.
ip crypto-list 901
   local-address <Branch Office Internet public Static IP Address>
         source-ip host <Branch GRE Tunnel end point IP Address>
        destination-ip host <Primary Main Office GRE Tunnel end point IP
protect crypto map 1
ip-rule 2
         source-ip host <Branch GRE Tunnel end point IP Address>
        destination-ip host <Backup Main Office GRE Tunnel end point
protect crypto map 2
        exit
     exit
ip access-control-list 301
      ip-rule 30
               source-ip any
               destination-ip any
               ip-protocol udp
               udp destination-port eq Ike
               composite-operation Permit
               exit
      ip-rule 31
              source-ip any
             destination-ip any
              ip-protocol
                            udp
             udp destination-port eq Ike-nat-t
              composite-operation permit
              exit
     ip-rule 32
               source-ip any
               destination-ip any
               ip-protocol
                              udp
               udp destination-port eq Ike-nat-t-vsu
              composite-operation permit
```

```
exit
     ip-rule 40
               source-ip any
               destination-ip any
               ip-protocol esp
               composite-operation Permit
               exit
     ip-rule 50
               source-ip any
               destination-ip host <Branch Office Public Internet Static
               ip-protocol icmp
               composite-operation Permit
               exit
     ip-rule 60
               source-ip any
               destination-ip any
                        composite-operation Permit
     ip-rule 70
               source-ip host <Backup Main Office GRE Tunnel end point
               destination-ip host <Branch GRE Tunnel end point IP
               composite-operation Permit
               exit
      ip-rule default
              composite-operation deny
               exit
     exit
ip access-control-list 302
ip-rule 30
               source-ip any
               destination-ip any
               ip-protocol udp
               udp destination-port eq Ike
               composite-operation Permit
              exit
      ip-rule 31
              source-ip any
             destination-ip any
              ip-protocol
                           udp
              udp destination-port eq Ike-nat-t
             composite-operation permit
              exit
     ip-rule 32
              source-ip any
               destination-ip any
               ip-protocol
                             udp
               udp destination-port eq Ike-nat-t-vsu
               composite-operation permit
               exit
      ip-rule 40
               source-ip any
               destination-ip any
               ip-protocol esp
               composite-operation Permit
               exit
     ip-rule 50
               source-ip any
               destination-ip any
               ip-protocol icmp
               exit
     ip-rule 60
```

Ad

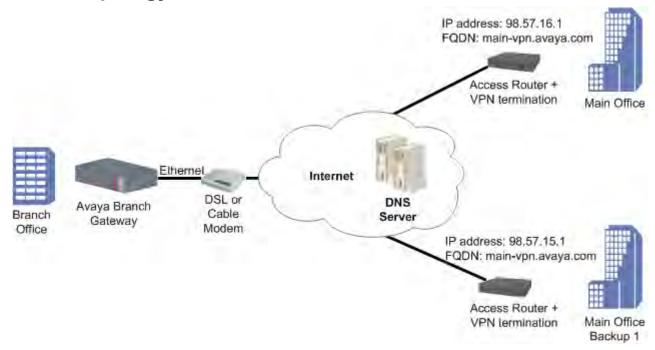
```
source-ip host <Branch GRE Tunnel end point IP Address>
               destination-ip host <Primary Main Office GRE Tunnel end
                                                                                              point
               composite-operation Permit
               exit
      ip-rule 70
               source-ip host <Branch GRE Tunnel end point IP Address>
               destination-ip host <Backup Main Office GRE Tunnel end
                                                                                              point
               composite-operation Permit
               exit
      ip-rule default
               composite-operation deny
               exit
     exit
interface vlan 1
   description "VoIP_VLAN"
    ip address <branch voice subnet IP address> <branch voice subnet mask>
   icc-vlan
   pmi
   exit
interface vlan 2
  description "DATA VLAN"
   ip address <branch data subnet IP address> <branch data subnet mask>
   exit
interface fastethernet 10/3
     encapsulation pppoe
traffic-shape rate 256000
     ip address <Branch Office Internet public Static IP Address> <Branch
                                                                   Office Internet public net mask>
ip crypto-group 901
                          301 in
     ip access-group
                          302 out
     ip access-group
     exit
interface Tunnel 1
! The following two backup commands specify redundant mode.
! To specify load-sharing mode, omit them.
backup interface tunnel 2
backup delay 20 15
keepalive 10 3
   tunnel source <Branch GRE Tunnel end point IP Address>
    tunnel destination <Primary MainPrimary Main Office GRE Tunnel end point IP
   ip address 10.10.10.1 255.255.255.252
   exit
interface Tunnel 2
   keepalive 10 3
  tunnel source <Branch GRE Tunnel end point IP Address>
  tunnel destination <Backup Main Office GRE Tunnel end point IP
                                                                                                Addr
  ip address 20.20.20.1 255.255.255.252
  exit
ip route <Primary Main Offfice GRE Tunnel end point IP Address>
                                                            255.255.255.255 FastEthernet 10/3 high
ip route <Backup Main Offfice GRE Tunnel end point IP Address>
                                                            255.255.255.255 FastEthernet 10/3 high
router ospf
  network 10.10.10.0 0.0.0.3 area 0.0.0.0
  network 20.20.20.0 0.0.0.3 area 0.0.0.0
exit
```

## Failover using DNS

The VPN DNS topology provides failover by utilizing the DNS resolver feature.

Use this feature when your DNS server supports failover through health-checking of redundant hosts. On your DNS server configure a hostname to translate to two or more redundant hosts, which act as redundant VPN peers. On the Branch Gateway configure that hostname as your remote peer. The Gateway will perform a DNS query in order to resolve the hostname to an IP address before establishing an IKE connection. Your DNS server should be able to provide an IP address of a living host. The Branch Gateway will perform a new DNS query and try to re-establish the VPN connection to the newly provided IP address whenever it senses that the currently active remote peer stops responding. The Branch Gateway can sense that a peer is dead when IKE negotiation times-out through DPD keepalives and through object tracking.

## VPN DNS topology



## Note:

For an explanation of DNS resolver, see DNS resolver on page 70.

## Configuring the VPN DNS topology

### **Procedure**

- 1. Define the private VLAN1 and VLAN2 interfaces (IP address and mask), and define one of them as the PMI and ICC-VLAN.
- 2. Define the public FastEthernet10/3 interface (IP address and mask).
- 3. Define the default gateway (the IP of the next router).

4. Define the DNS name-server-list and the IP address of the DNS server.



### Note:

Alternatively, you can use DHCP Client or PPPoE to dynamically learn the DNS server's IP address. Use the ip dhcp client request command when using DHCP client, or use the ppp ipcp dns request command when using PPPoE.

- Define the ISAKMP policy, using the crypto isakmp policy command.
- 6. Define the remote peer with FQDN, using the crypto isakmp peer address command, including:
  - the pre-shared key
  - the ISAKMP policy
- 7. Define the IPSEC transform-set, using the crypto ipsec transform-set command.
- 8. Define the crypto map, using the crypto map command.
- 9. Define the crypto list as follows:
  - a. Set the local address to the public interface name (for example, FastEthernet 10/3.0)
  - b. For each private interface, define an ip-rule using the following format:
    - source-ip <private subnet> <private subnet wild card mast>. For example, 10.10.10.0 0.0.0.255
    - destination-ip any
    - protect crypto map 1
- 10. Define the ingress access control list (ACL) to protect the device from Incoming traffic from the public interface, as follows:
  - a. Permit DNS traffic to allow clear (unencrypted) DNS traffic
  - b. Permit IKE Traffic (UDP port 500) for VPN control traffic (IKE)
  - c. Permit ESP traffic (IP Protocol ESP) for VPN data traffic (IPSEC)
  - d. Permit ICMP traffic, to support PMTU application support, for a better fragmentation process
  - e. For each private subnet, add a permit rule, with the destination being the private subnet and the source being any.
    - This traffic will be allowed only if it tunnels under the VPN, because of the crypto list.
  - f. Define all other traffic (default rule) as deny in order to protect the device from nonsecure traffic
- 11. Define the egress access control list to protect the device from sending traffic that is not allowed to the public interface (optional):
  - a. Permit DNS traffic to allow clear (unencrypted) DNS traffic

- b. Permit IKE Traffic (UDP port 500) for VPN control traffic (IKE)
- c. Permit ESP traffic (IP Protocol ESP) for VPN data traffic (IPSEC)
- d. Permit ICMP traffic, to support PMTU application support, for a better fragmentation process
- e. For each private subnet, add a permit rule, with the source being the private subnet, and the destination being any
- f. Define all other traffic (default rule) as deny in order to protect the device from sending non-secure traffic
- 12. Activate the crypto list, the ingress access control list, and the egress access control list, on the public interface.

## **VPN DNS topology example**

```
Define the Private Subnet1
interface vlan 1
  description "Branch Subnet1"
  ip address 10.0.10.1 255.255.255.0
  icc-vlan
  pmi
  exit
! Define the Private Subnet2
interface vlan 2
  description "Branch Subnet2"
  ip address 10.0.20.1 255.255.255.0
  exit
! Define the Public Subnet
interface fastethernet 10/3
  ip address 100.0.0.2 255.255.255.0
  exit
! Define the default gateway to be on the public subnet
ip default-gateway 100.0.0.1
! Define the DNS name server
! that is accessible without VPN.
ip domain name-server-list 1
  name-server 1 123.124.125.126
! Define the IKE Entity
crypto isakmp policy 1
  encryption aes
  hash sha
  group 2
  authentication pre-share
  exit
```

```
! Define the remote peer as FQDN (DNS Name)
crypto isakmp peer fqdn main-vpn.avaya.com
  pre-shared-key <key1>
  isakmp-policy 1
! Define the IPSEC Entity
crypto ipsec transform-set ts1 esp-3des esp-sha-hmac
! Define the VPN Tunnel
crypto map 1
 set peer main-vpn.avaya.com
  set transform-set ts1
  exit
! Define the crypto list for the public interface
ip crypto-list 901
  local-address "Fast Ethernet 10/3.0"
! ip-rule 5 allows un-encrypted traffic for DNS
  ip-rule 5
     source-ip
                   any
     destination-ip 123.124.125.126
     no protect
     exit
   ip-rule 10
     source-ip
                   10.0.10.0 0.0.0.255
      destination-ip any
     protect crypto map 1
     exit
  ip-rule 20
                   10.0.20.0 0.0.0.255
      source-ip
      destination-ip any
     protect crypto map 1
     exit
  exit
! Define the Ingress access control list for the public interface
ip access-control-list 301
  ip-rule 5
     source-ip
                          any
      destination-ip
                          any
                      udp
     ip-protocol
     udp destination-port eq Dns
     composite-operation Permit
     exit
   ip-rule 10
     source-ip
                          any
     destination-ip any in-protocol udp
     udp destination-port eq Ike
      composite-operation Permit
      exit
   ip-rule 11
     source-ip any
      destination-ip any
     ip-protocol udp
```

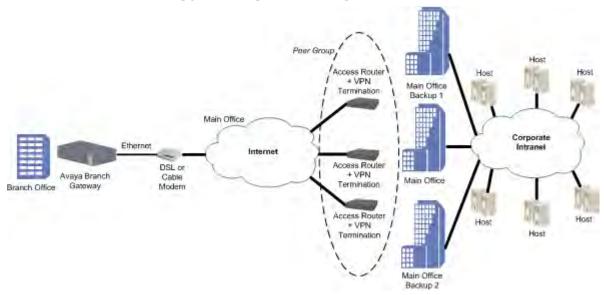
```
udp destination-port eq Ike-nat-t
     composite-operation permit
     exit
  ip-rule 12
     source-ip any
     destination-ip any
     ip-protocol udp
     udp destination-port eq Ike-nat-t-vsu
     composite-operation permit
     exit
  ip-rule 20
     source-ip
                         any
     destination-ip any
     ip-protocol
                          esp
     composite-operation Permit
     exit
  ip-rule 30
     source-ip
                          any
     destination-ip ip-protocol
                          any
                          icmp
     composite-operation Permit
     exit
  ip-rule 40
     source-ip
                          any
     destination-ip
                          10.0.10.0 0.0.0.255
     composite-operation Permit
     exit
  ip-rule 50
     source-ip
                          any
     destination-ip 10.0.20.0 0.0.0.255
     composite-operation Permit
     exit
ip-rule default
     composite-operation deny
     exit
   exit
! Define the Egress access control list for the public interface
ip access-control-list 302
  ip-rule 5
     source-ip
                         any
     destination-ip any ip-protocol udb
     udp destination-port eq dns
     composite-operation Permit
     exit
  ip-rule 10
     source-ip
                         any
     destination-ip any ip-protocol udp
     udp destination-port eq Ike
     composite-operation Permit
     exit
  ip-rule 11
     source-ip any
     destination-ip any
     ip-protocol udp
     udp destination-port eq Ike-nat-t
     composite-operation permit
     exit
  ip-rule 12
     source-ip any
     destination-ip any
     ip-protocol udp
```

```
udp destination-port eq Ike-nat-t-vsu
      composite-operation permit
      exit
   ip-rule 20
     source-ip any destination-ip any ip-protocol esp
      composite-operation Permit
      exit
   ip-rule 30
      source-ip any destination-ip any ip-protocol icmp
                              icmp
      composite-operation Permit
      exit
   ip-rule 40
      source-ip 10.0.10.0 0.0.0.255 destination-ip any composite-operation Permit
      exit.
 ip-rule 50
      source-ip 10.0.20.0 0.0.0.255 destination-ip any
      composite-operation Permit
      exit
   ip-rule default
      composite-operation deny
      exit.
    exit
! Activate the crypto list and the access control list on the public
interface fastethernet 10/3
   ip crypto-group 901
   ip access-group 301 in
   ip access-group 302 out
  exit
```

## Failover using a peer-group

The failover VPN topology utilizes a peer-group which lists a group of redundant peers. At any point in time, only one peer is active and acting as the remote peer. An object tracker monitors the state of the active peer. If the active peer is presumed dead, the next peer in the peer-group becomes the active remote peer. For more information on object trackers, see <a href="Object tracking">Object tracking</a> on page 258.

## Failover VPN topology using a peer-group



## Configuring the failover VPN topology using a peer-group

- 1. Define the private VLAN1 and VLAN2 interfaces (IP address and mask), and define one of them as the PMI and ICC-VLAN.
- 2. Define the public FastEthernet 10/3 interface (IP address and mask).
- 3. Define the default gateway (the IP address of the next router).
- 4. Define the object tracking configuration, and define when an object tracker is considered down, as follows:
  - Define a track list that will monitor (by ICMP) five hosts behind the specific peer. If two or more hosts are not working then the object tracker is down. The Branch Gateway will then pass on to the next peer in the peer group list.
- 5. Define the ISAKMP policy, using the crypto isakmp policy command.
- 6. Define the 3 remote peers, using the **crypto isakmp peer address** command, and specify for each one:
  - the pre-shared key
  - the ISAKMP policy
  - keepalive track. This track is the object tracker that checks if the peer is still alive. If an active peer is considered dead, the next peer in the peer group becomes the active peer.
- 7. Define a peer group that include all three remote peers, using the crypto isakmp peer-group command.
- 8. Define the IPSEC transform-set, using the crypto ipsec transform-set command.

- 9. Define the Crypto map entity, using the crypto map command.
- 10. Define the crypto list as follows:
  - a. Set the local address to the public interface name (for example, FastEthernet 10/3.0).
  - b. For each private interface, define an ip-rule using the following format:
    - source-ip <private subnet> <private subnet wild card mast>. For example, 10.10.10.0 0.0.0.255
    - destination-ip any
    - · protect crypto map 1
- 11. Define the ingress access control list to protect the device from incoming traffic from the public interface, as follows:
  - a. Permit IKE Traffic (UDP port 500) for VPN control traffic (IKE)
    - Note:

If you are using NAT Traversal, you must also open UDP port 4500 and 2070.

- b. Permit ESP traffic (IP Protocol ESP) for VPN data traffic (IPSEC)
- c. Permit ICMP traffic, to support PMTU application support, for a better fragmentation process
- d. For each private subnet, add a permit rule, with the destination being the private subnet, and the source being any. This traffic will be allowed only if it tunnels under the VPN, because of the crypto list.
- e. Define all other traffic (default rule) as deny in order to protect the device from nonsecure traffic
- 12. Optionally, define the egress access control list to protect the device from sending traffic that is not allowed to the public interface:
  - a. Permit IKE Traffic (UDP port 500) for VPN control traffic (IKE)
    - **⊗** Note:

If you are using NAT Traversal, you also need to open UDP port 4500 and 2070.

- b. Permit ESP traffic (IP Protocol ESP) for VPN data traffic (IPSEC)
- c. Permit ICMP traffic, to support the PMTU application, for a better fragmentation process
- d. For each private subnet add a permit rule, with the source being the private subnet, and the destination being any
- e. Define all other traffic (default rule) as deny in order to protect the device from sending non-secure traffic
- 13. Activate the crypto list, the ingress access control list, and the egress access control list, on the public interface.

## Failover VPN topology using a peer-group example

```
! Define the Private Subnet1
interface vlan 1
  description "Branch Subnet1"
  ip address 10.0.10.1 255.255.255.0
  icc-vlan
  pmi
  exit
! Define the Private Subnet2
interface vlan 2
  description "Branch Subnet2"
  ip address 10.0.20.1 255.255.255.0
  exit
! Define the Public Subnet
interface fastethernet 10/3
  ip address 100.0.0.2 255.255.255.0
! Define the default gateway the public interfce
ip default-gateway 100.0.0.1
! We wish to check 5 hosts in the Corporate intranet behind the current VPN
! remote peer, and if 2 or more hosts don't work then keepalive-track will fail ,
! and we will move to the next peer in the peer-group
rtr 1
  type echo protocol ipIcmpEcho <host1 IP>
  exit
rtr-schedule 1 start-time now life forever
  type echo protocol ipIcmpEcho <host2 IP>
rtr-schedule 2 start-time now life forever
   type echo protocol ipIcmpEcho <host3 IP>
rtr-schedule 3 start-time now life forever
  type echo protocol ipIcmpEcho <host4 IP>
rtr-schedule 4 start-time now life forever
  type echo protocol ipIcmpEcho <host5 IP>
rtr-schedule 5 start-time now life forever
track 11 rtr 1
 exit
track 12 rtr 2
 exit
track 13 rtr 3
 exit
track 14 rtr 4
 exit
track 15 rtr 5
```

```
exit
track 1 list threshold count
 threshold count up 5 down 3
 object 11
 object 12
 object 13
 object 14
 object 15
 exit
! Define the IKE Entity
crypto isakmp policy 1
  encryption aes
  hash sha
  group 2
  authentication pre-share
  exit
! Define the remote peers (3 main offices)
crypto isakmp peer address <First Main Office VPN address>
  pre-shared-key <key1>
  isakmp-policy 1
  keepalive-track 1
  exit
crypto isakmp peer address < Second Main Office VPN address>
  pre-shared-key <key2>
  isakmp-policy 1
  keepalive-track 1
  exit
crypto isakmp peer address < Third Main Office VPN address>
  pre-shared-key <key3>
  isakmp-policy 1
  keepalive-track 1
  exit
crypto isakmp peer-group main-hubs
   set peer <First Main Office VPN address>
   set peer <Second Main Office VPN address>
   set peer <Third Main Office VPN address>
   exit
! Define the IPSEC Entity
crypto ipsec transform-set ts1 esp-3des esp-sha-hmac
  exit
! Define the VPN Tunnel
crypto map 1
  set peer-group main-hubs
  set transform-set ts1
! Define the crypto list for the public interface
ip crypto-list 901
  local-address "Fast Ethernet 10/3.0"
  ip-rule 10
     source-ip
                   10.0.10.0 0.0.0.255
     destination-ip any
     protect crypto map 1
     exit
  ip-rule 20
                  10.0.20.0 0.0.0.255
     source-ip
     destination-ip any
```

```
protect crypto map 1
     exit.
  exit
! Define the Ingress access control list for the public interface
ip access-control-list 301
  ip-rule 10
     source-ip
                          any
     destination-ip any ip-protocol udp
     udp destination-port eq Ike
     composite-operation Permit
     exit
  ip-rule 11
     source-ip any
     destination-ip any
     ip-protocol udp
     udp destination-port eq Ike-nat-t
     composite-operation permit
     exit
  ip-rule 12
     source-ip any
     destination-ip any
     ip-protocol udp
     udp destination-port eq Ike-nat-t-vsu
     composite-operation permit
     exit
  ip-rule 20
      source-ip
                          any
     destination-ip
                         any
     ip-protocol
     composite-operation Permit
     exit
  ip-rule 30
     source-ip
                          any
     destination-ip any ip-protocol icmp
                          icmp
     composite-operation Permit
     exit
  ip-rule 40
     source-ip
                          any
     destination-ip 10.0.10.0 0.0.0.255
     composite-operation Permit
     exit
  ip-rule 50
     source-ip any destination-ip 10.0.20.0 0.0.0.255
     source-ip
     composite-operation Permit
     exit
  ip-rule default
     composite-operation deny
     exit
   exit
! Define the Egress access control list for the public interface
ip access-control-list 302
  ip-rule 10
     source-ip
                          any
     destination-ip
                          any
     ip-protocol
                          udp
     udp destination-port eq Ike
     composite-operation Permit
     exit
  ip-rule 11
```

```
source-ip any
      destination-ip any
      ip-protocol udp
      udp destination-port eq Ike-nat-t
      composite-operation permit
   ip-rule 12
      source-ip any
      destination-ip any
      ip-protocol udp
      udp destination-port eq Ike-nat-t-vsu
      composite-operation permit
      exit
   ip-rule 20
      source-ip
      destination-ip any ip-protocol esp
      composite-operation Permit
      exit
   ip-rule 30
      source-ip any destination-ip any ip-protocol icmp
      composite-operation Permit
      exit
   ip-rule 40
     source-ip 10.0.10.0 0.0.0.255 destination-ip any composite-operation Permit
      exit
   ip-rule 50
      source-ip 10.0.20.0 0.0.255 destination-ip any
      composite-operation Permit
      exit
   ip-rule default
      composite-operation deny
! Activate the crypto list and the access control list on the public
interface
interface fastethernet 10/3
   ip crypto-group 901
   ip access-group 301 in
   ip access-group 302 out
```

## Checklist for configuring site-to-site IPSec VPN

Use the following table to gather the information for simple Gateway site-to-site IPSec VPN.

Parameter	Possible values	Actual value
1. Type of connection to the ISP	• ADSL	
	Cable Modem	
2. VPN Interface	FastEthernet10/3	
	Serial port X/Y	

Parameter	Possible values	Actual value
3. VPN Local IP Address	Type:	
	Static	
	– If static, provide:	
	IP Address	
	Mask	
	Next-hop Router	
	Dynamic (DHCP/PPPoE)	
4. Coordinating with the VPN Remote pe	eer	
a.) VPN IKE (Control) Phase 1 Paramete	ers	
— Encryption	• des	
	• 3des	
	• aes	
	• aes-192	
	• aes-256	
— Authentication Hash	• sha	
	• md5	
— DH Group	• 1	
	• 2	
	• 5	
	• 14	
— Lifetime seconds	• 60 to 86,400 default: 86,400 (1 day)	
b.) VPN IPSEC (Data) Phase 2 Paramet	I	
— Encryption	• esp-des	
	• esp-3des	
	• esp-aes	
	• esp-aes-192	
	• esp-aes-256	
— Authentication Hash	esp-sha-hmac	
	esp-md5-hmac	
— IP compression	enable (comp-lzs)	
	disable	

Parameter	Possible values	Actual value	
— PFS Group	no pfs (default)		
	• 1		
	• 2		
	• 5		
	• 14		
— Lifetime seconds	• 120 to 86,400 default: 3,600 (1 hour)		
— Lifetime kilobytes	• 2,560 to 536,870,912 default: 4,608,000 kb		
	disable		
5. Which packets should be secured			
a. Protect rules matching options	IP source address		
	IP destination address		
b. Bypass rules matching options	IP source address		
	IP destination address		
	• udp		
	• tcp		
	• dscp		
	fragment		
	• icmp		
	IP protocol		
6. The remote peer (crypto isakmp peer)	) parameters		
a. Remote peer	IP address		
	FQDN (dns name)		
b. Pre-shared key	1 to 127 alphanumerical characters.     1 to 64 bytes in hexadecimal notation		
7. If the branch IP is dynamic			
	If the branch IP is an initiator, set initiate mode to none (device is a responder)		
	If the branch IP is a responder, set initiate mode to aggressive (device is an initiator)		
	Set self identity to identify the device in the remote peer		

## **Summary of VPN commands**

For more information about these commands, see the *Avaya Branch Gateway G450 CLI Reference*.

Root level command	First level command	Second level command	Description
clear crypto isakmp			Flush a specific ISAKMP SA or all the ISAKMP SAs
clear crypto sa			Clear all or specific IPSec SAs
clear crypto sa counters			Clear the crypto SA counters
crypto ipsec nat- transparency udp- encapsulation			Re-enable NAT Traversal if it was disabled
crypto ipsec transform-set			Enter the IKE phase 2 (IPSec) transform-set context and create or edit IPSec parameters for the VPN tunnel
	mode		Set security-association lifetime
	set pfs		Specify whether each IKE phase 2 negotiation will employ PFS and, if yes, which Diffie-Hellman group to employ
	set security- association lifetime		Set the IKE phase 2 (IPSec) SA lifetime
crypto isakmp invalid-spi- recovery			Enable invalid SPI recovery (default setting)
crypto isakmp nat keepalive			Re-enable NAT Traversal keepalive if it was disabled, and configure the keepalive interval. This command keeps the NAT devices tables updated.
crypto isakmp peer			Enter the crypto ISAKMP peer context and create or edit an ISAKMP peer
	continuous- channel		Enable continuous-channel IKE, which keeps the IKE phase1 session always up and running, even if there is no traffic
	description		Enter a description for the ISAKMP peer

Root level command	First level command	Second level command	Description
	initiate mode		Specify which IKE Phase-1 mode to use when communicating with the peer: aggressive or none
	isakmp- policy		Set the ISAKMP policy for the ISAKMP peer
	keepalive		Enable DPD keepalives that check whether the remote peer is up
	keepalive- track		Bind an object tracker to a remote VPN peer or to an interface, to check whether the remote peer or the interface is up
	pre-shared- key		Configure the IKE pre-shared key
	self- identity		Set the identity of this device
	suggest-key		Generate a random string which you can use as a pre-shared key for IKE. You must use the same key on both peers.
crypto isakmp peer-group			Enter the crypto ISAKMP peer-group context and create or edit an ISAKMP peer group
	description		Enter a description for the ISAKMP peer group
	set peer		Add a peer to the peer-group
crypto isakmp policy			Enter the crypto ISAKMP policy context and create or edit IKE Phase 1 parameters
	authentication		Set the authentication of ISAKMP policy to pre-shared secret
	description		Enter a description for the ISAKMP policy
	encryption		Set the encryption algorithm for an ISAKMP policy
	group		Set the Diffie-Hellman group for an ISAKMP policy
	hash		Set the hash method for an ISAKMP policy
	lifetime		Set the lifetime of the ISAKMP SA in seconds

Root level command	First level command	Second level command	Description
crypto isakmp suggest-key			Generate a random string which you can use as a pre-shared key for IKE. You must use the same key on both peers.
crypto map			Enter crypto map context and create or edit a crypto map
	continuous- channel		In a crypto ISAKMP peer context, enable continuous-channel IKE, which keeps the IKE phase1 session always up and running, even if there is no traffic
	description		Enter a description for the crypto map
	set dscp		Set the DSCP value in the tunneled packet
	set peer		Attach a peer to a crypto map
	set peer-group		Attach a peer-group to a crypto map
	set transform- set		Configure the transform-set
<pre>interface (fastethernet  dialer serial  vlan)</pre>			Enter the FastEthernet, Dialer, Serial, or VLAN interface context
	crypto ipsec df-bit		Set the Don't-Fragment bit to clear mode or copy mode
	crypto ipsec minimal-pmtu		Set the minimal PMTU value that can be applied to an SA when the Branch Gateway participates in PMTUD for the tunnel pertaining to that SA
	ip crypto-group		Activate a crypto list in the context of the interface on which the crypto list is activated
ip crypto-list			Enter crypto list context and create or edit a crypto list
	ip-rule		Enter ip-rule context and create or modify a specific rule
		description	Enter a description for the ip-rule in the ip crypto list

Root level command	First level command	Second level command	Description
	Command	destination-	Specify the destination IP address of packets to which the current rule applies
		protect crypto map	Protect traffic that matches this rule by applying the IPSec processing configured by the specific crypto map
		source-ip	Indicate that the current rule applies to packets from the specified source IP address
	local-address		Set the local IP address for the IPSec tunnels derived from this crypto list
show crypto ipsec			Display the IPSec SA database and related runtime, statistical, and configuration information
			<b>☆</b> Note:
			The detail option in the various show crypto ipsec sa commands, provides detailed counters information on each IPSec SA. To pinpoint the source of a problem, it is useful to check for a counter whose value grows with time.
show crypto ipsec transform-set			Display the configuration for the specified transform-set or all transform-sets
show crypto isakmp peer			Display crypto ISAKMP peer configuration
show crypto isakmp peer-group			Display crypto ISAKMP peer-group configuration
show crypto isakmp policy			Display ISAKMP policy configuration
show crypto isakmp			Display the ISAKMP SA database status
show crypto map			Display all or specific crypto map configurations
show ip active- lists			Display information about a specific policy list or all lists

Root level command	First level command	Second level command	Description
show ip crypto- list			Display all or specific crypto list configurations

## **Chapter 22: Policy lists**

Policy lists enable you to control the ingress and egress of traffic to a router or port. You can use policies to manage security, determine packet priority through an interface, implement quality of service, or determine routing for a specific application or user. Each policy list consists of a set of rules determining the behavior of a packet entering or leaving the interface on which the list is applied.



### Note:

Policy lists are supported on IPv4 only.

## Types of policy lists

There are various policy lists on the Branch Gateway, including access control lists, QoS lists, and Policy-based routing.

### Access control lists

Access lists include the following:

**Global rules:** A set of rules that are executed before the list is evaluated.

Rule list: A list of filtering rules that determine the action taken by Branch Gateway. These actions are pointers to the composite operation table.

Actions (composite operation table): A table that describes actions to be performed when a packet matches a rule. The table includes predefined actions, such as permit and deny. To configure more complex rules, see Composite operations on page 510.

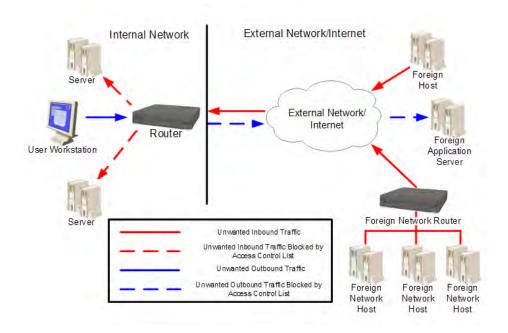
## Access control list rule specifications

You can use access control lists to control which packets are authorized to pass through an interface. When a packet matches a rule on the access control list, the rule specifies whether the Branch Gateway:

- Accepts the packet or drops the packet.
- Sends an ICMP error reply if it drops the packet.
- Sends an SNMP trap if it drops the packet.

### **Network security using access control lists**

The primary use of access control lists is to act as a component of network security. You can use access control lists to determine which applications, networks, and users can access hosts on your network. Also, you can restrict internal users from accessing specific sites or applications outside the network. Access control lists can be based on permitting or denying specific values or groups of IP addresses, protocols, ports, IP fragments, or DSCP values. The following figure illustrates how access control lists are used to control traffic into and out of your network:



## **QoS lists**

You can use QoS lists to change the DSCP and Ethernet IEEE 802.1p CoS fields in packets. Changing these fields adjusts the priority of packets meeting the criteria of the QoS list. DSCP values are mapped to a CoS value. Rules can be created determining the priority behavior of either individual DSCP values or CoS values, and can be based on specific values or groups of IP addresses, protocols, ports, IP fragments, or DSCP values. When a packet matches a rule on the QoS list, the Branch Gateway sets one or both of the QoS fields in the packet. See Allowed values on QoS fields on page 499.

Each QoS list also includes a DSCP table. The DSCP table enables you to set one or both of the QoS fields in a packet, based on the previous value of the DSCP field in the packet.

## **QoS list parts**

**Rule list:** A list of filtering rules and actions for the Branch Gateway to take when a packet matches the rule. Match actions on this list are pointers to the composite operation table.

**Actions (composite operation table):** A table that describes actions to be performed when a packet matches a rule. The table includes pre-defined actions, such as permit and deny. You can configure more complex rules. Refer to Composite operations on page 510.

**DSCP map:** A table that contains DSCP code points and match action pairs. Match actions are pointers to the composite operation table. Refer to <a href="DSCP table">DSCP table</a> on page 513.

### Allowed values on QoS fields

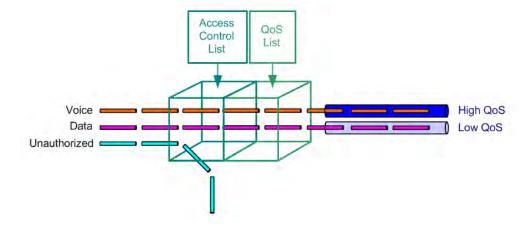
Layer	QoS field	Allowed values
2	802.1p	0–7
3	DSCP	0–63

## Use of policy-based routing

You can use policy-based routing to determine the routing path a packet takes based on the type of packet, or the packet's source or destination IP addresses, or its DSCP field. This enables you to route different types of traffic over different routes or interfaces. For example, you use policy-based routing to route voice traffic over a WAN interface and data traffic over the Internet. Policy-based routing is implemented by means of policy-based routing (PBR) lists. PBR lists are similar in many respects to access control lists and QoS lists. However, since there are also some key differences, policy-based routing is explained in a separate chapter. Refer to Policy-based routing section.

## **Policy list management**

You can manage policy lists on the Branch Gateway with CLI commands. You can also manage policy lists throughout your network with Avaya QoS Manager. Avaya QoS Manager is part of Avaya Integrated Management. The following figure illustrates the operation of policy lists on the Branch Gateway:



## **Policy list configuration**

You can create and edit policy lists, and define the list identification attributes. You can also delete an unnecessary policy list.

## Creating or editing a policy list

### **Procedure**

To create or edit a list, do one of the following tasks:

- To create or edit a policy list, enter the context of the list.
  - If the list already exists, you can edit the list from the list context. If the list does not exist, entering the list context creates the list.
- To create or edit an access control list, enter ip access-control-list followed by a list number in the range 300-399. The Branch Gateway includes one pre-configured access control list. The pre-configured access control list is list number 300.

For example, to create access control list 301, enter the following command:

```
ip access-control-list 301
```

• To create or edit a QoS list, enter ip qos-list followed by a list number in the range 400-499. The Branch Gateway includes one pre-configured QoS list. The pre-configured QoS list is list number 400.

For example, to create a new QoS list 401, enter the following command:

```
ip qos-list 401
```

## Creating a list based on an existing list

#### **Procedure**

1. To create a new policy list based on an existing list, use the ip policy-list-copy command followed by the name of the list from which you want to copy.

The source and destination lists must be of the same type. For example, you cannot copy an access control list to a QoS list.

The following example creates a new access control list, number 340, based on access control list 330. You can then enter the context of access control list 340 to modify it.

```
Gxxx-001(super)# ip policy-list-copy 330 340
Done!
```

- 2. Once you have entered the list context, you can perform the following actions:
  - Configure rules see <u>Policy rule configuration</u> on page 505
  - Configure composite operations see Composite operations on page 510
  - Configure DSCP mapping (QoS lists only) see <u>DSCP table</u> on page 513

## **Defining list identification attributes**

### About this task

The policy list attributes including name, owner, and cookie, are used by Avaya QoS Manager software to identify policy lists.

### **Procedure**

- 1. Enter the context of the policy list in which you want to define the attribute.
- 2. Enter one of the following commands, followed by a text string or integer:
  - name
  - owner
  - cookie
- 3. To set a policy list attribute to its default setting, use the **no** form of the appropriate command.

For example, to set a list to its default name, use the command no name.

4. To view the attributes, use the show list command in the context of the list.

## **Policy list attributes**

Command	Description
name	Defines a list name (text string). The default value is owner.
owner	Defines a list owner (text string). The default value is list#
cookie	Defines a list cookie (integer). The Avaya QoS Manager uses the cookie attribute internally. Normally, you should not change this attribute.
show list	View the attributes.

## **Default actions**

When no rule matches a packet, the Branch Gateway applies the default action for the list. The following table shows the default action for each type of policy list:

List	Default action
Access control list	Accept all packets
QoS list	No change to the priority or DSCP

## Deleting a policy list

#### **Procedure**

To delete a list, enter one of the following commands:

- To delete an access control list, enter no ip access-control-list followed by the number of the list you want to delete.
- To delete a QoS list, enter no ip gos-list followed by the number of the list you want to delete

## **Policy list attachments**

Attached to each interface on the Branch Gateway are policy lists, including the ingress access control list, ingress QoS list, egress access control list, and egress QoS list.



### Note:

You can also attach PBR lists to certain interfaces, but PBR lists are not attached to any interface by default.

## Packets entering the interface

When a packet enters the Branch Gateway through an interface, the Branch Gateway applies the policy lists in the following order:

- 1. Apply the ingress access control list.
- 2. If the ingress access control list does not drop the packet:
  - Apply the ingress QoS list.
  - Apply the PBR list (if any).

The packet enters the Branch Gateway through the interface.

## Packets exiting the interface

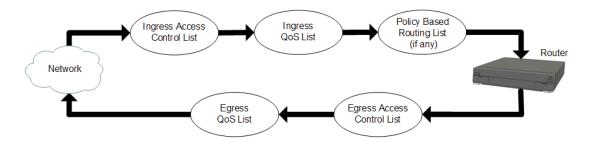
When a packet exits the Branch Gateway through an interface, the Branch Gateway applies the policy lists in the following order:

- 1. Apply the egress access control list.
- 2. If the egress access control list does not drop the packet, apply the egress QoS list.

The packet exits the Branch Gateway through the interface.

## Policy lists to packets

The following figure illustrates the order in which the Branch Gateway applies policy lists to packets.



## Policy list attachment configuration

You can configure which policy lists are attached to each interface. You can choose:

- The ingress access control list and the egress access control list from among the access control lists that are configured on the Branch Gateway.
- The ingress QoS list and the egress QoS list from among the QoS lists that are configured on the Branch Gateway.

## Attaching policy lists and access control lists

#### **Procedure**

Choose one of the following commands:

- To attach an access control list to an interface as its ingress access control list, enter the interface context and enter ip access-group list number in.
- To attach an access control list to an interface as its egress access control list, enter the interface context and enter ip access-group list number out.

## Attaching policy lists and QoS lists

### **Procedure**

Choose one of the following commands:

- To attach a QoS list to an interface as its ingress QoS list, enter the interface context and enter ip qos-group list number in.
- To attach an access control list to an interface as its egress QoS list, enter the interface context and enter ip qos-group list number out.

For example, the following sequence of commands attach policy lists to the VLAN 2 interface. Access control list 301 becomes the ingress access control list for VLAN 2. QoS list 401 becomes the egress QoS list for VLAN 2.

