Administration for the Avaya G430 Branch Gateway

Release 6.2
03-603228
Issue 3.0
December 2012

© 2012 Avaya Inc.

All Rights Reserved.

Notice

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

Warranty

Avaya provides a limited warranty on its hardware and Software ("Product(s)"). Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this Product while under warranty is available to Avaya customers and other parties through the Avaya Support website: http://support.avaya.com. Please note that if you acquired the Product(s) from an authorized Avaya reseller outside of the United States and Canada, the warranty is provided to you by said Avaya reseller and not by Avaya. "Software" means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products or pre-installed on hardware products, and any upgrades, updates, bug fixes, or modified versions.

Third Party Components

"Third Party Components" mean certain software programs or portions thereof included in the Software that 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"). 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 Documentation or on Avaya's website at: http://support.avaya.com/Copyright. You agree to the Third Party Terms for any such Third Party Components.

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: http://support.avaya.com. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Documentation disclaimer

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

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked 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, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AUTHORIZED AVAYA RESELLER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED AVAYA RESELLER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA AUTHORIZED RESELLER; AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE ("AVAYA").

Avaya grants you a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to you. "Designated Processor" means a single stand-alone computing device. "Server" means a Designated Processor that hosts a software application to be accessed by multiple users.

License types

- Designated System(s) License (DS). End User may install and use each copy 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, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.
- Concurrent User License (CU). End User may install and use the Software on multiple Designated Processors or one or more Servers, so long as only the licensed number of Units are accessing and using the Software at any given time. A "Unit" means the unit on which Avaya, at its sole discretion, bases the pricing of its licenses and can be, without limitation, an agent, port or user, an e-mail or voice mail account in the name of a person or corporate function (e.g., webmaster or helpdesk), or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software. Units may be linked to a specific, identified Server.
- Database License (DL). End User may install and use each copy of the Software on one Server or on multiple Servers provided that each of the Servers on which the Software is installed communicates with no more than a single instance of the same database.
- CPU License (CP). End User may install and use each copy of the Software on a number of Servers up to the number indicated

in the order provided that the performance capacity of the Server(s) does not exceed the performance capacity specified for the Software. End User may not re-install or operate the Software on Server(s) with a larger performance capacity without Avaya's prior consent and payment of an upgrade fee.

- Named User License (NU). You may: (i) install and use the Software on a single Designated Processor or Server per authorized Named User (defined below); or (ii) install and use the Software on a Server so long as only authorized Named Users access and use the Software. "Named User", means a user or device that has been expressly authorized by Avaya to access and use the Software. At Avaya's sole discretion, a "Named User" may be, without limitation, designated by name, corporate function (e.g., webmaster or helpdesk), an e-mail or voice mail account in the name of a person or corporate function, or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software.
- Shrinkwrap License (SR). You may install and use the Software in accordance with the terms and conditions of the applicable license agreements, such as "shrinkwrap" or "clickthrough" license accompanying or applicable to the Software ("Shrinkwrap License").

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 currently available for license from Avaya is the software contained within the list of Heritage Nortel Products located at http://support.avaya.com/LicenseInfo under the link "Heritage Nortel Products". 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 (in the event the applicable Documentation permits installation on non-Avaya equipment) 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, or hardware provided by Avaya. All content on this site, the documentation and the Product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

How to Get Help

For additional support telephone numbers, go to the Avaya support Website: http://www.avaya.com/support. 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 60950-1 latest edition, including all relevant national deviations as listed in the IECEE Bulletin—Product Category OFF: IT and Office Equipment.
- CAN/CSA-C22.2 No. 60950-1 / UL 60950-1 latest edition.

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 22, including all national standards based on CISPR 22.
- CISPR 24, including all national standards based on CISPR 24.
- 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:

1. 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
2. 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:

Manufacturer'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 interface	04DU9.BN	6.0F	RJ48C, RJ48M
	04DU9.1KN	6.0F	RJ48C, RJ48M
	04DU9.1SN	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 on the following Web site: http://support.avaya.com/DoC.

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 Radio and Telecommunications Terminal Equipment Directive (1999/5/EC), including the Electromagnetic Compatibility Directive (2004/108/EC) and Low Voltage Directive (2006/95/EC).

Copies of these Declarations of Conformity (DoCs) can be obtained by contacting your local sales representative and are available on the following Web site: http://support.avaya.com/DoC.

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

Avaya is a registered trademark of Avaya Inc.

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

Downloading Documentation

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

Contact Avaya Support

See the Avaya Support website: http://support.avaya.com for product notices and articles, or to report a problem with your Avaya product. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: http://support.avaya.com, scroll to the bottom of the page, and select Contact Avaya Support.

Contents

Chapter 1: Introduction 13
- Purpose 13
- Intended audience 13
- Related resources 13
  - Documentation 13
  - Training 14
  - Avaya Mentor videos 15
- Support 15
- Warranty 15

Chapter 2: Supported LAN deployments 17
- Supported LAN deployments 17
  - Basic configuration 17
  - Port redundancy configuration 17
  - Port and switch redundancy configuration 18
  - RSTP configuration 18
  - RSTP and switch redundancy configuration 19

Chapter 3: Configuration overview 21
- Configuration overview 21
  - About defining the Services interface 21
  - Defining the USB-modem interface 22
  - Other interfaces 22
  - Configuration using CLI 23
  - Configuration using GUI applications 23