```
Gxxx-001# interface vlan 2
Gxxx-001(if:VLAN 2)# ip access-group 301 in
Done!
Gxxx-001(if:VLAN 2)# ip qos-group 401 out
Done!
```

## Removing a list

### **Procedure**

To remove a list from an interface, use the no form of the appropriate command.

For example, if the ingress access control list for the VLAN 1 interface is list number 302, you can remove the list from the interface by entering the following commands:

```
Gxxx-001(super) # interface vlan 1
Gxxx-001(super-if:VLAN 1) # no ip access-group in
Done!
```



### 🔀 Note:

You cannot change or delete a default list. You cannot change or delete any list when it is attached to an interface. In order to change or delete a list that is attached to an interface, you must first remove the list from the interface. You can then change or delete the list. After changing the list, you can reattach the list to the interface.

## **Device-wide policy lists**

You can attach a policy list (other than a policy-based routing list) to every interface on the Branch Gateway using one command. To do this, attach a list to the Loopback 1 interface. For more information, see Policy list attachments on page 502.



### Note:

If you attach a policy list to a Loopback interface other than Loopback 1, the policy list has no effect.

When you attach a policy list to the Loopback 1 interface, thereby creating a device-wide policy list, and you also attach policy lists to specific interfaces, the Branch Gateway applies the lists in the following order:

- Incoming packets:
  - 1. Apply the ingress policy lists that are attached to the interface
  - 2. Apply the device-wide ingress policy lists
- Outgoing packets:
  - 1. Apply the device-wide egress policy lists
  - 2. Apply the egress policy lists that are attached to the interface

# **Defining global rules**

#### About this task

In an access control list, you can define global rules for packets that contain IP fragments and IP options. These rules apply to all packets. This is in contrast to individual rules, which apply to packets that match certain defined criteria. See <u>Policy rule configuration</u> on page 505.

The Branch Gateway applies global rules before applying individual rules.

#### **Procedure**

- 1. Enter the context of the access control list in which you want to define the rule.
- 2. Enter one of the following commands, followed by the name of a composite command:
  - ip-fragments-in. Applies to incoming packets that contain IP fragments
  - ip-option-in. Applies to incoming packets that contain IP options

#### Result

The composite command can be any command defined in the composite operation list. These commands are case-sensitive. To view the composite operation list for the access control list you are working with, use the command **show composite-operation** in the context of the access control list.

#### **Example**

The following example defines a rule in access control list 301 that denies access to all incoming packets that contain IP fragments:

```
Gxxx-001(super)# ip access-control-list 301
Gxxx-001(super/ACL 301)# ip-fragments-in Deny
Done!
```

# Policy rule configuration

You can configure policy rules to match packets based on one or more of the following criteria:

- Source IP address, or a range of addresses
- Destination IP address, or a range of addresses
- IP protocol, such as TCP, UDP, ICMP, or IGMP
- Source TCP or UDP port or a range of ports
- Destination TCP or UDP port or a range of ports
- · ICMP type and code
- Fragment
- DSCP

Use IP wildcards to specify a range of source or destination IP addresses. The zero bits in the wildcard correspond to bits in the IP address that remain fixed. The one bits in the wildcard

correspond to bits in the IP address that can vary. Note that this is the opposite of how bits are used in a subnet mask.

For access control lists, you can require the packet to be part of an established TCP session. If the packet is a request for a new TCP session, the packet does not match the rule. You can also specify whether an access control list accepts packets that have an IP option field.

## **Editing and creating rules**

#### About this task

To create or edit a policy rule, you must enter the context of the rule. If the rule already exists, you can edit the rule from the rule context. If the rule does not exist, entering the rule context creates the rule.

#### **Procedure**

- 1. Enter the context of the list in which you want to create or edit a rule.
- 2. Enter ip-rule followed by the number of the rule you want to create or edit.

For example, to create rule 1, enter ip-rule 1.

## Policy lists rule criteria

Rules work in the following ways, depending on the type of list and the type of information in the packet:

- Layer 4 rules in an access control list with a *Permit* operation are applied to non-initial fragments
- Layer 4 rules in an access control list with a *Deny* operation are not applied to non-initial fragments, and the device continues checking the next IP rule. This is to prevent cases in which fragments that belong to other L4 sessions may be blocked by the other L4 session which is blocked.
- Layer 3 rules apply to non-initial fragments
- Layer 3 rules that include the fragment criteria do not apply to initial fragments or nonfragment packets
- Layer 3 rules that do not include the fragment criteria apply to initial fragments and nonfragment packets
- Layer 4 rules apply to initial fragments and non-fragment packets
- Layer 3 and Layer 4 rules in QoS and policy-based routing lists apply to non-initial fragments

## **Specifying IP protocol**

#### **Procedure**

To specify the IP protocol to which the rule applies, enter ip-protocol followed by the name of an IP protocol.

If you want the rule to apply to all protocols, use **any** with the command. If you want the rule to apply to all protocols except for one, use the **no** form of the command, followed by the name of the protocol to which you do not want the rule to apply.

#### **Example**

The following command specifies the UDP protocol for rule 1 in QoS list 401:

```
Gxxx-001(QoS 401/rule 1) # ip-protocol udp
```

The following command specifies any IP protocol except IGMP for rule 3 in access control list 302:

```
Gxxx-001(ACL 302/ip rule 3) # no ip-protocol igmp
```

## Specifying a range of IP addresses

#### **Procedure**

To specify a range of source and destination IP addresses to which the rule applies, use the commands source-ip and destination-ip, followed by the IP range criteria.

Choose one of the following options as the IP range criteria:

- To specify a range, type two IP addresses to set a range of IP addresses to which the rule applies
- To specify a single address, type host, followed by an IP address to set a single IP address to
  which the rule applies
- To specify a wildcard, type host, followed by an IP address using wildcards to set a range of IP addresses to which the rule applies
- To specify all addresses, type any to apply the rule to all IP addresses

Use the **no** form of the appropriate command to specify that the rule does not apply to the IP address or addresses defined by the command.

#### Example

The following command specifies a source IP address of 10.10.10.20 for rule 1 in access control list 301:

```
Gxxx-001(ACL 301/ip rule 1) # source-ip host 10.10.10.20
```

The following command allows any destination IP address for rule 3 in QoS list 404:

```
Gxxx-001(QoS 404/rule 3)# destination-ip any
```

The following command specifies a source IP address in the range 10.10.0.0 through 10.10.255.255 for rule 1 in access control list 301:

```
Gxxx-001(ACL 301/ip rule 1) # source-ip 10.10.0.0 0.0.255.255
```

The following command specifies a source IP address outside the range 64.236.24.0 through 64.236.24.255 for rule 7 in access control list 308:

```
Gxxx-001(ACL 308/ip rule 7) # no source-ip 64.236.24.0 0.0.0.255
```

The following command specifies a source IP address in the range 64.<any>.24.<any> for rule 6 in access control list 350:

```
Gxxx-001(ACL 350/ip rule 6) # source-ip 64.*.24.*
```

## Specifying source and destination port range Procedure

- 1. To specify a range of source and destination ports to which the rule applies, use any of the following commands followed by either port name or port number range criteria:
  - tcp source-port
  - tcp destination-port
  - udp source-port
  - udp destination-port

This command also sets the IP protocol parameter to TCP or UDP.

For more information about these commands, see <u>Summary of access control list</u> <u>commands</u> on page 516, <u>Summary of QoS list commands</u> on page 518, or *Avaya CLI Reference*.

- 2. Select the port name or number range criteria using one of the following options:
  - To set a range of port numbers to which the rule applies, type range, followed by two
    port numbers.
  - To set a port name or port number to which the rule applies, type eq (equal) followed by a port name or number.
  - To apply the rule to all ports with a name or number greater than the specified name or number, type gt (greater than) followed by a port name or port number.
  - To apply the rule to all ports with a name or number less than the specified name or number, type 1t (less than) followed by a port name or port number.
  - To apply the rule to all port names and port numbers, type any

Use the **no** form of the appropriate command to specify that the rule does not apply to the ports defined by the command.

#### **Example**

The following command specifies a source TCP port named "telnet" for rule 1 in access control list 301:

```
Gxxx-001(ACL 301/ip rule 1) # tcp source-port eq telnet
```

The following command specifies any destination UDP port less than 1024 for rule 3 in QoS list 404:

```
Gxxx-001(QoS 404/rule 3) # udp destination-port 1t 1024
```

The following command specifies any destination TCP port in the range 5000 through 5010 for rule 1 in access control list 301:

```
Gxxx-001(ACL 301/ip rule 1)# tcp destination-port range 5000 5010
```

The following command specifies any source TCP port except a port named "http" for rule 7 in access control list 304:

```
Gxxx-001(ACL 304/ip rule 7) # no tcp source-port eq http
```

## Applying the rule to ICMP type and code

#### **Procedure**

1. To apply the rule to a specific type of ICMP packet, use the icmp command.

This command sets the IP protocol parameter to ICMP, and specifies an ICMP type and code to which the rule applies. You can specify the ICMP type and code by integer or text string, as shown in the examples below.

2. To apply the rule to all ICMP packets except the specified type and code, enter no icmp

#### **Example**

For example, the following command specifies an ICMP echo reply packet for rule 1 in QoS list 401:

```
Gxxx-001(QoS 401/rule 1) # icmp Echo-Reply
```

The following command specifies any ICMP packet except type 1 code 2 for rule 5 in access control list 321:

```
Gxxx-001(ACL 321/ip rule 5) # no icmp 1 2
```

## Specifying TCP establish bit

#### About this task

This procedure is applicable to access control lists only.

#### **Procedure**

- 1. To specify that the rule only applies to packets that are part of an established TCP session (a session in with the TCP ACK or RST flag is set), use the tcp established command.
- 2. Enter no tcp established to specify that the rule applies to all TCP packets.

In either case, the command also sets the IP protocol parameter to TCP.

#### **Example**

The following command specifies that rule 6 in access control list 301 only matches packets that are part of an established TCP session:

```
Gxxx-001(ACL 301/ip rule 6) # tcp established
```

## **Specifying fragments**

#### **Procedure**

Enter fragment to apply the rule to non-initial fragments.

You cannot use the **fragment** command in a rule that includes UDP or TCP source or destination ports.

```
Gxxx-001(super-ACL 301/ip rule 5) # fragment
Done!
Gxxx-001(super-ACL 301/ip rule 5) #
```

## **Specifying DSCP**

#### **Procedure**

- 1. Enter dscp, followed by a DSCP value (from 0 to 63), to apply the rule to all packets with the specified DSCP value.
- 2. Enter no dscp to remove the rule from the list.

#### **Example**

For example, the following command specifies that rule 5 in access control list 301 only matches packets in which the DSCP value is set to 56:

Gxxx-001 (ACL 301/ip rule 5) # dscp 56

## **Composite operation instructions**

For instructions on assigning a composite operation to an ip rule, see <u>Adding composite operation</u> to an ip rule on page 512.

# **Composite operations**

A composite operation is a set of operations that the Branch Gateway can perform when a rule matches a packet. Every rule in a policy list has an **operation** field that specifies a composite operation. The **operation** field determines how the Branch Gateway handles a packet when the rule matches the packet.

There are different composite operations for access control list rules and QoS list rules. For each type of list, the Branch Gateway includes a pre-configured list of composite operations. You cannot change or delete pre-configured composite operations. You can define additional composite operations.

## Pre-configured composite operations for access control lists

The following table lists the pre-configured entries in the composite operation table for rules in an access control list:

No	Name	Access	Notify	Reset Connection
0	Permit	forward	no trap	no reset
1	Deny	deny	no trap	no reset
2	Deny-Notify	deny	trap all	no reset
3	Deny-Rst	deny	no trap	reset
4	Deny-Notify-Rst	deny	trap all	reset

Each column represents the following:

**No:** A number identifying the operation

**Name:** A name identifying the operation. Use this name to attach the operation to a rule.

Access: Determines whether the operation forwards (forward) or drops (deny) the packet

**Notify:** Determines whether the operation causes the Branch Gateway to send a trap when it drops a packet

**Reset Connection:** Determines whether the operation causes the Branch Gateway to reset the connection when it drops a packet

## Pre-configured composite operations for QoS lists

The following table lists the pre-configured entries in the composite operation table for rules in a QoS list:

No	Name	CoS	DSCP	Trust
0	CoS0	cos0	no change	No
1	CoS1	cos1	no change	No
2	CoS2	cos2	no change	No
3	CoS3	cos3	no change	No
4	CoS4	cos4	no change	No
5	CoS5	cos5	no change	No
6	CoS6	cos6	no change	No
7	CoS7	cos7	no change	No
9	No-Change	no change	no change	No
10	Trust-DSCP	-	-	DSCP
11	Trust-DSCP-CoS	-	-	DSCP and CoS

Each column represents the following:

**No:** A number identifying the operation

**Name:** A name identifying the operation. Use this name to attach the operation to a rule.

**CoS:** The operation sets the **Ethernet IEEE 802.1p CoS:** field in the packet to the value listed in this column

**DSCP:** The operation sets the **DSCP:** field in the packet to the value listed in this column

**Trust:** Determines how to treat packets that have been tagged by the originator or other network devices. If the composite operation is set to Trust-DSCP, the packet's CoS tag is set to 0 before the QoS list rules and DSCP map are executed. If the composite operation is set to CoSX, the DSCP map is ignored, but the QoS list rules are executed on the **Ethernet IEEE 802.1p** CoS field. (For example, the composite operation CoS3 changes the **CoS** field to 3.) If the composite operation is set to Trust-DSCP-CoS, the operation uses the greater of the CoS or the DSCP value. If the composite operation is set to No Change, the operation makes no change to the packet's QoS tags.

## Configuring composite operations

#### About this task

You can configure additional composite operations for QoS lists. You can also edit composite operations that you configured. You cannot edit pre-configured composite operations.



#### Note:

You cannot configure additional composite operations for access control lists, since all possible composite operations are pre-configured.

#### **Procedure**

- 1. Enter the context of a QoS list.
- 2. Enter composite-operation followed by an index number.

The number must be 12 or higher, since numbers 1 through 11 are assigned to preconfigured lists.

- 3. Use one or more of the following commands to set the parameters of the composite operation:
  - dscp to ignore the DSCP field, use the argument no change, or enter no dscp.
  - cos to ignore the CoS field, use the argument no change, or enter no cos.
- 4. Enter name, followed by a text string, to assign a name to the composite operation.

You must assign a name to the composite operation, because when you attach the composite operation to a rule, you use the name, not the index number, to identify the composite operation.

## Adding composite operation to an IP rule

#### **Procedure**

To add or delete composite operations to or from an IP rule, use the [no] compositeoperation command followed by the name of the composite operation you want to add or delete, in the context of the rule.

For an example, see Composite operation example on page 512.

## Composite operation example

The following commands create a new composite operation called "dscp5" and assign the new composite operation to rule 3 in QoS list 402. If the packet matches a rule, the Branch Gateway changes the value of the DSCP field in the packet to 5.

```
Gxxx-001# ip gos-list 402
Gxxx-001(QoS 402) # composite-operation 12
Gxxx-001 (QoS 402/cot 12) # name dscp5
Done!
Gxxx-001(QoS 402/cot 12) # dscp 5
Done!
Gxxx-001(QoS 402/cot 12)# cos no-change
```

```
Done!

Gxxx-001(QoS 402/cot 12)# exit

Gxxx-001(QoS 402)# ip-rule 3

Gxxx-001(QoS 402/rule 3)# composite-operation dscp5

Done!
```

## **DSCP** table

DSCP is a standards-defined method for determining packet priority through an interface, either into or out of a router.

There are three ways you can use the **DSCP** field:

**Classifier:** Select a packet based on the contents of some portions of the packet header and apply behavioral policies based on service characteristic defined by the DSCP value

Marker: Set the DSCP field based on the traffic profile, as determined by the defined rules

**Metering:** Check compliance to traffic profile using filtering functions

A DSCP value can be mapped to a Class of Service (CoS). Then, for a CoS, rules can be applied to determine priority behavior for packets meeting the criteria for the entire CoS. Multiple DSCP values can be mapped to a single CoS. Rules can also be applied to individual DSCP values.

The default value of DSCP in a packet is 0, which is defined as "best-effort." You can determine a higher priority for a traffic type by changing the DSCP value of the packet using a QoS rule or composite operation.

Each QoS list includes a DSCP table. A DSCP lists each possible DSCP value, from 0 to 63. For each value, the list specifies a composite operation. See <u>Pre-configured composite operations for QoS lists</u> on page 511.

QoS rules on the list take precedence over the DSCP table. If a QoS rule other than the default matches the packet, the Branch Gateway does not apply the DSCP table to the packet. The Branch Gateway applies only the operation specified in the QoS rule.

## Changing an entry in the DSCP table

#### **Procedure**

- 1. Enter the context of a QoS list.
- 2. Enter dscp-table followed by the number of the DSCP value for which you want to change its composite operation.
- 3. Enter composite-operation followed by the name of the composite operation you want to execute for packets with the specified DSCP value.

#### Result

The following commands specify the pre-configured composite operation CoS5 for DSCP table entry 33 in QoS list 401. Every packet with DSCP equal to 33 is assigned CoS priority 5.

```
Gxxx-001# ip qos-list 401
Gxxx-001(QoS 401)# dscp-table 33
Gxxx-001(QoS 401/dscp 33)# composite-operation CoS5
Done!
```

The following commands create a new composite operation called dscp5 and assign the new composite operation to DSCP table entry 7 in QoS list 402. Every packet with DSCP equal to 7 is assigned a new DSCP value of 5.

```
Gxxx-001(super)# ip qos-list 402
Gxxx-001(super/QoS 402)# composite-operation 12
Gxxx-001(super/QoS 402/CompOp 12)# name dscp5
Done!
Gxxx-001(super/QoS 402/CompOp 12)# dscp 5
Done!
Gxxx-001(super/QoS 402/CompOp 12)# cos No-Change
Done!
Gxxx-001(super/QoS 402/CompOp 12)# exit
Gxxx-001(super/QoS 402/CompOp 12)# exit
Gxxx-001(super/QoS 402)# dscp-table 7
Gxxx-001(super/QoS 402/dscp 7)# composite-operation dscp5
Done!
```

Composite operation dscp5 changes the mapping of packets entering the router with a DSCP values of 7. DSCP value 5 is most likely to be mapped to a different CoS, making these packets subject to a different set of behavioral rules.

# Policy list displays and tests

To verify access control lists, QoS lists, and policy-based routing (PBR) lists, you can view the configuration of the lists. You can also test the effect of the lists on simulated IP packets.

## Policy list commands in context

When viewing information about policy lists and their components, these commands produce different results in different contexts.

- In general context:
  - show ip access-control-list. Displays a list of all configured access control lists, with their list numbers and owners
  - show ip access-control-list list number detailed. Displays all the parameters of the specified access control list
  - show ip qos-list. Displays a list of all configured QoS lists, with their list numbers and owners
  - show ip qos-list detailed. Displays all the parameters of the specified QoS list.

- In ip access-control-list context:
  - show composite-operation
  - show ip-rule. Displays a list of all rules configured for the list
  - show list. displays the parameters of the current list, including its rules
- In ip access-control-list/ip-rule context:
  - show composite-operation. Displays the parameters of the composite operation assigned to the current rule
  - show ip-rule. Displays the parameters of the current rule
- In ip qos-list context:
  - show composite-operation. Displays a list of all composite operations configured for the list
  - show dscp-table. Displays the current list's DSCP table
  - show ip-rule. Displays a list of all rules configured for the list
  - show list. Displays the parameters of the current list, including its rules
- In ip qos-list/ip-rule context:
  - show composite-operation. Displays the parameters of the composite operation assigned to the current rule
  - show dscp-table. Displays the current list's DSCP table
  - show ip-rule. Displays the parameters of the current rule
- In ip gos-list/dscp-table context:
  - show dscp-table. Displays the parameters of the current DSCP table entry
- In ip gos-list/composite-operation context:
  - show composite-operation. Displays the parameters of the current composite operation

# Simulating packets

#### **Procedure**

Use the ip simulate command in the context of an interface to test a policy list.

The command tests the effect of the policy list on a simulated IP packet in the interface. Specify the number of a policy list, the direction of the packet (in or out), and a source and destination IP address. You may also specify other parameters. For a full list of parameters, see *Avaya Branch Gateway G450 CLI Reference*.

#### **Example**

For example, the following command simulates the effect of applying QoS list number 401 to a packet entering Branch Gateway through interface VLAN 2:

```
Gxxx-001(if:VLAN 2)# ip simulate 401 in CoS1 dscp46 10.1.1.1 10.2.2.2 tcp 1182 20
```

When you use the ip simulate command, the Branch Gateway displays the effect of the policy rules on the simulated packet. For example:

```
Gxxx-001(super-if:VLAN 2)# ip simulate 401 in CoS1 dscp46 10.1.1.1
10.2.2.2 tcp 1182 20
Rule match for simulated packet is the default rule
Composite action for simulated packet is CoS6
New priority value is fwd6
Dscp value is not changed
```

## Simulated packet properties

- · CoS priority is 1
- DSCP is 46
- source IP address is 10.1.1.1
- destination IP address is 10.2.2.2
- IP protocol is TCP
- source TCP port is 1182
- destination TCP port is 20

# Summary of access control list commands

For more information about these commands, see the Avaya Branch Gateway G450 CLI Reference.

Root level command	Command	Command	Description
interface {dialer  loopback  fastethernet  tunnel  vlan}			Enter the Dialer, Loopback, FastEthernet, Tunnel or VLAN interface configuration context
	ip access-group		Activate a specific Access Control list, for a specific direction, on the current interface
	ip simulate		Test the action of a policy on a simulated packet

Table continues...

Root level command	Command	Command	Description
	show ip access- control-list		Display the attributes of a specific access control list or of all access control lists on the current interface
ip access- control-list			Enter configuration mode for the specified policy access control list, and create the list if it does not exist
	cookie		Set the cookie for the current list
	ip-fragments-in		Specify the action taken on incoming IP fragmentation packets for the current access control list
	ip-option-in		Specify the action taken on incoming packets carrying an IP option for the current access control list
	ip-rule		Enter configuration mode for a specified policy rule or, if the rule doesn't exist, create it and enter its configuration mode
		composite- operation	Assign the specified composite operation to the current rule
		destination-ip	Apply the current rule to packets with the specified destination IP address
		dscp	Apply the current rule to packets with the specified DSCP value
		fragment	Apply the current rule for non-initial fragments only
		icmp	Apply the current rule to a specific type of ICMP packet
		ip-protocol	Apply the current rule to packets with the specified IP protocol
		show composite- operation	Display the parameters of the composite operation assigned to the current rule
		show ip-rule	Display the attributes of the current rule
		source-ip	Apply the current rule to packets from the specified source IP address

Table continues...

Root level command	Command	Command	Description
		tcp destination- port	Apply the current rule to TCP packets with the specified destination port
		tcp established	Apply the current rule only to packets that are part of an established TCP session
		tcp source-port	Apply the current rule to TCP packets from ports with specified source port
		udp destination- port	Apply the rule to UDP packets with the specified destination port
		udp source-port	Apply the rule to UDP packets from the specified source port
	name		Assign a name to the current list
	owner		Specify the owner of the current list
	show composite- operation		Display the composite operations configured for the list
	show ip-rule		Display the rules configured for the current list attributes of a specific rule
	show list		Display the attributes of the current list, including its rules
ip policy-list- copy			Copy an existing policy list to a new list
show ip access- control-list			Display the attributes of a specific access control list or of all access control lists

# **Summary of QoS list commands**

For more information about these commands, see the *Avaya Branch Gateway G450 CLI Reference*.

Root level command	Command	Command	Description
interface {dialer  loopback  fastethernet  tunnel  vlan}			Enter the Dialer, Loopback, FastEthernet, Tunnel, or VLAN interface configuration context
	ip qos-group		Activate a specific QoS list, for a specific direction, on the current interface
	ip simulate		Test the action of a policy on a simulated packet
	show ip qos-list		Display the attributes of a specific QoS list or all QoS lists for the current interface
ip policy-list-copy			Copy an existing policy list to a new list
ip qos-list			Enter configuration mode for the specified QoS list, and create the list if it does not exist
	composite-operation		Enter the configuration mode for one of the current list's composite operations
		cos	Set the CoS priority value for the current composite operation
		dscp	Set the DSCP value for the current composite operation
		name	Assign a name to the current composite operation
		show composite- operation	Display the attributes of the current composite operation
	cookie		Set the cookie for the current list
	dscp-table		Enter the DSCP table entry context for a particular DSCP value for the current QoS list
		composite- operation	Specify the composite operation to execute for packets with the specified DSCP value
		name	Assign a name to the current DSCP table entry
		show dscp- table	Display the parameters of the current DSCP table entry

Table continues...

Root level command	Command	Command	Description
	ip-rule		Enter configuration mode for a specified policy rule or, if the rule does not exist, create it and enter its configuration mode
		composite- operation	Assign the specified composite operation to the current rule
		destination- ip	Apply the current rule to packets with the specified destination IP address
		dscp	Apply the current rule to packets with the specified DSCP value
		fragment	Apply the current rule for non-initial fragments only
		icmp	Apply the current rule to a specific type of ICMP packet
		ip-protocol	Apply the current rule to packets with the specified IP protocol
		show composite- operation	Display the parameters of the composite operation assigned to the current rule
		show dscp- table	Display the current list's DSCP table
		show ip-rule	Display the attributes of the current rule
		source-ip	Apply the current rule to packets from the specified source IP address
		tcp destination- port	Apply the current rule to TCP packets with the specified destination port
		tcp source- port	Apply the current rule to TCP packets from ports with specified source port
		udp destination- port	Apply the rule to UDP packets with the specified destination port
		udp source- port	Apply the rule to UDP packets from the specified source port
	name		Assign a name to the current list
	owner		Specify the owner of the current list

Table continues...

Root level command	Command	Command	Description
	pre-classification		Specify which priority tag the current QoS list uses for data flows
	show composite- operation		Display all composite operations configured for the list
	show dscp-table		Display the current list's DSCP table
	show ip-rule		Display the rules configured for the current list attributes of a specific rule
	show list		Display the attributes of the current list, including its rules
show ip qos- list			Display the attributes of a specific QoS list or all QoS lists

# **Chapter 23: Policy-based routing**

# **Policy-based routing**

Policy-based routing enables you to configure a routing scheme based on traffic's source IP address, destination IP address, IP protocol, and other characteristics. You can use policy-based routing (PBR) lists to determine the routing of packets that match the rules defined in the list. Each PBR list includes a set of rules, and each rule includes a next hop list. Each next hop list contains up to 20 next hop destinations to which the Branch Gateway sends packets that match the rule. A destination can be either an IP address or an interface.

Policy-based routing takes place only when the packet enters the interface, not when it leaves. Policy-based routing takes place after the packet is processed by the Ingress Access Control List and the Ingress QoS list. Thus, the PBR list evaluates the packet after the packet's DSCP field has been modified by the Ingress QoS List. See Policy lists to packets on page 502.

#### Note:

The Loopback 1 interface is an exception to this rule. On the Loopback 1 interface, PBR lists are applied when the packet leaves the interface. This enables the PBR list to handle packets sent by the Branch Gateway device itself, as explained below.

#### Note:

ICMP keepalive provides the interface with the ability to determine whether a next hop is or is not available. See ICMP keepalive on page 253.

## Note:

Policy-based routing is supported on IPv4 only.

Policy-based routing only operates on routed packets. Packets traveling within the same subnet are not routed, and are, therefore, not affected by policy-based routing.

The Loopback interface is a logical interface which handles traffic that is sent to and from the Branch Gateway itself. This includes ping packets to or from the Branch Gateway, as well as Telnet, SSH, FTP, DHCP Relay, TFTP, HTTP, NTP, SNMP, H.248, and other types of traffic. The Loopback interface is also used for traffic to and from analog and DCP phones connected to the device via IP phone entities.

The Loopback interface is always up. You should attach a PBR list to the Loopback interface if you want to route specific packets generated by the Branch Gateway to a specific next-hop.

Unlike the case with other interfaces, PBR lists on the Loopback interface are applied to packets when they leave the Branch Gateway, rather than when they enter.

Certain types of packets are not considered router packets (on the Loopback interface only), and are, therefore, not affected by policy-based routing. These include RIP, OSPF, VRRP, GRE, and keepalive packets. On the other hand, packets using SNMP, Telnet, Bootp, ICMP, FTP, SCP, TFTP, HTTP, NTP, and H.248 protocols are considered routed packets, and are, therefore, affected by policy-based routing on the Loopback interface.

# **Chapter 24: Synchronization**

If the Branch Gateway contains an MM710 T1/E1 media module, it is advisable to define the MM710 as the primary synchronization source for the Branch Gateway. In so doing, clock synchronization signals from the Central Office (CO) are used by the MM710 to synchronize all operations of the Branch Gateway. ISDN BRI trunks Media Modules (MM720, MM722) can also use signals from the Central Office, to synchronize all operations of the Branch Gateway. If MM710, MM720 and MM722 are not present, it is not necessary to set synchronization.

Where traditional synchronization is not available, you can use Clock Synchronization over IP (CSoIP). CSoIP to provide timing information across IP networks. CSoIP is also needed to support TDM-based devices, such as an H.320 video device, that customers would like to retain and transmit within an IP infrastructure. Use the CM SAT Administration forms to administer Synchronization over IP.

The relevant screens are:

- change system features to enable the synchronization over IP feature
- change media gateway <n> to enable synchronization over IP for the gateway.
- **change synchronization media-gateway** <n> to configure synchronization sources on the gateway

# Defining a stratum clock source

#### **Procedure**

Enter set sync interface primary | secondary mmID portID to define a potential stratum clock source (T1/E1 Media Module, ISDN-BRI), where:

- *mmID* is the Media Module ID of an MM stratum clock source of the form **v***n*, where *n* is the MM slot number
- *portID* is the port number for an ISDN clock source candidate. The port ID consists of the slot number of the media module and the number of the port. You can set more than one port. For example, v2 1, 3, 5-8.

## Note:

The port ID parameter only applies if the source is a BRI module.

By setting the clock source to primary, normal failover occurs. The identity of the current synchronization source is not stored in persistent storage. Persistent storage is used to preserve the parameters set by this command.



#### Note:

Setting the source to secondary overrides normal failover, generates a trap, and asserts a fault. Thus, it is only recommended to set the clock source to secondary for testing purposes.

# Setting the synchronization source

#### **Procedure**

To determine which reference source is the active source, use the set sync source primary | secondary command.

If you choose secondary, the secondary source becomes active, and the primary source goes on standby. In addition, fallback to the primary source does not occur even when the primary source becomes available.

#### Result

If neither primary nor secondary sources are identified, the local clock becomes the active source.

#### Example

The following example sets the MM710 media module located in slot 2 of the Branch Gateway chassis as the primary clock synchronization source for the Branch Gateway.

```
set sync interface primary v2
set sync source primary
```

If the Branch Gateway includes a second MM710 media module, enter the following command:

```
set sync interface secondary v3
set sync source secondary
```

If, for any reason, the primary MM710 media module cannot function as the clock synchronization source, the system uses the MM710 media module located in slot 3 of the Branch Gateway chassis as the clock synchronization source. If neither MM710 media module can function as the clock synchronization source, the system defaults to the local clock running on the chassis.

# Disassociating a clock source

#### **Procedure**

To disassociate an interface previously specified as the primary or secondary clock synchronization source, enter clear sync interface primary or clear sync interface secondary.

# Enabling and disabling automatic failover and failback Procedure

To enable or disable automatic failover and failback between designated primary and secondary synchronization sources, enter set sync switching enable or set sync switching disable.

# Synchronization status

The yellow ACT LED on the front of the MM710 media module displays the synchronization status of that module.

- If the yellow ACT LED is solidly on or off, it has not been defined as a synchronization source. If it is on, one or more channels is active. If it is an ISDN facility, the D-channel counts as an active channel and causes the yellow ACT LED to be on.
- When the MM710 is operating as a clock synchronization source, the yellow ACT LED indicates that the MM710 is the clock synchronization source by flashing at three second intervals, as follows:
  - The yellow ACT LED is on for 2.8 seconds and off for 200 milliseconds if the MM710 media module has been specified as a clock synchronization source and is receiving a signal that meets the minimum requirements for the interface
  - The yellow ACT LED is on for 200 milliseconds and off for 2.8 seconds if the MM710 media module has been specified as a synchronization source and is not receiving a signal, or is receiving a signal that does not meet the minimum requirements for the interface

# **Displaying synchronization status**

#### **Procedure**

Enter show sync timing to display the status of the local and remote primary, secondary, and local clock sources.

The status can be Active, Standby, or Not Configured. The status is Not Configured when a source has not been defined, for example, when there are no T1 cards installed.

#### Example

Done!

# **Summary of synchronization commands**

For more information about these commands, see Avaya Branch Gateway G450 CLI Reference.

Command	Description		
clear sync interface	Disassociate a previously specified interface as the primary or secondary clock synchronization source		
set sync interface	Define the specified module and port as a potential source for clock synchronization for the Branch Gateway		
set sync source	Specify which clock source is the active clock source. The identity of the current synchronization source is not stored in persistent storage.		
set sync switching	Toggle automatic sync source switching		
show sync timing	Display the status of the primary, secondary, and local clock sources		

# Chapter 25: TLS / Certificate Management

## **TLS**

TLS is the recommended protocol to be selected for H.248 communications between the G430, G450 Media Gateway, and CM. TLS is also used by the Media Gateway SLA Monitor Agent to communicate with the SLA Monitor Server, Avaya Diagnostic Server (ADS).

To use TLS with CM, the link-encryption type must be set on both CM and the Media Gateway.

On CM, you can specify whether TLS must be used for H.248 communication . Selecting **tls-only** restricts the use to only TLS communication, whereas when you select **any**, either TLS or PTLS can be used. Avaya recommends TLS as it is more secure whereas PTLS is an older proprietary protocol that was used by older gateway releases prior to TLS being supported.

Similarly, the types of link encryption the gateway will use is administered using the set link-encryption CLI command on the gateway. When using this command, ensure that at least one TLS version is enabled and that the version is also supported on CM. By default, TLS version 1.2 is enabled on the gateway.

For more information, see Administering Avaya Aura® Communication Manager, Avaya Aura® G430 Branch Gateway CLI Reference, and Avaya Aura® G450 Branch Gateway CLI Reference.

## TLS certificate stores

The Gateway currently maintains two certificate stores to hold TLS CA and Identity certificates for the following applications:

- h248reg: Used for H.248 Media Gateway TLS communication with Communication Manager operating in the following modes:
  - Enterprise: The default mode of the gateway in which the gateway operates with the local enterprise IP address and is connected to the Communication Manager.
  - Edge: Media Gateway uses h248reg certificate store to set up a TLS connection with Avaya SBCE. Edge gateway mode operates with the NATed IP address.

Media Gateway uses this connection to send the H.248 signaling messages to Avaya SBCE H.248 proxy server application, which forwards the messages to Communication Manager.

In the Edge gateway mode, MGSBC management link uses h248reg certificate store and TCP port 2946 to create a TLS connection with Avaya SBCE.

- sla: For providing diagnostic information to the SLA Monitor Server.
- syslog: For syslog certificates.
- web: For web applications.

## Note:

The HTTP or HTTPS upload and download commands use the web trust store. For more information about the HTTPS commands, see *Avaya Branch Gateway G430 CLI Reference* and *Avaya Branch Gateway G450 CLI Reference*.

#### Note:

TLS connections can only be established if valid certificates are installed on both the gateway and the server it communicates with. Specifically, TLS communication on the gateway requires the following:

- A CM Identity certificate must be installed on Communication Manager, and a corresponding CM CA certificate must be installed on the Gateway.
- To use SLA Monitor Agent, a SLA Monitor Server Identity certificate must be installed on the SLA Monitor Server and a corresponding SLA Monitor CA certificate must be installed on the Gateway.
- When the gateway is operating in the Edge mode and therefore connected to Avaya SBCE, it is recommended to use an identity certificate.
- If an Identity certificate is installed on the Gateway, a corresponding Gateway CA certificate must be installed on CM.

## Note:

A Gateway Identity certificate only needs to be installed if mutual authentication is set to **Required** on the Communication Manager Media Gateway form.

The commands used to copy, show, and erase certificates on the Gateway are provided through the Gateway CLI interface. For more information, see *Avaya Branch Gateway G430 CLI Reference* and *Avaya Branch Gateway G450 CLI Reference*.

The forms and commands used to copy, show, and erase certificates on CM and the ADS SLA Monitor Server are available in their corresponding administration guides.

Monitoring Certificate Expiration shall be extended to include the user provided certificates in the Web Trust store as follows:

- When the certificate expiration date reaches 60 days before expiration, Media Gateway shall raise a minor trap alarm.
- When the certificate expiration date is reached, Media Gateway shall raise a major trap alarm.

## **Certificate validation**

The gateway provides a variety of options for certificate validation, including Common Name Validation, Subject Alternate Name validation, and the degree of Certificate Revocation checking to be performed using CRLs and/or OCSP.

For more information about the types of certificate validation that can be enabled on the gateway, see Avaya Aura® G430 Branch Gateway CLI Reference and Avaya Aura® G450 Branch Gateway CLI Reference.

## **Mutual authentication**

Mutual Authentication is required when Media Gateway is operating in the Edge mode and is connected to Avaya SBCE.

Requiring mutual authentication sets a condition where both CM and the gateway are required to exchange and validate each other's identity certificates.

The **Mutual Authentication** field on the **Communication Manager Media Gateway** form supports the following keyword options:

- Optional
- Required

Avaya recommends administrators to select the **Required** option because it provides a higher degree of security. If **Optional** is selected, and no identity certificate is loaded in the gateway's H248 application directory; CM establishes a TLS connection without the gateway having to offer an identity certificate. For more information, see *Administering Avaya Aura Communication Manager*.

# Chapter 26: Federal Information Processing Standards (FIPS)

# **Federal Information Processing Standards**

Federal Information Processing Standards (FIPS) are a set of publicly announced standards developed by the National Institute of Standards and Technology (NIST) that describe document processing, encryption algorithms and other information technology standards for use within non-military government agencies and by government contractors and vendors who work with the agencies.

G430 or G450 gateways with FIPS approved mode enabled will operate as a FIPS 140-2 Cryptographic Module (Level 1) if and only if your organization complies with all policies defined in the following Security Policy publications:

- Avaya G430 FIPS 140-2 Cryptographic Module Security Policy
- Avaya G450 FIPS 140-2 Cryptographic Module Security Policy

These documents are later referred in this administration guide as the "Security Policy".

Strict adherence to the Security Policy is necessary to assure FIPS 140-2 compliance. Therefore, it is recommended that you do not enable FIPS approved mode until the Security Policy has been completely read and its requirements fully understood.

# FIPS Security Level of the Cryptographic Module

The gateway's cryptographic module meets the overall requirements applicable to Level 1 security of FIPS 140-2. The following are security rules enforced by the cryptographic module to implement the security requirements of this FIPS 140-2 Level 1 module:

- When entering or exiting FIPS-140-2 approved mode, the gateway will be zeroized.
   Zeroization will erase the entire existing gateway configuration including Critical Security Parameters (CSPs) and the gateway will return to its factory default settings.
- The cryptographic module performs Power up Self-Tests (POST) to confirm that it can reliably perform FIPS compliant operations. These include:
  - Non-Volatile Random-Access Memory (NVRAM) Integrity Tests
  - Electronically Erasable Programmable Read Only Memory (E2PROM) Integrity Tests

- · Cryptographic algorithm Tests
- Gateway Software/Firmware Integrity Tests
- Digital Signal Processor (DSP) Power Up Self-Tests (POST)
- Critical Functions Tests
- · Conditional Self-Tests
- 3. Users can instruct the module to perform the power-up self-tests at any time by executing the reset CLI command or by power cycling the gateway.
- 4. Prior to each use, the internal entropy source is tested using FIPS 140-2 approved conditional tests.
- 5. Data output is inhibited at power-up during self-tests, zeroization, and error states.
- 6. When the gateway is in FIPS approved mode, the gateway's cryptographic module will only provide FIPS approved algorithms and the gateway will be FIPS compliant provided that all policies described in the Security Policy are strictly adhered to.

# **Determining FIPS Certified Firmware is installed**

#### **Procedure**

To determine if the crypotographic module of the gateway has FIPS certified firmware installed in both Bank A and Bank B, run the following command:

#### show image version

Both gateway firmware banks must be running a FIPS-approved firmware version to be considered FIPS-compliant.

To verify that the version(s) you have installed is certified for FIPS 140-2 compliance, see the *Certificate Module Validation Program (CMVP)* lists on the NIST website at <a href="http://www.nist.gov">http://www.nist.gov</a>.

# **FIPS Approved Mode of Operation**

When the gateway is in FIPS approved mode, the gateway's cryptographic module will only provide FIPS approved algorithms and the gateway will be FIPS compliant provided that all policies described in the Security Policy are strictly adhered to.

When not in FIPS approved mode, the gateway's cryptographic module may provide both approved and unapproved algorithms and the gateway may freely operate in non-FIPS-compliant ways.

Details of the algorithms used in both FIPS approved and unapproved modes are described in the Security Policy.

# **Prerequisites for entering FIPS Approved Mode**

- User type Cryptographic Officer with administration privileges. For example, root.
- FIPS-approved Media Gateway hardware. G430 or G450 Version 3.0.x or higher.
- FIPS-approved Media Gateway firmware.
- Strict adherence to all policies described in the following publications:
  - Avaya G430 FIPS 140-2 Cryptographic Module Security Policy
  - Avaya G450 FIPS 140-2 Cryptographic Module Security Policy

To verify that the version(s) you have installed is certified for FIPS 140-2 compliance, see the Certificate Module Validation Program (CMVP) lists on the NIST website at <a href="http://www.nist.gov">http://www.nist.gov</a>.

# **Determining FIPS Approved Mode is enabled**

#### **Procedure**

To determine whether FIPS approved mode is enabled or disabled, run the following command:

show fips-mode

# **Determining Configuration is FIPS Compliant**

Both gateway firmware banks must be running a FIPS-approved firmware version to be considered FIPS-compliant. To determine if the cryptographic module of the gateway has FIPS certified firmware, run the **show image version** command and verify that both Bank A and Bank B have FIPS-approved firmware versions installed.

To verify that the version(s) you have installed is certified for FIPS 140-2 compliance, see the *Certificate Module Validation Program (CMVP)* lists on the NIST website at <a href="http://www.nist.gov">http://www.nist.gov</a>.

Prior to enabling FIPS approved mode, the **show fips-mode** command will attempt to detect whether any non-FIPS compliant CLI commands are currently configured. This may help identify whether any currently configured CLI commands will automatically be disabled when FIPS approved mode is enabled.

In the example below, the show fips-mode command reveals that FIPS approved mode is currently disabled and that PTLS link encryption for H.248 registration with CM will not be allowed if FIPS approved mode were to be enabled.

```
G450(super)# show fips-mode
FIPS Mode: Disabled
These configuration settings are not FIPS-compliant and
will be automatically disabled if FIPS-mode is enabled:
set link-encryption h248reg ptls yes
```

Be aware that the **show fips-mode** command might not detect all non-compliant configurations. Therefore, the Security Policy must be always used as the definitive source for determining whether a configuration is FIPS compliant.

# **Backup and restore of Gateway configuration**

Backup configuration can only be restored to a gateway that is in the same mode as the one on which the backup is taken. The following rules apply when you backup or restore configuration:

- Backup made in non-FIPS approved mode can only be restored to a gateway in non-FIPS approved mode.
- Backup made in FIPS approved mode can only be restored to the same gateway.
- In addition, backup made in FIPS approved mode can no longer be restored if the nvram init or zeroize CLI commands are executed, or if FIPS approved mode is disabled at any time after the backup has been made.

Avaya<sup>™</sup> recommends that you obtain a complete copy of the gateway's current running configuration before enabling or disabling FIPS approved mode.

For more information about the backup and restore commands, see Avaya Branch Gateway G430 CLI Reference and Avaya Branch Gateway G450 CLI Reference.

# Before Enabling or Disabling FIPS Approved Mode

Before enabling or disabling FIPS approved mode, it is recommended that you keep a complete copy of the gateway's current running configuration. The gateway's current running configuration can be viewed by executing the following command:

• show running-config

Alternatively, the **running-config** command made be saved to an external text file for later viewing by using one of the following commands:

- copy running-config ftp <destination file name> <ip address>
- copy running-config tftp <destination file name> <ip address>
- copy running-config scp <destination file name> <ip address>

This can be especially helpful when enabling or disabling FIPS approved mode since the gateway configuration will not be able to be restored from a backup made in a different mode.

# **Enabling FIPS Approved Mode**

#### **Procedure**

To enable the FIPS Approved Mode, run the following CLI command:

• set fips-mode enable



When FIPS approved mode is first enabled, the gateway's existing configuration will be erased and replaced with a basic configuration that is FIPS compliant. The basic FIPS compliant configuration must then be further customized as needed.

# **Maintaining FIPS Approved Mode**

It is imperative that you consult the Security Policy before changing any gateway configuration.

When changing the gateway's configuration via CLI commands, an error or warning will be issued any time a command is entered that is not FIPS compliant. The "show fips-mode" CLI command may be used to verify whether FIPS approved mode is currently enabled. The command will also attempt to detect whether any non-compliant CLI commands are currently configured. However, the Security Policy must be used as the definitive source for FIPS compliance since not all non-compliant configurations may be detected.

# **Disabling FIPS Approved Mode**

#### **Procedure**

To disable FIPS Approved Mode, run the following CLI command:

• set fips-mode disable



When FIPS approved mode is first disabled, the gateway's existing configuration will be erased and replaced with a basic configuration. The basic configuration must then be further customized as needed.

# Administration procedures

Administration procedures consist of the commands required to enable or disable FIPS approved mode, limitations and the prerequisites. It also includes failure scenarios and repair actions.

## **FIPS-related CLI commands**

- set fips-mode
- show fips-mode
- show image version

For a full description of these commands, see *Avaya Branch Gateway G430 CLI Reference* and *Avaya Branch Gateway G450 CLI Reference*.

# Non-compliant CLI Commands in FIPS Approved Mode

The following CLI commands are not permitted in FIPS approved mode:

Command name	Syntax		
CHAP	ppp chap		
IP License Server	ip license-server		
Link Encryption for H.248 Registration (Proprietary TLS)	set link-encryption h248reg ptls		
Master Key	key config-key password-encryption		
OSPF	router ospf		
PAP	ppp pap		
PPP	encapsulation pppoe		
	• interface USB-Modem		
	• interface console		
	• interface Serial		
	• ppp		
RADIUS	set radius authentication enable		
RIP	router rip		
SLA Monitor for Avaya Diagnostic Server (ADS)	set sla-monitor enable		
SLS	set sls enable		
SNMPv1 and SNMPv2	• set snmp-community		
	• snmp-server remote-user <username> <engineid> <group- name&gt; auth md5</group- </engineid></username>		
	• snmp-server remote-user <username> <engineid> <group- name&gt; auth sha priv des56</group- </engineid></username>		
	• snmp-server user <username> <group-name> v1</group-name></username>		
	• snmp-server user <username> <group-name> v2c</group-name></username>		
Telnet Client	ip telnet-client		

Table continues...

Command name	Syntax	
Telnet Server	ip telnet	
Telnet Services	ip telnet-services	
VPN (IPSEC)	• crypto ipsec	
	• crypto isakmp	
	• crypto map	
	• ip crypto-list	
	• vpn hw	
	• vpn init	
	• vpn memory	
	• vpn monitor	
	• vpn policy	
	• vpn report	
	• vpn show	

For a full description of these commands, see Avaya Branch Gateway G450 CLI Reference guide.



#### Note:

Details about non-compliant CLI commands can be found in the Security Policy.

## Warnings for unencrypted communication in FIPS Approved Mode

Although the following commands are all FIPS-compliant, a warning is given and confirmation is requested if any of the following CLI commands are executed while in FIPS approved mode:

- set link-encryption h248reg unencrypted yes
- set link-encryption h248reg all yes
- set allow-unencrypted rtp yes

In addition, the show fips-mode command indicates a warning if any of the above commands are enabled. The warning is given to alert the user that an unsecure form of communication is requested.

For a full description of these commands, see Avaya Branch Gateway G430 CLI Reference and Avaya Branch Gateway G450 CLI Reference.

## **Enabling FIPS Approved Mode**

#### About this task

The gateway's current configuration will be zeroized anytime FIPS Approved Mode is enabled or disabled.

#### **Procedure**

1. Log in to the gateway using a user login account that has administrative privileges.

#### For example:

```
Login:root
Password: ****
Password accepted
```



#### Note:

It is recommended that the gateway's serial console or IP services port be used when logging onto the gateway to enable FIPs mode. This way FIPS related test results and error states that occur during boot-up can be viewed when the gateway attempts to first enter FIPS mode. The gateway's serial console or IP services port is also required to login to the gateway for the first time after FIPS approved mode is enabled because the zeroization that accompanies the enabling of FIPS mode erases all network configuration.

2. Verify that both firmware banks contain FIPS-approved firmware images using the show image version command as shown below.

To verify that the version(s) you have installed is certified for FIPS 140-2 compliance, see the Certificate Module Validation Program (CMVP) lists on the NIST website at http:// www.nist.gov.

```
G450-001(super) # show image version
   Version
           39.27.0
B (current) 41.9.0
```



#### Note:

Banks that do not have a FIPS-approved firmware image must be upgraded.

3. To review the impact FIPS Approved Mode will have on the existing configuration, run the show fips-mode command as shown below.

```
G450(super) # show fips-mode
FIPS Mode: Disabled
These configuration settings are not FIPS-compliant and
will be automatically disabled if FIPS-mode is enabled:
  set link-encryption h248reg unencrypted yes
 set allow-unencrypted rtp yes
```

4. Run the show running-config command and make a copy of its output since the current gateway configuration will be erased once FIPS approved mode is enabled.

```
G450 (super) # show running-config
```



#### Note:

Alternatively, the gateway's current running configuration can be saved to an external text file for later viewing by using the copy running-config command.

5. Run the set fips-mode enable command to enable FIPS mode as shown below.

```
G450(super)# set fips-mode enable

WARNING: This Gateway will be ZEROIZED and RESET if you continue to enable FIPS mode.

Do you want to continue (Y/N)? Y

Enabling FIPS Mode.

The Gateway will now be Zeroized and Reset...
```

6. The gateway will reset and perform a variety of FIPS related Power On Self Tests (POST) as shown below.

```
FIPS POST TEST - STARTED
NVRAM POST Integrity Test OK
E2PROM POST Integrity Test OK
FIPS Object Module POST Started
        Integrity Test OK
DRBG AES-256-CTR DF Test OK
        DRBG AES-256-CTR Test OK
        Digest SHA1 Test OK
        Digest SHA1 Test OK
        Digest SHA1 Test OK
        Digest SHA256 Test OK
        Digest SHA256 Test OK
        Digest SHA256 Test OK
        Digest SHA512 Test OK
        Digest SHA512 Test OK
        Digest SHA512 Test OK
       HMAC SHA1 Test OK
        HMAC SHA224 Test OK
        HMAC SHA256 Test OK
        HMAC SHA384 Test OK
        HMAC SHA512 Test OK
        Cipher AES-128-ECB Test OK
        GCM Test OK
        Cipher DES-EDE3-ECB Test OK
        Cipher DES-EDE3-ECB Test OK
        Signature RSA 2048 SHA256 PKCS#1 Test OK
        Signature RSA 3072 SHA256 PKCS#1 Test OK
        Signature ECDSA P-256 Test OK
        Signature ECDSA P-384 Test OK
        Signature ECDSA P-521 Test OK
FIPS Object Module POST Success
SW/FW POST Integrity Test OK
VoIP DSP0 FIPS POST Started
        CoreO AES Test OK
        CoreO HMAC Test OK
        Core0 SHA1 Test OK
        Corel AES Test OK
        Corel HMAC Test OK
        Corel SHA1 Test OK
        Core2 AES Test OK
        Core2 HMAC Test OK
        Core2 SHA1 Test OK
        Core3 AES Test OK
        Core3 HMAC Test OK
        Core3 SHA1 Test OK
VoIP DSP0 FIPS POST Success
VoIP DSP1 FIPS POST Started
     CoreO AES Test OK
   Core0 HMAC Test OK
```

```
Core0 SHA1 Test OK
        Corel AES Test OK
        Corel HMAC Test OK
        Corel SHA1 Test OK
        Core2 AES Test OK
        Core2 HMAC Test OK
        Core2 SHA1 Test OK
        Core3 AES Test OK
Core3 HMAC Test OK
        Core3 SHA1 Test OK
VoIP DSP1 FIPS POST Success
Generating RSA key, This command may take a few minutes...
. . . . . . . . . . . . .
Key was created!
Key version: SSH2, RSA
Key Fingerprint: SHA256:X31EqBa0+ikMUASGS0zbFVcjFUCkKzw+U3OGYY/aI/o
FIPS POST TEST - COMPLETED
Enabling External Data Ports
```

 After verifying successful completion of the Power-On Self Tests (POST), the Cryptographic Officer must log in to the gateway using the root login account and default root password as shown below.

```
G450 Login: root
Password: ****
Response accepted
Password accepted
```

## Note:

Only the root user login may be initially used after enabling FIPS approved mode since all other administrative accounts are deleted during zeroization.

8. The Cryptographic Officer must change the root password from the default password to a new, more secure password as shown below.

```
Enter new password:
Confirm new password:
```

9. The Cryptographic Officer must confirm whether Enhanced Access Security Access (EASG) is to be enabled or disabled as shown below.

```
By disabling Avaya Logins you are preventing Avaya access to your system.

Enter 1 to Enable EASG or 2 to Disable EASG? 2

You have requested Avaya Logins be Disabled.

Do you want to continue (Y/N)? Y

Avaya Logins have been Disabled.
```

10. If you use the Gateway Configuration script to complete basic configuration of the gateway complete the required process as shown below. The gateway will then reset.

```
--- Gateway Configuration Script ---
The script will provide you basic gateway connectivity configuration. Configuration Script - do you want to continue (Y/N)? Y
Default settings are in square brackets '[]'.
Vlan [1] :
IPv4 Enabled (Y/N)? [Y]:
IPv4 address [169.254.0.2] :172.16.1.230
IPv4 Subnet mask [255.255.255.0] :255.255.254.0
IPv4 Default gateway [172.16.1.1] :172.16.1.254
IPv6 Enabled (Y/N)? [N]:
MGC controllers [0.0.0.0] :172.16.1.168
Hostname [G450] :G450
Enable Spanning Tree on LAN ports (Y/N/Help)? [Y] :
The following parameters are about to be configured:
Vlan : 1
IPv4 address : 172.16.1.230
Subnet mask : 255.255.254.0
Default gateway : 172.16.1.254
MGC controllers : 172.16.1.168
Hostname : G450
                          : 255.255.254.0
Spanning Tree Protocol: enabled
The gateway will save those parameters in startup-config and then reset
 - do you want to continue (Y/N)? Y
Please connect your gateway to the network via any Ethernet port
Saving configuration...
Resetting the device ...
```

11. The Cryptographic Officer must log in to the gateway using a user login account that has administrative privileges as shown below.

```
Login: root
Password: ****
Password accepted
```

12. Run the **show fips-mode** command to verify if FIPS-mode and any non-recommended commands are enabled as shown below.

```
G450G450(super) # show fips
FIPS Mode: Enabled
```

 Run the username command to define new user logins for Crypto-officer, administrators, and users as required.

```
G450(super)# username crypto-officer access-type admin
Enter new password: ********
```

```
Confirm password : ******
User account added.
```

Run the show username command to verify the successful addition of users.

```
G450-???(super) # show username
User
                            Access
                                       Account
                                                 Active
account
                            level
                                       type
                            admin local
root.
                                                yes
                            admin
crypto-officer
                                     local yes
```

15. To define SNMPv3 parameters for SNMPv3 users, run auth sha priv aes128.

```
G450-001(super) # snmp-server user fips snmp user v3ReadWriteG v3 auth sha priv
aes128
Enter authentication password : ******
Confirm authentication password : ******
Enter privacy password : ******
Confirm privacy password : ******
Done!
```

#### Note:

Other combinations of auth-type and priv-type are not permitted in FIPS approved mode.

16. If you have saved a copy of your previous configuration prior to enabling FIPS approved mode, refer to it now to perform any additional configuration as needed. For more information, see Configuration changes and backup on page 28.

#### Note:

When changing the gateway's configuration using CLI commands, the system displays an error or warning, if the entered command is not FIPS compliant. However, it is important that you consult the Security Policy when making changes to the gateway configuration to insure FIPS compliance.

### **Disabling FIPS Approved Mode**

#### About this task

The gateway's current configuration will be zeroized anytime FIPS Approved Mode is enabled or disabled.

#### **Procedure**

1. The Cryptographic Officer must log in to the gateway using a user login account that has administrative privileges.

#### For example:

```
Login:root
Password: ****
Password accepted
```

### Note:

It is recommended that the gateway's serial console or IP services port be used when logging onto the gateway to disable FIPs mode. The gateway's serial console or IP services port is required to login to the gateway for the first time after FIPS approved mode is disabled because the zeroization that accompanies the disabling of FIPS mode erases all network configuration.

2. Run the set fips-mode disable command to disable FIPS mode.

```
G450(super)# set fips-mode disable

WARNING: This Gateway will be ZEROIZED and RESET if you continue to disable FIPS mode.

Do you want to continue (Y/N)? Y

Disabling FIPS Mode.

The Gateway will now be Zeroized and Reset...
```

3. The gateway will reset and perform a variety of FIPS related Power On Self Tests (POST) as shown below.

```
FIPS POST TEST - STARTED
NVRAM POST Integrity Test OK
E2PROM POST Integrity Test OK
FIPS Object Module POST Started
        Integrity Test OK
DRBG AES-256-CTR DF Test OK
        DRBG AES-256-CTR Test OK
        Digest SHA1 Test OK
        Digest SHA1 Test OK
        Digest SHA1 Test OK
        Digest SHA256 Test OK
        Digest SHA256 Test OK
        Digest SHA256 Test OK
        Digest SHA512 Test OK
        Digest SHA512 Test OK
        Digest SHA512 Test OK
        HMAC SHA1 Test OK
        HMAC SHA224 Test OK
        HMAC SHA256 Test OK
        HMAC SHA384 Test OK
        HMAC SHA512 Test OK
        Cipher AES-128-ECB Test OK
        GCM Test OK
        Cipher DES-EDE3-ECB Test OK
        Cipher DES-EDE3-ECB Test OK
        Signature RSA 2048 SHA256 PKCS#1 Test OK
        Signature RSA 3072 SHA256 PKCS#1 Test OK
        Signature ECDSA P-256 Test OK
        Signature ECDSA P-384 Test OK
        Signature ECDSA P-521 Test OK
FIPS Object Module POST Success
SW/FW POST Integrity Test OK
VoIP DSP0 FIPS POST Started
        CoreO AES Test OK
        CoreO HMAC Test OK
        CoreO SHA1 Test OK
        Corel AES Test OK
Corel HMAC Test OK
```

```
Corel SHA1 Test OK
        Core2 AES Test OK
        Core2 HMAC Test OK
        Core2 SHA1 Test OK
        Core3 AES Test OK
        Core3 HMAC Test OK
        Core3 SHA1 Test OK
VoIP DSP0 FIPS POST Success
VoIP DSP1 FIPS POST Started
        CoreO AES Test OK
        CoreO HMAC Test OK
        Core0 SHA1 Test OK
        Corel AES Test OK
Corel HMAC Test OK
        Corel SHA1 Test OK
        Core2 AES Test OK
        Core2 HMAC Test OK
        Core2 SHA1 Test OK
        Core3 AES Test OK
Core3 HMAC Test OK
        Core3 SHA1 Test OK
VoIP DSP1 FIPS POST Success
Generating RSA key, This command may take a few minutes...
. . . . . . . . . . . . .
Key was created!
Key version: SSH2, RSA
Key Fingerprint: SHA256:X31EqBa0+ikMUASGS0zbFVcjFUCkKzw+U30GYY/aI/o
FIPS POST TEST - COMPLETED
Enabling External Data Ports
```

4. After verifying successful completion of the Power-On Self Tests (POST), the Cryptographic Officer must log in to the gateway using the root login account and default root password as shown below.

```
G450 Login: root
Password: ****
Response accepted
Password accepted
```

### Note:

Only the root user login may be initially used after disabling FIPS approved mode since all other administrative accounts are deleted during zeroization.

5. The Cryptographic Officer must change the root password from the default password to a new, more secure password as shown below.

```
Enter new password:
Confirm new password:
```

6. The Cryptographic Officer must confirm whether Enhanced Access Security Access (EASG) is to be enabled or disabled as shown below.

```
By enabling Avaya Logins you are granting Avaya access to your system.
This is necessary to maximize the performance and value of your Avaya support
entitlements, allowing Avaya to resolve product issues in a timely manner.
In addition to enabling the Avaya Logins, this product should be registered
with Avaya and technically onboarded for remote connectivity and alarming.
Please see the Avaya support site (support.avaya.com/registration) for
additional information for registering products and establishing remote
access and alarming.
Disable EASG:
By disabling Avaya Logins you are preventing Avaya access to your system.
This is not recommended, as it impacts Avaya's ability to provide support
for the product. Unless the customer is well versed in managing the
product themselves, Avaya Logins should not be disabled.
Enter 1 to Enable EASG (Recommended) or 2 to Disable EASG? 1
You have requested Avaya Logins be Enabled.
Do you want to continue (Y/N)? Y
Avaya Logins have been Enabled.
```

7. If you use the Gateway Configuration script to complete basic configuration of the gateway complete the required process as shown below. The gateway will then reset.

```
--- Gateway Configuration Script ---
The script will provide you basic gateway connectivity configuration.
Configuration Script - do you want to continue (Y/N)? Y
Default settings are in square brackets '[]'.
Vlan [1] :
IPv4 Enabled (Y/N)? [Y]:
IPv4 address [169.254.0.2] :172.16.1.230
IPv4 Subnet mask [255.255.255.0] :255.255.254.0
IPv4 Default gateway [172.16.1.1] :172.16.1.254
IPv6 Enabled (Y/N)? [N]:
MGC controllers [0.0.0.0] :172.16.1.168
Hostname [G450] :G450
Enable Spanning Tree on LAN ports (Y/N/Help)? [Y] :
The following parameters are about to be configured:
Vlan : 1
IPv4 address : 172.16.1.230
Subnet mask
Default gateway
MGC controllors
                      : 255.255.254.0
                      : 172.16.1.254
                      : 172.16.1.168
Hostname
                       : G450
Spanning Tree Protocol : enabled
The gateway will save those parameters in startup-config and then reset
- do you want to continue (Y/N)? Y
Please connect your gateway to the network via any Ethernet port
Saving configuration...
Resetting the device ...
```

8. The Cryptographic Officer must log in to the gateway using a user login account that has administrative privileges as shown below.

```
Login: root
Password: ****
Password accepted
```

9. Run the **show fips-mode** command to verify if FIPS-mode is disabled.

```
G450G450(super)# show fips
FIPS Mode: Disabled
```

 Run the username command to define new user logins for Cryptographic officer, administrators and users as shown below.

```
G450(super)# username crypto-officer access-type admin
Enter new password: *******
Confirm password: ********
User account added.
```

11. Run the **show username** command to verify the successful addition of users as shown below.

```
G450-???(super)# show username

User Access Account Active type

root admin local yes crypto-officer admin local yes
```

12. If you have saved a copy of your previous configuration prior to disabling FIPS approved mode, refer to it to perform any additional configuration as needed. For more information, see <u>Configuration changes and backup</u> on page 28.

### FIPS Error States and LED Status Indicators

The CPU, ALM, MDM, and PWR LED lamps on the gateway's faceplate provide status and error states during power-up self-tests. Status messages and error states may be also be viewed on a monitor using the G450 Branch Gateway's serial console port.

### **Power-up Testing**

When the Module is performing Power-up Self-Test, the LED states will be as follows:

- CPU LED: flashing
- ALM LED: on

If FIPS power-up testing completes successfully, the System CPU and ALM LEDS will resume their normal operational state:

- CPU LED: on
- ALM LED: off

If Power-up Self-Test does not complete successfully, the Module will reset and enter the Error State 1 or Error State 3 depending on the nature of the failure.

### **Error States**

The gateway's cryptographic module defines three Error States which may be entered due to hard or soft operational failures. Upon entering an Error State, the System CPU and ALM LED lamps will indicate the type of failure by providing a unique pattern of flashing and/or steadily lit lamps on the LEDS of the gateway's faceplate. Additionally, G450 Branch Gateway has a serial console port that allows one to view status and error states using a monitor.

#### **Error State 1**

Error State 1 processes hard errors due to failures of the Module's Power-up Self-Tests. Exit is via operator selection of reboot or zeroization with reboot.

#### LED flash patterns:

- MDM: continuous ON 15 seconds, OFF 15 seconds
- ALM: continuous ON-OFF flash
- CPU: continuous cycles of two ON-OFF flashes separated by 2.25s OFF
- PWR: on if all power supplies are healthy, flashing otherwise

#### **Error State 2**

Error State 2 processes soft errors related to conditional self-test failures. Exit is through automatic reboot.

#### LED flash patterns:

- MDM: on
- ALM: continuous on-off flash
- · CPU: continuous cycles of three on-off flashes
- PWR: on if all power supplies are healthy, flashing otherwise

#### **Error State 3**

Error State 3 processes hard errors linked to critical function failures. Exit is automatic with immediate zeroization.

#### LED flash patterns:

- MDM: on
- · ALM: continuous on-off flashes
- CPU: continuous cycles of four on-off flashes
- PWR: on if all power supplies are healthy, flashing otherwise

### **Zeroization Status during Error State 1**

When the user is given the option to zeroize as a result of being in Error State 1, the CPU and ALM LEDs will indicate this using the following unique pattern:

• CPU LED: 2 blinks

· ALM LED: flashing

For a 2-hour period, the MDM LED will alternate on and off in 15 second intervals to indicate whether zeroization will occur when the reset button is pressed.

- 1. MDM LED On: Zeroize and Reset
- 2. MDM LED Off: Reset only

After 2 hours, the MDM LED will remain off and the user will no longer be given the option to zeroize using the reset button. However,G450 Branch Gateway users may also use the serial console port to select the appropriate action.

# **Chapter 27: Resources**

## **Branch Gateway documentation**

The following table lists the documents related to Branch Gateway. Download the documents from the Avaya Support website at <a href="http://support.avaya.com">http://support.avaya.com</a>.

Title	Description	Audience
Installing and implementing		
Quick Start for Hardware Installation: Avaya G450 Branch Gateway	Describes how to install G450 Branch Gateway in the basic configuration.	Solution architects, implementation engineers, and support personnel
Deploying and Upgrading Avaya G450 Branch Gateway	Describes how to install and upgrade G450 Branch Gateway, perform basic configuration tasks, insert media modules, and connect external devices.	Solution architects, implementation engineers, and support personnel
Administering		
Administering Avaya G450 Branch Gateway	Describes how to configure and manage G450 Branch Gateway after the installation. Contains the detailed information about G450 Branch Gateway features and their implementation.	Solution architects, implementation engineers, and support personnel
Avaya Branch Gateway G450 CLI Reference	Describes the CLI commands for G450 Branch Gateway configuration.	Solution architects, implementation engineers, and support personnel
Avaya Aura <sup>®</sup> G450 Data Privacy Guidelines	Describes how to administer G450 Branch Gateway to fulfill Data Privacy requirements.	Solution architects, implementation engineers, and support personnel

## Finding documents on the Avaya Support website

#### **Procedure**

- 1. Go to https://support.avaya.com.
- 2. At the top of the screen, type your username and password and click Login.
- 3. Click Support by Product > Documents.

- 4. In **Enter your Product Here**, type the product name and then select the product from the list
- 5. In **Choose Release**, select the appropriate release number.

The Choose Release field is not available if there is only one release for the product.

6. In the **Content Type** filter, click a document type, or click **Select All** to see a list of all available documents.

For example, for user guides, click **User Guides** in the **Content Type** filter. The list only displays the documents for the selected category.

7. Click Enter.

### Accessing the port matrix document

#### **Procedure**

- 1. Go to <a href="https://support.avaya.com">https://support.avaya.com</a>.
- 2. Log on to the Avaya website with a valid Avaya user ID and password.
- 3. On the Avaya Support page, click **Support by Product > Documents**.
- 4. In **Enter Your Product Here**, type the product name, and then select the product from the list of suggested product names.
- 5. In **Choose Release**, select the required release number.
- 6. In the **Content Type** filter, select one or both the following categories:
  - Application & Technical Notes
  - Design, Development & System Mgt

The list displays the product-specific Port Matrix document.

7. Click Enter.

## **Avaya Documentation Center navigation**

For some programs, the latest customer documentation is now available on the Avaya Documentation Center website at <a href="https://documentation.avaya.com">https://documentation.avaya.com</a>.

### Important:

For documents that are not available on Avaya Documentation Center, click **More Sites** > **Support** on the top menu to open https://support.avaya.com.

Using the Avaya Documentation Center, you can:

Search for keywords.

To filter by product, click **Filters** and select a product.

· Search for documents.

From **Products & Solutions**, select a solution category and product, and then select the appropriate document from the list.

- Sort documents on the search results page.
- Click **Languages** ( ((a)) to change the display language and view localized documents.
- Publish a PDF of the current section in a document, the section and its subsections, or the entire document.
- Add content to your collection using My Docs (☆).

Navigate to the **Manage Content > My Docs** menu, and do any of the following:

- Create, rename, and delete a collection.
- Add topics from various documents to a collection.
- Save a PDF of the selected content in a collection and download it to your computer.
- Share content in a collection with others through email.
- Receive collection that others have shared with you.
- Add yourself as a watcher using the Watch icon (○).

Navigate to the **Manage Content > Watchlist** menu, and do the following:

- Enable **Include in email notification** to receive email alerts.
- Unwatch selected content, all content in a document, or all content on the Watch list page.

As a watcher, you are notified when content is updated or deleted from a document, or the document is removed from the website.

- Share a section on social media platforms, such as Facebook, LinkedIn, and Twitter.
- Send feedback on a section and rate the content.

#### Note:

Some functionality is only available when you log in to the website. The available functionality depends on your role.

## **Training**

The following courses are available on <a href="https://www.avaya-learning.com">https://www.avaya-learning.com</a>. To search for the course, in the **Search** field, enter the course code and click **Go**.

Course code	Course title
20980W	What's New with Avaya Aura®

## **Viewing 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.

- To find videos on the Avaya Support website, go to <a href="https://support.avaya.com/">https://support.avaya.com/</a> and do one of the following:
  - In Search, type Avaya Mentor Videos, click Clear All and select Video in the Content Type.
  - In **Search**, type the product name. On the Search Results page, click **Clear All** and select **Video** in the **Content Type**.

The **Video** content type is displayed only when videos are available for that product.

In the right pane, the page displays a list of available videos.

- To find the Avaya Mentor videos on YouTube, go to <a href="www.youtube.com/AvayaMentor">www.youtube.com/AvayaMentor</a> and do one of the following:
  - Enter a key word or key words in the **Search Channel** to search for a specific product or topic.
  - Scroll down Playlists, and click a topic name to see the list of videos available for the topic. For example, Contact Centers.



#### Note:

Videos are not available for all products.

## **Support**

Go to the Avaya Support website at <a href="https://support.avaya.com">https://support.avaya.com</a> 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.

# **Appendix A: Traps and MIBs**

## **Branch Gateway traps**

Name	Parameters (MIB variables)	Class	Msg Facility	Severity	Trap Name / Mnemonic	Format	Description
coldStart		STD	Boot	Warning	coldStart	Agent Up with Possible Changes (coldStart Trap) enterprise:\$E (\$e) args(\$#):\$*	A coldStart trap indicates that the entity sending the protocol is reinitializing itself in such a way as to potentially cause the alteration of either the agent's configuration or the entity's implementatio n.
warmStart		STD	Boot	Warning	warmStart	Agent Up with No Changes (warmStart Trap) enterprise:\$E (\$e) args(\$#):\$*	A warmStart trap indicates that the entity sending the protocol is reinitializing itself in such a way as to keep both the agent configuration and the entity's implementation intact.
LinkUp	ifIndex, ifAdminStat us,	STD	System	Warning	LinkUp	Agent Interface Up (linkUp Trap)	A linkUp trap indicates that the entity

Name	Parameters (MIB variables)	Class	Msg Facility	Severity	Trap Name / Mnemonic	Format	Description
	ifOperStatu s					enterprise:\$E (\$e) on interface \$1	sending the protocol recognizes that one of the communication links represented in the agent's configuration has come up.
							The data passed with the event is
							1) The name and value of the ifIndex instance for the affected interface. The name of the interface can be retrieved via an snmpget of.1.3.6.1.2.1.2 .2.1.2.INST, where INST is the instance returned with the trap.
linkDown	ifIndex, ifAdminStat us, ifOperStatu s	STD	System	Warning	linkDown	Agent Interface Down (linkDown Trap) enterprise:\$E (\$e) on interface \$1	A linkDown trap indicates that the entity that is sending the protocol recognizes a failure in one of the communication links represented in the agent's configuration.

Name	Parameters (MIB variables)	Class	Msg Facility	Severity	Trap Name / Mnemonic	Format	Description
							The data passed with the event is
							1) The name and value of the ifIndex instance for the affected interface. The name of the interface can be retrieved via an snmpget of.1.3.6.1.2.1.2 .2.1.2.INST, where INST is the instance returned with the trap.
SNMP_Au then_		P330	SECURI TY	Notificati on	authentic Failure	Incorrect Community	An authentication
Failure					Tallule	Name (authenticatio n Failure Trap) enterprise:\$E (\$e) args(\$#):\$*	failure trap indicates that the protocol is not properly authenticated.
risingAlar m	alarmIndex, alarmVariab le, alarmSampl e Type, alarmValue, alarmRising Threshold	RMON	THRES HOLD	Warning	rising Alarm	Rising Alarm: \$2 exceeded threshold \$5; value = \$4. (Sample type = \$3; alarm index = \$1)	The SNMP trap that is generated when an alarm entry crosses its rising threshold and generates an event that is configured for sending SNMP traps
fallingAlar m	alarmIndex, alarmVariab le, alarmSampl	RMON	THRES HOLD	Warning	falling Alarm	Falling Alarm: \$2 fell below threshold \$5; value = \$4.	The SNMP trap that is generated when an alarm

Name	Parameters (MIB variables)	Class	Msg Facility	Severity	Trap Name / Mnemonic	Format	Description
	e Type, alarmValue, alarmRising Threshold, alarmFalling Threshold					(Sample type = \$3; alarm index = \$1)	entry crosses its falling threshold and generates an event that is configured for sending SNMP traps
deleteSW Redundan cy Trap	soft Redundanc y Status	P330	SWITCH FABRIC	Info	deleteSWRe dundancyTra p	Software Redundancy \$1 definition deleted	The trap notifies the manager of the deletion of the specified redundant link, which is identified by the softRedundanc yld. It is enabled/disabled by chLntAgConfig ChangeTraps.
createSW Redundan cy Trap	soft Redundanc y Status	P330	SWITCH FABRIC	Info	createSWRe dundancyTra p	Software Redundancy \$1 definition created	The trap is generated on the creation of the redundant links for the specified ports. It gives the logical name of the redundant link the identification of the main and secondary ports and the status of the link. The softRedundanc yld defines the instances of the abovementioned variables. The trap is

Name	Parameters (MIB variables)	Class	Msg Facility	Severity	Trap Name / Mnemonic	Format	Description
							enabled/ disabled by chLntAgConfig ChangeTraps.
IseIntPort CAMLastC hange Trap	IseIntPortC AMLastCha nge	P330	SWITCH FABRIC	Info	IseIntPort CAMLast Change Trap	CAM Change at \$1	This trap reports of the occurred configuration changes. It is enabled/ disabled by chLntAgCAMC hangeTraps.
duplicatel P Trap	ipNetToMed iaPhysAddr ess, ipNetToMed iaNetAddre ss	P330	ROUTER	Warning	duplicateIPT rap	Duplicate IP address \$2 detected; MAC address \$1	This trap reports to the Management station on Duplicate IP identification. CRP identify the new IP on the network. If it similar to one of its IP interfaces, the CRP will issue a SNMP trap, containing the MAC of the intruder.
IntPolicy ChangeEv ent	ipPolicy Activation EntID, ipPolicy ActivationLi st, ipPolicy Activationif Index, ipPolicy ActivationS ub Context	P330	POLICY	Info	IntPolicyCha ngeEvent	Module \$1 - Active policy list changed to \$2	The trap reports a change in the active list specific for a policy-enabled box or module.
IntPolicy AccessCo ntrolViolati onFIt	ipPolicy AccessCont rol	P330	POLICY	Warning	IntPolicy Access Control ViolationFlt	IP PolicyAccess Control violation, if-	This trap reports to the Management station on IP

Name	Parameters (MIB variables)	Class	Msg Facility	Severity	Trap Name / Mnemonic	Format	Description
	ViolationEnt ID, ipPolicy AccessCont rolViolation Src Addr, ipPolicy AccessCont rol ViolationDst Addr,					index\$9 ip- protocol=\$4 src-ip=\$2 dst- ip=\$3 src- port=\$5 dst- port=\$6 rule- id=\$8 rule- list=\$\$9	PolicyAccess Control violation. The trap includes in its varbind information about the slot where the event occurred. The
	ipPolicy AccessCont rol						id of the rule that was violated in the current rules
	Violation Protocol, ipPolicy AccessCont rol						table, and the quintuplet that identifies the faulty packet. A
	Violation						management application
	L4SrcPort, ipPolicy AccessCont rol						would display this trap and the relevant information in
	ViolationL4 DstPort, ipPolicy AccessCont rolViolation Established, ipPolicyRul eID, ipPolicyRul e ListID, ipPolicy AccessCont rolViolationI						a log entry. This trap will not be sent at intervals smaller than one minute for identical information in the varbinds list variables.
	f Index, ipPolicy AccessCont rol						
	ViolationSu b Ctxt, ipPolicy						

Name	Parameters (MIB variables)	Class	Msg Facility	Severity	Trap Name / Mnemonic	Format	Description
	AccessCont rol ViolationTim e						
DormantP ort Fault	genPortSW RdFault, genPortGro up Id, genPortId	P330	SWITCH FABRIC	Warning	Dormant PortFault	Dormant Port Connection Lost on Module \$2 Port \$3;	This trap reports the loss of connection on a dormant port.
DormantP ort Ok	genPortSW RdFault, genPortGro up Id, genPortId	P330	SWITCH FABRIC	Notificati on	Dormant PortOk	Dormant Port Connection Returned to Normal on Module \$2 Port \$3;	This trap reports the return of connection on a dormant port.
InlinePwrF It	genGroup FaultMask, genGroupId , genGroup BUPSActivit y Status	P330	POE	Error	InlinePwr Flt	Module \$2 Inline Power Supply failure	This trap reports the failure of an inline power supply.
InlinePwrF ItOK	genGroup FaultMask, genGroupId , genGroup BUPSActivit y Status	P330	POE	Notificati on	InlinePwr FItOK	Module \$2 Inline Power Supply failure was cleared	This trap reports the correction of a failure on an inline power supply.
WanPhysi cal AlarmOn	ifIndex, ifAdminStat us, ifOperStatu s, ifName, ifAlias, dsx1Line Status	WAN	WAN	Critical	Wan Physical AlarmOn	Cable Problem on port \$4	An E1/T1/ serial cable was disconnected.
wanPhysic al AlarmOff	ifIndex, ifAdminStat us, ifOperStatu s, ifName, ifAlias, dsx1Line Status	WAN	WAN	Notificati on	wan Physical AlarmOff	Cable Problem on port \$4 was cleared	An E1/T1/ serial cable was reconnected.

Name	Parameters (MIB variables)	Class	Msg Facility	Severity	Trap Name / Mnemonic	Format	Description
wanLocal AlarmOn	ifIndex, ifAdminStat us, ifOperStatu s, ifName, ifAlias, dsx1Line Status	WAN	WAN	Error	wanLocal AlarmOn	Local Alarm on interface \$4	Local alarms, such as LOS.
wanLocal AlarmOff	ifIndex, ifAdminStat us, ifOperStatu s, ifName, ifAlias, dsx1Line Status	WAN	WAN	Notificati on	wanLocal AlarmOff	Local Alarm on interface \$4 was cleared	Local alarms, such as LOS, was cleared.
wanRemot e AlarmOn	ifIndex, ifAdminStat us, ifOperStatu s, ifName, ifAlias, dsx1Line Status	WAN	WAN	Error	wan Remote AlarmOn	Remote Alarm on interface \$4	Remote alarms, such as AIS.
wanRemot e AlarmOff	ifIndex, ifAdminStat us, ifOperStatu s, ifName, ifAlias, dsx1Line Status	WAN	WAN	Notificati on	wan Remote AlarmOff	Remote Alarm on interface \$4 was cleared	Remote alarms, such as AIS, was cleared.
wanMinor AlarmOn	ifIndex, ifAdminStat us, ifOperStatu s, ifName, ifAlias, dsx1Line Status	WAN	WAN	Warning	wanMinor AlarmOn	Minor Alarm on interface \$4	Low BER.
wanMinor Alarm Off	ifIndex, ifAdminStat us, ifOperStatu	WAN	WAN	Notificati on	wanMinor AlarmOff	Minor Alarm on interface \$4 was cleared	Normal BER.

Name	Parameters (MIB variables)	Class	Msg Facility	Severity	Trap Name / Mnemonic	Format	Description
	s, ifName, ifAlias, dsx1Line Status						
AvEntFan FIt	entPhysical Index, entPhysical Descr, entPhySens orValue, avEntPhy SensorLo Warning	AVAYA -ENTIT Y	TEMP		AvEntFan Flt	Fan \$2 is Faulty	This trap reports a faulty fan.
AvEntFan Ok	entPhysical Index, entPhysical Descr, entPhySens or Value, avEntPhy SensorLo Warning	AVAYA -ENTIT Y	TEMP	Notificati on	AvEntFanOk	Fan \$2 is OK	This trap reports the return to function of a faulty fan.
avEnt48vP wr Flt	entPhysical Index, entPhysical Descr, entPhySens or Value, avEntPhy SensorHi Warning, avEntPhy SensorLo Warningent Physical ParentRelP os	AVAYA -ENTIT Y	SUPPLY		avEnt48v PwrFlt	48V power supply Fault	This trap reports a problem with a 48V power supply.
avEnt5vP wrFlt	entPhysical Index, entPhysical Descr, entPhySens or Value, avEntPhy SensorHi	AVAYA -ENTIT Y	SUPPLY		avEnt5v PwrFlt	5V power supply Fault	This trap reports a problem with a 5V power supply.

Name	Parameters (MIB variables)	Class	Msg Facility	Severity	Trap Name / Mnemonic	Format	Description
	Warning, avEntPhy SensorLo Warningent Physical ParentRelP os						
avEnt3300 mv PwrFlt	entPhysical Index, entPhysical Descr, entPhySens or Value, avEntPhy SensorHi Warning, avEntPhy SensorLo Warningent Physical ParentRelP os	AVAYA -ENTIT Y	SUPPLY		avEnt3300m v PwrFlt	3.3V (3300mv) power supply Fault	This trap reports a problem with a 3.3V power supply.
avEnt2500 mv PwrFlt	entPhysical Index, entPhysical Descr, entPhySens or Value, avEntPhy SensorHi Warning, avEntPhy SensorLo Warningent Physical ParentRelP os	AVAYA -ENTIT Y	SUPPLY		avEnt2500m v PwrFlt	2.5V (2500mv) power supply Fault	This trap reports a problem with a 2.5V power supply.
avEnt1800 mv PwrFlt	entPhysical Index, entPhysical Descr, entPhySens or Value, avEntPhy SensorHi	AVAYA -ENTIT Y	SUPPLY		avEnt1800m v PwrFlt	1.8V (1800mv) power supply Fault	This trap reports a problem with a 1.8V power supply.

Name	Parameters (MIB variables)	Class	Msg Facility	Severity	Trap Name / Mnemonic	Format	Description
	Warning, avEntPhy SensorLo Warningent Physical ParentRelP os						
avEnt1600 mv PwrFlt	entPhysical Index, entPhysical Descr, entPhySens or Value, avEntPhy SensorHi Warning, avEntPhy SensorLo Warningent Physical ParentRelP os	AVAYA -ENTIT Y	SUPPLY		avEnt1600m v PwrFlt	1.6V (1600mv) power supply Fault	This trap reports a problem with a 1.6V power supply.
avEnt48vP wr FltOk	entPhysical Index, entPhysical Descr, entPhySens or Value, avEntPhy SensorHi Warning, avEntPhy SensorLo Warningent Physical ParentRelP os	AVAYA -ENTIT Y	SUPPLY	Notificati	avEnt48v PwrFltOk	48V power supply Fault Cleared	This trap reports the correction of a problem with a 48V power supply.
avEnt5vP wrFltOk	entPhysical Index, entPhysical Descr, entPhySens or Value, avEntPhy SensorHi	AVAYA -ENTIT Y	SUPPLY	Notificati on	avEnt5v PwrFltOk	5V power supply Fault Cleared	This trap reports the correction of a problem with a 5V power supply.

Name	Parameters (MIB variables)	Class	Msg Facility	Severity	Trap Name / Mnemonic	Format	Description
	Warning, avEntPhy SensorLo Warningent Physical ParentRelP os						
avEnt3300 mv PwrFltOk	entPhysical Index, entPhysical Descr, entPhySens or Value, avEntPhy SensorHi Warning, avEntPhy SensorLo Warningent Physical ParentRelP os	AVAYA -ENTIT Y	SUPPLY	Notificati on	avEnt3300m v PwrFlt Ok	3.3V (3300mv) power supply Fault Cleared	This trap reports the correction of a problem with a 3.3V power supply.
avEnt2500 mv PwrFltOk	entPhysical Index, entPhysical Descr, entPhySens or Value, avEntPhy SensorHi Warning, avEntPhy SensorLo Warningent Physical ParentRelP os	AVAYA -ENTIT Y	SUPPLY	Notificati on	avEnt2500m vPwrFlt Ok	2.5V (2500mv) power supply Fault Cleared	This trap reports the correction of a problem with a 2.5V power supply.
avEnt1800 mv PwrFltOk	entPhysical Index, entPhysical Descr, entPhySens or Value, avEntPhy SensorHi	AVAYA -ENTIT Y	SUPPLY	Notificati on	avEnt1800m vPwrFlt Ok	1.8V (1800mv) power supply Fault Cleared	This trap reports the correction of a problem with a 1.8V power supply.

Name	Parameters (MIB variables)	Class	Msg Facility	Severity	Trap Name / Mnemonic	Format	Description
	Warning, avEntPhy SensorLo Warningent Physical ParentRelP os						
avEnt1600 mv PwrFltOk	entPhysical Index, entPhysical Descr, entPhySens or Value, avEntPhy SensorHi Warning, avEntPhy SensorLo Warningent Physical ParentRelP os	AVAYA -ENTIT Y	SUPPLY	Notificati	avEnt1600m v PwrFlt Ok	1.6V (1600mv) power supply Fault Cleared	This trap reports the correction of a problem with a 1.6V power supply.
avEntAmbi ent TempFlt	entPhysical Index, entPhysical Descr, entPhySens or Value, avEntPhy SensorHi Warning, entPhysical ParentRelP os	AVAYA -ENTIT Y	TEMP		avEnt Ambient TempFlt	Ambient Temperature fault (\$3)	This trap reports that the ambient temperature in the device is not within the acceptable temperature range for the device.
avEntAmbi ent TempOk	entPhysical Index, entPhysical Descr, entPhySens or Value, avEntPhy SensorHi Warning, entPhysical ParentRelP os	AVAYA - ENTIT Y	TEMP	Notificati on	avEnt Ambient TempOk	Ambient Temperature fault (\$3) cleared	This trap reports that the ambient temperature in the device has returned to the acceptable range for the device.

# **Branch Gateway MIB files**

MIB File	MIB Module Supported by Branch Gateway
Load.MIB	LOAD-MIB
RFC1315-MIB.my	RFC1315-MIB
Q-BRIDGE-MIB.my	Q-BRIDGE-MIB
ENTITY-MIB.my	ENTITY-MIB
IP-FORWARD-MIB.my	IP-FORWARD-MIB
VRRP-MIB.my	VRRP-MIB
UTILIZATION-MANAGEMENT-MIB.my	UTILIZATION-MANAGEMENT-MIB
ENTITY-SENSOR-MIB.my	ENTITY-SENSOR-MIB
RSTP-MIB.my	RSTP-MIB
APPLIC-MIB.MY	APPLIC-MIB
PPP-IP-NCP-MIB.my	PPP-IP-NCP-MIB
RFC1213-MIB.my	RFC1213-MIB
AVAYA-ENTITY-MIB.MY	AVAYA-ENTITY-MIB
Rnd.MIB	RND-MIB
XSWITCH-MIB.MY	XSWITCH-MIB
CROUTE-MIB.MY	CROUTE-MIB
RS-232-MIB.my	RS-232-MIB
RIPv2-MIB.my	RIPv2-MIB
IF-MIB.my	IF-MIB
DS0-MIB.my	DS0-MIB
POLICY-MIB.MY	POLICY-MIB
BRIDGE-MIB.my	BRIDGE-MIB
CONFIG-MIB.MY	CONFIG-MIB
G700-MG-MIB.MY	G700-MG-MIB
FRAME-RELAY-DTE-MIB.my	FRAME-RELAY-DTE-MIB
IP-MIB.my	IP-MIB
Load12.MIB	LOAD-MIB
PPP-LCP-MIB.my	PPP-LCP-MIB
WAN-MIB.MY	WAN-MIB
SNMPv2-MIB.my	SNMPv2-MIB
USM-MIB.my	USM-MIB
VACM-MIB.my	VACM-MIB
OSPF-MIB.my	OSPF-MIB
Tunnel-MIB.my	TUNNEL-MIB

## MIB objects in the Load.MIB file

The following table provides a list of the MIBs in the Load.MIB file that are supported by the Branch Gateway and their OIDs:

Object	OID
genOpModuleId	1.3.6.1.4.1.1751.2.53.1.2.1.1
genOpIndex	1.3.6.1.4.1.1751.2.53.1.2.1.2
genOpRunningState	1.3.6.1.4.1.1751.2.53.1.2.1.3
genOpSourceIndex	1.3.6.1.4.1.1751.2.53.1.2.1.4
genOpDestIndex	1.3.6.1.4.1.1751.2.53.1.2.1.5
genOpServerIP	1.3.6.1.4.1.1751.2.53.1.2.1.6
genOpUserName	1.3.6.1.4.1.1751.2.53.1.2.1.7
genOpPassword	1.3.6.1.4.1.1751.2.53.1.2.1.8
genOpProtocolType	1.3.6.1.4.1.1751.2.53.1.2.1.9
genOpFileName	1.3.6.1.4.1.1751.2.53.1.2.1.10
genOpRunningStateDisplay	1.3.6.1.4.1.1751.2.53.1.2.1.11
genOpLastFailureIndex	1.3.6.1.4.1.1751.2.53.1.2.1.12
genOpLastFailureDisplay	1.3.6.1.4.1.1751.2.53.1.2.1.13
genOpLastWarningDisplay	1.3.6.1.4.1.1751.2.53.1.2.1.14
genOpErrorLogIndex	1.3.6.1.4.1.1751.2.53.1.2.1.15
genOpResetSupported	1.3.6.1.4.1.1751.2.53.1.2.1.16
genOpEnableReset	1.3.6.1.4.1.1751.2.53.1.2.1.17
genOpNextBootImageIndex	1.3.6.1.4.1.1751.2.53.1.2.1.18
genOpLastBootImageIndex	1.3.6.1.4.1.1751.2.53.1.2.1.19
genOpFileSystemType	1.3.6.1.4.1.1751.2.53.1.2.1.20
genOpReportSpecificFlags	1.3.6.1.4.1.1751.2.53.1.2.1.21
genOpOctetsReceived	1.3.6.1.4.1.1751.2.53.1.2.1.22
genAppFileId	1.3.6.1.4.1.1751.2.53.2.1.1.1
genAppFileName	1.3.6.1.4.1.1751.2.53.2.1.1.2
genAppFileType	1.3.6. 1.4.1.1751.2.53.2.1.1.3
genAppFileDescription	1.3.6.1.4.1.1751.2.53.2.1.1.4
genAppFileSize	1.3.6.1.4.1.1751.2.53.2.1.1.5
genAppFileVersionNumber	1.3.6.1.4.1.1751.2.53.2.1.1.6
genAppFileLocation	1.3.6.1.4.1.1751.2.53.2.1.1.7
genAppFileDateStamp	1.3.6.1.4.1.1751.2.53.2.1.1.8
genAppFileRowStatus	1.3.6.1.4.1.1751.2.53.2.1.1.9

## MIB objects in the RFC1315-MIB.my file

The following table provides a list of the MIBs in the RFC1315-MIB.my file that are supported by the Branch Gateway and their OIDs:

Object	OID
frDlcmilfIndex	1.3.6.1.2.1.10.32.1.1.1
frDlcmiState	1.3.6.1.2.1.10.32.1.1.2
frDlcmiAddress	1.3.6.1.2.1.10.32.1.1.3
frDlcmiAddressLen	1.3.6.1.2.1.10.32.1.1.4
frDlcmiPollingInterval	1.3.6.1.2.1.10.32.1.1.5
frDlcmiFullEnquiryInterval	1.3.6.1.2.1.10.32.1.1.6
frDlcmiErrorThreshold	1.3.6.1.2.1.10.32.1.1.7
frDlcmiMonitoredEvents	1.3.6.1.2.1.10.32.1.1.8
frDlcmiMaxSupportedVCs	1.3.6.1.2.1.10.32.1.1.9
frDlcmiMulticast	1.3.6.1.2.1.10.32.1.1.10
frCircuitlfIndex	1.3.6.1.2.1.10.32.2.1.1
frCircuitDlci	1.3.6.1.2.1.10.32.2.1.2
frCircuitState	1.3.6.1.2.1.10.32.2.1.3
frCircuitReceivedFECNs	1.3.6.1.2.1.10.32.2.1.4
frCircuitReceivedBECNs	1.3.6.1.2.1.10.32.2.1.5
frCircuitSentFrames	1.3.6.1.2.1.10.32.2.1.6
frCircuitSentOctets	1.3.6.1.2.1.10.32.2.1.7
frCircuitReceivedFrames	1.3.6.1.2.1.10.32.2.1.8
frCircuitReceivedOctets	1.3.6.1.2.1.10.32.2.1.9
frCircuitCreationTime	1.3.6.1.2.1.10.32.2.1.10
frCircuitLastTimeChange	1.3.6.1.2.1.10.32.2.1.11
frCircuitCommittedBurst	1.3.6.1.2.1.10.32.2.1.12
frCircuitExcessBurst	1.3.6.1.2.1.10.32.2.1.13
frCircuitThroughput	1.3.6.1.2.1.10.32.2.1.14
frErrlfIndex	1.3.6.1.2.1.10.32.3.1.1
frErrType	1.3.6.1.2.1.10.32.3.1.2
frErrData	1.3.6.1.2.1.10.32.3.1.3
frErrTime	1.3.6.1.2.1.10.32.3.1.4
frTrapState	1.3.6.1.2.1.10.32.4.1

## MIB objects in the Q-BRIDGE-MIB.my file

The following table provides a list of the MIBs in the Q-BRIDGE-MIB.my file that are supported by the Branch Gateway and their OIDs:

Object	OID
dot1qVlanVersionNumber	1.3.6.1.2.1.17.7.1.1.1
dot1qMaxVlanId	1.3.6.1.2.1.17.7.1.1.2
dot1qMaxSupportedVlans	1.3.6.1.2.1.17.7.1.1.3
dot1qNumVlans	1.3.6.1.2.1.17.7.1.1.4
dot1qGvrpStatus	1.3.6.1.2.1.17.7.1.1.5
dot1qVlanTimeMark	1.3.6.1.2.1.17.7.1.4.2.1.1
dot1qVlanIndex	1.3.6.1.2.1.17.7.1.4.2.1.2
dot1qVlanFdbld	1.3.6.1.2.1.17.7.1.4.2.1.3
dot1qVlanCurrentEgressPorts	1.3.6.1.2.1.17.7.1.4.2.1.4
dot1qVlanCurrentUntaggedPorts	1.3.6.1.2.1.17.7.1.4.2.1.5
dot1qVlanStatus	1.3.6.1.2.1.17.7.1.4.2.1.6
dot1qVlanCreationTime	1.3.6.1.2.1.17.7.1.4.2.1.7
dot1qVlanStaticName	1.3.6.1.2.1.17.7.1.4.3.1.1
dot1qVlanStaticEgressPorts	1.3.6.1.2.1.17.7.1.4.3.1.2
dot1qVlanForbiddenEgressPorts	1.3.6.1.2.1.17.7.1.4.3.1.3
dot1qVlanStaticUntaggedPorts	1.3.6.1.2.1.17.7.1.4.3.1.4
dot1qVlanStaticRowStatus	1.3.6.1.2.1.17.7.1.4.3.1.5
dot1qNextFreeLocalVlanIndex	1.3.6.1.2.1.17.7.1.4.4
dot1qPvid	1.3.6.1.2.1.17.7.1.4.5.1.1
dot1qPortAcceptableFrameTypes	1.3.6.1.2.1.17.7.1.4.5.1.2
dot1qPortIngressFiltering	1.3.6.1.2.1.17.7.1.4.5.1.3
dot1qPortGvrpStatus	1.3.6.1.2.1.17.7.1.4.5.1.4
dot1qPortGvrpFailedRegistrations	1.3.6.1.2.1.17.7.1.4.5.1.5
dot1qPortGvrpLastPduOrigin	1.3.6.1.2.1.17.7.1.4.5.1.6

## MIB objects in the ENTITY-MIB.my file

The following table provides a list of the MIBs in the ENTITY-MIB.my file that are supported by the Branch Gateway and their OIDs:

Object	OID
entPhysicalIndex	1.3.6.1.2.1.47.1.1.1.1
entPhysicalDescr	1.3.6.1.2.1.47.1.1.1.2
entPhysicalVendorType	1.3.6.1.2.1.47.1.1.1.3
entPhysicalContainedIn	1.3.6.1.2.1.47.1.1.1.4
entPhysicalClass	1.3.6.1.2.1.47.1.1.1.5
entPhysicalParentRelPos	1.3.6.1.2.1.47.1.1.1.6

Object	OID
entPhysicalName	1.3.6.1.2.1.47.1.1.1.7
entPhysicalHardwareRev	1.3.6.1.2.1.47.1.1.1.8
entPhysicalFirmwareRev	1.3.6.1.2.1.47.1.1.1.9
entPhysicalSoftwareRev	1.3.6.1.2.1.47.1.1.1.10
entPhysicalSerialNum	1.3.6.1.2.1.47.1.1.1.11
entPhysicalMfgName	1.3.6.1.2.1.47.1.1.1.12
entPhysicalModelName	1.3.6.1.2.1.47.1.1.1.13
entPhysicalAlias	1.3.6.1.2.1.47.1.1.1.14
entPhysicalAssetID	1.3.6.1.2.1.47.1.1.1.15
entPhysicalIsFRU	1.3.6.1.2.1.47.1.1.1.16

## MIB objects in the IP-FORWARD-MIB.my file

The following table provides a list of the MIBs in the IP-FORWARD-MIB.my file that are supported by the Branch Gateway and their OIDs:

Object	OID
ipCidrRouteNumber	1.3.6.1.2.1.4.24.3
ipCidrRouteDest	1.3.6.1.2.1.4.24.4.1.1
ipCidrRouteMask	1.3.6.1.2.1.4.24.4.1.2
ipCidrRouteTos	1.3.6.1.2.1.4.24.4.1.3
ipCidrRouteNextHop	1.3.6.1.2.1.4.24.4.1.4
ipCidrRouteIfIndex	1.3.6.1.2.1.4.24.4.1.5
ipCidrRouteType	1.3.6.1.2.1.4.24.4.1.6
ipCidrRouteProto	1.3.6.1.2.1.4.24.4.1.7
ipCidrRouteAge	1.3.6.1.2.1.4.24.4.1.8
ipCidrRouteInfo	1.3.6.1.2.1.4.24.4.1.9
ipCidrRouteNextHopAS	1.3.6.1.2.1.4.24.4.1.10
ipCidrRouteMetric1	1.3.6.1.2.1.4.24.4.1.11
ipCidrRouteMetric2	1.3.6.1.2.1.4.24.4.1.12
ipCidrRouteMetric3	1.3.6.1.2.1.4.24.4.1.13
ipCidrRouteMetric4	1.3.6.1.2.1.4.24.4.1.14
ipCidrRouteMetric5	1.3.6.1.2.1.4.24.4.1.15
ipCidrRouteStatus	1.3.6.1.2.1.4.24.4.1.16

### MIB objects in the VRRP-MIB.my file

The following table provides a list of the MIBs in the VRRP-MIB.my file that are supported by the Branch Gateway and their OIDs:

Object	OID
vrrpNodeVersion	1.3.6.1.2.1.68.1.1.1
vrrpOperVrld	1.3.6.1.2.1.68.1.1.3.1.1
vrrpOperVirtualMacAddr	1.3.6.1.2.1.68.1.1.3.1.2
vrrpOperState	1.3.6.1.2.1.68.1.1.3.1.3
vrrpOperAdminState	1.3.6.1.2.1.68.1.1.3.1.4
vrrpOperPriority	1.3.6.1.2.1.68.1.1.3.1.5
vrrpOperIpAddrCount	1.3.6.1.2.1.68.1.1.3.1.6
vrrpOperMasterIpAddr	1.3.6.1.2.1.68.1.1.3.1.7
vrrpOperPrimaryIpAddr	1.3.6.1.2.1.68.1.1.3.1.8
vrrpOperAuthType	1.3.6.1.2.1.68.1.1.3.1.9
vrrpOperAuthKey	1.3.6.1.2.1.68.1.1.3.1.10
vrrpOperAdvertisementInterval	1.3.6.1.2.1.68.1.1.3.1.11
vrrpOperPreemptMode	1.3.6.1.2.1.68.1.1.3.1.12
vrrpOperVirtualRouterUpTime	1.3.6.1.2.1.68.1.1.3.1.13
vrrpOperProtocol	1.3.6.1.2.1.68.1.1.3.1.14
vrrpOperRowStatus	1.3.6.1.2.1.68.1.1.3.1.15
vrrpAssoIpAddr	1.3.6.1.2.1.68.1.1.4.1.1
vrrpAssoIpAddrRowStatus	1.3.6.1.2.1.68.1.1.4.1.2

## MIB objects in the UTILIZATION-MANAGEMENT-MIB.my file

The following table provides a list of the MIBs in the UTILIZATION-MANAGEMENT-MIB.my file that are supported by Branch Gateway and their OIDs:

Object	OID
genCpuIndex	1.3.6.1.4.1.6889.2.1.11.1.1.1.1
genCpuUtilizationEnableMonitoring	1.3.6.1.4.1.6889.2.1.11.1.1.1.2
genCpuUtilizationEnableEventGeneration	1.3.6.1.4.1.6889.2.1.11.1.1.1.3
genCpuUtilizationHighThreshold	1.3.6.1.4.1.6889.2.1.11.1.1.1.4
genCpuAverageUtilization	1.3.6.1.4.1.6889.2.1.11.1.1.1.5
genCpuCurrentUtilization	1.3.6.1.4.1.6889.2.1.11.1.1.1.6
genCpuUtilizationHistorySampleIndex	1.3.6.1.4.1.6889.2.1.11.1.1.2.1.1
genCpuHistoryUtilization	1.3.6.1.4.1.6889.2.1.11.1.1.2.1.2
genMemUtilizationTotalRAM	1.3.6.1.4.1.6889.2.1.11.1.2.1
genMemUtilizationOperationalImage	1.3.6.1.4.1.6889.2.1.11.1.2.2
genMemUtilizationDynAllocMemUsed	1.3.6.1.4.1.6889.2.1.11.1.2.3.1
genMemUtilizationDynAllocMemMaxUsed	1.3.6.1.4.1.6889.2.1.11.1.2.3.2

Object	OID
genMemUtilizationDynAllocMemAvailable	1.3.6.1.4.1.6889.2.1.11.1.2.3.3
genMemUtilizationAllocationFailures	1.3.6.1.4.1.6889.2.1.11.1.2.4
genMemUtilizationID	1.3.6.1.4.1.6889.2.1.11.1.2.6.1.1
genMemUtilizationPhyRam	1.3.6.1.4.1.6889.2.1.11.1.2.6.1.2
genMemUtilizationPercentUsed	1.3.6.1.4.1.6889.2.1.11.1.2.6.1.3

## MIB objects in the ENTITY-SENSOR-MIB.my file

The following table provides a list of the MIBs in the ENTITY-SENSOR-MIB.my file that are supported by the Branch Gateway and their OIDs:

Object	OID
entPhySensorType	1.3.6.1.2.1.99.1.1.1.1
entPhySensorScale	1.3.6.1.2.1.99.1.1.1.2
entPhySensorPrecision	1.3.6.1.2.1.99.1.1.1.3
entPhySensorValue	1.3.6.1.2.1.99.1.1.1.4
entPhySensorOperStatus	1.3.6.1.2.1.99.1.1.1.5
entPhySensorUnitsDisplay	1.3.6.1.2.1.99.1.1.1.6
entPhySensorValueTimeStamp	1.3.6.1.2.1.99.1.1.1.7
entPhySensorValueUpdateRate	1.3.6.1.2.1.99.1.1.1.8

### MIB objects in the RSTP-MIB.my file

The following table provides a list of the MIBs in the RSTP-MIB.my file that are supported by the Branch Gateway and their OIDs:

Object	OID
dot1dStpVersion	1.3.6.1.2.1.17.2.16
dot1dStpTxHoldCount	1.3.6.1.2.1.17.2.17
dot1dStpPathCostDefault	1.3.6.1.2.1.17.2.18
dot1dStpPortProtocolMigration	1.3.6.1.2.1.17.2.19.1.1
dot1dStpPortAdminEdgePort	1.3.6.1.2.1.17.2.19.1.2
dot1dStpPortOperEdgePort	1.3.6.1.2.1.17.2.19.1.3
dot1dStpPortAdminPointToPoint	1.3.6.1.2.1.17.2.19.1.4
dot1dStpPortOperPointToPoint	1.3.6.1.2.1.17.2.19.1.5
dot1dStpPortAdminPathCost	1.3.6.1.2.1.17.2.19.1.6

## MIB objects in the APPLIC-MIB.my file

The following table provides a list of the MIBs in the APPLIC-MIB.my file that are supported by the Branch Gateway and their OIDs:

Object	OID
IseIntPortGroupId	1.3.6.1.4.1.81.19.1.2.1.1.1
IseIntPortId	1.3.6.1.4.1.81.19.1.2.1.1.2
IseIntPortCAMLastChange	1.3.6.1.4.1.81.19.1.2.1.1.39
IseIntPortMACAddGroupId	1.3.6.1.4.1.81.19.1.2.2.1.1.1
IseIntPortMACAddPortId	1.3.6.1.4.1.81.19.1.2.2.1.1.2
IseIntPortMACAddLAId	1.3.6.1.4.1.81.19.1.2.2.1.1.3
IseIntPortMACAddList	1.3.6.1.4.1.81.19.1.2.2.1.1.4

## MIB objects in the DS1-MIB.my file

The following table provides a list of the MIBs in the DS1-MIB.my file that are supported by Branch Gateway and their OIDs only for the MM340:

Object	OID
dsx1LineIndex	1.3.6.1.2.1.10.18.6.1.1
dsx1lfIndex	1.3.6.1.2.1.10.18.6.1.2
dsx1TimeElapsed	1.3.6.1.2.1.10.18.6.1.3
dsx1ValidIntervals	1.3.6.1.2.1.10.18.6.1.4
dsx1LineType	1.3.6.1.2.1.10.18.6.1.5
dsx1LineCoding	1.3.6.1.2.1.10.18.6.1.6
dsx1SendCode	1.3.6.1.2.1.10.18.6.1.7
dsx1CircuitIdentifier	1.3.6.1.2.1.10.18.6.1.8
dsx1LoopbackConfig	1.3.6.1.2.1.10.18.6.1.9
dsx1LineStatus	1.3.6.1.2.1.10.18.6.1.10
dsx1SignalMode	1.3.6.1.2.1.10.18.6.1.11
dsx1TransmitClockSource	1.3.6.1.2.1.10.18.6.1.12
dsx1Fdl	1.3.6.1.2.1.10.18.6.1.13
dsx1InvalidIntervals	1.3.6.1.2.1.10.18.6.1.14
dsx1LineLength	1.3.6.1.2.1.10.18.6.1.15
dsx1LineStatusLastChange	1.3.6.1.2.1.10.18.6.1.16
dsx1LineStatusChangeTrapEnable	1.3.6.1.2.1.10.18.6.1.17
dsx1LoopbackStatus	1.3.6.1.2.1.10.18.6.1.18
dsx1Ds1ChannelNumber	1.3.6.1.2.1.10.18.6.1.19
dsx1Channelization	1.3.6.1.2.1.10.18.6.1.20
dsx1CurrentIndex	1.3.6.1.2.1.10.18.7.1.1
dsx1CurrentESs	1.3.6.1.2.1.10.18.7.1.2
dsx1CurrentSESs	1.3.6.1.2.1.10.18.7.1.3

Object	OID
dsx1CurrentSEFSs	1.3.6.1.2.1.10.18.7.1.4
dsx1CurrentUASs	1.3.6.1.2.1.10.18.7.1.5
dsx1CurrentCSSs	1.3.6.1.2.1.10.18.7.1.6
dsx1CurrentPCVs	1.3.6.1.2.1.10.18.7.1.7
dsx1CurrentLESs	1.3.6.1.2.1.10.18.7.1.8
dsx1CurrentBESs	1.3.6.1.2.1.10.18.7.1.9
dsx1CurrentDMs	1.3.6.1.2.1.10.18.7.1.10
dsx1CurrentLCVs	1.3.6.1.2.1.10.18.7.1.11
dsx1IntervalIndex	1.3.6.1.2.1.10.18.8.1.1
dsx1IntervalNumber	1.3.6.1.2.1.10.18.8.1.2
dsx1IntervalESs	1.3.6.1.2.1.10.18.8.1.3
dsx1IntervalSESs	1.3.6.1.2.1.10.18.8.1.4
dsx1IntervalSEFSs	1.3.6.1.2.1.10.18.8.1.5
dsx1IntervalUASs	1.3.6.1.2.1.10.18.8.1.6
dsx1IntervalCSSs	1.3.6.1.2.1.10.18.8.1.7
dsx1IntervalPCVs	1.3.6.1.2.1.10.18.8.1.8
dsx1IntervalLESs	1.3.6.1.2.1.10.18.8.1.9
dsx1IntervalBESs	1.3.6.1.2.1.10.18.8.1.10
dsx1IntervalDMs	1.3.6.1.2.1.10.18.8.1.11
dsx1IntervalLCVs	1.3.6.1.2.1.10.18.8.1.12
dsx1IntervalValidData	1.3.6.1.2.1.10.18.8.1.13
dsx1TotalIndex	1.3.6.1.2.1.10.18.9.1.1
dsx1TotalESs	1.3.6.1.2.1.10.18.9.1.2
dsx1TotalSESs	1.3.6.1.2.1.10.18.9.1.3
dsx1TotalSEFSs	1.3.6.1.2.1.10.18.9.1.4
dsx1TotalUASs	1.3.6.1.2.1.10.18.9.1.5
dsx1TotalCSSs	1.3.6.1.2.1.10.18.9.1.6
dsx1TotalPCVs	1.3.6.1.2.1.10.18.9.1.7
dsx1TotalLESs	1.3.6.1.2.1.10.18.9.1.8
dsx1TotalBESs	1.3.6.1.2.1.10.18.9.1.9
dsx1TotalDMs	1.3.6.1.2.1.10.18.9.1.10
dsx1TotalLCVs	1.3.6.1.2.1.10.18.9.1.11

## MIB objects in the PPP-IP-NCP-MIB.my file

The following table provides a list of the MIBs in the PPP-IP-NCP-MIB.my file that are supported by Branch Gateway and their OIDs:

Object	OID
ppplpOperStatus	1.3.6.1.2.1.10.23.3.1.1.1
ppplpLocalToRemoteCompressionProtocol	1.3.6.1.2.1.10.23.3.1.1.2
pppIpRemoteToLocalCompressionProtocol	1.3.6.1.2.1.10.23.3.1.1.3
ppplpRemoteMaxSlotId	1.3.6.1.2.1.10.23.3.1.1.4
ppplpLocalMaxSlotId	1.3.6.1.2.1.10.23.3.1.1.5
ppplpConfigAdminStatus	1.3.6.1.2.1.10.23.3.2.1.1
ppplpConfigCompression	1.3.6.1.2.1.10.23.3.2.1.2

## MIB objects in the RFC1213-MIB.my file

The following table provides a list of the MIBs in the RFC1213-MIB.my file that are supported by the Branch Gateway and their OIDs:

Object	OID
sysDescr	1.3.6.1.2.1.1.1
sysObjectID	1.3.6.1.2.1.1.2
sysUpTime	1.3.6.1.2.1.1.3
sysContact	1.3.6.1.2.1.1.4
sysName	1.3.6.1.2.1.1.5
sysLocation	1.3.6.1.2.1.1.6
sysServices	1.3.6.1.2.1.1.7
ifNumber	1.3.6.1.2.1.2.1
ifIndex	1.3.6.1.2.1.2.2.1.1
ifDescr	1.3.6.1.2.1.2.2.1.2
ifТуре	1.3.6.1.2.1.2.2.1.3
ifMtu	1.3.6.1.2.1.2.2.1.4
ifSpeed	1.3.6.1.2.1.2.2.1.5
ifPhysAddress	1.3.6.1.2.1.2.2.1.6
ifAdminStatus	1.3.6.1.2.1.2.2.1.7
ifOperStatus	1.3.6.1.2.1.2.2.1.8
ifLastChange	1.3.6.1.2.1.2.2.1.9
ifInOctets	1.3.6.1.2.1.2.2.1.10
ifInUcastPkts	1.3.6.1.2.1.2.2.1.11
ifInNUcastPkts	1.3.6.1.2.1.2.2.1.12
ifInDiscards	1.3.6.1.2.1.2.2.1.13
ifInErrors	1.3.6.1.2.1.2.2.1.14
iflnUnknownProtos	1.3.6.1.2.1.2.2.1.15

Object	OID
ifOutOctets	1.3.6.1.2.1.2.2.1.16
ifOutUcastPkts	1.3.6.1.2.1.2.2.1.17
ifOutNUcastPkts	1.3.6.1.2.1.2.2.1.18
ifOutDiscards	1.3.6.1.2.1.2.2.1.19
ifOutErrors	1.3.6.1.2.1.2.2.1.20
ifOutQLen	1.3.6.1.2.1.2.2.1.21
ifSpecific	1.3.6.1.2.1.2.2.1.22
ipForwarding	1.3.6.1.2.1.4.1
ipDefaultTTL	1.3.6.1.2.1.4.2
ipInReceives	1.3.6.1.2.1.4.3
ipInHdrErrors	1.3.6.1.2.1.4.4
ipInAddrErrors	1.3.6.1.2.1.4.5
ipForwDatagrams	1.3.6.1.2.1.4.6
ipInUnknownProtos	1.3.6.1.2.1.4.7
ipInDiscards	1.3.6.1.2.1.4.8
ipInDelivers	1.3.6.1.2.1.4.9
ipOutRequests	1.3.6.1.2.1.4.10
ipOutDiscards	1.3.6.1.2.1.4.11
ipOutNoRoutes	1.3.6.1.2.1.4.12
ipReasmTimeout	1.3.6.1.2.1.4.13
ipReasmReqds	1.3.6.1.2.1.4.14
ipReasmOKs	1.3.6.1.2.1.4.15
ipReasmFails	1.3.6.1.2.1.4.16
ipFragOKs	1.3.6.1.2.1.4.17
ipFragFails	1.3.6.1.2.1.4.18
ipFragCreates	1.3.6.1.2.1.4.19
ipAdEntAddr	1.3.6.1.2.1.4.20.1.1
ipAdEntIfIndex	1.3.6.1.2.1.4.20.1.2
ipAdEntNetMask	1.3.6.1.2.1.4.20.1.3
ipAdEntBcastAddr	1.3.6.1.2.1.4.20.1.4
ipAdEntReasmMaxSize	1.3.6.1.2.1.4.20.1.5
ipRouteDest	1.3.6.1.2.1.4.21.1.1
ipRoutelfIndex	1.3.6.1.2.1.4.21.1.2
ipRouteMetric1	1.3.6.1.2.1.4.21.1.3
ipRouteMetric2	1.3.6.1.2.1.4.21.1.4

Object	OID
ipRouteMetric3	1.3.6.1.2.1.4.21.1.5
ipRouteMetric4	1.3.6.1.2.1.4.21.1.6
ipRouteNextHop	1.3.6.1.2.1.4.21.1.7
ipRouteType	1.3.6.1.2.1.4.21.1.8
ipRouteProto	1.3.6.1.2.1.4.21.1.9
ipRouteAge	1.3.6.1.2.1.4.21.1.10
ipRouteMask	1.3.6.1.2.1.4.21.1.11
ipRouteMetric5	1.3.6.1.2.1.4.21.1.12
ipRouteInfo	1.3.6.1.2.1.4.21.1.13
ipNetToMedialfIndex	1.3.6.1.2.1.4.22.1.1
ipNetToMediaPhysAddress	1.3.6.1.2.1.4.22.1.2
ipNetToMediaNetAddress	1.3.6.1.2.1.4.22.1.3
ipNetToMediaType	1.3.6.1.2.1.4.22.1.4
ipRoutingDiscards	1.3.6.1.2.1.4.23
snmpInPkts	1.3.6.1.2.1.11.1
snmpOutPkts	1.3.6.1.2.1.11.2
snmpInBadVersions	1.3.6.1.2.1.11.3
snmpInBadCommunityNames	1.3.6.1.2.1.11.4
snmpInBadCommunityUses	1.3.6.1.2.1.11.5
snmpInASNParseErrs	1.3.6.1.2.1.11.6
snmpInTooBigs	1.3.6.1.2.1.11.8
snmpInNoSuchNames	1.3.6.1.2.1.11.9
snmpInBadValues	1.3.6.1.2.1.11.10
snmpInReadOnlys	1.3.6.1.2.1.11.11
snmpInGenErrs	1.3.6.1.2.1.11.12
snmpInTotalReqVars	1.3.6.1.2.1.11.13
snmpInTotalSetVars	1.3.6.1.2.1.11.14
snmpInGetRequests	1.3.6.1.2.1.11.15
snmpInGetNexts	1.3.6.1.2.1.11.16
snmpInSetRequests	1.3.6.1.2.1.11.17
snmpInGetResponses	1.3.6.1.2.1.11.18
snmpInTraps	1.3.6.1.2.1.11.19
snmpOutTooBigs	1.3.6.1.2.1.11.20
snmpOutNoSuchNames	1.3.6.1.2.1.11.21
snmpOutBadValues	1.3.6.1.2.1.11.22

Object	OID
snmpOutGenErrs	1.3.6.1.2.1.11.24
snmpOutGetRequests	1.3.6.1.2.1.11.25
snmpOutGetNexts	1.3.6.1.2.1.11.26
snmpOutSetRequests	1.3.6.1.2.1.11.27
snmpOutGetResponses	1.3.6.1.2.1.11.28
snmpOutTraps	1.3.6.1.2.1.11.29
snmpEnableAuthenTraps	1.3.6.1.2.1.11.30

### MIB objects in the AVAYA-ENTITY-MIB.my file

The following table provides a list of the MIBs in the AVAYA-ENTITY-MIB.my file that are supported by the Branch Gateway and their OIDs:

Object	OID
avEntPhySensorHiShutdown	1.3.6.1.4.1.6889.2.1.99.1.1.1
avEntPhySensorHiWarning	1.3.6.1.4.1.6889.2.1.99.1.1.2
avEntPhySensorHiWarningClear	1.3.6.1.4.1.6889.2.1.99.1.1.3
avEntPhySensorLoWarningClear	1.3.6.1.4.1.6889.2.1.99.1.1.4
avEntPhySensorLoWarning	1.3.6.1.4.1.6889.2.1.99.1.1.5
avEntPhySensorLoShutdown	1.3.6.1.4.1.6889.2.1.99.1.1.6
avEntPhySensorEventSupportMask	1.3.6.1.4.1.6889.2.1.99.1.1.7

### MIB objects in the Rnd-MIB.my file

The following table provides a list of the MIBs in the Rnd.MIB file that are supported by the Branch Gateway and their OIDs:

Object	OID
genGroupHWVersion	1.3.6.1.4.1.81.8.1.1.24
genGroupConfigurationSymbol	1.3.6.1.4.1.81.8.1.1.21
genGroupHWStatus	1.3.6.1.4.1.81.8.1.1.17

### MIB objects in the XSWITCH-MIB.my file

The following table provides a list of the MIBs in the XSWITCH-MIB.my file that are supported by the Branch Gateway and their OIDs:

Object	OID
scGenPortGroupId	1.3.6.1.4.1.81.28.1.4.1.1.1
scGenPortId	1.3.6.1.4.1.81.28.1.4.1.1.2
scGenPortVLAN	1.3.6.1.4.1.81.28.1.4.1.1.3

Object	OID
scGenPortPriority	1.3.6.1.4.1.81.28.1.4.1.1.4
scGenPortSetDefaults	1.3.6.1.4.1.81.28.1.4.1.1.5
scGenPortLinkAggregationNumber	1.3.6.1.4.1.81.28.1.4.1.1.9
scGenPortGenericTrap	1.3.6.1.4.1.81.28.1.4.1.1.15
scGenPortLagCapability	1.3.6.1.4.1.81.28.1.4.1.1.20
scGenPortCapability	1.3.6.1.4.1.81.28.1.4.1.1.21
scGenSwitchId	1.3.6.1.4.1.81.28.1.5.1.1.1
scGenSwitchSTA	1.3.6.1.4.1.81.28.1.5.1.1.13
scEthPortGroupId	1.3.6.1.4.1.81.28.2.1.1.1.1
scEthPortId	1.3.6.1.4.1.81.28.2.1.1.1.2
scEthPortFunctionalStatus	1.3.6.1.4.1.81.28.2.1.1.1.27
scEthPortMode	1.3.6.1.4.1.81.28.2.1.1.1.28
scEthPortSpeed	1.3.6.1.4.1.81.28.2.1.1.1.29
scEthPortAutoNegotiation	1.3.6.1.4.1.81.28.2.1.1.1.30
scEthPortAutoNegotiationStatus	1.3.6.1.4.1.81.28.2.1.1.1.31
scEthPortPauseCapabilities	1.3.6.1.4.1.81.28.2.1.1.1.44
scEthPortFlowControl	1.3.6.1.4.1.81.28.2.1.1.1.47

## MIB objects in the CROUTE-MIB.my file

The following table provides a list of the MIBs in the CROUTE-MIB.my file that are supported by Branch Gateway and their OIDs:

Object	OID
ipGlobalsBOOTPRelayStatus	1.3.6.1.4.1.81.31.1.1.1
ipGlobalsICMPErrMsgEnable	1.3.6.1.4.1.81.31.1.1.2
ipGlobalsARPInactiveTimeout	1.3.6.1.4.1.81.31.1.1.3
ipGlobalsPrimaryManagementIPAddress	1.3.6.1.4.1.81.31.1.1.4
ipGlobalsNextPrimaryManagementIPAddress	1.3.6.1.4.1.81.31.1.1.5
ipInterfaceAddr	1.3.6.1.4.1.81.31.1.2.1.1
ipInterfaceNetMask	1.3.6.1.4.1.81.31.1.2.1.2
ipInterfaceLowerIfAlias	1.3.6.1.4.1.81.31.1.2.1.3
ipInterfaceType	1.3.6.1.4.1.81.31.1.2.1.4
ipInterfaceForwardIpBroadcast	1.3.6.1.4.1.81.31.1.2.1.5
ipInterfaceBroadcastAddr	1.3.6.1.4.1.81.31.1.2.1.6
ipInterfaceProxyArp	1.3.6.1.4.1.81.31.1.2.1.7
ipInterfaceStatus	1.3.6.1.4.1.81.31.1.2.1.8

Object	OID
ipInterfaceMainRouterAddr	1.3.6.1.4.1.81.31.1.2.1.9
ipInterfaceARPServerStatus	1.3.6.1.4.1.81.31.1.2.1.10
ipInterfaceName	1.3.6.1.4.1.81.31.1.2.1.11
ipInterfaceNetbiosRebroadcast	1.3.6.1.4.1.81.31.1.2.1.12
ipInterfaceIcmpRedirects	1.3.6.1.4.1.81.31.1.2.1.13
ipInterfaceOperStatus	1.3.6.1.4.1.81.31.1.2.1.14
ipInterfaceDhcpRelay	1.3.6.1.4.1.81.31.1.2.1.15
ripGlobalsRIPEnable	1.3.6.1.4.1.81.31.1.3.1
ripGlobalsLeakOSPFIntoRIP	1.3.6.1.4.1.81.31.1.3.2
ripGlobalsLeakStaticIntoRIP	1.3.6.1.4.1.81.31.1.3.3
ripGlobalsPeriodicUpdateTimer	1.3.6.1.4.1.81.31.1.3.4
ripGlobalsPeriodicInvalidRouteTimer	1.3.6.1.4.1.81.31.1.3.5
ripGlobalsDefaultExportMetric	1.3.6.1.4.1.81.31.1.3.6
ripInterfaceAddr	1.3.6.1.4.1.81.31.1.4.1.1
ripInterfaceMetric	1.3.6.1.4.1.81.31.1.4.1.2
ripInterfaceSplitHorizon	1.3.6.1.4.1.81.31.1.4.1.3
ripInterfaceAcceptDefaultRoute	1.3.6.1.4.1.81.31.1.4.1.4
ripInterfaceSendDefaultRoute	1.3.6.1.4.1.81.31.1.4.1.5
ripInterfaceState	1.3.6.1.4.1.81.31.1.4.1.6
ripInterfaceSendMode	1.3.6.1.4.1.81.31.1.4.1.7
ripInterfaceVersion	1.3.6.1.4.1.81.31.1.4.1.8
ospfGlobalsLeakRIPIntoOSPF	1.3.6.1.4.1.81.31.1.5.1
ospfGlobalsLeakStaticIntoOSPF	1.3.6.1.4.1.81.31.1.5.2
ospfGlobalsLeakDirectIntoOSPF	1.3.6.1.4.1.81.31.1.5.3
ospfGlobalsDefaultExportMetric	1.3.6.1.4.1.81.31.1.5.4
relayVIIndex	1.3.6.1.4.1.81.31.1.6.1.1
relayVIPrimaryServerAddr	1.3.6.1.4.1.81.31.1.6.1.2
relayVISeconderyServerAddr	1.3.6.1.4.1.81.31.1.6.1.3
relayVIStatus	1.3.6.1.4.1.81.31.1.6.1.4
relayVIRelayAddr	1.3.6.1.4.1.81.31.1.6.1.5
ipRedundancyStatus	1.3.6.1.4.1.81.31.1.9.1
ipRedundancyTimeout	1.3.6.1.4.1.81.31.1.9.2
ipRedundancyPollingInterval	1.3.6.1.4.1.81.31.1.9.3
ipShortcutARPServerStatus	1.3.6.1.4.1.81.31.1.10.1
distributionListRoutingProtocol	1.3.6.1.4.1.81.31.1.12.1.1

Object	OID
distributionListDirection	1.3.6.1.4.1.81.31.1.12.1.2
distributionListIfIndex	1.3.6.1.4.1.81.31.1.12.1.3
distributionListRouteProtocol	1.3.6.1.4.1.81.31.1.12.1.4
distributionListProtocolSpecific1	1.3.6.1.4.1.81.31.1.12.1.5
distributionListProtocolSpecific2	1.3.6.1.4.1.81.31.1.12.1.6
distributionListProtocolSpecific3	1.3.6.1.4.1.81.31.1.12.1.7
distributionListProtocolSpecific4	1.3.6.1.4.1.81.31.1.12.1.8
distributionListProtocolSpecific5	1.3.6.1.4.1.81.31.1.12.1.9
distributionListAccessListNumber	1.3.6.1.4.1.81.31.1.12.1.10
distributionListEntryStatus	1.3.6.1.4.1.81.31.1.12.1.11
ipVRRPAdminStatus	1.3.6.1.4.1.81.31.1.14.1
iphclfIndex	1.3.6.1.4.1.81.31.1.15.1.1.1
iphcControlTcpAdminStatus	1.3.6.1.4.1.81.31.1.15.1.1.2
iphcTcpSessions	1.3.6.1.4.1.81.31.1.15.1.1.3
iphcNegotiatedTcpSessions	1.3.6.1.4.1.81.31.1.15.1.1.4
iphcControlRtpAdminStatus	1.3.6.1.4.1.81.31.1.15.1.1.5
iphcRtpSessions	1.3.6.1.4.1.81.31.1.15.1.1.6
iphcNegotiatedRtpSessions	1.3.6.1.4.1.81.31.1.15.1.1.7
iphcControlNonTcpAdminStatus	1.3.6.1.4.1.81.31.1.15.1.1.8
iphcNonTcpSessions	1.3.6.1.4.1.81.31.1.15.1.1.9
iphcNegotiatedNonTcpSessions	1.3.6.1.4.1.81.31.1.15.1.1.10
iphcMaxPeriod	1.3.6.1.4.1.81.31.1.15.1.1.11
iphcMaxTime	1.3.6.1.4.1.81.31.1.15.1.1.12
iphcControRtpMinPortNumber	1.3.6.1.4.1.81.31.1.15.1.1.13
iphcControRtpMaxPortNumber	1.3.6.1.4.1.81.31.1.15.1.1.14
iphcControlRtpCompressionRatio	1.3.6.1.4.1.81.31.1.15.1.1.15
iphcControlNonTcpMode	1.3.6.1.4.1.81.31.1.15.1.1.16
ospfXtndIflpAddress	1.3.6.1.4.1.81.31.1.16.1.1
ospfXtndIfAddressLessIf	1.3.6.1.4.1.81.31.1.16.1.2
ospfXtndIfPassiveMode	1.3.6.1.4.1.81.31.1.16.1.3
vlConfIndex	1.3.6.1.4.1.81.31.3.1.1.1
vlConfAlias	1.3.6.1.4.1.81.31.3.1.1.2
vlConfStatus	1.3.6.1.4.1.81.31.3.1.1.3

## MIB objects in the RS-232-MIB.my file

The following table provides a list of the MIBs in the RS-232-MIB.my file that are supported by the Branch Gateway and their OIDs:

Object	OID
rs232Number	1.3.6.1.2.1.10.33.1
rs232PortIndex	1.3.6.1.2.1.10.33.2.1.1
rs232PortType	1.3.6.1.2.1.10.33.2.1.2
rs232PortInSigNumber	1.3.6.1.2.1.10.33.2.1.3
rs232PortOutSigNumber	1.3.6.1.2.1.10.33.2.1.4
rs232PortInSpeed	1.3.6.1.2.1.10.33.2.1.5
rs232PortOutSpeed	1.3.6.1.2.1.10.33.2.1.6
rs232PortInFlowType	1.3.6.1.2.1.10.33.2.1.7
rs232PortOutFlowType	1.3.6.1.2.1.10.33.2.1.8
rs232SyncPortIndex	1.3.6.1.2.1.10.33.4.1.1
rs232SyncPortClockSource	1.3.6.1.2.1.10.33.4.1.2
rs232SyncPortFrameCheckErrs	1.3.6.1.2.1.10.33.4.1.3
rs232SyncPortTransmitUnderrunErrs	1.3.6.1.2.1.10.33.4.1.4
rs232SyncPortReceiveOverrunErrs	1.3.6.1.2.1.10.33.4.1.5
rs232SyncPortInterruptedFrames	1.3.6.1.2.1.10.33.4.1.6
rs232SyncPortAbortedFrames	1.3.6.1.2.1.10.33.4.1.7
rs232SyncPortRole	1.3.6.1.2.1.10.33.4.1.8
rs232SyncPortEncoding	1.3.6.1.2.1.10.33.4.1.9
rs232SyncPortRTSControl	1.3.6.1.2.1.10.33.4.1.10
rs232SyncPortRTSCTSDelay	1.3.6.1.2.1.10.33.4.1.11
rs232SyncPortMode	1.3.6.1.2.1.10.33.4.1.12
rs232SyncPortIdlePattern	1.3.6.1.2.1.10.33.4.1.13
rs232SyncPortMinFlags	1.3.6.1.2.1.10.33.4.1.14
rs232InSigPortIndex	1.3.6.1.2.1.10.33.5.1.1
rs232InSigName	1.3.6.1.2.1.10.33.5.1.2
rs232InSigState	1.3.6.1.2.1.10.33.5.1.3
rs232InSigChanges	1.3.6.1.2.1.10.33.5.1.4
rs232OutSigPortIndex	1.3.6.1.2.1.10.33.6.1.1
rs232OutSigName	1.3.6.1.2.1.10.33.6.1.2
rs232OutSigState	1.3.6.1.2.1.10.33.6.1.3
rs232OutSigChanges	1.3.6.1.2.1.10.33.6.1.4

## MIB objects in the RIPv2-MIB.my file

The following table provides a list of the MIBs in the RIPv2-MIB.my file that are supported by the Branch Gateway and their OIDs:

Object	OID
rip2GlobalRouteChanges	1.3.6.1.2.1.23.1.1
rip2GlobalQueries	1.3.6.1.2.1.23.1.2
rip2lfStatAddress	1.3.6.1.2.1.23.2.1.1
rip2lfStatRcvBadPackets	1.3.6.1.2.1.23.2.1.2
rip2lfStatRcvBadRoutes	1.3.6.1.2.1.23.2.1.3
rip2lfStatSentUpdates	1.3.6.1.2.1.23.2.1.4
rip2lfStatStatus	1.3.6.1.2.1.23.2.1.5
rip2lfConfAddress	1.3.6.1.2.1.23.3.1.1
rip2lfConfDomain	1.3.6.1.2.1.23.3.1.2
rip2IfConfAuthType	1.3.6.1.2.1.23.3.1.3
rip2lfConfAuthKey	1.3.6.1.2.1.23.3.1.4
rip2lfConfSend	1.3.6.1.2.1.23.3.1.5
rip2lfConfReceive	1.3.6.1.2.1.23.3.1.6
rip2lfConfDefaultMetric	1.3.6.1.2.1.23.3.1.7
rip2lfConfStatus	1.3.6.1.2.1.23.3.1.8
rip2lfConfSrcAddress	1.3.6.1.2.1.23.3.1.9

## MIB objects in the IF-MIB.my file

The following table provides a list of the MIBs in the IF-MIB.my file that are supported by the Branch Gateway and their OIDs:

Object	OID
ifNumber	1.3.6.1.2.1.2.1
ifIndex	1.3.6.1.2.1.2.2.1.1
ifDescr	1.3.6.1.2.1.2.2.1.2
ifType	1.3.6.1.2.1.2.2.1.3
ifMtu	1.3.6.1.2.1.2.2.1.4
ifSpeed	1.3.6.1.2.1.2.2.1.5
ifPhysAddress	1.3.6.1.2.1.2.2.1.6
ifAdminStatus	1.3.6.1.2.1.2.2.1.7
ifOperStatus	1.3.6.1.2.1.2.2.1.8
ifLastChange	1.3.6.1.2.1.2.2.1.9

Object	OID
ifInOctets	1.3.6.1.2.1.2.2.1.10
ifInUcastPkts	1.3.6.1.2.1.2.2.1.11
ifInNUcastPkts	1.3.6.1.2.1.2.2.1.12
ifInDiscards	1.3.6.1.2.1.2.2.1.13
ifInErrors	1.3.6.1.2.1.2.2.1.14
iflnUnknownProtos	1.3.6.1.2.1.2.2.1.15
ifOutOctets	1.3.6.1.2.1.2.2.1.16
ifOutUcastPkts	1.3.6.1.2.1.2.2.1.17
ifOutNUcastPkts	1.3.6.1.2.1.2.2.1.18
ifOutDiscards	1.3.6.1.2.1.2.2.1.19
ifOutErrors	1.3.6.1.2.1.2.2.1.20
ifOutQLen	1.3.6.1.2.1.2.2.1.21
ifSpecific	1.3.6.1.2.1.2.2.1.22
ifName	1.3.6.1.2.1.31.1.1.1
ifInMulticastPkts	1.3.6.1.2.1.31.1.1.1.2
ifInBroadcastPkts	1.3.6.1.2.1.31.1.1.3
ifOutMulticastPkts	1.3.6.1.2.1.31.1.1.4
ifOutBroadcastPkts	1.3.6.1.2.1.31.1.1.5
ifHCInOctets	1.3.6.1.2.1.31.1.1.6
ifHCInUcastPkts	1.3.6.1.2.1.31.1.1.7
ifHCInMulticastPkts	1.3.6.1.2.1.31.1.1.1.8
ifHCInBroadcastPkts	1.3.6.1.2.1.31.1.1.1.9
ifHCOutOctets	1.3.6.1.2.1.31.1.1.10
ifHCOutUcastPkts	1.3.6.1.2.1.31.1.1.11
ifHCOutMulticastPkts	1.3.6.1.2.1.31.1.1.1.12
ifHCOutBroadcastPkts	1.3.6.1.2.1.31.1.1.13
ifLinkUpDownTrapEnable	1.3.6.1.2.1.31.1.1.14
ifHighSpeed	1.3.6.1.2.1.31.1.1.15
ifPromiscuousMode	1.3.6.1.2.1.31.1.1.16
ifConnectorPresent	1.3.6.1.2.1.31.1.1.17
ifAlias	1.3.6.1.2.1.31.1.1.1.18
ifCounterDiscontinuityTime	1.3.6.1.2.1.31.1.1.1.19

## MIB objects in the DS0BUNDLE-MIB.my file

The following table provides a list of the MIBs in the DS0BUNDLE-MIB.my file that are supported by Branch Gateway and their OIDs only for the MM340:

Object	OID
dsx0BundleIndex	1.3.6.1.2.1.10.82.3.1.1
dsx0BundlelfIndex	1.3.6.1.2.1.10.82.3.1.2
dsx0BundleCircuitIdentifier	1.3.6.1.2.1.10.82.3.1.3
dsx0BundleRowStatus	1.3.6.1.2.1.10.82.3.1.4

## MIB objects in the RFC1406-MIB.my file

The following table provides a list of the MIBs in the RFC1406-MIB.my file that are supported by Branch Gateway and their OIDs only for the MM340:

Object	OID
dsx1LineIndex	1.3.6.1.2.1.10.18.6.1.1
dsx1lfIndex	1.3.6.1.2.1.10.18.6.1.2
dsx1TimeElapsed	1.3.6.1.2.1.10.18.6.1.3
dsx1ValidIntervals	1.3.6.1.2.1.10.18.6.1.4
dsx1LineType	1.3.6.1.2.1.10.18.6.1.5
dsx1LineCoding	1.3.6.1.2.1.10.18.6.1.6
dsx1SendCode	1.3.6.1.2.1.10.18.6.1.7
dsx1CircuitIdentifier	1.3.6.1.2.1.10.18.6.1.8
dsx1LoopbackConfig	1.3.6.1.2.1.10.18.6.1.9
dsx1LineStatus	1.3.6.1.2.1.10.18.6.1.10
dsx1SignalMode	1.3.6.1.2.1.10.18.6.1.11
dsx1TransmitClockSource	1.3.6.1.2.1.10.18.6.1.12
dsx1Fdl	1.3.6.1.2.1.10.18.6.1.13
dsx1CurrentIndex	1.3.6.1.2.1.10.18.7.1.1
dsx1CurrentESs	1.3.6.1.2.1.10.18.7.1.2
dsx1CurrentSESs	1.3.6.1.2.1.10.18.7.1.3
dsx1CurrentSEFSs	1.3.6.1.2.1.10.18.7.1.4
dsx1CurrentUASs	1.3.6.1.2.1.10.18.7.1.5
dsx1CurrentCSSs	1.3.6.1.2.1.10.18.7.1.6
dsx1CurrentPCVs	1.3.6.1.2.1.10.18.7.1.7
dsx1CurrentLESs	1.3.6.1.2.1.10.18.7.1.8
dsx1CurrentBESs	1.3.6.1.2.1.10.18.7.1.9
dsx1CurrentDMs	1.3.6.1.2.1.10.18.7.1.10
dsx1CurrentLCVs	1.3.6.1.2.1.10.18.7.1.11
dsx1IntervalIndex	1.3.6.1.2.1.10.18.8.1.1
dsx1IntervalNumber	1.3.6.1.2.1.10.18.8.1.2

Object	OID
dsx1IntervalESs	1.3.6.1.2.1.10.18.8.1.3
dsx1IntervalSESs	1.3.6.1.2.1.10.18.8.1.4
dsx1IntervalSEFSs	1.3.6.1.2.1.10.18.8.1.5
dsx1IntervalUASs	1.3.6.1.2.1.10.18.8.1.6
dsx1IntervalCSSs	1.3.6.1.2.1.10.18.8.1.7
dsx1IntervalPCVs	1.3.6.1.2.1.10.18.8.1.8
dsx1IntervalLESs	1.3.6.1.2.1.10.18.8.1.9
dsx1IntervalBESs	1.3.6.1.2.1.10.18.8.1.10
dsx1IntervalDMs	1.3.6.1.2.1.10.18.8.1.11
dsx1IntervalLCVs	1.3.6.1.2.1.10.18.8.1.12
dsx1TotalIndex	1.3.6.1.2.1.10.18.9.1.1
dsx1TotalESs	1.3.6.1.2.1.10.18.9.1.2
dsx1TotalSESs	1.3.6.1.2.1.10.18.9.1.3
dsx1TotalSEFSs	1.3.6.1.2.1.10.18.9.1.4
dsx1TotalUASs	1.3.6.1.2.1.10.18.9.1.5
dsx1TotalCSSs	1.3.6.1.2.1.10.18.9.1.6
dsx1TotalPCVs	1.3.6.1.2.1.10.18.9.1.7
dsx1TotalLESs	1.3.6.1.2.1.10.18.9.1.8
dsx1TotalBESs	1.3.6.1.2.1.10.18.9.1.9
dsx1TotalDMs	1.3.6.1.2.1.10.18.9.1.10
dsx1TotalLCVs	1.3.6.1.2.1.10.18.9.1.11

## MIB objects in the DS0-MIB.my file

The following table provides a list of the MIBs in the DS0-MIB.my file that are supported by the Branch Gateway and their OIDs:

Object	OID
dsx0Ds0ChannelNumber	1.3.6.1.2.1.10.81.1.1.1
dsx0RobbedBitSignalling	1.3.6.1.2.1.10.81.1.1.2
dsx0CircuitIdentifier	1.3.6.1.2.1.10.81.1.1.3
dsx0ldleCode	1.3.6.1.2.1.10.81.1.1.4
dsx0SeizedCode	1.3.6.1.2.1.10.81.1.1.5
dsx0ReceivedCode	1.3.6.1.2.1.10.81.1.1.6
dsx0TransmitCodesEnable	1.3.6.1.2.1.10.81.1.1.7
dsx0Ds0BundleMappedIfIndex	1.3.6.1.2.1.10.81.1.1.8
dsx0ChanMappedIfIndex	1.3.6.1.2.1.10.81.3.1.1

## MIB objects in the POLICY-MIB.my file

The following table provides a list of the MIBs in the POLICY-MIB.MY file that are supported by Branch Gateway and their OIDs:

Object	OID
ipPolicyListSlot	1.3.6.1.4.1.81.36.1.1.1
ipPolicyListID	1.3.6.1.4.1.81.36.1.1.2
ipPolicyListName	1.3.6.1.4.1.81.36.1.1.3
ipPolicyListValidityStatus	1.3.6.1.4.1.81.36.1.1.4
ipPolicyListChecksum	1.3.6.1.4.1.81.36.1.1.5
ipPolicyListRowStatus	1.3.6.1.4.1.81.36.1.1.6
ipPolicyListDefaultOperation	1.3.6.1.4.1.81.36.1.1.7
ipPolicyListCookie	1.3.6.1.4.1.81.36.1.1.8
ipPolicyListTrackChanges	1.3.6.1.4.1.81.36.1.1.9
ipPolicyListOwner	1.3.6.1.4.1.81.36.1.1.10
ipPolicyListErrMsg	1.3.6.1.4.1.81.36.1.1.11
ipPolicyListTrustedFields	1.3.6.1.4.1.81.36.1.1.12
ipPolicyListScope	1.3.6.1.4.1.81.36.1.1.13
ipPolicyListIpOptionOperation	1.3.6.1.4.1.81.36.1.1.14
ipPolicyListIpFragmentationOperation	1.3.6.1.4.1.81.36.1.1.15
ipPolicyListType	1.3.6.1.4.1.81.36.1.1.16
ipPolicyListEtherTypeDefaultOperation	1.3.6.1.4.1.81.36.1.1.17
ipPolicyRuleSlot	1.3.6.1.4.1.81.36.2.1.1
ipPolicyRuleListID	1.3.6.1.4.1.81.36.2.1.2
ipPolicyRuleID	1.3.6.1.4.1.81.36.2.1.3
ipPolicyRuleSrcAddr	1.3.6.1.4.1.81.36.2.1.4
ipPolicyRuleSrcAddrWild	1.3.6.1.4.1.81.36.2.1.5
ipPolicyRuleDstAddr	1.3.6.1.4.1.81.36.2.1.6
ipPolicyRuleDstAddrWild	1.3.6.1.4.1.81.36.2.1.7
ipPolicyRuleProtocol	1.3.6.1.4.1.81.36.2.1.8
ipPolicyRuleL4SrcPortMin	1.3.6.1.4.1.81.36.2.1.9
ipPolicyRuleL4SrcPortMax	1.3.6.1.4.1.81.36.2.1.10
ipPolicyRuleL4DestPortMin	1.3.6.1.4.1.81.36.2.1.11
ipPolicyRuleL4DestPortMax	1.3.6.1.4.1.81.36.2.1.12
ipPolicyRuleEstablished	1.3.6.1.4.1.81.36.2.1.13
ipPolicyRuleOperation	1.3.6.1.4.1.81.36.2.1.14
ipPolicyRuleApplicabilityPrecedence	1.3.6.1.4.1.81.36.2.1.15

Object	OID
ipPolicyRuleApplicabilityStatus	1.3.6.1.4.1.81.36.2.1.16
ipPolicyRuleApplicabilityType	1.3.6.1.4.1.81.36.2.1.17
ipPolicyRuleErrMsg	1.3.6.1.4.1.81.36.2.1.18
ipPolicyRuleStatus	1.3.6.1.4.1.81.36.2.1.19
ipPolicyRuleDSCPOperation	1.3.6.1.4.1.81.36.2.1.20
ipPolicyRuleDSCPFilter	1.3.6.1.4.1.81.36.2.1.21
ipPolicyRuleDSCPFilterWild	1.3.6.1.4.1.81.36.2.1.22
ipPolicyRuleIcmpTypeCode	1.3.6.1.4.1.81.36.2.1.23
ipPolicyRuleSrcAddrNot	1.3.6.1.4.1.81.36.2.1.24
ipPolicyRuleDstAddrNot	1.3.6.1.4.1.81.36.2.1.25
ipPolicyRuleProtocolNot	1.3.6.1.4.1.81.36.2.1.26
ipPolicyRuleL4SrcPortNot	1.3.6.1.4.1.81.36.2.1.27
ipPolicyRuleL4DestPortNot	1.3.6.1.4.1.81.36.2.1.28
ipPolicyRuleIcmpTypeCodeNot	1.3.6.1.4.1.81.36.2.1.29
ipPolicyRuleSrcPolicyUserGroupName	1.3.6.1.4.1.81.36.2.1.30
ipPolicyRuleDstPolicyUserGroupName	1.3.6.1.4.1.81.36.2.1.31
ipPolicyControlSlot	1.3.6.1.4.1.81.36.3.1.1
ipPolicyControlActiveGeneralList	1.3.6.1.4.1.81.36.3.1.2
ipPolicyControlAllowedPolicyManagers	1.3.6.1.4.1.81.36.3.1.3
ipPolicyControlCurrentChecksum	1.3.6.1.4.1.81.36.3.1.4
ipPolicyControlMinimalPolicyManagmentVersion	1.3.6.1.4.1.81.36.3.1.5
ipPolicyControlMaximalPolicyManagmentVersion	1.3.6.1.4.1.81.36.3.1.6
ipPolicyControlMIBversion	1.3.6.1.4.1.81.36.3.1.7
ipPolicyDiffServSlot	1.3.6.1.4.1.81.36.4.1.1
ipPolicyDiffServDSCP	1.3.6.1.4.1.81.36.4.1.2
ipPolicyDiffServOperation	1.3.6.1.4.1.81.36.4.1.3
ipPolicyDiffServName	1.3.6.1.4.1.81.36.4.1.4
ipPolicyDiffServAggIndex	1.3.6.1.4.1.81.36.4.1.5
ipPolicyDiffServApplicabilityPrecedence	1.3.6.1.4.1.81.36.4.1.6
ipPolicyDiffServApplicabilityStatus	1.3.6.1.4.1.81.36.4.1.7
ipPolicyDiffServApplicabilityType	1.3.6.1.4.1.81.36.4.1.8
ipPolicyDiffServErrMsg	1.3.6.1.4.1.81.36.4.1.9
ipPolicyQuerySlot	1.3.6.1.4.1.81.36.5.1.1
ipPolicyQueryListID	1.3.6.1.4.1.81.36.5.1.2
ipPolicyQuerySrcAddr	1.3.6.1.4.1.81.36.5.1.3

Object	OID
ipPolicyQueryDstAddr	1.3.6.1.4.1.81.36.5.1.4
ipPolicyQueryProtocol	1.3.6.1.4.1.81.36.5.1.5
ipPolicyQueryL4SrcPort	1.3.6.1.4.1.81.36.5.1.6
ipPolicyQueryL4DestPort	1.3.6.1.4.1.81.36.5.1.7
ipPolicyQueryEstablished	1.3.6.1.4.1.81.36.5.1.8
ipPolicyQueryDSCP	1.3.6.1.4.1.81.36.5.1.9
ipPolicyQueryOperation	1.3.6.1.4.1.81.36.5.1.10
ipPolicyQueryRuleID	1.3.6.1.4.1.81.36.5.1.11
ipPolicyQueryDSCPOperation	1.3.6.1.4.1.81.36.5.1.12
ipPolicyQueryPriority	1.3.6.1.4.1.81.36.5.1.13
ipPolicyQueryIfIndex	1.3.6.1.4.1.81.36.5.1.14
ipPolicyQuerySubContext	1.3.6.1.4.1.81.36.5.1.15
ipPolicyQueryEtherTypeType	1.3.6.1.4.1.81.36.5.1.16
ipPolicyQueryEtherTypeTrafficType	1.3.6.1.4.1.81.36.5.1.17
ipPolicyQueryIcmpTypeCode	1.3.6.1.4.1.81.36.5.1.18
ipPolicyDiffServControlSlot	1.3.6.1.4.1.81.36.6.1.1
ipPolicyDiffServControlChecksum	1.3.6.1.4.1.81.36.6.1.2
ipPolicyDiffServControlTrustedFields	1.3.6.1.4.1.81.36.6.1.3
ipPolicyDiffServControlValidityStatus	1.3.6.1.4.1.81.36.6.1.4
ipPolicyDiffServControlErrMsg	1.3.6.1.4.1.81.36.6.1.5
ipPolicyAccessControlViolationEntID	1.3.6.1.4.1.81.36.7.1.1
ipPolicyAccessControlViolationSrcAddr	1.3.6.1.4.1.81.36.7.1.2
ipPolicyAccessControlViolationDstAddr	1.3.6.1.4.1.81.36.7.1.3
ipPolicyAccessControlViolationProtocol	1.3.6.1.4.1.81.36.7.1.4
ipPolicyAccessControlViolationL4SrcPort	1.3.6.1.4.1.81.36.7.1.5
ipPolicyAccessControlViolationL4DstPort	1.3.6.1.4.1.81.36.7.1.6
ipPolicyAccessControlViolationEstablished	1.3.6.1.4.1.81.36.7.1.7
ipPolicyAccessControlViolationDSCP	1.3.6.1.4.1.81.36.7.1.8
ipPolicyAccessControlViolationIfIndex	1.3.6.1.4.1.81.36.7.1.9
ipPolicyAccessControlViolationSubCtxt	1.3.6.1.4.1.81.36.7.1.10
ipPolicyAccessControlViolationTime	1.3.6.1.4.1.81.36.7.1.11
ipPolicyAccessControlViolationRuleType	1.3.6.1.4.1.81.36.7.1.12
ipPolicyCompositeOpEntID	1.3.6.1.4.1.81.36.8.1.1
ipPolicyCompositeOpListID	1.3.6.1.4.1.81.36.8.1.2
ipPolicyCompositeOpID	1.3.6.1.4.1.81.36.8.1.3

Object	OID
ipPolicyCompositeOpName	1.3.6.1.4.1.81.36.8.1.4
ipPolicyCompositeOp802priority	1.3.6.1.4.1.81.36.8.1.5
ipPolicyCompositeOpAccess	1.3.6.1.4.1.81.36.8.1.6
ipPolicyCompositeOpDscp	1.3.6.1.4.1.81.36.8.1.7
ipPolicyCompositeOpRSGQualityClass	1.3.6.1.4.1.81.36.8.1.8
ipPolicyCompositeOpNotify	1.3.6.1.4.1.81.36.8.1.9
ipPolicyCompositeOpRowStatus	1.3.6.1.4.1.81.36.8.1.10
ipPolicyCompositeOpErrorReply	1.3.6.1.4.1.81.36.8.1.11
ipPolicyCompositeOpKeepsState	1.3.6.1.4.1.81.36.8.1.12
ipPolicyDSCPmapEntID	1.3.6.1.4.1.81.36.9.1.1
ipPolicyDSCPmapListID	1.3.6.1.4.1.81.36.9.1.2
ipPolicyDSCPmapDSCP	1.3.6.1.4.1.81.36.9.1.3
ipPolicyDSCPmapOperation	1.3.6.1.4.1.81.36.9.1.4
ipPolicyDSCPmapName	1.3.6.1.4.1.81.36.9.1.5
ipPolicyDSCPmapApplicabilityPrecedence	1.3.6.1.4.1.81.36.9.1.6
ipPolicyDSCPmapApplicabilityStatus	1.3.6.1.4.1.81.36.9.1.7
ipPolicyDSCPmapApplicabilityType	1.3.6.1.4.1.81.36.9.1.8
ipPolicyDSCPmapErrMsg	1.3.6.1.4.1.81.36.9.1.9
ipPolicyActivationEntID	1.3.6.1.4.1.81.36.10.1.1
ipPolicyActivationifIndex	1.3.6.1.4.1.81.36.10.1.2
ipPolicyActivationSubContext	1.3.6.1.4.1.81.36.10.1.3
ipPolicyActivationSubContextName	1.3.6.1.4.1.81.36.10.1.4
ipPolicyActivationList	1.3.6.1.4.1.81.36.10.1.5
ipPolicyActivationAclList	1.3.6.1.4.1.81.36.10.1.6
ipPolicyActivationQoSList	1.3.6.1.4.1.81.36.10.1.7
ipPolicyActivationSourceNatList	1.3.6.1.4.1.81.36.10.1.8
ipPolicyActivationDestinationNatList	1.3.6.1.4.1.81.36.10.1.9
ipPolicyActivationAntiSpoofignList	1.3.6.1.4.1.81.36.10.1.10
ipPolicyActivationPBRList	1.3.6.1.4.1.81.36.10.1.11
ipPolicyValidListEntID	1.3.6.1.4.1.81.36.11.1.1.1
ipPolicyValidListIfIndex	1.3.6.1.4.1.81.36.11.1.1.2
ipPolicyValidListSubContext	1.3.6.1.4.1.81.36.11.1.1.3
ipPolicyValidListListID	1.3.6.1.4.1.81.36.11.1.1.4
ipPolicyValidListStatus	1.3.6.1.4.1.81.36.11.1.1.5
ipPolicyValidListErrMsg	1.3.6.1.4.1.81.36.11.1.1.6

Object	OID
ipPolicyValidListIpOption	1.3.6.1.4.1.81.36.11.1.1.7
ipPolicyValidListIpFragmentation	1.3.6.1.4.1.81.36.11.1.1.8
ipPolicyValidRuleEntID	1.3.6.1.4.1.81.36.11.2.1.1
ipPolicyValidRuleIfIndex	1.3.6.1.4.1.81.36.11.2.1.2
ipPolicyValidRuleSubContext	1.3.6.1.4.1.81.36.11.2.1.3
ipPolicyValidRuleListID	1.3.6.1.4.1.81.36.11.2.1.4
ipPolicyValidRuleRuleID	1.3.6.1.4.1.81.36.11.2.1.5
ipPolicyValidRuleStatus	1.3.6.1.4.1.81.36.11.2.1.6
ipPolicyValidRuleApplicabilityType	1.3.6.1.4.1.81.36.11.2.1.7
ipPolicyValidRuleErrMsg	1.3.6.1.4.1.81.36.11.2.1.8
ipPolicyValidDSCPEntID	1.3.6.1.4.1.81.36.11.3.1.1
ipPolicyValidDSCPIfIndex	1.3.6.1.4.1.81.36.11.3.1.2
ipPolicyValidDSCPSubContext	1.3.6.1.4.1.81.36.11.3.1.3
ipPolicyValidDSCPListID	1.3.6.1.4.1.81.36.11.3.1.4
ipPolicyValidDSCPvalue	1.3.6.1.4.1.81.36.11.3.1.5
ipPolicyValidDSCPStatus	1.3.6.1.4.1.81.36.11.3.1.6
ipPolicyValidDSCPApplicabilityType	1.3.6.1.4.1.81.36.11.3.1.7
ipPolicyValidDSCPErrMsg	1.3.6.1.4.1.81.36.11.3.1.8

## MIB objects in the BRIDGE-MIB.my file

The following table provides a list of the MIBs in the BRIDGE-MIB.my file that are supported by Branch Gateway and their OIDs:

Object	OID
dot1dBaseBridgeAddress	1.3.6.1.2.1.17.1.1
dot1dBaseNumPorts	1.3.6.1.2.1.17.1.2
dot1dBaseType	1.3.6.1.2.1.17.1.3
dot1dBasePort	1.3.6.1.2.1.17.1.4.1.1
dot1dBasePortIfIndex	1.3.6.1.2.1.17.1.4.1.2
dot1dBasePortCircuit	1.3.6.1.2.1.17.1.4.1.3
dot1dBasePortDelayExceededDiscards	1.3.6.1.2.1.17.1.4.1.4
dot1dBasePortMtuExceededDiscards	1.3.6.1.2.1.17.1.4.1.5
dot1dStpProtocolSpecification	1.3.6.1.2.1.17.2.1
dot1dStpPriority	1.3.6.1.2.1.17.2.2
dot1dStpTimeSinceTopologyChange	1.3.6.1.2.1.17.2.3
dot1dStpTopChanges	1.3.6.1.2.1.17.2.4

Object	OID
dot1dStpDesignatedRoot	1.3.6.1.2.1.17.2.5
dot1dStpRootCost	1.3.6.1.2.1.17.2.6
dot1dStpRootPort	1.3.6.1.2.1.17.2.7
dot1dStpMaxAge	1.3.6.1.2.1.17.2.8
dot1dStpHelloTime	1.3.6.1.2.1.17.2.9
dot1dStpHoldTime	1.3.6.1.2.1.17.2.10
dot1dStpForwardDelay	1.3.6.1.2.1.17.2.11
dot1dStpBridgeMaxAge	1.3.6.1.2.1.17.2.12
dot1dStpBridgeHelloTime	1.3.6.1.2.1.17.2.13
dot1dStpBridgeForwardDelay	1.3.6.1.2.1.17.2.14
dot1dStpPort	1.3.6.1.2.1.17.2.15.1.1
dot1dStpPortPriority	1.3.6.1.2.1.17.2.15.1.2
dot1dStpPortState	1.3.6.1.2.1.17.2.15.1.3
dot1dStpPortEnable	1.3.6.1.2.1.17.2.15.1.4
dot1dStpPortPathCost	1.3.6.1.2.1.17.2.15.1.5
dot1dStpPortDesignatedRoot	1.3.6.1.2.1.17.2.15.1.6
dot1dStpPortDesignatedCost	1.3.6.1.2.1.17.2.15.1.7
dot1dStpPortDesignatedBridge	1.3.6.1.2.1.17.2.15.1.8
dot1dStpPortDesignatedPort	1.3.6.1.2.1.17.2.15.1.9
dot1dStpPortForwardTransitions	1.3.6.1.2.1.17.2.15.1.10
dot1dTpAgingTime	1.3.6.1.2.1.17.4.2
dot1dTpFdbAddress	1.3.6.1.2.1.17.4.3.1.1
dot1dTpFdbPort	1.3.6.1.2.1.17.4.3.1.2
dot1dTpFdbStatus	1.3.6.1.2.1.17.4.3.1.3

## MIB objects in the CONFIG-MIB.my file

The following table provides a list of the MIBs in the CONFIG-MIB.MY file that are supported by Branch Gateway and their OIDs:

Object	OID
chHWType	1.3.6.1.4.1.81.7.1
chNumberOfSlots	1.3.6.1.4.1.81.7.2
chReset	1.3.6.1.4.1.81.7.7
chLntAgMaxNmbOfMngrs	1.3.6.1.4.1.81.7.9.3.1
chLntAgPermMngrld	1.3.6.1.4.1.81.7.9.3.2.1.1
chLntAgPermMngrAddr	1.3.6.1.4.1.81.7.9.3.2.1.2

Object	OID
chLntAgMngrTraps	1.3.6.1.4.1.81.7.9.3.2.1.3
chLntAgTrapsPermMngrld	1.3.6.1.4.1.81.7.9.3.7.1.1
chLntAgTrapsId	1.3.6.1.4.1.81.7.9.3.7.1.2
chLntAgTrapsEnableFlag	1.3.6.1.4.1.81.7.9.3.7.1.3
chLntAgMaxTrapsNumber	1.3.6.1.4.1.81.7.9.3.100
chGroupList	1.3.6.1.4.1.81.7.18
chLogFileGroupId	1.3.6.1.4.1.81.7.22.1.1
chLogFileIndex	1.3.6.1.4.1.81.7.22.1.2
chLogFileName	1.3.6.1.4.1.81.7.22.1.3
chLogFileAbsoluteTime	1.3.6.1.4.1.81.7.22.1.4
chLogFileMessage	1.3.6.1.4.1.81.7.22.1.5
chLogFileEncryptedMessage	1.3.6.1.4.1.81.7.22.1.6
genGroupId	1.3.6.1.4.1.81.8.1.1.1
genGroupSWVersion	1.3.6.1.4.1.81.8.1.1.2
genGroupKernelVersion	1.3.6.1.4.1.81.8.1.1.3
genGroupType	1.3.6.1.4.1.81.8.1.1.4
genGroupDescr	1.3.6.1.4.1.81.8.1.1.5
genGroupNumberOfPorts	1.3.6.1.4.1.81.8.1.1.6
genGroupNumberOfIntPorts	1.3.6.1.4.1.81.8.1.1.7
genGroupReset	1.3.6.1.4.1.81.8.1.1.8
genGroupAutoMan	1.3.6.1.4.1.81.8.1.1.9
genGroupFullConfig	1.3.6.1.4.1.81.8.1.1.10
genGroupRedun12	1.3.6.1.4.1.81.8.1.1.11
genGroupRedun34	1.3.6.1.4.1.81.8.1.1.12
genGroupStandAloneMode	1.3.6.1.4.1.81.8.1.1.14
genGroupInterProcCommStatus	1.3.6.1.4.1.81.8.1.1.15
genGroupCommStatus	1.3.6.1.4.1.81.8.1.1.16
genGroupHWStatus	1.3.6.1.4.1.81.8.1.1.17
genGroupSupplyVoltageFault	1.3.6.1.4.1.81.8.1.1.18
genGroupIntTemp	1.3.6.1.4.1.81.8.1.1.19
genGroupSpecificOID	1.3.6.1.4.1.81.8.1.1.20
genGroupConfigurationSymbol	1.3.6.1.4.1.81.8.1.1.21
genGroupLastChange	1.3.6.1.4.1.81.8.1.1.22
genGroupRedunRecovery	1.3.6.1.4.1.81.8.1.1.23
genGroupHWVersion	1.3.6.1.4.1.81.8.1.1.24

Object	OID
genGroupHeight	1.3.6.1.4.1.81.8.1.1.25
genGroupWidth	1.3.6.1.4.1.81.8.1.1.26
genGroupIntrusionControl	1.3.6.1.4.1.81.8.1.1.27
genGroupThresholdStatus	1.3.6.1.4.1.81.8.1.1.28
genGroupEavesdropping	1.3.6.1.4.1.81.8.1.1.29
genGroupMainSWVersion	1.3.6.1.4.1.81.8.1.1.30
genGroupMPSActivityStatus	1.3.6.1.4.1.81.8.1.1.31
genGroupBUPSActivityStatus	1.3.6.1.4.1.81.8.1.1.32
genGroupPrepareCounters	1.3.6.1.4.1.81.8.1.1.33
genGroupPortLastChange	1.3.6.1.4.1.81.8.1.1.34
genGroupIntPortLastChange	1.3.6.1.4.1.81.8.1.1.35
genGroupFaultMask	1.3.6.1.4.1.81.8.1.1.36
genGroupTypeName	1.3.6.1.4.1.81.8.1.1.37
genGroupAgentSlot	1.3.6.1.4.1.81.8.1.1.38
genGroupMngType	1.3.6.1.4.1.81.8.1.1.39
genGroupNumberOfLogicalPorts	1.3.6.1.4.1.81.8.1.1.40
genGroupNumberOfInterfaces	1.3.6.1.4.1.81.8.1.1.41
genGroupCascadUpStatus	1.3.6.1.4.1.81.8.1.1.42
genGroupCascadDownStatus	1.3.6.1.4.1.81.8.1.1.43
genGroupSTARootPortID	1.3.6.1.4.1.81.8.1.1.44
genGroupCopyPortInstruction	1.3.6.1.4.1.81.8.1.1.45
genGroupLicenseKey	1.3.6.1.4.1.81.8.1.1.46
genGroupLogFileClear	1.3.6.1.4.1.81.8.1.1.47
genGroupBootVersion	1.3.6.1.4.1.81.8.1.1.48
genGroupResetLastStamp	1.3.6.1.4.1.81.8.1.1.49
genGroupSerialNumber	1.3.6.1.4.1.81.8.1.1.50
genGroupShowModuleInformation	1.3.6.1.4.1.81.8.1.1.51
genGroupCascadingUpFault	1.3.6.1.4.1.81.8.1.1.52
genGroupCascadingDownFault	1.3.6.1.4.1.81.8.1.1.53
genGroupPortClassificationMask	1.3.6.1.4.1.81.8.1.1.54
genGroupPSUType	1.3.6.1.4.1.81.8.1.1.55
genGroupPolicyType	1.3.6.1.4.1.81.8.1.1.56
genPortGroupId	1.3.6.1.4.1.81.9.1.1.1
genPortId	1.3.6.1.4.1.81.9.1.1.2
genPortFunctionality	1.3.6.1.4.1.81.9.1.1.3

Object	OID
genPortType	1.3.6.1.4.1.81.9.1.1.4
genPortDescr	1.3.6.1.4.1.81.9.1.1.5
genPortAdminStatus	1.3.6.1.4.1.81.9.1.1.10
genPortFaultMask	1.3.6.1.4.1.81.9.1.1.14
genPortSWRdFault	1.3.6.1.4.1.81.9.1.1.15
genPortVLANMode	1.3.6.1.4.1.81.9.1.1.19
genPortAdminPermission	1.3.6.1.4.1.81.9.1.1.20
genPortName	1.3.6.1.4.1.81.9.1.1.21
genPortClassification	1.3.6.1.4.1.81.9.1.1.22
genPortVLANBindingMode	1.3.6.1.4.1.81.9.1.1.23
softRedundancyld	1.3.6.1.4.1.81.11.1.1
softRedundancyName	1.3.6.1.4.1.81.11.1.1.2
softRedundancyGroupId1	1.3.6.1.4.1.81.11.1.3
softRedundancyPortId1	1.3.6.1.4.1.81.11.1.4
softRedundancyGroupId2	1.3.6.1.4.1.81.11.1.5
softRedundancyPortId2	1.3.6.1.4.1.81.11.1.6
softRedundancyStatus	1.3.6.1.4.1.81.11.1.7
softRedundancyGlobalStatus	1.3.6.1.4.1.81.11.2
softRedundancyMinTimeBetweenSwitchOvers	1.3.6.1.4.1.81.11.4
softRedundancySwitchBackInterval	1.3.6.1.4.1.81.11.5

## MIB objects in the G700-MG-MIB.my file

The following table provides a list of the MIBs in the G700-MG-MIB.MY file that are supported by the Branch Gateway and their OIDs:

Object	OID
cmgHWType	1.3.6.1.4.1.6889.2.9.1.1.1
cmgModelNumber	1.3.6.1.4.1.6889.2.9.1.1.2
cmgDescription	1.3.6.1.4.1.6889.2.9.1.1.3
cmgSerialNumber	1.3.6.1.4.1.6889.2.9.1.1.4
cmgHWVintage	1.3.6.1.4.1.6889.2.9.1.1.5
cmgHWSuffix	1.3.6.1.4.1.6889.2.9.1.1.6
cmgStackPosition	1.3.6.1.4.1.6889.2.9.1.1.7
cmgModuleList	1.3.6.1.4.1.6889.2.9.1.1.8
cmgReset	1.3.6.1.4.1.6889.2.9.1.1.9
cmgHardwareFaultMask	1.3.6.1.4.1.6889.2.9.1.1.10.12

Object	OID
cmgHardwareStatusMask	1.3.6.1.4.1.6889.2.9.1.1.10.13
cmgModuleSlot	1.3.6.1.4.1.6889.2.9.1.1.11.1.1
cmgModuleType	1.3.6.1.4.1.6889.2.9.1.1.11.1.2
cmgModuleDescription	1.3.6.1.4.1.6889.2.9.1.1.11.1.3
cmgModuleName	1.3.6.1.4.1.6889.2.9.1.1.11.1.4
cmgModuleSerialNumber	1.3.6.1.4.1.6889.2.9.1.1.11.1.5
cmgModuleHWVintage	1.3.6.1.4.1.6889.2.9.1.1.11.1.6
cmgModuleHWSuffix	1.3.6.1.4.1.6889.2.9.1.1.11.1.7
cmgModuleFWVersion	1.3.6.1.4.1.6889.2.9.1.1.11.1.1.8
cmgModuleNumberOfPorts	1.3.6.1.4.1.6889.2.9.1.1.11.1.1.9
cmgModuleFaultMask	1.3.6.1.4.1.6889.2.9.1.1.11.1.1.10
cmgModuleStatusMask	1.3.6.1.4.1.6889.2.9.1.1.11.1.11
cmgModuleReset	1.3.6.1.4.1.6889.2.9.1.1.11.1.1.12
cmgModuleNumberOfChannels	1.3.6.1.4.1.6889.2.9.1.1.11.1.13
cmgGatewayNumber	1.3.6.1.4.1.6889.2.9.1.2.1.1
cmgMACAddress	1.3.6.1.4.1.6889.2.9.1.2.1.2
cmgFWVersion	1.3.6.1.4.1.6889.2.9.1.2.1.3
cmgCurrentlpAddress	1.3.6.1.4.1.6889.2.9.1.2.1.4
cmgMgpFaultMask	1.3.6.1.4.1.6889.2.9.1.2.1.15
cmgQosControl	1.3.6.1.4.1.6889.2.9.1.2.2.1
cmgRemoteSigDscp	1.3.6.1.4.1.6889.2.9.1.2.2.2
cmgRemoteSig802Priority	1.3.6.1.4.1.6889.2.9.1.2.2.3
cmgLocalSigDscp	1.3.6.1.4.1.6889.2.9.1.2.2.4
cmgLocalSig802Priority	1.3.6.1.4.1.6889.2.9.1.2.2.5
cmgStatic802Vlan	1.3.6.1.4.1.6889.2.9.1.2.2.6
cmgCurrent802Vlan	1.3.6.1.4.1.6889.2.9.1.2.2.7
cmgPrimaryClockSource	1.3.6.1.4.1.6889.2.9.1.2.3.1
cmgSecondaryClockSource	1.3.6.1.4.1.6889.2.9.1.2.3.2
cmgActiveClockSource	1.3.6.1.4.1.6889.2.9.1.2.3.3
cmgRegistrationState	1.3.6.1.4.1.6889.2.9.1.3.1
cmgActiveControllerAddress	1.3.6.1.4.1.6889.2.9.1.3.2
cmgH248LinkStatus	1.3.6.1.4.1.6889.2.9.1.3.3
cmgH248LinkErrorCode	1.3.6.1.4.1.6889.2.9.1.3.4
cmgUseDhcpForMgcList	1.3.6.1.4.1.6889.2.9.1.3.5
cmgStaticControllerHosts	1.3.6.1.4.1.6889.2.9.1.3.6

Object	OID
cmgDhcpControllerHosts	1.3.6.1.4.1.6889.2.9.1.3.7
cmgPrimarySearchTime	1.3.6.1.4.1.6889.2.9.1.3.8
cmgTotalSearchTime	1.3.6.1.4.1.6889.2.9.1.3.9
cmgTransitionPoint	1.3.6.1.4.1.6889.2.9.1.3.10
cmgVoipEngineUseDhcp	1.3.6.1.4.1.6889.2.9.1.4.1
cmgActiveControllerSoftwareVersion	1.3.6.1.4.1.6889.2.9.1.3.11
cmgActiveControllerInetAddressType	1.3.6.1.4.1.6889.2.9.1.3.12
cmgActiveControllerInetAddress	1.3.6.1.4.1.6889.2.9.1.3.13
cmgVoipQosControl	1.3.6.1.4.1.6889.2.9.1.4.2
cmgVoipRemoteBbeDscp	1.3.6.1.4.1.6889.2.9.1.4.3.1.1
cmgVoipRemoteEfDscp	1.3.6.1.4.1.6889.2.9.1.4.3.1.2
cmgVoipRemote802Priority	1.3.6.1.4.1.6889.2.9.1.4.3.1.3
cmgVoipRemoteMinRtpPort	1.3.6.1.4.1.6889.2.9.1.4.3.1.4
cmgVoipRemoteMaxRtpPort	1.3.6.1.4.1.6889.2.9.1.4.3.1.5
cmgVoipRemoteRtcpEnabled	1.3.6.1.4.1.6889.2.9.1.4.3.2.1
cmgVoipRemoteRtcpMonitorIpAddress	1.3.6.1.4.1.6889.2.9.1.4.3.2.2
cmgVoipRemoteRtcpMonitorPort	1.3.6.1.4.1.6889.2.9.1.4.3.2.3
cmgVoipRemoteRtcpReportPeriod	1.3.6.1.4.1.6889.2.9.1.4.3.2.4
cmgVoipRemoteRsvpEnabled	1.3.6.1.4.1.6889.2.9.1.4.3.3.1
cmgVoipRemoteRetryOnFailure	1.3.6.1.4.1.6889.2.9.1.4.3.3.2
cmgVoipRemoteRetryDelay	1.3.6.1.4.1.6889.2.9.1.4.3.3.3
cmgVoipRemoteRsvpProfile	1.3.6.1.4.1.6889.2.9.1.4.3.3.4
cmgVoipLocalBbeDscp	1.3.6.1.4.1.6889.2.9.1.4.4.1.1
cmgVoipLocalEfDscp	1.3.6.1.4.1.6889.2.9.1.4.4.1.2
cmgVoipLocal802Priority	1.3.6.1.4.1.6889.2.9.1.4.4.1.3
cmgVoipLocalMinRtpPort	1.3.6.1.4.1.6889.2.9.1.4.4.1.4
cmgVoipLocalMaxRtpPort	1.3.6.1.4.1.6889.2.9.1.4.4.1.5
cmgVoipLocalRtcpEnabled	1.3.6.1.4.1.6889.2.9.1.4.4.2.1
cmgVoipLocalRtcpMonitorIpAddress	1.3.6.1.4.1.6889.2.9.1.4.4.2.2
cmgVoipLocalRtcpMonitorPort	1.3.6.1.4.1.6889.2.9.1.4.4.2.3
cmgVoipLocalRtcpReportPeriod	1.3.6.1.4.1.6889.2.9.1.4.4.2.4
cmgVoipLocalRsvpEnabled	1.3.6.1.4.1.6889.2.9.1.4.4.3.1
cmgVoipLocalRetryOnFailure	1.3.6.1.4.1.6889.2.9.1.4.4.3.2
cmgVoipLocalRetryDelay	1.3.6.1.4.1.6889.2.9.1.4.4.3.3
cmgVoipLocalRsvpProfile	1.3.6.1.4.1.6889.2.9.1.4.4.3.4

Object	OID
cmgVoipSlot	1.3.6.1.4.1.6889.2.9.1.4.5.1.1
cmgVoipMACAddress	1.3.6.1.4.1.6889.2.9.1.4.5.1.2
cmgVoipStaticlpAddress	1.3.6.1.4.1.6889.2.9.1.4.5.1.3
cmgVoipCurrentIpAddress	1.3.6.1.4.1.6889.2.9.1.4.5.1.4
cmgVoipJitterBufferSize	1.3.6.1.4.1.6889.2.9.1.4.5.1.5
cmgVoipTotalChannels	1.3.6.1.4.1.6889.2.9.1.4.5.1.6
cmgVoipChannelsInUse	1.3.6.1.4.1.6889.2.9.1.4.5.1.7
cmgVoipAverageOccupancy	1.3.6.1.4.1.6889.2.9.1.4.5.1.8
cmgVoipHyperactivity	1.3.6.1.4.1.6889.2.9.1.4.5.1.9
cmgVoipAdminState	1.3.6.1.4.1.6889.2.9.1.4.5.1.10
cmgVoipDspFWVersion	1.3.6.1.4.1.6889.2.9.1.4.5.1.11
cmgVoipDspStatus	1.3.6.1.4.1.6889.2.9.1.4.5.1.12
cmgVoipEngineReset	1.3.6.1.4.1.6889.2.9.1.4.5.1.13
cmgVoipFaultMask	1.3.6.1.4.1.6889.2.9.1.4.5.1.14
cmgCcModule	1.3.6.1.4.1.6889.2.9.1.6.1.1.1
cmgCcPort	1.3.6.1.4.1.6889.2.9.1.6.1.1.2
cmgCcRelay	1.3.6.1.4.1.6889.2.9.1.6.1.1.3
cmgCcAdminState	1.3.6.1.4.1.6889.2.9.1.6.1.1.4
cmgCcPulseDuration	1.3.6.1.4.1.6889.2.9.1.6.1.1.5
cmgCcStatus	1.3.6.1.4.1.6889.2.9.1.6.1.1.6
cmgEtrModule	1.3.6.1.4.1.6889.2.9.1.7.1.1.1
cmgEtrAdminState	1.3.6.1.4.1.6889.2.9.1.7.1.1.2
cmgEtrNumberOfPairs	1.3.6.1.4.1.6889.2.9.1.7.1.1.3
cmgEtrStatus	1.3.6.1.4.1.6889.2.9.1.7.1.1.4
cmgEtrCurrentLoopDetect	1.3.6.1.4.1.6889.2.9.1.7.1.1.5
cmgDynCacStatus	1.3.6.1.4.1.6889.2.9.1.8.1
cmgDynCacRBBL	1.3.6.1.4.1.6889.2.9.1.8.2
cmgDynCacLastUpdate	1.3.6.1.4.1.6889.2.9.1.8.3
cmgSLAMonitorState	1.3.6.1.4.1.6889.2.9.1.9.1
cmgSLAMonitorServerInetAddressType	1.3.6.1.4.1.6889.2.9.1.9.2
cmgSLAMonitorServerInetAddress	1.3.6.1.4.1.6889.2.9.1.9.3
cmgSLAMonitorServerPort	1.3.6.1.4.1.6889.2.9.1.9.4
cmgSLAMonitorPacketCaptureMode	1.3.6.1.4.1.6889.2.9.1.9.10
cmgSLAMonitorVersion	1.3.6.1.4.1.6889.2.9.1.9.99

## MIB objects in the FRAME-RELAY-DTE-MIB.my file

The following table provides a list of the MIBs in the FRAME-RELAY-DTE-MIB.my file that are supported by the Branch Gateway and their OIDs:

Object	OID
frDlcmilfIndex	1.3.6.1.2.1.10.32.1.1.1
frDlcmiState	1.3.6.1.2.1.10.32.1.1.2
frDlcmiAddress	1.3.6.1.2.1.10.32.1.1.3
frDlcmiAddressLen	1.3.6.1.2.1.10.32.1.1.4
frDlcmiPollingInterval	1.3.6.1.2.1.10.32.1.1.5
frDlcmiFullEnquiryInterval	1.3.6.1.2.1.10.32.1.1.6
frDlcmiErrorThreshold	1.3.6.1.2.1.10.32.1.1.7
frDlcmiMonitoredEvents	1.3.6.1.2.1.10.32.1.1.8
frDlcmiMaxSupportedVCs	1.3.6.1.2.1.10.32.1.1.9
frDlcmiMulticast	1.3.6.1.2.1.10.32.1.1.10
frDlcmiStatus	1.3.6.1.2.1.10.32.1.1.11
frDlcmiRowStatus	1.3.6.1.2.1.10.32.1.1.12
frCircuitlfIndex	1.3.6.1.2.1.10.32.2.1.1
frCircuitDlci	1.3.6.1.2.1.10.32.2.1.2
frCircuitState	1.3.6.1.2.1.10.32.2.1.3
frCircuitReceivedFECNs	1.3.6.1.2.1.10.32.2.1.4
frCircuitReceivedBECNs	1.3.6.1.2.1.10.32.2.1.5
frCircuitSentFrames	1.3.6.1.2.1.10.32.2.1.6
frCircuitSentOctets	1.3.6.1.2.1.10.32.2.1.7
frCircuitReceivedFrames	1.3.6.1.2.1.10.32.2.1.8
frCircuitReceivedOctets	1.3.6.1.2.1.10.32.2.1.9
frCircuitCreationTime	1.3.6.1.2.1.10.32.2.1.10
frCircuitLastTimeChange	1.3.6.1.2.1.10.32.2.1.11
frCircuitCommittedBurst	1.3.6.1.2.1.10.32.2.1.12
frCircuitExcessBurst	1.3.6.1.2.1.10.32.2.1.13
frCircuitThroughput	1.3.6.1.2.1.10.32.2.1.14
frCircuitMulticast	1.3.6.1.2.1.10.32.2.1.15
frCircuitType	1.3.6.1.2.1.10.32.2.1.16
frCircuitDiscards	1.3.6.1.2.1.10.32.2.1.17
frCircuitReceivedDEs	1.3.6.1.2.1.10.32.2.1.18
frCircuitSentDEs	1.3.6.1.2.1.10.32.2.1.19
frCircuitLogicallfIndex	1.3.6.1.2.1.10.32.2.1.20

Object	OID
frCircuitRowStatus	1.3.6.1.2.1.10.32.2.1.21
frErrlfIndex	1.3.6.1.2.1.10.32.3.1.1
frErrType	1.3.6.1.2.1.10.32.3.1.2
frErrData	1.3.6.1.2.1.10.32.3.1.3
frErrTime	1.3.6.1.2.1.10.32.3.1.4
frErrFaults	1.3.6.1.2.1.10.32.3.1.5
frErrFaultTime	1.3.6.1.2.1.10.32.3.1.6
frTrapState	1.3.6.1.2.1.10.32.4.1
frTrapMaxRate	1.3.6.1.2.1.10.32.4.2

## MIB objects in the IP-MIB.my file

The following table provides a list of the MIBs in the IP-MIB.my file that are supported by Branch Gateway and their OIDs:

Object	OID
ipForwarding	1.3.6.1.2.1.4.1
ipDefaultTTL	1.3.6.1.2.1.4.2
ipInReceives	1.3.6.1.2.1.4.3
ipInHdrErrors	1.3.6.1.2.1.4.4
ipInAddrErrors	1.3.6.1.2.1.4.5
ipForwDatagrams	1.3.6.1.2.1.4.6
ipInUnknownProtos	1.3.6.1.2.1.4.7
ipInDiscards	1.3.6.1.2.1.4.8
ipInDelivers	1.3.6.1.2.1.4.9
ipOutRequests	1.3.6.1.2.1.4.10
ipOutDiscards	1.3.6.1.2.1.4.11
ipOutNoRoutes	1.3.6.1.2.1.4.12
ipReasmTimeout	1.3.6.1.2.1.4.13
ipReasmReqds	1.3.6.1.2.1.4.14
ipReasmOKs	1.3.6.1.2.1.4.15
ipReasmFails	1.3.6.1.2.1.4.16
ipFragOKs	1.3.6.1.2.1.4.17
ipFragFails	1.3.6.1.2.1.4.18
ipFragCreates	1.3.6.1.2.1.4.19
ipAdEntAddr	1.3.6.1.2.1.4.20.1.1
ipAdEntIfIndex	1.3.6.1.2.1.4.20.1.2

Object	OID
ipAdEntNetMask	1.3.6.1.2.1.4.20.1.3
ipAdEntBcastAddr	1.3.6.1.2.1.4.20.1.4
ipAdEntReasmMaxSize	1.3.6.1.2.1.4.20.1.5
ipNetToMedialfIndex	1.3.6.1.2.1.4.22.1.1
ipNetToMediaPhysAddress	1.3.6.1.2.1.4.22.1.2
ipNetToMediaNetAddress	1.3.6.1.2.1.4.22.1.3
ipNetToMediaType	1.3.6.1.2.1.4.22.1.4
ipRoutingDiscards	1.3.6.1.2.1.4.23

## MIB objects in the Load12-MIB.my file

The following table provides a list of the MIBs in the Load-MIB.my file that are supported by the Branch Gateway and their OIDs:

Object	OID
genOpModuleId	1.3.6.1.4.1.1751.2.53.1.2.1.1
genOpIndex	1.3.6.1.4.1.1751.2.53.1.2.1.2
genOpRunningState	1.3.6.1.4.1.1751.2.53.1.2.1.3
genOpSourceIndex	1.3.6.1.4.1.1751.2.53.1.2.1.4
genOpDestIndex	1.3.6.1.4.1.1751.2.53.1.2.1.5
genOpServerIP	1.3.6.1.4.1.1751.2.53.1.2.1.6
genOpUserName	1.3.6.1.4.1.1751.2.53.1.2.1.7
genOpPassword	1.3.6.1.4.1.1751.2.53.1.2.1.8
genOpProtocolType	1.3.6.1.4.1.1751.2.53.1.2.1.9
genOpFileName	1.3.6.1.4.1.1751.2.53.1.2.1.10
genOpRunningStateDisplay	1.3.6.1.4.1.1751.2.53.1.2.1.11
genOpLastFailureIndex	1.3.6.1.4.1.1751.2.53.1.2.1.12
genOpLastFailureDisplay	1.3.6.1.4.1.1751.2.53.1.2.1.13
genOpLastWarningDisplay	1.3.6.1.4.1.1751.2.53.1.2.1.14
genOpErrorLogIndex	1.3.6.1.4.1.1751.2.53.1.2.1.15
genOpResetSupported	1.3.6.1.4.1.1751.2.53.1.2.1.16
genOpEnableReset	1.3.6.1.4.1.1751.2.53.1.2.1.17
genOpNextBootImageIndex	1.3.6.1.4.1.1751.2.53.1.2.1.18
genOpLastBootImageIndex	1.3.6.1.4.1.1751.2.53.1.2.1.19
genOpFileSystemType	1.3.6.1.4.1.1751.2.53.1.2.1.20
genOpReportSpecificFlags	1.3.6.1.4.1.1751.2.53.1.2.1.21
genOpOctetsReceived	1.3.6.1.4.1.1751.2.53.1.2.1.22

Object	OID
genAppFileId	1.3.6.1.4.1.1751.2.53.2.1.1.1
genAppFileName	1.3.6.1.4.1.1751.2.53.2.1.1.2
genAppFileType	1.3.6.1.4.1.1751.2.53.2.1.1.3
genAppFileDescription	1.3.6.1.4.1.1751.2.53.2.1.1.4
genAppFileSize	1.3.6.1.4.1.1751.2.53.2.1.1.5
genAppFileVersionNumber	1.3.6.1.4.1.1751.2.53.2.1.1.6
genAppFileLocation	1.3.6.1.4.1.1751.2.53.2.1.1.7
genAppFileDateStamp	1.3.6.1.4.1.1751.2.53.2.1.1.8
genAppFileRowStatus	1.3.6.1.4.1.1751.2.53.2.1.1.9

### MIB objects in the PPP-LCP-MIB.my file

The following table provides a list of the MIBs in the PPP-LCP-MIB.my file that are supported by Branch Gateway and their OIDs:

Object	OID
pppLinkStatusPhysicalIndex	1.3.6.1.2.1.10.23.1.1.1.1
pppLinkStatusBadAddresses	1.3.6.1.2.1.10.23.1.1.1.2
pppLinkStatusBadControls	1.3.6.1.2.1.10.23.1.1.1.3
pppLinkStatusPacketTooLongs	1.3.6.1.2.1.10.23.1.1.1.4
pppLinkStatusBadFCSs	1.3.6.1.2.1.10.23.1.1.1.5
pppLinkStatusLocalMRU	1.3.6.1.2.1.10.23.1.1.1.6
pppLinkStatusRemoteMRU	1.3.6.1.2.1.10.23.1.1.1.7
pppLinkStatusLocalToPeerACCMap	1.3.6.1.2.1.10.23.1.1.1.8
pppLinkStatusPeerToLocalACCMap	1.3.6.1.2.1.10.23.1.1.1.9
pppLinkStatusLocalToRemoteACCompression	1.3.6.1.2.1.10.23.1.1.1.12
pppLinkStatusRemoteToLocalACCompression	1.3.6.1.2.1.10.23.1.1.1.13
pppLinkStatusTransmitFcsSize	1.3.6.1.2.1.10.23.1.1.1.14
pppLinkStatusReceiveFcsSize	1.3.6.1.2.1.10.23.1.1.1.15
pppLinkConfigInitialMRU	1.3.6.1.2.1.10.23.1.1.2.1.1
pppLinkConfigReceiveACCMap	1.3.6.1.2.1.10.23.1.1.2.1.2
pppLinkConfigTransmitACCMap	1.3.6.1.2.1.10.23.1.1.2.1.3
pppLinkConfigMagicNumber	1.3.6.1.2.1.10.23.1.1.2.1.4
pppLinkConfigFcsSize	1.3.6.1.2.1.10.23.1.1.2.1.5

### MIB objects in the WAN-MIB.my file

The following table provides a list of the MIBs in the WAN-MIB.my file that are supported by the Banch Gateway and their OIDs:

Object	OID
ds0BundleMemmbersList	1.3.6.1.4.1.6889.2.1.6.1.1.2.1.1
ds0BundleSpeedFactor	1.3.6.1.4.1.6889.2.1.6.1.1.2.1.2
ds1DeviceMode	1.3.6.1.4.1.6889.2.1.6.2.1.1
ifTableXtndIndex	1.3.6.1.4.1.6889.2.1.6.2.2.1.1.1
ifTableXtndPeerAddress	1.3.6.1.4.1.6889.2.1.6.2.2.1.1.2
ifTableXtndVoIPQueue	1.3.6.1.4.1.6889.2.1.6.2.2.1.1.3
ifTableXtndCableLength	1.3.6.1.4.1.6889.2.1.6.2.2.1.1.4
ifTableXtndGain	1.3.6.1.4.1.6889.2.1.6.2.2.1.1.5
ifTableXtndDescription	1.3.6.1.4.1.6889.2.1.6.2.2.1.1.6
ifTableXtndKeepAlive	1.3.6.1.4.1.6889.2.1.6.2.2.1.1.7
ifTableXtndMtu	1.3.6.1.4.1.6889.2.1.6.2.2.1.1.8
ifTableXtndInvertTxClock	1.3.6.1.4.1.6889.2.1.6.2.2.1.1.9
ifTableXtndDTELoopback	1.3.6.1.4.1.6889.2.1.6.2.2.1.1.10
ifTableXtndIgnoreDCD	1.3.6.1.4.1.6889.2.1.6.2.2.1.1.11
ifTableXtndIdleChars	1.3.6.1.4.1.6889.2.1.6.2.2.1.1.12
ifTableXtndBandwidth	1.3.6.1.4.1.6889.2.1.6.2.2.1.1.13
ifTableXtndEncapsulation	1.3.6.1.4.1.6889.2.1.6.2.2.1.1.14
ifTableXtndOperStatus	1.3.6.1.4.1.6889.2.1.6.2.2.1.1.15
ifTableXtndBackupCapabilities	1.3.6.1.4.1.6889.2.1.6.2.2.1.1.16
ifTableXtndBackupIf	1.3.6.1.4.1.6889.2.1.6.2.2.1.1.17
ifTableXtndBackupEnableDelay	1.3.6.1.4.1.6889.2.1.6.2.2.1.1.18
ifTableXtndBackupDisableDelay	1.3.6.1.4.1.6889.2.1.6.2.2.1.1.19
ifTableXtndPrimaryIf	1.3.6.1.4.1.6889.2.1.6.2.2.1.1.20
ifTableXtndCarrierDelay	1.3.6.1.4.1.6889.2.1.6.2.2.1.1.21
ifTableXtndDtrRestartDelay	1.3.6.1.4.1.6889.2.1.6.2.2.1.1.22
ifTableXtndDtrPulseTime	1.3.6.1.4.1.6889.2.1.6.2.2.1.1.23
ifTableXtndLoadInterval	1.3.6.1.4.1.6889.2.1.6.2.2.1.1.24
ifTableXtndInputRate	1.3.6.1.4.1.6889.2.1.6.2.2.1.1.25
ifTableXtndOutputRate	1.3.6.1.4.1.6889.2.1.6.2.2.1.1.26
ifTableXtndInputLoad	1.3.6.1.4.1.6889.2.1.6.2.2.1.1.27
ifTableXtndOutputLoad	1.3.6.1.4.1.6889.2.1.6.2.2.1.1.28
ifTableXtndReliability	1.3.6.1.4.1.6889.2.1.6.2.2.1.1.29
ifTableXtndCacBBL	1.3.6.1.4.1.6889.2.1.6.2.2.1.1.31
ifTableXtndCacPriority	1.3.6.1.4.1.6889.2.1.6.2.2.1.1.32
ifTableXtndCacifStatus	1.3.6.1.4.1.6889.2.1.6.2.2.1.1.33

Object	OID
frDlcmiXtndIndex	1.3.6.1.4.1.6889.2.1.6.2.4.1.1.1
frDlcmiXtndLMIAutoSense	1.3.6.1.4.1.6889.2.1.6.2.4.1.1.2
frStaticCircuitSublfIndex	1.3.6.1.4.1.6889.2.1.6.2.4.2.1.1
frStaticCircuitDLCI	1.3.6.1.4.1.6889.2.1.6.2.4.2.1.2
frStaticCircuitDLCIrole	1.3.6.1.4.1.6889.2.1.6.2.4.2.1.3
frStaticCircuitStatus	1.3.6.1.4.1.6889.2.1.6.2.4.2.1.4
frSublfDlcmiIndex	1.3.6.1.4.1.6889.2.1.6.2.4.3.1.1
frSubIfSubIndex	1.3.6.1.4.1.6889.2.1.6.2.4.3.1.2
frSubIfType	1.3.6.1.4.1.6889.2.1.6.2.4.3.1.3
frSubIfStatus	1.3.6.1.4.1.6889.2.1.6.2.4.3.1.4

## MIB objects in the SNMPv2-MIB.my file

The following table provides a list of the MIBs in the SNMPv2-MIB.my file that are supported by the Branch Gateway and their OIDs:

Object	OID
sysDescr	1.3.6.1.2.1.1.1
sysObjectID	1.3.6.1.2.1.1.2
sysUpTime	1.3.6.1.2.1.1.3
sysContact	1.3.6.1.2.1.1.4
sysName	1.3.6.1.2.1.1.5
sysLocation	1.3.6.1.2.1.1.6
sysServices	1.3.6.1.2.1.1.7
snmpInPkts	1.3.6.1.2.1.11.1
snmpInBadVersions	1.3.6.1.2.1.11.3
snmpInBadCommunityNames	1.3.6.1.2.1.11.4
snmpInBadCommunityUses	1.3.6.1.2.1.11.5
snmpInASNParseErrs	1.3.6.1.2.1.11.6
snmpEnableAuthenTraps	1.3.6.1.2.1.11.30
snmpOutPkts	1.3.6.1.2.1.11.2
snmpInTooBigs	1.3.6.1.2.1.11.8
snmpInNoSuchNames	1.3.6.1.2.1.11.9
snmpInBadValues	1.3.6.1.2.1.11.10
snmpInReadOnlys	1.3.6.1.2.1.11.11
snmpInGenErrs	1.3.6.1.2.1.11.12
snmpInTotalReqVars	1.3.6.1.2.1.11.13

Object	OID
snmpInTotalSetVars	1.3.6.1.2.1.11.14
snmpInGetRequests	1.3.6.1.2.1.11.15
snmpInGetNexts	1.3.6.1.2.1.11.16
snmpInSetRequests	1.3.6.1.2.1.11.17
snmpInGetResponses	1.3.6.1.2.1.11.18
snmpInTraps	1.3.6.1.2.1.11.19
snmpOutTooBigs	1.3.6.1.2.1.11.20
snmpOutNoSuchNames	1.3.6.1.2.1.11.21
snmpOutBadValues	1.3.6.1.2.1.11.22
snmpOutGenErrs	1.3.6.1.2.1.11.24
snmpOutGetRequests	1.3.6.1.2.1.11.25
snmpOutGetNexts	1.3.6.1.2.1.11.26
snmpOutSetRequests	1.3.6.1.2.1.11.27
snmpOutGetResponses	1.3.6.1.2.1.11.28
snmpOutTraps	1.3.6.1.2.1.11.29

## MIB objects in the OSPF-MIB.my file

The following table provides a list of the MIBs in the OSPF-MIB.my file that are supported by the Branch Gateway and their OIDs:

Object	OID
ospfRouterId	1.3.6.1.2.1.14.1.1
ospfAdminStat	1.3.6.1.2.1.14.1.2
ospfVersionNumber	1.3.6.1.2.1.14.1.3
ospfAreaBdrRtrStatus	1.3.6.1.2.1.14.1.4
ospfASBdrRtrStatus	1.3.6.1.2.1.14.1.5
ospfExternLsaCount	1.3.6.1.2.1.14.1.6
ospfExternLsaCksumSum	1.3.6.1.2.1.14.1.7
ospfTOSSupport	1.3.6.1.2.1.14.1.8
ospfOriginateNewLsas	1.3.6.1.2.1.14.1.9
ospfRxNewLsas	1.3.6.1.2.1.14.1.10
ospfExtLsdbLimit	1.3.6.1.2.1.14.1.11
ospfMulticastExtensions	1.3.6.1.2.1.14.1.12
ospfExitOverflowInterval	1.3.6.1.2.1.14.1.13
ospfDemandExtensions	1.3.6.1.2.1.14.1.14
ospfAreald	1.3.6.1.2.1.14.2.1.1

Object	OID
ospfAuthType	1.3.6.1.2.1.14.2.1.2
ospflmportAsExtern	1.3.6.1.2.1.14.2.1.3
ospfSpfRuns	1.3.6.1.2.1.14.2.1.4
ospfAreaBdrRtrCount	1.3.6.1.2.1.14.2.1.5
ospfAsBdrRtrCount	1.3.6.1.2.1.14.2.1.6
ospfAreaLsaCount	1.3.6.1.2.1.14.2.1.7
ospfAreaLsaCksumSum	1.3.6.1.2.1.14.2.1.8
ospfAreaSummary	1.3.6.1.2.1.14.2.1.9
ospfAreaStatus	1.3.6.1.2.1.14.2.1.10
ospfLsdbAreald	1.3.6.1.2.1.14.4.1.1
ospfLsdbType	1.3.6.1.2.1.14.4.1.2
ospfLsdbLsid	1.3.6.1.2.1.14.4.1.3
ospfLsdbRouterId	1.3.6.1.2.1.14.4.1.4
ospfLsdbSequence	1.3.6.1.2.1.14.4.1.5
ospfLsdbAge	1.3.6.1.2.1.14.4.1.6
ospfLsdbChecksum	1.3.6.1.2.1.14.4.1.7
ospfLsdbAdvertisement	1.3.6.1.2.1.14.4.1.8
ospflflpAddress	1.3.6.1.2.1.14.7.1.1
ospfAddressLessIf	1.3.6.1.2.1.14.7.1.2
ospflfAreald	1.3.6.1.2.1.14.7.1.3
ospflfType	1.3.6.1.2.1.14.7.1.4
ospflfAdminStat	1.3.6.1.2.1.14.7.1.5
ospflfRtrPriority	1.3.6.1.2.1.14.7.1.6
ospflfTransitDelay	1.3.6.1.2.1.14.7.1.7
ospflfRetransInterval	1.3.6.1.2.1.14.7.1.8
ospflfHelloInterval	1.3.6.1.2.1.14.7.1.9
ospflfRtrDeadInterval	1.3.6.1.2.1.14.7.1.10
ospflfPollInterval	1.3.6.1.2.1.14.7.1.11
ospflfState	1.3.6.1.2.1.14.7.1.12
ospflfDesignatedRouter	1.3.6.1.2.1.14.7.1.13
ospflfBackupDesignatedRouter	1.3.6.1.2.1.14.7.1.14
ospflfEvents	1.3.6.1.2.1.14.7.1.15
ospflfAuthKey	1.3.6.1.2.1.14.7.1.16
ospflfStatus	1.3.6.1.2.1.14.7.1.17
ospflfMulticastForwarding	1.3.6.1.2.1.14.7.1.18

Object	OID
ospflfDemand	1.3.6.1.2.1.14.7.1.19
ospflfAuthType	1.3.6.1.2.1.14.7.1.20
ospflfMetriclpAddress	1.3.6.1.2.1.14.8.1.1
ospflfMetricAddressLessIf	1.3.6.1.2.1.14.8.1.2
ospflfMetricTOS	1.3.6.1.2.1.14.8.1.3
ospflfMetricValue	1.3.6.1.2.1.14.8.1.4
ospflfMetricStatus	1.3.6.1.2.1.14.8.1.5
ospfNbrlpAddr	1.3.6.1.2.1.14.10.1.1
ospfNbrAddressLessIndex	1.3.6.1.2.1.14.10.1.2
ospfNbrRtrld	1.3.6.1.2.1.14.10.1.3
ospfNbrOptions	1.3.6.1.2.1.14.10.1.4
ospfNbrPriority	1.3.6.1.2.1.14.10.1.5
ospfNbrState	1.3.6.1.2.1.14.10.1.6
ospfNbrEvents	1.3.6.1.2.1.14.10.1.7
ospfNbrLsRetransQLen	1.3.6.1.2.1.14.10.1.8
ospfNbmaNbrStatus	1.3.6.1.2.1.14.10.1.9
ospfNbmaNbrPermanence	1.3.6.1.2.1.14.10.1.10
ospfNbrHelloSuppressed	1.3.6.1.2.1.14.10.1.11
ospfExtLsdbType	1.3.6.1.2.1.14.12.1.1
ospfExtLsdbLsid	1.3.6.1.2.1.14.12.1.2
ospfExtLsdbRouterId	1.3.6.1.2.1.14.12.1.3
ospfExtLsdbSequence	1.3.6.1.2.1.14.12.1.4
ospfExtLsdbAge	1.3.6.1.2.1.14.12.1.5
ospfExtLsdbChecksum	1.3.6.1.2.1.14.12.1.6
ospfExtLsdbAdvertisement	1.3.6.1.2.1.14.12.1.7

## MIB objects in the TUNNEL-MIB.my file

The following table provides a list of the MIBs in the TUNNEL-MIB.my file that are supported by the Branch Gateway and their OIDs:

Object	OID
tunnellfLocalAddress	1.3.6.1.2.1.10.131.1.1.1.1
tunnellfRemoteAddress	1.3.6.1.2.1.10.131.1.1.1.2
tunnellfEncapsMethod	1.3.6.1.2.1.10.131.1.1.1.3
tunnellfTOS	1.3.6.1.2.1.10.131.1.1.1.4
tunnellfHopLimit	1.3.6.1.2.1.10.131.1.1.1.5

Object	OID
tunnelConfigLocalAddress	1.3.6.1.2.1.10.131.1.1.2.1.1
tunnelConfigRemoteAddress	1.3.6.1.2.1.10.131.1.1.2.1.2
tunnelConfigEncapsMethod	1.3.6.1.2.1.10.131.1.1.2.1.3
tunnelConfigID	1.3.6.1.2.1.10.131.1.1.2.1.4
tunnelConfigStatus	1.3.6.1.2.1.10.131.1.1.2.1.5
ipTunnellfIndex	1.3.6.1.4.1.81.31.8.1.1.1
ipTunnellfChecksum	1.3.6.1.4.1.81.31.8.1.1.2
ipTunnellfKey	1.3.6.1.4.1.81.31.8.1.1.3
ipTunnellfkeyMode	1.3.6.1.4.1.81.31.8.1.1.4
ipTunnellfAgingTimer	1.3.6.1.4.1.81.31.8.1.1.5
ipTunnelIfMTUDiscovery	1.3.6.1.4.1.81.31.8.1.1.6
ipTunnelIfMTU	1.3.6.1.4.1.81.31.8.1.1.7
ipTunnellfKeepaliveRate	1.3.6.1.4.1.81.31.8.1.1.8
ipTunnellfKeepaliveRetries	1.3.6.1.4.1.81.31.8.1.1.9

# **Appendix B: ASG authentication**

#### **ASG** authentication CLI commands



#### Note:

ASG is no longer supported from Release 7.1.2 and has been replaced with EASG. ASG authentication file commands can be used if you downgrade to the release previous to Release 7.1.2.

The commands listed in the table manage ASG authentication. For more information about these commands, see Avaya G450 Branch Gateway CLI Reference.

Command	Description		
copy ftp auth-file	Download an ASG authentication file from a remote FTP server		
copy scp auth-file	Download an ASG authentication file from a remote SCP server		
copy tftp auth-file	Download an ASG authentication file from a remote TFTP server		
copy usb auth-file	Download an ASG authentication file from a USB mass storage device		
erase auth-file	Erase the gateway's ASG authentication file		
no login authentication services-logins	Deactivate all Avaya Services logins.		
show auth-file info	Display ASG authentication file information		
show login authentication	Display login authentication settings and information.		
show download auth-file status	Display download status of ASG authentication file, after using copy ftp scp tftp usb auth-file to download an authentication file to the gateway		

## Replacing the ASG authentication file

#### Before you begin

If you need to install an authentication file with a different ID, delete the current authentication file using the erase auth-file command. This command requires Supervisor level access and can be used only when directly connecting to the Console or Services port. You can delete the authentication file and replace it with one that has a new ID. However, you must ensure that the authentication file label on the gateway chassis is replaced.

#### About this task

If there are any problems with the ASG authentication file, you can download a new authentication file from Authentication File System (AFS). You cannot install an authentication file with an authentication file ID different from the authentication file installed on Branch Gateway.



ASG is no longer supported from Release 7.1.2 and has been replaced with EASG. ASG authentication file commands can be used if you downgrade to the release previous to Release 7.1.2.

#### **Procedure**

1. Use the show auth-file info command to view the current ASG authentication file.

#### For example:

```
Gxxx-001(super)# show auth-file info
Authentication File (AF) information:
AF-ID :7000012345
Date/time : 15:02:27 23-AUG-2015
Major release : 6.x
```

2. Use Windows File Explorer or another file management program to create a directory on an FTP, SCP or TFTP server for storing authentication files.

For example, C:\licenses.

- 3. Open Internet Explorer and go to rfa.avaya.com.
- 4. Log in using your SSO login and password.

The AFS and RFA information home page displays.

5. Start the AFS application from the RFA information page.

Follow the instructions outlined in *Authentication File System (AFS) Guide* to create and download the authentication file.

6. Download the authentication file on to Branch Gateway from an FTP, SCP or TFTP server, or a USB mass storage device.

filename contains the name of the authentication file and the path of the file. ip is the IP address of the host. source-usb-device is the source USB mass storage device and source-filename contains the name of the authentication file and the path of the file. Branch Gateway prompts you for a user name and password after you enter the command. To install the authentication file, use one of the following commands:

- copy ftp auth-file filename ip
- copy scp auth-file filename ip
- copy tftp auth-file filename ip

- copy usb auth-file source-usb-device Source-filename
- Auth-files are used in releases prior to Release 7.1.2.
- 7. After the authentication file is downloaded, you can view the download status using the show download auth-file status command.

# Index

A		Auto Route Selection (ARS) Access Code 1	
		automatic failover and failback	
Access Code 2	<u>138</u>	automatically activating ETR	
Access control list		autoneg	
CLI commands		Autonomous System Boundary Router	<u>420</u>
access control list rule specifications		Avaya Aura Communication Manager	
access control lists, see policy	<u>497</u>	accessing	<u>3</u> 4
Access through Services port	<u>32</u>	configuring for SLS	<u>108</u>
access-control-list	<u>245</u>	functions	<u>3</u> 4
Accessing		Avaya Aura <sup>™</sup> Communication Manager	
Avaya Aura Communication Manager	<u>34</u>	configuring for SLS	<u>108</u>
MGC	<u>34</u>	Avaya courses	<u>55</u> 1
via modem	<u>32</u>	Avaya Services	
Accessing Branch Gateway	<u>30</u>	authenticating logins with EASG	<u>58</u>
accessing port matrix	<u>550</u>	Avaya Site Administration	<u>3</u> 4
Active PMI		Avaya support website	<u>552</u>
add nfas-interface	<u>160, 163</u>	Avaya Voice Announcement Manager (VAM)	
add port			
Address Resolution Protocol table	<u>411</u>	В	
Administering Encrypted SRTCP	<u>294</u>	В	
Administering Media encryption		Backing up the Branch Gateway	
administration		using the Branch Gateway USB port	81
fips	535	Backup and Restore of Gateway Configuration	
AES-256	291	backup config usb	
analog telephones	<u>101</u>	backup control for data and VoIP	
analog-test		backup delay	
Announcement files		backup interface	
CLI commands	304	Backup interfaces	
managing and transferring using SCP		CLI commands	
area		dynamic bandwidth reporting	
arp		GRE tunnels as	
ARP table	411	limitations	
changing an entry	413	modem dial backup, Modem dial backup	
CLI commands		modem dial backup, see Modem dial backup	
description	<u>411</u>	overview	
dynamic entries	<u>411</u>	backup mechanism configuration	
static entries		backup peer mechanism	
ARP table entries		Backup service	
arp timeout	413	bandwidth	
ARS		Bandwidth <u>ZZZ, ZZ4,</u>	413, 420
ARS Dial Patterns		dynamic reporting	250
ARS dial patterns data	139	manual adjustment	
ARS FAC		reducing via header compression	
ASG commands		used to calculate Cost	
Associated Signaling		Basic	418
async mode interactive			20
async mode terminal		LAN deployment	
async-limit-string		bc out	
async-reset-modem		be out  Before Enabling or Disabling FIPS Approved Mode	
Authenticating			
Service logins	58	Bit Rate	
authentication		bootfile BOOTP	<u>408</u>
Auto Fallback in SLS			400
	<u></u>	description	<u>400</u>

BOOTP relay	<u>400</u>	CHAP	<u>211</u>
BOOTstrap Protocol		CIR	<u>27</u> 1
see BOOTP	400	cir out	<mark>272</mark>
BPDU	314, 315	Class values in SLS station context	146
Branch Gateway		class-identifier	
documentation	549	clear arp-cache	
Branch Gateway access		clear attendant	
Branch Office 1 configuration		clear bri	
Branch Office 2 configuration		clear capture-buffer	
bri		clear crypto isakmp	
Bridge Protocol Data Units	<u>101</u> , <u>100</u>	clear crypto sa	
see BPDU	314	clear crypto sa all	
Bridges	<u>011</u>	clear crypto sa counters	
direct handshaking	315	clear dial-pattern	
loops		clear ds1	
Broadcast relay	<u>514</u>	clear dynamic-trap-manager	
CLI commands	410	clear extension	
description		clear fac	
directed broadcast forwarding		clear fragment	
NetBIOS rebroadcast	<u>410</u>	clear frame-relay counters	
		clear incoming-routing	
C		clear ip dhcp-client statistics	
		clear ip dhcp-server binding	
cable length long	221	clear ip dhcp-server statistics	
cable length short		clear ip domain statistics	
cablelength long		clear ip route	<u>390</u>
cablelength short		clear ip rtp header-compression	<u>204,</u> <u>206</u>
CAC-BL		clear ip tcp header-compression	<u>204,</u> <u>206</u>
Call admission control	<u>200</u>	clear logging file	<u>191, 199</u>
Dynamic CAC	256	clear logging server	<u>189</u>
Call admission control, see Dynamic CAC		clear mgc list	
Call Type ARS only	<u>200</u>	clear port mirror	
AAR and ARS Digit Analysis Table	110	clear port static-vlan	
call types		clear profile	
• •		clear radius authentication server	
Called Number		clear rmon statistics	
Called Number		clear sig-group	
cancel		clear slot-config	
capture buffer mode		clear ssh-client known-hosts	
capture buffer-mode		clear station	
capture buffer-size		clear survivable-config	
capture filter-group		clear sync interface	
capture interface			
capture max-frame-size		clear tac	
capture start		clear tcp syn-cookies	
capture stop		clear tcp syn-cookies counters	
captured packets		clear trunk-group	
CAS Remote Hold/Answer Hold-Unhold Access	Code <u>138</u>	clear vlan	<u>307</u> , <u>310</u>
CDR, SLS information	<u>106</u>	CLI	
certificate validation	<u>530</u>	accessing from local network	
Challenge Handshake Authentication Protocol .		accessing from remote location	
Changing crypto list parameters		accessing with modem	
Channel Groups		commands	the state of the s
creating	218	contexts	<u>30</u>
illustration		contexts example	<u>31</u>
mapping		FIPS	<u>536</u>
Channel Numbering		listing files	
		managing configuration files	
channel-group	<u>८ 10</u> , <u>८८ 1</u>	0 0 0	

CLI (continued)		Commands (continued)		
managing firmware banks	<u>78</u>	interface dialer	<u>38</u>	83
online help		interface fastethernet, interface configuration	38	83
upgrading firmware using SCP/FTP/TFT	P/HTTPS <u>79</u>	interface loopback		
using to configure the system		interface serial, interface configuration	38	83
viewing device status		interface tunnel		
CLI access using a PC device		interface usb-modem	38	83
CLI output per RTP session		interface vlan	38	83
client identifier		ip address, console port		
client identifiers		ip admin-state		
clock source		ip broadcast-address		
Codec		ip capture-list		
Codecs in SLS	139	ip peer address		
collection		ip rtp compression-connections		
delete	550	ip rtp header-compression		
edit name		ip rtp max-period		
generating PDF	550	ip rtp max-time		
sharing content		ip rtp non-tcp-mode		
command sequence		ip rtp port-range		
Commands		ip tcp compression-connections		
async modem-init-string		ip top header-compression		
async reset-modem		ip-protocol, packet sniffing		
bri		ip-rule, packet sniffing		
capture filter-group		key config-key password-encryption		
capture interface		login authentication local-craft-password		
capture ipsec		login authentication lockout		
capture max-frame-size		login authentication response-time		
capture start		login authentication services-logins		
capture stop		name, packet sniffing		
capture-service		owner, packet sniffing		
clear capture-buffer		ping		
composite-operation, packet sniffing		ppp authentication, ASG authentication		
cookie, capture list		ppp authentication, roosole port		
copy auth-file ftp		ppp chap-secret		
copy auth-file scp		ppp timeout authentication, console port		
copy auth-file tftp		rtp-stat qos-trap-rate-limit		
copy auth-file usb		set logging session, object tracking		
copy capture-file ftp		set mgc list		
copy capture-file scp		set sls		
copy capture-file tftp		show auth-file info		
copy capture-file usb		show auth-file status		
copy ftp auth-file		show capture		
copy running-config startup-config		show capture show capture show capture shows captureshow capture shows capture sh		
copy scp auth-file		show controllers		
copy tftp auth-file		show frame-relay fragment		
		show frame-relay Indymentshow frame-relay Imi		
copy usb auth-file crypto ipsec df-bit		show frame-relay map		
destination-ip, packet sniffing				
		show frame-relay pvc		
dial-pattern		show frame-relay traffic		
ds1		show interfaces, WAN configuration		
dscp, packet sniffing		show in interface		
dscp, policy lists		show in interface hrief		
erase auth-file		show ip interface brief		
fragment, packet sniffing		show login authentication		
icmp		show map-class frame-relay		
incoming-routing		show ppp authentication		
interface console	<u>383</u>	show rtp-stat config	<u>3</u> 4	<u> 20</u>

Commands <i>(continued)</i>	Configuration <i>(continued)</i>
show rtp-stat detailed331	switching <u>306</u>
show rtp-stat sessions331	using GUI applications <u>27</u>
show running-config	using the CLI
show startup-config	WAN ethernet port <u>176</u>
show traffic-shape <u>233</u>	Configuration file
show upload auth-file status <u>609</u>	CLI commands <u>91</u>
show upload status <u>368</u>	Configured PMI <u>61</u>
shutdown, console port <u>213</u>	Connect
sig-group <u>141</u>	Console device
sls	configuring console port to detect213
snmp-server view	console interface26
source-ip, packet sniffing <u>368</u>	Console messages249
speed <u>213</u>	Console port
station <u>141</u>	associating with Dialer interface
tcp destination-port <u>368</u>	CLI commands213
tcp source-port <u>368</u>	configuring for modem use <u>34</u>
timeout absolute	configuring to detect console device
trunk-group <u>141</u>	configuring to detect modem213
tunnel path-mtu-discovery395	connecting modem34
udp destination-port <u>368</u>	description213
udp source-port368	entering interface context
Committed Burst size <u>271</u>	contact closure <u>105</u>
communication methods for agents and managers on	Contact closure
SNMP <u>280</u>	activating when access code dialed
composite operations <u>510</u>	closure modes296
Composite operations	configuring software
adding to IP rule <u>512</u>	deactivating manually <u>296</u>
configuring <u>512</u>	displaying status <u>297</u>
deleting from IP rule <u>512</u>	overview
example <u>512</u>	relay control methods
pre-configured for access control lists <u>510</u>	setting manually <u>296</u>
composite-operation	setting pulse duration
IP rule configuration <u>512</u>	using in SLS mode
composite-operation, access control list <u>516</u>	Contact Closure Close Code
composite-operation, DSCP table <u>513</u> , <u>518</u>	Contact closure configuration
composite-operation, MSS configuration <u>50</u>	CLI commands
composite-operation, QoS list <u>512</u> , <u>518</u>	Contact Closure Open Code
Computer, connecting to fixed router port	Contact Closure Pulse Code
conference call <u>351</u>	content
Configuration	publishing PDF output <u>550</u>
defining an interface <u>59</u>	searching <u>550</u>
DHCP client	sharing <u>550</u>
dynamic trap manager <u>288</u>	sort by last updated <u>550</u>
header compression	watching for updates <u>550</u>
installation and setup <u>26</u>	Contexts <u>30</u>
LLDP <u>183</u>	Contexts example <u>31</u>
managing configuration files <u>91</u>	Continuous channel in VPN456
MGC list <u>65</u>	continuous-channel
modem	controller
primary management interface <u>60</u>	Controller
RTCP <u>201</u>	configuring mode218
RTP <u>201</u>	displaying configuration218
running configuration28	entering context218
saving configuration changes <u>28</u>	cookie, access control list <u>516</u>
startup <u>233</u>	cookie, capture list <u>356</u>
startup configuration <u>28</u>	cookie, policy list <u>501</u>

cookie, QoS list	<u>518</u>	copy usb announcement-file	<u>83</u> , <u>300</u> , <u>304</u>
copy announcement-file ftp	<u>82, 83, 298, 299, 304</u>	copy usb auth-file	<u>83</u> , <u>609</u>
copy announcement-file https	<u>300</u> , <u>301</u>	copy usb modules	<u>83</u>
copy announcement-file scp	<u>82, 83, 298, 304</u>	copy usb phone-image	<u>83</u>
copy announcement-file usb	81, 83, 299, 300, 304	copy usb phone-script	
copy auth-file ftp	<u>82</u> , <u>83</u> , <u>609</u>	copy usb startup-config	<u>83</u> , <u>91</u>
copy auth-file scp		copy usb SW_image	
copy auth-file tftp		copyedge announcement-file scp	
copy auth-file usb		copyedge running-config scp	
copy capture-file ftp		copyedge scp announcement-file	
copy capture-file scp		copyedge scp startup-config	
copy capture-file usb		copyedge startup-config scp	
copy cdr-file ftp		copyedge syslog-file https	
copy cdr-file scp		copying and installing EASG site certi	
copy cdr-file usb		copying EASG site certificate	
copy dhcp-binding ftp		copying and installing EASG site certi	
copy dhcp-binding scp		device	neare deling deb
copy dhcp-binding usb		copying EASG site certificate usi	na ush device 56
copy file usb		cos	_
copy ftp announcement-file		Cost	
copy ftp auth-file		Country Protocol	
copy ftp module		crypto ipsec df-bit	
copy ftp modulecopy ftp startup-config		crypto ipsec minimal pmtu	
copy ftp startup-corning			
., . = -		crypto ipsec minimal-pmtu	
copy ftp SW_imageAcopy ftp SW_imageB		crypto ipsec nat-transparency udp-en- crypto ipsec transform-set	
		• • •	
copy https announcement-file		crypto isakmp invalid-spi-recovery	
copy https startup-config		crypto isakmp nat keepalive	
copy https SW_imageA		crypto isakmp peer	
copy license-file usb		crypto isakmp peer-group	
copy phone-script usb		crypto isakmp policy	
copy running-config ftp		crypto isakmp suggest-key	
copy running-config https		crypto ispec nat-transparency udp-en	
copy running-config scp		crypto ispec transform-set	
copy running-config startup-config		crypto key generate	<u>41, 42</u>
copy running-config tftp		crypto list	
copy scp announcement-file		overview	<u>429</u>
copy scp auth-file		Crypto list	
copy scp startup-config		configuring	
copy scp SW_imageA		deactivating	<u>443</u>
copy startup-config ftp		crypto list parameters	
copy startup-config https	<u>91</u>		<u>444</u>
copy startup-config scp	<u>91</u>	crypto map	<u>439, 478, 484, 492</u>
copy startup-config tftp		Crypto map	
copy startup-config usb	<u>81</u> , <u>83</u> , <u>91</u>	configuring	<u>439</u>
copy syslog-file ftp	<u>190,</u> <u>199</u>	overview	<u>429</u>
copy syslog-file https	<u>190</u>	crypto-group	<u>446</u>
copy syslog-file scp	<u>190</u> , <u>199</u>	cyrpto isakmp policy	<u>433</u>
copy syslog-file tftp			
copy syslog-file usb	<u>81, 83, 190, 199</u>	D	
copy tftp auth-file			
copy tftp module		data and VoIP control backup	467
copy tftp startup-config		Data Link Connection Identifier	
copy tftp sw_imageA		see DLCI	
copy tftp SW_imageA		Date Format on Terminals	
copy tftp SW_imageB		DCP stations data	
copy usb		DCP telephones	
		POI 1010h1101169	<u>10 1</u>

DCP/ANALOG Bearer Capability	132	DHCP client (continued)	
decrypted IPSec VPN packets		CLI logging, enabling	181
Default gateway		CLI logging, setting logging session conditions	
defining	62	CLI logging, viewing	
default sink severity levels		configuring	
default-metric		determining DHCP option requests	
default-router		displaying configuration	
default-routers		displaying parameters	
defining other interfaces	<mark>27</mark>	enabling	
Del	_	interface fastethernet, DHCP client	
AAR Digit Conversion Table	119	ip address dhcp	
ARS Digit Conversion Table		ip dhcp client client-id	
Incoming Call Handling Treatment		ip dhcp client hostname	
Deleting EASG site certificate		ip dhcp client lease	
deleting site certificate	56	ip dhcp client request	
deleting site certificate		ip dhcp client route track	
DeMilitarized Zone	<u>s                                </u>	lease, releasing	
see DMZ	381	lease, renewing	
Denial of Service reporting		maintaining	
Deployments	<u></u>	overview	
basic	23	setting the client identifier	
introduction		setting the client lease	
overview		setting the hostname	
port redundancy		show ip dhcp-client	
RSTP		DHCP Client configuration	
RSTP and switch redundancy		DHCP options	
switch redundancy		DHCP relay	
description, crypto list rule		DHCP server	<u>+00</u>
description, crypto map		CLI commands	408
description, DNS servers list		configuration examples	
description, ISAKMP peer		configuring DHCP options	
description, ISAKMP peer-group		configuring brief options	
description, ISAKMP policy		overview	
description, object tracker		typical application	
description, object trackerdescription, policy rule		Diagnosing	<u>400</u>
destination-ip	<u>500</u>	and monitoring the network	320
packet sniffing	358	Dial On Demand Routing (DDR)	
destination-ip, access control list		dial-pattern	
destination-ip, access control listdestination-ip, crypto list rule		Dialed String	101, 100
destination-ip, MSS configuration		AAR and ARS Digit Analysis Table	110 140
destination-ip, mos configurationdestination-ip, policy list		AAR and ARS Digit Conversion Table	
destination-ip, QoS listdestination-ip, QoS list		dialer interface	
determining		Dialer interface	<u>241</u>
enabled or disabled		activating with object tracking	242
FIPS		as backup for Loopback interface	
Determining Configuration is FIPS Compliant			
Device status	<u>555</u>	as backup for WAN interfaceassigning access control list to	
CLI commands	76		
		assigning to Console port	
viewing	<u>/5</u>	authentication method	
DHCP	400	CHAP authentication	
BOOTP relay		CLI commands	
description	<u>400</u>	configuring	
DHCP and BOOTP relay	404	configuring as backup	
CLI commands	<u>401</u>	configuring backup routing	
DHCP client	470	dynamic IP	
applications		dynamic routing	
CLI commands	<u>181</u>	giving priority to VoIP	<u>236</u>

Dialer interface (continued)		documentation center	<u>550</u>
logging		finding content	<u>550</u>
setting IP address	<u>239</u>	navigation	<u>550</u>
static routing	<u>236</u>	documentation portal	<u>550</u>
unnumbered IP	236, 242, 384	finding content	
verifying connection		navigation	
Dialer Messages		domain-name	
dialer modem-interface		lease	
dialer order		DoS reporting	
dialer persistent		dos-classification	
dialer persistent delay		downloading announcement files	
dialer persistent initial delay		ds-mode	The second secon
dialer persistent max-attempts		ds1	
dialer persistent re-enable		dscp	<u>100</u>
•		•	250
dialer string		packet sniffing DSCP	<u>330</u>
Dialer strings			E10
dialer wait-for-ipcp		as access control list rule criteria	
dir		as policy-based routing rule criteria	
Directed broadcast forwarding		as QoS list rule criteria	
Directory Number		in RTR probes	
disabling EASG	<u>53</u>	in VPN packets	<u>439</u>
disabling EASG authentication		DSCP table	
disabling EASG		Policy	
disabling EASG authentication for a specified	user	DSCP table, see Policy	<u>513</u>
disabling EASG for user	<u>54</u>	dscp-table	<u>513</u> , <u>518</u>
disabling EASG for specified user	<u>54</u>	dscp, access control list	<u>516</u>
disabling FIPS		dscp, object tracking	
administration	542	dscp, QoS list	
Disabling FIPS Approved Mode		duplex	
Discard routes		Dynamic CAC	<u></u>
disconnect ssh		and modem dial backup	236 242
displaying DHCP server information		CLI commands	
Distribution access lists		description	
distribution list		Dynamic CAC tasks	
distribution-list			<u>231</u>
DLCI	<u>417</u>	Dynamic Host Configuration Protocol see DHCP	400
	220		<u>400</u>
configuring for frame relay sub-interface		Dynamic IP	454
OSPF mapping		configuring	
Priority		Dialer interface	
Priority, see Priority DLCI		overview	
DMZ	<u>381</u>	dynamic local peer IP	
DNS resolver		dynamic MTU discovery	<u>395</u>
CLI commands		Dynamic routes	
configuration example	<u>73</u>	redistributing	<u>422</u>
features	<u>70</u>	Dynamic time slots allocation	
maintaining	<u>74</u>	CLI commands	<u>305</u>
overview	<u>70</u>	overview	305
typical application		Dynamic trap manager	
when not necessary		CLI commands	289
DNS servers		configuring	
requesting list of DNS servers during a F	PP/IPCP	dynamic trap manager parameters	
session		dynamic-cac	
requesting list of DNS servers from a DH		ayriairiio-oao	<u>231</u>
		_	
dns-server		E	
document changes	<u>22</u>		
documentation	540	E1/T1 default settings	<u>220</u>
Branch Gateway	<u>549</u>	E1/T1 lines	

Enhanced Access Security Gateway 52 EASG authentication 40, 58 EASG site crifficate information 57 EASG Status enabled or disabled 57 EASG users list 54 EASG users list 55 EASG users list 54 EASG users list 55 EAC data 136 Eailver 526 Eailver 526 Eailver 526 Eailver 526 Eailver 526 Eailver 626 Eail	E1/T1 lines (continued)	ETR (continued)	
Elitrol ports   218	CLI commands	manual activation	<u>278</u>
Elitrol ports   218	connecting to WAN media module	setting state	<u>278</u>
EI/TI ports		trunk-to-port latchings	278
EASG Enhanced Access Security Gateway		· · · · · · · · · · · · · · · · · · ·	
Enhanced Access Security Gateway	EASG		
EASG authentication			
EASG site certificate information			
F		Expansion Wodalo	<u></u>
EASG users list		_	
Echo cancellation   CLI commands   372		F	
CLI commands			
See ETR   See See See See See See See See See S			
ECMP		fail-retries	<u>259, 270</u>
See ETR			
See ETR		failover	<u>526</u>
Part		Fair VoIP queue	<u>208</u>
eadge mode	<del></del>	fair-queue-limit	<u>208</u>
enabling EASG authentication enabling EASG authentication for a specified user enabling EASG authentication for a specified user enabling EASG authentication for a specified user enabling EASG for specified user enabling EASG for specified user enabling FIPS enabling FIPS administration  537 Enabling FIPS Approved Mode encapsulation ppoce encapsulation popoc encapsulation ppoce encapsulation encapsulation ppoce encapsulation encapsulation ppoce encapsulation ppoce encapsulation encapsulati		fair-voip-queue	208
enabling EASG authentication         52           enabling EASG authentication for a specified user         52           enabling EASG for user         54           enabling EASG for user         54           enabling EASG for specified user         54           enabling FIPS         381           administration         537           Enabling FIPS Approved Mode         535           encapsulation ppoc         225, 226, 230, 232           encapsulation ppoe         227, 228           encapsulation ppoe         227, 228           encapsulation ppoe         227, 228           encrypted SRTCP         293           Encrypting gateway secrets         44           encrypting gateway secrets         44           encrypting gateway secrets         44           encrypting gateway (EASG)         52           authentication         403           Enhanced Access Security Gateway         52           Enhanced Access Security Gateway         58           erase auth-file         300, 302, 304           erase auth-file         300, 302, 304           erase auth-file         300, 302, 304           FIPS         54           Ethernet ports         54	<del>-</del>	·	
enabling EASG authentication         52           enabling EASG authentication for a specified user         54           enabling EASG for user         54           enabling EASG for user         54           enabling FIPS         54           administration         537           Enabling FIPS Approved Mode         535           encapsulation         225, 226, 230, 232           encapsulation ppoe         227, 228           encrypted SRTCP         293           Encryptide SRTCP         293           Encrypting gateway secrets         44           end-ip-addr         403, 402           Endpal Init         136           Enhanced Access Security Gateway         52           Enhanced Access Security Gateway (EASG)         344           authentication         58           erase auth-file         300, 302, 304           error states 1         51PS (Federal Information Processing Standards)         531           FIPS         547           Ehernet ports         54           CLI commands         174           configuring switch port         174           configuring switch port         176           Ehrente ports         176		configuring PPPoE	226
enabling EASG authentication for a specified user enabling EASG for user	enabling EASG authentication		
enabling EASG authentication for a specified user enabling FASG for user enabling FASG for specified user enabling FIPS administration Enabling FIPS Approved Mode encapsulation encapsulation 225, 226, 230, 232 encapsulation 225, 226, 230, 232 encrypted SRTCP 233 Encrypted SRTCP 293 Encrypted SRTCP 293 Encrypting gateway secrets 294 encrypting gateway secrets 295 Endpt Init 296 Endpt Init 297 Enabling FIPS ETIPS CLI commands CLI co	enabling EASG <u>52</u>		
enabling EASG for user	enabling EASG authentication for a specified user		
FastEthernet interface   Checking status   Saster   Sas			
enabling FIPS			<u>00 1</u>
Administration			253
Enabling FIPS Approved Mode			
FastEthernet Interface   Security Gateway   Security Gateway (EASG)   authentication   Security Governor states   Security Governor states   Security Governor states   Security Governor states   Security Level of the Cryptographic Module   Security Gateway   Security Level of the Cryptographic Module   Security Gateway   Security Level of the Cryptographic Module   Security Gateway   Security Level of the Cryptographic Module			
described   381		·	<u>255</u>
Encrypted SRTCP   293   Encrypting SRTCP   293   Encrypting SRTCP   293   Encrypting gateway secrets			004
Encrypted SRTCP         293         File transfer           Encrypting gateway secrets         44           encryption         433, 492           end-ip-addr         403, 408           Endpt Init         136           Enhanced Access Security Gateway         52           Enhanced Access Security Gateway (EASG)         58           authentication         58           erase announcement-file         300, 302, 304           erase auth-file         609           error states 1         51           FIPS         547           Ethernet ports         547           CLI commands         174           configuring switch port         174           connecting devices to         173           list of         173           port redundancy         311           WAN Ethernet port         176           Ethernet ports on the router			-
SCP, FTP or TFTP   77   77   77   77   77   77   77			<u>221</u>
encryption			
end-ip-addr			
Endpt Init         136         finding port matrix         550           Enhanced Access Security Gateway         52         FIPS         next hops static routes         388           erase announcement-file         300, 302, 304         FIPS         file         531           erase auth-file         609         FIPS Certified Firmware is Installed         532           error states 1         FIPS         FIPS Certified Firmware is Installed         532           FIPS error states         FIPS ceruity Level of the Cryptographic Module         531           FIPS security Level of the Cryptographic Module         531           Firmware         CLI commands         174           configuring switch port         174         174           configuring switch port         174         175           list of         173         firmware bank defaults         83           firmware banks         29           port redundancy         311         load with ASB button         79           WAN Ethernet port         176         managing firmware banks         29           WAN Ethernet port, see WAN Ethernet port         176         managing firmware banks         29           Ethernet portsor the router         173         port redundancy         78			
Enhanced Access Security Gateway         52         FIPS           Enhanced Access Security Gateway (EASG)         next hops static routes         388           authentication         58         FIPS (Federal Information Processing Standards)         531           erase announcement-file         300, 302, 304         FIPS Approved Mode of Operation         532           error states 1         547         FIPS Certified Firmware is Installed         532           FIPS error states         546         FIPS Security Level of the Cryptographic Module         531           FIPS security Level of the Cryptographic Module         531         Firewall         381           CLI commands         174         connecting devices to         173         Firmware         CLI commands         83           list of         173         Firmware bank defaults         78         Firmware banks         29           budy the port redundancy         311         MAN Ethernet port, see WAN Ethernet port         176         MAN Ethernet port, see WAN Ethernet port         176         MAN Ethernet port so the router         173         Firmware banks         29           Ethernet ports on the router         173         Firmware banks         78         redundancy         78           Upgrading using SCP/FTP/TFTP/HTTPS         79	· · · · · · · · · · · · · · · · · · ·		
Enhanced Access Security Gateway (EASG) authentication 58 erase announcement-file 300, 302, 304 erase auth-file 609 error states 1 FIPS 547 Ethernet ports CLI commands 174 configuring switch port 174 connecting devices to 173 list of 173 port redundancy 311 WAN Ethernet port 174 WAN Ethernet port 175 Ethernet ports 071 Ethernet ports 073 ETR CLI commands 279 deactivating 4000000000000000000000000000000000000		finding port matrix	<u>550</u>
authentication         58           erase announcement-file         300, 302, 304           erase auth-file         609           error states 1         FIPS (Federal Information Processing Standards)         531           FIPS         547           Ethernet ports         547           CLI commands         174           configuring switch port         174           connecting devices to         173           list of         173           port redundancy         311           WAN Ethernet port         176           WAN Ethernet port, see WAN Ethernet port         176           Ethernet ports on the router         173           Ethernet ports on the router         173           Ethernet ports on the router         176           CLI commands         279           deactivating         278           description         278           description         278           firmware versions in the banks displays         78           firmware versions in the banks displays         78		FIPS	
erase announcement-file         300, 302, 304         FIPS Approved Mode of Operation         532           error states 1         FIPS         547           FIPS         547         FIPS Security Level of the Cryptographic Module         531           Ethernet ports         532         FIPS Security Level of the Cryptographic Module         531           CLI commands         174         531           connecting devices to         173         firmware         633           list of         173         firmware bank defaults         78           port redundancy         311         load with ASB button         79           WAN Ethernet port, see WAN Ethernet port         176         managing firmware banks         78           Ethernet ports on the router         173         upgrade overview         78           ETR         upgrading using SCP/FTP/TFTP/HTTPS         79           deactivating         278         version control         29           description         278         versions in the banks displays         78		next hops static routes	<u>388</u>
erase announcement-file         300, 302, 304         FIPS Approved Mode of Operation         532           erase auth-file         609         FIPS Certified Firmware is Installed         532           error states 1         FIPS         547         FIPS error states         546           Ethernet ports         517         FIPS Security Level of the Cryptographic Module         531           CLI commands         174         531           connecting devices to         173         Firmware         CLI commands         83           connecting devices to         173         firmware bank defaults         78           port redundancy         311         load with ASB button         79           WAN Ethernet port         176         managing firmware banks         29           WAN Ethernet port, see WAN Ethernet port         176         managing firmware banks         78           redundancy         78         redundancy         78           Ethernet ports on the router         173         upgrading using SCP/FTP/TFTP/HTTPS         79           Upgrading using USB mass storage device         80           version control         29           description         278           description         278           description		FIPS (Federal Information Processing Standards)	<u>531</u>
erase auth-file         609         FIPS Certified Firmware is Installed         532           error states 1         547         FIPS error states         546           Ethernet ports         FIPS Security Level of the Cryptographic Module         531           CLI commands         174         532           CLI commands         174         531           connecting devices to         173         firmware         609           list of         173         firmware bank defaults         78           firmware banks         29           port redundancy         311         load with ASB button         79           WAN Ethernet port, see WAN Ethernet port         176         managing firmware banks         78           Ethernet ports on the router         173         redundancy         78           ETR         upgrade overview         78           CLI commands         279         upgrading using SCP/FTP/TFTP/HTTPS         79           upgrading using USB mass storage device         80           version control         29           firmware versions in the banks displays         78	erase announcement-file <u>300</u> , <u>302</u> , <u>304</u>		
FIPS         547         FIPS error states         546           Ethernet ports         FIPS Security Level of the Cryptographic Module         531           CLI commands         174         531           connecting devices to         173         Firewall         381           list of         173         firmware bank defaults         78           port redundancy         311         firmware banks         29           WAN Ethernet port         176         managing firmware banks         78           Ethernet ports on the router         173         redundancy         78           Ethernet ports on the router         173         upgrade overview         78           ETR         upgrading using SCP/FTP/TFTP/HTTPS         79           upgrading using USB mass storage device         80           version control         29           firmware versions in the banks displays         78	erase auth-file <u>609</u>		
FIPS	error states 1		
Ethernet ports  CLI commands	FIPS <u>547</u>		
CLI commands	Ethernet ports		
configuring switch port	CLI commands		<u>00 1</u>
connecting devices to			83
list of			
port redundancy 311 WAN Ethernet port 176 WAN Ethernet port, see WAN Ethernet port 176 Ethernet ports on the router 173 ETR CLI commands 279 deactivating 278 description 278  First 279  CLI commands 279 description 278  First 279  CLI commands 279 firmware versions in the banks displays 78			
WAN Ethernet port			
WAN Ethernet port, see WAN Ethernet port			
Ethernet ports on the router			
ETR  CLI commands upgrading using SCP/FTP/TFTP/HTTPS 79  deactivating 278 description 278 firmware versions in the banks displays 78			
CLI commands		upgrade overview	<u>78</u>
deactivating			
description		upgrading using USB mass storage device	<u>80</u>
Illinware versions in the banks displays		version control	<u>29</u>
	•	firmware versions in the banks displays	<u>78</u>
	LED <u>278</u>		

fragment	<u>272</u>	GRE application example	<u>397</u>
fragment chain	<u>426</u>	GRE tunnel	<u>397</u>
fragment size		GRE tunneling	
fragment timeout	426	applications	391
fragment, access control list		checking tunnel status394	
fragment, QoS list		CLI commands	
Fragmentation	<del></del>	compared to VPN	
as map class parameter	271	dynamic bandwidth reporting	
CLI commands		dynamic MTU discovery	
description		optional features	
GRE tunneling		overview381	
Frame relay	<u>000</u>	preventing recursive routing	
displaying configuration	233	routing packets to tunnel	
enabling traffic shaping		group	
Frame relay encapsulation	<u>27 1</u>	GUI tools, configuring the system with	
CLI commands	222	GOI tools, configuring the system with	<u>21</u>
down status			
		Н	
encapsulation types			
establishing Layer 3 interface		hash <u>433</u>	, <u>492</u>
IETF		Header compression	
illustration		clearing rtp header compression statistics	<u>206</u>
non-IETF		clearing tcp header compression statistics	206
supported features		decompression	<u>201</u>
supported on Serial interfaces	<u>215,</u> <u>382</u>	IPCH method - RTP and TCP header compression,	
Frame relay traffic shaping		CLI commands	<u>204</u>
CLI commands		IPCH method - RTP and TCP header compression,	
configuring within map classes		disabling	202
description		IPCH method - RTP and TCP header compression,	
displaying configuration		enabling	202
enabling	<u>271</u>	IPCH method - RTP and TCP header compression,	
frame-relay class-dlci	<u>232</u>	overview	. 202
frame-relay counters	<u>232</u>	IPHC method - RTP and TCP header compression,	
frame-relay interface-dlci	<u>230, 232</u>	configuring UDP ports range	202
frame-relay lmi-n391dte		methods	
frame-relay lmi-n392dte		overview	
frame-relay lmi-n393dte		show ip rtp header-compression	
frame-relay lmi-type		show ip tcp header-compression	
frame-relay priority-dlci-group		showing rtp header compression statistics	
frame-relay traffic-shaping		showing tcp header compression statisticsshowing tcp header compression statistics	
framing		supported methods per interface type	
frequency		transmission rate	
FRF.12 fragmentation		Van Jacobson Method - TCP header compression,	201
configuring within map classes	271		206
description		CLI commands	<u>206</u>
FTP		Van Jacobson Method - TCP header compression,	005
1 11	<u>11</u>	configuring	205
		Van Jacobson Method - TCP header compression,	
G		disabling	<u>205</u>
		Van Jacobson Method - TCP header compression,	
General context		enabling	<u>205</u>
General context example	<u>31</u>	Van Jacobson Method - TCP header compression,	
Generic Routing Encapsulation		overview	
GRE tunneling		help	<u>31</u>
Generic Routing Encapsulation, see GRE	tunneling <u>391</u>	Help	
Gigabit Ethernet port		CLI	
port redundancy	<u>311</u>	commands	<u>31</u>
global parameters	<u>444</u>	High Preference static routes	<u>388</u>
GRE	<u>397</u>	hostname4	1, 42

HTTPS	<u>77</u>	interface fastethernet, DHCP and BOOTP	relay 401
hub-and-spoke with VPN	<u>467</u>	interface fastethernet, DHCP client	<u>181</u>
·		interface fastethernet, PPPoE	
		interface fastethernet, WAN Ethernet port	
1		interface Loopback	
icc-vlan	308 310	interface serial	
ICC-VLAN		E1/T1 ports	<mark>22</mark> 1
configuring		frame relay	
		frame relay traffic shaping	
Configuringicc-vlan		interface Serial	
		interface serial, frame relay	
ICC-VLAN		interface serial, PPP	
icmp		interface serial, USP port	
ICMP errors		Interface status	
CLI commands		CLI commands	371
ICMP keepalive		interface tunnel	
and policy-based routing		interface usb-modem	
CLI commands		interface vlan	
ICMP keepalive feature, enabling		Interfaces	<u>300</u> , <u>310</u>
idle character		adjusting bandwidth	440
idle-character			
IGAR		assigning Cost	
ignore dcd	<u>222,</u> <u>224</u>	assigning IP addresses	
IKE		backup	
phase 1	<u>428</u>	configuration	
phase 2		configuration examples	
incoming call handling data	<u>140</u>	defining	
incoming-routing	<u>162, 163</u>	disabling	
Ingress Access Control List	<u>522</u>	displaying information	
Ingress QoS List	<u>522</u>	displaying status	
initiate mode		dynamic bandwidth reporting	
Insert		fastethernet	
Incoming Call Handling Treatment	<u>141</u>	frame relay	
installing EASG site certificate		GRE tunnel, GRE tunneling	
installing EASG site certificate using usb device		GRE tunnel, see GRE tunneling	
Integrated analog testing		IP	
CLI commands	377	IP, see IP interfaces	<u>382</u>
displaying corrections		Layer 2	
displaying test results		Layer 3	
healing trunks		logical	<u>382</u>
overview		Loopback	<u>381</u> , <u>522</u>
profiles, clearing		physical	
profiles, configuring		Serial	<u>215</u> , <u>382</u>
profiles, displaying		Serial, see Serial interfaces	<u>215</u>
test cancelling		setting load calculation intervals	
test launching		switching	
test lines		testing configuration	
types of tests		USP WAN	
	<u>575</u>	virtual	
Inter-Gateway Alternate Routing IGAR	256	WAN	381
Inter-Gateway Alternate Routing, see IGAR		Internet Key Exchange (IKE)	
Inter-Gateway Alternate Routing, see IGAR Interactions for Encrypted SRTCP		invalid SPI recovery	
		invert txclock	
interface		ip access group	
Interface	<u>131</u> , <u>133</u>	ip access-control-list	
Interface configuration	000	ip access-group	
CLI commands		ip address	
interface console	<u>213, 245</u> 239 245 252	E1/T1 ports	
interface dialer	739 745 757	_ i, i i poito	<u>22</u>

IP address		ip ospf message-digest-key	<u>420</u>
assigning to USB port	<u>27</u>	ip ospf network point-to-multipoint	<u>217</u> , <u>420</u>
defining	<u>382</u>	ip ospf priority	<u>420</u>
obtaining via DHCP	<u>178</u>	ip ospf router-id	
obtaining via PPP/IPCP negotia	tion	ip peer address	<u>212</u>
storing in ARP table		ip policy-list-copy	
ip address dhcp	<u>71, 181</u>	ip proxy-arp	
ip address negotiated	. 227, 228, 239, 252, 454	ip qos-group	503, 518
ip address, dialer interface		ip gos-list	
ip address, E1/T1 ports		ip redirects	
ip address, frame relay		ip rip authentications key	
ip address, interface configuration		ip rip authentications mode	
ip address, PPP		ip rip default-route-mode	
ip address, PPPoE		ip rip poison-reverse	
ip address, USB port		ip rip-version	
ip bootp-dhcp network		ip rip send-receive-mode	
ip bootp-dhcp relay		ip rip split-horizon	
ip bootp-dhcp server		ip route	
ip capture-list		ip routing	
ip crypto list		ip rtp compression-connections	
ip crypto-group		ip rtp header-compression	
ip crypto-list		ip rtp max-period	
ip default-gateway		ip rtp max-time	
ip default-gateway dialer		ip rtp non-tcp-mode	
ip dhcp activate pool		ip rtp port-range	
ip dhop client client-id		ip rule	
ip dhop client hostname		IP Security	
ip dhop client lease		VPN	428
ip dhop client request		IP Security, see VPN	
ip dhop client route track		ip show rule	
ip dhop ping packets		ip simulate	
ip dhcp ping timeout		ip ssh	
ip dhcp pool		IP stations data	
ip dhcp pools		ip tcp compression-connections	
ip dhcp-server		ip tcp header-compression	
ip directed-broadcast		IP telephones	
ip distribution access-default-action .		ip telnet	
ip distribution access-list		ip telnet-client	
ip distribution access-list-cookie		ip telnet-services	
ip distribution access-list-copy		ip unnumbered	
ip distribution access-list-name		IP unnumbered interface configuration	
ip distribution access-list-owner		CLI commands	386
ip domain list		ip vrrp	
ip domain lookup		ip vrrp address	
ip domain name-server-list		ip vrrp auth-key	
ip domain retry		ip vrrp override addr owner	
ip domain timeout		ip vrrp preempt	
ip icmp-errors		ip vrrp primary	
IP interfaces		ip vrrp priority	
ip max-arp-entries		ip vrrp timer	
ip netbios-rebroadcast		ip-fragments-in	
ip netmask-format		ip-option-in	
ip ospf authentication		ip-protocol	<u>000</u> , <u>010</u>
ip ospf authentication-key		packet sniffing	358
ip ospf cost		ip-protocol, access control list	
ip ospf dead-interval		ip-protocol, MSS configuration	
ip ospf hello-interval		ip-protocol, policy list	

ip-protocol, QoS list	<u>518</u>	list rule specification for access control	<u>497</u>
ip-rule, access control list	<u>516</u>	Listing files	<u>92</u>
ip-rule, crypto list	<u>441</u>	LLDP	
ip-rule, MSS configuration	<u>50</u>	802.1 TLVs (optional)	<u>183</u>
ip-rule, packet sniffing		CLI commands	
ip-rule, QoS list		configuration	183
ip-rule, VPN		enabling	
IPSec VPN		mandatory TLVs	
IPSec VPN configuration display		optional TLVs	
IPSec VPN packets decryption		overview	
IPSec VPN, see VPN		setting additional TLVs	
ISAKMP	<u>.==</u>	setting port status	
peer-group configuration	438	supported ports	
policies		supported TLVs	
VPN peer configuration		verify advertisements	
isakmp policy		LMI parameters	
isakmp-policy		Load balancing	<u>200</u>
ITN-C7 Long Timers		ECMP	420
TIN-O7 Long Timers	<u>100</u>	VRRP	
K		load sharing topologies	
		load-interval	
keepalive <u>225</u> – <u>228,</u>	<u>394, 396, 398, 435, 492</u>	local calls between IP and analog telephones	
configuring on PPP WAN line	<u>225</u>	Local Management Interface	
keepalive feature	<u>394</u>	see LMI parameters	
keepalive ICMP		local-address	<u>441, 492</u>
ICMP keepalive	<u>253</u>	Log file	
keepalive ICMP, see ICMP keepalive .	<u>253</u>	see Logging	
keepalive-icmp	<u>254, 255</u>	Log file generation	
keepalive-icmp failure-retries		log file messages	<u>19</u> 1
keepalive-icmp interval		Logging	
keepalive-icmp source-address		CLI commands	
keepalive-icmp success-retries		configuring and enabling the log file	
keepalive-icmp timeout		configuring session log	<u>193</u>
keepalive-track		configuring Syslog server	<u>187</u>
configuring in VPN		copying the Syslog file	<u>190</u>
configuring on PPPoE interface		default severity levels	<u>195</u>
Keepalive, GRE tunnel		defining filters	<u>195</u>
key config-key password-encryption		deleting log file	<u>19</u> 1
key dering key padeword eneryphen	<u>oo</u>	deleting Syslog server	<u>189</u>
_		Dialer interface	247
L		disabling log file	191
	004	disabling session log	
LAN		disabling Syslog server	
launch	<del></del>	displaying log file contents	
Layer 1 Stable		displaying Syslog server status	
Layer 2 interfaces		enabling session log	
Layer 2 logical interfaces	<u>382</u>	enabling Syslog server	
Layer 2 virtual interfaces	<u>381</u>	filtering by application	
Layer 3 interfaces	<u>389</u>	introduction	
lease	<u>403, 408</u>	limiting Syslog access	
LEDs, ETR	<u>278</u>		
legal notice		log file	
lifetime		log file example	
linecode		log file massage formet	
Link Layer Discovery Protocol		log file message format	
LLDP	182	modem dial backup	
Link Layer Discovery Protocol, see LL		object trackers	
I ink-state algorithm	419	object tracking	<u>26</u> 2

Logging (continued)		Master Configuration Key (continued)	
overview	<u>186</u>	configuring	<u>45</u>
RTR	<u>264</u>	Max	
saving settings	186	AAR Digit Conversion Table	119, 140
session log		ARS Digit Conversion Table	
session log example		MCG	
session log message format		CLI commands	69
setting filters		MCK (Master Configuration Key)	
sinks		Media encryption	
specifying Syslog output facility		media encryption using AES 256	
Syslog default settings		media gateway controller	<u>202</u>
Syslog server		setting the list	64
Syslog server example		Media Gateway Controller (MGC)	
		• • • • • • • • • • • • • • • • • • • •	<u>21</u>
Syslog server message format		Media modules	0.0
VPN	<u>448</u>	adding, using a USB mass-storage device	
Logging session	400	MM340 <u>217</u>	
Logging		MM342 <u>217</u>	
Logging session, see Logging		upgrading, using a USB mass-storage device .	
Logical interfaces		USP WAN, MM342 media module	
login authentication		USP WAN, see MM342 media module	
login authentication inactivity-period		WAN	
login authentication lockout		mesh VPN topology configuration	<u>458</u>
login authentication min-password-digit-chars	<u>36</u> , <u>38</u>	Metrics	<u>423</u>
login authentication min-password-length	<u>36,</u> <u>38</u>	MGC	
login authentication min-password-lower-chars	<u>36</u> , <u>38</u>	accessing	<u>3</u> 4
login authentication min-password-special-charge	s 36, 38	accessing the registered MGC	
login authentication min-password-upper-chars		auto fallback to primary	
login authentication password-expire		changing the list	
login authentication response-time		checking connectivity with	
loopback		clearing the list	
loopback activation on an E1/T1 line		displaying the list	
Loopback interface		monitoring the ICC	
loopback remote		monitoring the Survivable Remote Server	
Loops		reporting bandwidth to	
defined	21/	running Avaya Aura Communication Manager	
preventing in GRE tunneling		setting reset times	
		MGC list	<u>01</u>
preventing in RIP			0(
Low preference static routes	<u>388</u>	SLS entry	
		MGC settings	
M		MIB files	<u>566</u>
		Min	440 444
MAC addresses, storing in ARP table	<u>411</u>	AAR Digit Conversion Table	
Maintaining FIPS Approved Mode	<u>535</u>	ARS Digit Conversion Table	<u>119</u> , <u>140</u>
Managed Security Services		MM340 media module	
MSS	47	configuring	
Managed Security Services, see MSS		E1/T1 WAN interface	<u>38</u> 1
map classes		MM342 media module	
configuring		configuring	<u>222</u>
Map classes		USP WAN interface	<u>38</u> 1
applying to all configured Permanent Virtua	al	mode	434, 492
Channels		Modem	
default		configuring	21 <sup>2</sup>
		configuring console port to detect	
number that can be configured		connecting to Console port	
parameters		connecting to CONSOIC PORT	
map-class frame-relay	<u>272</u>	dial backup, Modem dial backup	
Master Configuration Key		dial backup, see Modem dial backup	
CLI commands	<u>47</u>	uiai backup, see wodeni diai backup	<u>230</u>

Modem (continued)		NAT Traversal (continued)	
serial	<u>213</u>	overview	<u>445</u>
USB	<u>211</u>	Nested tunneling	<u>392</u>
Modem dial backup		NetBIOS	<u>410</u>
activating with object tracking	<u>242</u>	network	<u>420</u>
and dynamic CAC	<u>236</u> , <u>242</u>	Network monitoring	
as backup interface		applications	<u>320</u>
authentication method	<u>239</u>	Next hops	<mark>388</mark>
bandwidth available for	<u>236</u>	next-hop	<u>259</u> , <u>270</u>
CHAP authentication	<u>239</u>	next-server	<u>408</u>
configuration example	<u>243</u>	no oob-interface	<u>77</u>
configuring backup routing	<u>239</u>	non-compliant CLI commands	
entering dialer strings	<u>239</u>	FIPS	<u>53</u> 6
feature interactions		nrzi-encoding	222, 224
logging	<u>247</u>	nslookup	
overview		•	,
policy lists and	<u>236</u>	•	
prerequisites		0	
RAS configuration		chicat	262 270
typical installations		object	
using VPN		object tracker	<u>202</u>
Weighted Fair Queuing and		object tracking	000
Monitoring applications	<u>200</u>	configuration workflow	<u>20</u> 2
configuring	320	Object tracking	0.46
MSS	<u>020</u>	activating Dialer interface	
CLI commands	51	applying to DHCP client	
configuring		applying to static routes	
example		backup for the FastEthernet interface	
Overview		CLI commands	
predefined DoS classes		configuration	
		enabling logging	
reporting mechanismuser-defined DoS classes		interface backup using policy-based routing	
		maintenance	
mtu		object tracker configuration	
Multipoint topology support		overview	
mutual	<u>530</u>	RTR configuration	
mutual authentication	F20	verifying MGC connectivity	
authentication		viewing log messages	
My Docs	<u>550</u>	VPN failover	
		oob-interface configuration	<u>76</u>
N		Open Shortest Path First protocol	
		see OSPF	
Name		option	<u>405</u> , <u>408</u>
DS1 Circuit Pack		OSPF	
ISDN BRI Trunk Circuit Pack	<u>135</u>	advertising static routes	
Station	<u>118</u>	CLI commands	<u>420</u>
name server	<u>71</u>	compared to RIP	<u>414</u> , <u>419</u>
name-server	<u>74</u>	default metric	<u>423</u>
name, access control list	<u>516</u>	description	419
name, crypto list	<u>441</u>	DLCI mapping	<u>273</u>
name, DHCP option	<u>405, 408</u>	dynamic Cost	
name, DHCP server		limitations	
name, DHCP vendor specific option		modem dial backup and	
name, packet sniffing		shortest-path-first algorithm	
name, policy list		using with RIP	
name, QoS list		OSPF Autonomous System Boundary Router	
NAT Traversal	<del>,</del>	overview	
configuring	445	edge gateway	62

overview (continued)		packets, simulating, see Policy	<u>515</u>
MGC	<u>62</u>	passive-interfaces	
owner, access control list	<u>516</u>	password	<u>38</u>
owner, packet sniffing	<u>356</u>	Password authentication process	<u>41</u>
owner, policy list	<u>501</u>	Password Authentication Protocol	<u>211</u>
owner, QoS list	<u>518</u>	password changes	<u>37</u>
		Passwords	
D		creating by the admin	<u>36</u>
		disabling	<u>37</u>
Packet sniffing		displaying password information	
analyzing capture file	367	managing	<u>35</u>
analyzing captured packets		managing contents	
applying a capture-list		managing expiry	
applying rules to an address range		managing length	<u>36</u>
applying rules to packets with DSCP values		managing lockout	<u>37</u>
applying rules to packets with ip protocols		overview	<u>35</u>
capture list examples		PBR lists	
clearing the capture buffer		attaching to Loopback interface	
CLI commands		PC device for CLI access	<u>32</u>
configuring		Permanent routes	<u>389</u>
creating capture-list		Permit / Deny	<u>120</u>
defining rule criteria		ping	<u>234</u>
disabling		Ping	<u>233</u>
enabling		pmi	. <u>60</u> , <u>61</u>
enabling the service		PMI	
excepting protocols from rules		CLI commands	<u>61</u>
identifying the interface		configuration	<u>60</u>
information, viewing		entering the interface context	<u>60</u>
overview		explanation	<u>60</u>
packets captured		resetting the interface	<u>60</u>
reducing the size of the capture file		setting location information	<u>60</u>
rule criteria commands		setting system contact information	<u>60</u>
scp file upload limit		setting the system name	<u>60</u>
service, starting		showing the PMI	<u>60</u>
service, stopping		PMI, active and configured	<u>61</u>
setting buffers		pmi6	
setting capture list context		Point to Multi-Point topology	
setting capture list parameters		Point-to-Point frame relay	<u>217</u>
setting max frame size		Poison-reverse	<u>415</u>
settings		policy	
simulating packets		access control lists	<u>497</u>
specifying and excluding ICMP type and code .		network security with access control lists	<u>498</u>
specifying bugger size		simulated packet properties	<u>515</u>
specifying capture actions		simulating packets	<u>515</u>
specifying interfaces		Policy	
streams that always be captured		attaching policy list to interface at IACL	<u>503</u>
streams that can be captured		attaching policy lists to an interface	
streams that can never be captured		attaching QoS list to interface at ingress QoS list .	
uploading capture file		changing DSCP table entries	
uploading capture files to remote servers or US		configuring composite operations	
storage device		copy list	
uploading capture files to the S8300		create access control lost	
		create QoS list	
viewing the captured packet box dump		creating policy lists	
viewing, captured packet hex dump		creating rules	
with conditional capture requirements	<u>354</u>	default actions	
packets, simulating	EAE	defining global rules	
Policy	<u>515</u>	==g giosai i aioo	<u>000</u>

Policy (continued)		Port (continued)	
defining list identification attributes	501	Station	116
defining policy lists		Port classification	
deleting a policy list		CLI commands	319
deleting a QoS list		Ports	
destination port range		Port classification, see Ports	
device wide policy lists		port matrix	
displaying access control lists		Port mirroring	
displaying composite operation lists		CLI commands	31/
displaying composite operation lists		description	
displaying policy lists in DSCP table context		Port redundancy	<u>010</u>
displaying policy lists in DSGF table context		CLI commands	245
displaying policy lists in QoS list context		configuration	
displaying policy lists in QoS list rule context		description	
DSCP as rule criteria		disabling	
DSCP default value		displaying information	
DSCP methods		enabling	
DSCP table		LAN deployment	
edit access control list		secondary port activation	
editing policy lists		setting redundancy-intervals	
editing rules	<u>506</u>	switchback	<u>312</u>
example composite operation	<u>512</u>	port redundancy schemes	<u>312</u>
fragments	<u>509</u>	Ports	
ICMP code	<u>509</u>	alternate	<u>315</u>
ICMP type	509	analog line	<mark>278</mark>
managing policy lists		backup	
mapping DSCP to a CoS		classification	319
modem dial backup and	236	configuring E1 port	
overview		configuring T1 port	
policy lists and loopback interfaces		Fast Ethernet, Fast Ethernet port	
policy-based routing, Policy-based routing		Fast Ethernet, see Fast Ethernet port	
policy-based routing, see Policy-based routing		FastEthernet	
precongifured composite operations		FastEthernet, see Fast Ethernet port	
precongifured for QoS lists		mirroring, see Port mirroring	
QoS fields		opening traffic	
QoS list		redundancy, Port redundancy	
QoS list parts		redundancy, see Port redundancy	
QoS lists		roles in RSTP	
rule criteria		USP, see USP ports	
sequence of device-wide policy list application		USP, USP ports	<u>222</u>
sequence of policy list application		power-up	
simulated packet properties		testing	<u>546</u>
source port range	<u>508</u>	PPP	
specifying a destination ip address	<u>507</u>	as default WAN protocol	<u>217</u>
specifying an ip protocol	<u>506</u>	CLI commands	<u>226</u>
specifying operations	<u>510</u>	configuring on WAN line	<u>225</u>
TCP, establish bit	<u>509</u>	connection	<u>33</u> , <u>34</u>
testing policy lists		establishing Layer 3 interface	
using ip wildcards		supported on Serial interfaces	
Policy-based routing		ppp authentication, USB port	
object tracking and	268	ppp chap hostname	
overview		ppp chap password	
packets not considered router packets		ppp chap refuse	
PBR lists, PBR lists		ppp chap-secret	
PBR lists, see PBR lists		PPP configuration	
routing to GRE tunnel		ppp ipcp dns request	
_	<u>382</u>		
Port		ppp pap refuse	<u>221</u> , <u>228</u>

ppp pap sent username	<u>228</u>	QoS (continued)	
ppp pap sent-username	<u>239</u>	metrics for RTP statistics application	<u>324</u>
ppp pap-sent username	<u>227</u>	policy, Policy	<u>207</u>
PPP protocol and USP ports	<u>216</u>	policy, see Policy	<u>207</u>
ppp timeout authentication	<u>211</u>	Priority DLCI, see Priority DLCI	<u>273</u>
ppp timeout authentication, USB port		Priority Queuing	
ppp timeout ncp		queue sizes for VoIP traffic	
ppp timeout retry	<u>225</u> – <u>228</u>	resolving conflicts	<u>207</u>
PPP VoIP configuration		SNMP traps	
PPP VoIP configuration example		traps in messages file	
PPP/IPCP address negotiation		traps, viewing	
PPPoE		VoIP Queuing	
authentication	227	Weighted Fair VoIP Queuing	
CLI commands		QoS allowed values	
description		QoS list	<u>100</u>
shutting down client		CLI commands	518
pppoe-client persistent delay		queue-limit	
pppoe-client persistent delaypppoe-client persistent max-attempts		Queues	<u>209</u>
			200
pppoe-client service-name		fair packet scheduling	
pppoe-client wait-for-ipcp		Priority	
pre-classification		Priority Queuing	
pre-shared-key		VoIP	
preparing SLS data set		VoIP Queuing	
Prerequisites for entering FIPS Approved Mode		Weighted Fair VoIP Queuing	<u>208</u>
Primary Management IP address (PMI)	<u>27</u>		
Priority DLCI		R	
applying map classes		IX.	
CLI commands	<u>274</u>	RADIUS authentication	35. 42
configuring	<u>230,</u> <u>273</u>	RAS	<u>so</u> , <u></u>
description	<u>273</u>	dialer strings for modem dial backup	245
Priority queueing		modem dial backup and	
CLI commands	<u>209</u>	modem dial backup configuration options	
Priority queuing		modem dial backup prerequisites	
general	271	serving multiple branch offices	
Priority Queuing		redistribute417,	
Priority VoIP queuing			<u>+20, 422, 423</u>
priority-queue		Registration Source Port	00
Privilege levels	<u>200</u> , <u>200</u>	H.248	
creating	36	release dhcp	<u>180</u> , <u>181</u>
description		Remote Access Server	
product-id		RAS	
profile		Remote Access Server, see RAS	
•		remote calls from analog to IP telephones	
protect crypto-map		remote calls from IP telephone to IP telephone	
Protocol Version		Remote services logins	
Proxy ARP		remove nfas-interface	<u>163</u>
CLI commands		remove port	<u>163</u>
PTMP, see Point to Multi-Point topology	<u>217</u>	rename announcement-file	<u>302</u> , <u>304</u>
		renew dhcp	180, 181
Q		Replacement String	
~		AAR Digit Conversion Table	119
QoS		ARS Digit Conversion Table	
analyzing fault and clear trap output	341	reset	
CLI commands		reset and display controller counters	
configuration		reset and display frame-relay counters	
displaying parameters		restore	
fair packet scheduling		restore usb	
fault and clear traps	<u>329</u>	restoring ETR to automatic activation	<u>279</u>

Restoring the Branch Gateway		Router (continued)	
using the Branch Gateway USB port	<u>86</u>	virtual	<u>423</u>
RIP		router ospf <u>245</u> , <u>252</u> , <u>42</u>	20, 423
advertising static routes	<u>387</u>	Router port, connecting to	
CLI commands		router rip4	
compared to OSPF	419	router vrrp	
default metric		Routes	
description		setting route preference	392
distribution access lists		Routing	
limitations		policy based, Policy	499
poison-reverse		policy based, see Policy	
preventing loops		Routing Information Protocol	<u></u>
RIPv1		see RIP	414
RIPv2		routing sources	
split-horizon		Routing table	<u>000</u>
using with OSPF		CLI commands	390
versions supported		deleting static routes	
RIPv1 and RIPv2 differences		description	
RMON	<u>413</u>	RSTP	<u>307</u>
	220		216
agent CLI commands		designating ports as edge portsdisplaying port point-to-point status	
overview			
		displaying the port edge state	
rmon alarm		fast network convergence	
RMON configuration examples		features	
rmon event		LAN deployment	
rmon history		manually configure uplink and backbone ports	
Route redistribution		role of ports	
CLI commands		setting port-to-port admin status	
configuration		RSVP	
description		RTCP	<u>201</u>
metric translation		RTP	
metrics		configuring	
Router		overview	
backup		statistics application functionality	
computing path		viewing configuration thresholds	<u>324</u>
configuration commands		RTP header compression	
configuring BOOTP		Header compression	
configuring broadcast relay		RTP header compression, see Header compression	
configuring DHCP		RTP session data	<u>322</u>
configuring unnumbered ip addresses		RTP statistics	
connecting to fixed router port		CLI commands	<u>352</u>
determining shortest path	<u>419</u>	RTP statistics application	
disabling		configuration and output examples	<u>343</u>
displaying interfaces	<u>385</u>	configuring	<u>323</u>
enabling	<u>380</u>	configuring additional trap destinations	<u>328</u>
features	<u>380</u>	configuring fault and clear traps	329
fragmentation	<u>426</u>	configuring QoS traps	
fragmentation, see Fragmentation	426	display session information	
interfaces		displaying RTP session statistics	
load balancing		displaying VoIP engine RTP statistics	
OSPF Autonomous System Boundary		enabling	
overview		enabling traps	
redundancy		modifying the statistics window	
RIP		QoS metric thresholds	
RIP, see RIP		QoS metrics	
setting the borrowed ip interface		resetting	
unnumbered ip interfaces in table		sample network	
amboroa ip intoriacco in table			<u>U 10</u>

RTP statistics application (continued)		set bearer-capability (bri)	<u>151</u> , <u>163</u>
setting QoS event thresholds	<u>325</u>	set bearer-capability (ds1)	<u>150</u> , <u>163</u>
setting QoS indicator thresholds	<u>325</u>	set bit-rate	<u>147</u> , <u>163</u>
setting the trap rate limiter	<u>330</u>	set boot bank	<u>78</u> , <u>83</u>
statistics summary report output	<u>330</u>	set busy-disconnect	<u>163</u>
viewing configuration		set cbc	
viewing QoS traps in messages file	<u>338</u>	set cbc-parameter	
rtp-stat clear	<u>326,</u> <u>352</u>	set cbc-service-feature	<u>163</u>
rtp-stat event-threshold	<u>325,</u> <u>352</u>	set channel-numbering	
rtp-stat fault		set channel-preferences	<u>153, 163</u>
rtp-stat min-stat-win	<u>328,</u> <u>352</u>	set codeset-display	<u>153</u> , <u>163</u>
rtp-stat qos-trap	<u>328,</u> <u>352</u>	set codeset-national	
rtp-stat qos-trap-rate-limit	<u>330</u> , <u>352</u>	set connect	
rtp-stat service	<u>352</u>	set contact-closure admin	
rtp-stat thresholds		set contact-closure pulse-duration	<u>296,</u> <u>297</u>
rtp-stat-service		set cor	
rtr	<u>259, 270</u>	set country-protocol (bri)	<u>151</u> , <u>163</u>
RTR		set country-protocol (ds1)	<u>147</u> , <u>149</u> , <u>163</u>
Object tracking	<u>259</u>	set crosstalk-destination	<u>374, 377</u>
rtr-schedule	<u>259,</u> <u>270</u>	set crosstalk-port	<u>374,</u> <u>377</u>
RTR, see Object tracking	<u>259</u>	set crosstalk-responder	<u>374,</u> <u>377</u>
running-config startup-config	<u>28, 29</u>	set date-format	<u>142,</u> <u>163</u>
		set delete-digits (dial-pattern)	<u>161</u> , <u>163</u>
S		set delete-digits (incoming-routing)	<u>162,</u> <u>163</u>
3		set deny	<u>161, 163</u>
safe-removal usb	90	set destination	<u>374,</u> <u>377</u>
SCP		set dial	<u>153</u> , <u>163</u>
transferring announcement files using		set digit-handling	<u>153</u> , <u>163</u>
SCP/FTP/TFTP used for upgrades		set digit-treatment	
searching for content		set digits	<u>153</u> , <u>163</u>
Secure Shell protocol		set directory-number-a	<u>151</u> , <u>163</u>
SSH	41	set directory-number-b	
Security	<del>_</del>	set dscp	
DoS attack detection	47	set echo-cancellation analog	
overview	35	set echo-cancellation config analog	
special features		set echo-cancellation config voip	
VLANs		set echo-cancellation voip	
Security Associations (SAs)		set endpoint-init	<u>151,</u> <u>163</u>
Security Code		set etr	<u>278</u>
self-identity		set etr 10 auto	
Serial interfaces		set expansion-module	
configuring encapsulation		set fac	
default encapsulation		set fault-threshold timeslot	<u>305</u>
dynamic bandwidth reporting		set icc-monitoring	
entering context		set incoming-destination	
serial modems		set incoming-dialtone	<u>153</u> , <u>163</u>
server-name		set insert-digits (dial-pattern)	
Services port		set insert-digits (incoming-routing)	
connecting console and PC devices	32	set interface (bri)	
session		set interface (ds1)	
Session log	<del></del>	set interface-companding (bri)	
Logging	193	set interface-companding (ds1)	
Session log, see Logging		set ip-codec-set	
session mgc		set japan-disconnect	
set associated-signaling		set layer 1-stable	
set attendant		set length	
	070 077	set lldn re-init-delay	183 184

set Ildp system-control	<u>183</u> , <u>184</u>	set port point-to-point admin status	<u>174, 316, 318</u>
set lldp tx-delay	<u>183, 184</u>	set port redundancy	<u>312</u> , <u>313</u>
set Ildp tx-hold-multiplier		set port redundancy enable disable	
set lldp tx-interval		set port redundancy-intervals	
set logging file		set port spantree	
set logging file condition		set port spantree cost	
set logging file disable		set port spantree force-protocol-migration	
set logging file enable		set port spantree priority	
set logging file retention		set port speed	
set logging server		set port static-vlan	
set logging server access level		set port trap	
set logging server access-level		set port vlan	
set logging server condition		set port vlan-binding-mode	
set logging server disable		set primary-dchannel	
set logging server disableset logging server enable		set protocol-version	
set logging server enableset logging server facility		set qos bearer	
set logging session		set qos control	
set logging session condition		set gos rtop	
set logging session condition dhcpc		set qos rtcp	
set logging session disable		set qos signal	
set logging session enable		set radius authentication	
set logging session, dialer interface		set radius authentication retry-number	
set logging session, DNS resolver		set radius authentication retry-time	
set logging session, session log		set radius authentication secret	
set logging session, VPN		set radius authentication server	
set long-timer		set radius authentication udp-port	
set match-pattern		set receive-gain	
set max-ip-registrations		set registration source-port-range	
set max-length		set reset-times	
set mediaserver		set responder	
set mgc list		set responder-type	
set min-length		set security-association lifetime	
set mss-notification rate		set security-association lifetime kilobytes	
set name (bri)		set security-association lifetime seconds	
set name (ds1)		set send-name	
set name (station)		set send-number	
set name (trunk-group)		set side (bri)	
set non-oob-interfaces		set side (ds1)	
set numbering-format		set signaling-mode	
set password	<u>144, 163</u>	set slot-config	
set peer		set sls	
set peer group	<u>439</u>	set snmp community	
set peer-group	<u>492</u>	set snmp retries	<u>287</u>
set pfs	<u>434, 492</u>	set snmp timeout	<u>287</u>
set pim-lockout	<u>142, 163</u>	set snmp trap	<u>286</u>
set port	<u>144, 163, 374, 377</u>	set spantree default-path-cost	<u>318</u>
set port auto-negotiation-flowcontrol-adve	ertisement <u>174</u>	set spantree enable/disable	<u>318</u>
set port classification	<u>319</u>	set spantree forward-delay	<u>318</u>
set port duplex		set spantree hello-time	
set port edge admin state		set spantree max-age	
set port flowcontrol		set spantree priority	
set port level		set spantree tx-hold-count	
set port lldp		set spantree version	
set port lldp tlv		set spid-a	
set port mirror		set spid-b	
set port name		set supervision	
set port negotiation		set swhook-flash	

set sync interface	<u>524, 527</u>	show crypto ispsec sa	<u>448</u>
set sync source	<u>524, 525, 527</u>	show crypto map	
set sync switching		show date-format	
set system contact		show dial-pattern	
set system location		show download announcement-file status	
set system name		show download software status	
set tac		show download status	
set tei-assignment		show ds-mode	
set tgnum		show ds1	
set transform-set		show dscp-table	
set transmit-gain		show dynamic-cac	
set trunk		show echo-cancellation	
set trunk-destination		show extension	
set trunk-group-chan-select		show fac	
set trunk-hunt		show fault-threshold timeslot	
		show faults	
set type			
set type (dial-pattern)		show fragment	
set type (station)		show frame-relay fragment	
set utilization cpu		show frame-relay lmi	
set vlan		show frame-relay map	
setting buffer-size	<u>362</u>	show frame-relay pvc	
Setting synchronization		show frame-relay traffic	
Synchronization		show icc-monitoring	
Setting synchronization, see Synchronization .		show icc-vlan	
sharing content		show image version	
show (bri)		show incoming-routing	<u>163</u>
show (dial-pattern)		show interface	<u>212</u>
show (ds1)	<u>147, 163</u>	show interfaces	
show (incoming-routing)	<u>162, 163</u>	frame relay	<u>232</u>
show (profile)	<u>375,</u> <u>377</u>	show interfaces, dialer interface	<u>239,</u> <u>252</u>
show (sig-group)	<u>160</u> , <u>163</u>	show interfaces, frame relay	<u>230</u>
show (station)	<u>144, 163</u>	show interfaces, GRE tunnel	3 <u>98</u>
show (trunk-group)	<u>153</u> , <u>163</u>	show interfaces, interface status	<u>370</u>
show all logs		show interfaces, PPP	225, 226
show announcement-file		show interfaces, unnumbered IP interface	
show announcements-files		show interfaces, VLANs	
show attendant		show interfaces, WAN configuration	
show auth-file info		show ip access-control-list	
show backup status		show ip active-lists	
show boot bank		show ip arp	
show bri		show ip capture-list	
show cam vlan		show ip crypto-list	
show capture-dummy-headers		show ip crypto-list list#	
show composite-operation, access control list		show ip crypto-lists	
show composite-operation, policy list		show ip dhcp-client	
show composite-operation, QoS listshow composite-operation, QoS list		show ip dhop-client statistics	
show contact-closure		show ip dhop-pool	
show controller		show ip dhcp-server bindings	
show controllers			
show controllersshow controllers remote		show in distribution access lists	
		show in domain	
show correction		show ip domain	
show crypto ipsec sa		show ip domain statistics	
show crypto ipsec transform-set		show ip icmp	
show crypto isakmp peer		show ip interfaces	
show crypto isakmp peer-group		show ip ospf	
show crypto isakmp policy		show ip ospf database	
show crypto isakmp sa	448 492	show in osof interface	420

show ip ospf neighbor	420	show ppp authentication	212
show ip ospf protocols		show profile	
· · ·		·	
show ip protocols		show protocol	
show ip qos-list		show protocols	
show ip reverse-arp		show qos-rtcp	
show ip route		show queue	
show ip route best-match	<u>390</u>	show queueing	
show ip route static	<u>390</u>	show radius authentication	
show ip route summary	<u>390</u>	show recovery	<u>68</u> , <u>69</u>
show ip rtp header-compression	<u>204</u>	show restart-log	<u>76</u>
show ip rtp header-compression brief		show restore status	
show ip ssh		show result	
show ip tcp header-compression		show result (profile)	
show ip tcp header-compression brief		show rmon alarm	
show ip telnet		show rmon event	
show ip track-table		show rmon history	
show ip vrrp		show rmon statistics	
show ip-codec-set		show rtp-stat config	
show ip-qos-list		show rtp-stat detailed	
show ip-rule, access control list		show rtp-stat sessions	
show ip-rule, policy list		show rtp-stat summary	
show ip-rule, QoS list		show rtp-stat thresholds	
show keepalive-icmp		show rtp-stat traceroute	
show last-pim-update	<u>163</u>	show rtr configuration	<u>263,</u> <u>270</u>
show list <u>50</u>	<u>1, 514, 516, 518</u>	show rtr operational-state	<u>263</u> , <u>270</u>
show lldp	<u>183</u> , <u>184</u>	show sig-group	<u>163</u>
show Ildp config	<u>184</u>	show slot-config	<u>163</u>
show logging file condition	<u>191, 199</u>	show sls	<u>163</u>
show logging file content	<u>191, 195, 199</u>	show snmp	47, 286, 287, 328
show logging file retention		show snmp engineID	
show logging server condition		show snmp group	
show logging session condition		show snmp retries	
show login authentication		show snmp timeout	
show map-class frame-relay		show snmp user	
show max-ip-registration		show snmp usertogroup	
show mediaserver		show snmp view	
show mg list_config		show spantree	
show mgc		show station	
show mgc list		show sync timing	
show mm		show system	
show module		show tcp syn-cookies	
show oob-interface		show temp	
show pim-lockout		show timeout	
show pmi		show track	
show point-to-point status		show traffic-shape	
show port auto-negotiation-flowcontrol-advert		show trunk	
show port classification		show trunk-group	
show port edge state		show upload announcement-file status	
show port edge status		show upload auth-file status	
		show upload statusshow upload status	
show port lide config		•	
show port lide view name config		show username	
show port lldp vlan-name config		show utilization	
show port mirror		show voltages	
show port point-to-point status		show voltages	
show port redundancy		shutdown	
show port trap		WAN port	
show nort vlan-hinding-mode	310	shutdown PPPoF	777 778

shutdown, USB port <u>21</u>	SLS (continued)	
Side	manual CLI configuration, preparing SLS data set	122
DS1 Circuit Pack	manual CLI configuration, prerequisites	<u>121</u>
sig-group <u>160</u> , <u>16</u>		
signaling groups data <u>13</u>	g preparing SLS data set, analog stations data	122
Signaling Mode <u>13</u>	preparing SLS data set, DS1 trunks data	129
sink severity levels defaults <u>19</u>	preparing SLS data set, ISDN-BRI trunks data	<u>134</u>
site certificates list5	6 provisioning data	<u>97</u>
site-to-site IPSec VPN <u>48</u>	g registered state process	99
SLA monitor	states	98
overview <u>37</u>	8 states, registered	99
sls	states, setup	99
SLS <u>12</u>	states, teardown	. 99
Avaya telephones supported in SLS9		
call processing not supported by SLS9		
call processing supported by SLS9		
capabilities9		
capacities <u>12</u>		105
capacities by Branch Gateway model		
CDR log		
CLI command hierarchy	agent and manager communication methods	280
configuring10		
configuring Avaya Aura <sup>™</sup> Communication Manager	configuration examples	
for SLS <u>10</u>	·	
configuring Communication Manager for SLS		
disabling		
enabling		
entry in MGC list9		
features9		
interaction with, call transfer		
interaction with, contact closure		
interaction with, Direct Inward Dialing		
interaction with, Hold feature		
interaction with, multiple call appearances		
interaction with, shared administrative identity with	potential agent residences	
softphone10		
introduction9		
IP Softphone administration in SLS mode10		
logging10		
manual CLI configuration, administering BRI	user groups	
parameters	· ·	
manual CLI configuration, administering dial-pattern	USM security levels	
parameters		
manual CLI configuration, administering DS1	version 2	
parameters <u>14</u>		
manual CLI configuration, administering incoming-	versions	
routing parameters		_
manual CLI configuration, administering signaling-	SNMP access configuration	
group parameters		287
manual CLI configuration, administering station	SNMP trap configuration	201
parameters14		286
manual CLI configuration, administering trunk-group	snmp trap link-status	
parameters		
manual CLI configuration, command sub-contexts 14		
manual CLI configuration, commands hierarchy 16		
manual CLI configuration, instructions		
manual CLI configuration, introduction		
<u>12</u>		

snmp-server group	<u>47</u> , <u>287</u>	support	<u>552</u>
snmp-server host	<u>47</u> , <u>286</u> , <u>328</u>	Survivability	
snmp-server informs	<u>286</u>	auto fallback to primary MGC	<u>63</u>
snmp-server remote-user	<u>287</u>	configuring the MGC list	<u>65</u>
snmp-server user	<u>47</u> , <u>283</u> , <u>287</u>	connection preserving migration	<u>63</u>
snmp-server view		ELS	<u>63</u>
Software		enhanced local survivability, ELS	<u>63</u>
Firmware	29	enhanced local survivability, see ELS	
Software, see Firmware	<mark>29</mark>	MGC list	
sort documents by last updated		modem dial-backup	
source-address		options	
source-ip		overview	
packet sniffing	358	setting reset times	
source-ip, access control list		SLS, see SLS	
source-ip, crypto list rule		SLS, SLS	
source-ip, policy list		Survivable COR	
source-ip, QoS list		Survivable GK Node Name	
Spanning tree		Survivable Trunk Dest	
CLI commands	318	Switch	<u></u>
configuration		connecting to fixed router port	173
disabling		displaying configuration	
examples		interface	
•			<u>301</u> , <u>302</u>
protocol		Switch ports	174
speed		configuring	<u>174</u>
speed, USB port		Switch redundancy	04.05
SPI recovery		LAN deployment	
SPID		Switchback	
Split-horizon	<u>415</u>	Switchhook Flash	<u>118</u>
SSH		Switching	000
configuration		configuring	
overview	<u>41</u>	interface	<u>381</u> , <u>382</u>
Standard Local Survivability		SYN attacks protection	
SLS		SYN cookies	
Standard Local Survivability, see SLS		SYN attacks protection, see SYN cookies	
start-ip-addr		SYN cookies	
static ARP table entries	<u>412</u>	attack notification	
Static routes		configuring	
advertising		introduction	<u>45</u>
applying object tracking	<u>387</u> , <u>388</u>	overview	
configuring next hops	<u>388</u>	strategies employed	<u>45</u>
deleting		SYN flood attack protection	
description	<u>387</u>		<u>45</u>
discard route	<u>390</u>	SYN flood attack protection, see SYN cookies	<u>45</u>
dropping packets to	<u>390</u>	Synchronization	
High Preference	<u>388</u>	CLI commands	<u>527</u>
inactive		defining a stratum clock source	524
IP addressed next hops	389	disassociating specified primary or secondar	
load-balancing		source	
Low Preference		displaying synchronization timing	
permanent		LED status	
redistributing to RIP and OSPF		overview	
types		setting interface	
via interface		setting the sync source	
station		toggling sync source switching	
subnet-mask		Syslog server	<u>020</u>
success-retries		see Logging	187
suggest-key		system parameters data	
	<u>+55</u> , <u>+32</u>	System parameters data	<u>130</u>

T	trunk-group	
	tunnel checksum	
tcp destination-port <u>359,</u> <u>508,</u> <u>516,</u> <u>5</u>		<u>396</u> , <u>398</u>
tcp established <u>509</u> , <u>5</u>		
TCP header compression	tunnel key	
Header compression2		
TCP header compression, see Header compression2		
tcp source-port <u>359</u> , <u>508</u> , <u>516</u> , <u>5</u>		
tcp syn-cookies <u>46</u> ,		<u>259</u> , <u>270</u>
TCP/IP connection33,		
Telephones supported in SLS mode		<u>111</u>
telnet	. <u>44</u>	
Telnet	24 U	
accessing gateway via33,	, <u>34</u>	
enabling and disabling access		
TFTP	ilcader compression	
threshold count		<u>359</u> , <u>508</u> , <u>516</u> , <u>518</u>
time constants, configuring	uup 30u100-port	<u>359</u> , <u>508</u> , <u>516</u> , <u>518</u>
Time slots, mapping		
timeout absolute	FIFS	<u>537</u>
timers basic4	Official interface	
timers spf4	Configurity	
TLS Certificate Stores		<u>236, 242</u>
TLS certificates5	examples	
TLVs	feature overview	
802.1 (optional)	11 Todang table	
mandatory	upgrade using OOI /I II / II II	<u>79</u>
optional	102	
supported1 Tools	OVCI VICW	
for monitoring3	upgrading firmware	<u>80</u>
VMON	OOD mass-storage device	
traceroute	backing up the branch Gateway	
track	070	
track list	nestoring the Dianon Gateway	
track rtr		
Traffic marking	00D port	
Traffic shaping	assigning ir address	
activating on frame relay interface2	CLI commands	
displaying configuration	oon garing for modelin dee	
DLCI	oon connecting modern	
enabling on frame relay interface	acidat parametere	
per Virtual Channel	074	
WAN Ethernet port	476	
traffic-shape rate176, 1	477	
training	50tting authoritioation motifod	<u>211</u>
Transform-sets	User accounts  CLI commands	20
overview4	420	
VPN, defining4	424	The second secon
transmitter-delay222, 2	224	
trap manager parameters	700	<u>41</u>
traps	0001 11011100	26
TRK port	Greating	
see Fixed analog trunk port2	user privilege changes 278 username	
Trunk Group1		<u>30</u>
trunk group data collection1		25
Trunk Group for Channel Selection 1	managing	
•	OVCI VICVV	<u>33</u>

USP default settings	224	VLANs (continued)	
USP port and PPP protocol		overview	306
USP ports		setting the VLAN	306
CLI commands	224	setting vlan 2 example	
configuring	2 <u>22</u>	switching interface	
illustration		table	
USP WAN lines	2 <u>215</u>	tagging	<mark>306</mark>
default settings	<u>222</u>	VLMS	415
USP WAN media module		VMON, for troubleshooting QoS	<u>322</u>
MM342 media module	<u>222</u>	VoIP	
USP WAN media module, see MM342 media modul	e <u>222</u>	assigning to unique Virtual Channel	<u>273</u>
		available transmission protocols	<u>201</u>
V		enabling queuing	<u>207</u>
V		fair packet scheduling	<u>208</u>
validation	530	overview	<u>201</u>
value		PPP configuration example	<u>274</u>
VAM	<i>,</i>	priority over Dialer interface	<u>236</u>
vendor-specific-option		queue delay	
via interface static routes		queue size	<u>207</u>
videos		RSVP protocol	<mark>207</mark>
viewing available EASG users list	<u>552</u>	VoIP queuing	
EASG users list	54	Weighted Fair VoIP Queuing	
viewing EASG product certificate information	<u>54</u>	VoIP Queuing	
EASG product certificate information	55	voip-queue	
viewing EASG status	<u>55</u>	voip-queue-delay	
EASG status	57	VPN	
viewing product id	<u>57</u>	activating	
product id	57	assigning an access control list	
viewing valid EASG site certificate information		basic parameters	
	<u>57</u>	clearing VPN data	
viewing valid EASG site certificates list viewing valid sites certificates list	56	CLI commands	
Virtual Channels	<u>50</u>	commands summary	· · · · · · · · · · · · · · · · · · ·
	271	components and relationships	
applying map classes		components overview	
assigning by QoS leveldescribed		configuration, overview	
Virtual interface		configuration, procedure	
Virtual Private Network	<u>30 1</u>	continuous channel	
see VPN	201	coordinating with the VPN peer	
VPN		crypto list, assigning to an interface	
VPNVirtual Private Network, see VPN		crypto list, configuring	
Virtual Private Network, see VPNVirtual router		crypto list, deactivating	
	<u>423</u>	crypto list, overview	
Virtual Router Redundancy Protocol	400	crypto map, configuring	
VRRP		crypto map, overview	
Virtual Router Redundancy Protocol, see VRRP		failover mechanisms	
Vlan 1	<u>30 1</u>	introduction	
VLANs	207	ISAKMP policies, configuring	
binding modes		ISAKMP policies, overview	
clearing the VLAN table		logging	
CLI commands		maintenance	
configuration examples		modem dial backup and	
description		NAT Traversal	
DHCP/BOOTP requests		object tracking for failover	
displaying the VLAN table		peer-group, configuring	
dynamic bandwidth reporting		peer-group, corniguringpeer-group, overview	
ICC-VLAN		peer, configuring	
ingress security		peer, corniguring	
multi VLAN binding	307	peei, uvei view	<u>428</u>

VPN (continued)	WFVQ (continued)	
show status448	Weighted Fair VoIP Queuing	208
simple VPN topology449	WFVQ, see Weighted Fair VoIP Queuing	
site-to-site configuration		
transform-sets, configuring434	7	
transform-sets, overview	Z	
typical failover applications, failover using a peer-	zeroization	
group	error state1	E 1.7
typical failover applications, failover using DNS478	status	
typical failover applications, failover using GRE472	Status	<u>541</u>
typical failover applications, failover using object-		
tracking483		
typical failover applications, overview471		
typical installations, configuring dynamic IP		
typical installations, enabling continuous channel 456		
typical installations, full or partial mesh		
typical installations, full solution466		
typical installations, hub and spokes installation 449		
VPN hub redundancy474		
VPN hub-and-spoke		
VPN topology		
VRRP		
CLI commands425		
configuration example424		
description		
· —		
W		
VV		
wait-interval259, 270		
WAN		
checking interface status253		
default encapsulation225		
default protocol217		
Dialer interface as backup236		
dynamic bandwidth reporting256		
features		
ICMP keepalive		
initial configuration217		
interfaces <u>381</u>		
overview		
PPP <u>217</u>		
PPP configuration225		
testing configuration		
testing configuration, CLI commands		
WAN endpoint device		
connecting to fixed router port		
WAN Ethernet port		
backup interfaces <u>177</u>		
configuring <u>176</u>		
traffic shaping <u>176</u>		
WAN Ethernet port feature configuration		
WAN Ethernet ports		
CLI commands		
watch list <u>550</u>		
Weighted Fair VoIP Queuing		
WFVQ		
CLI commands		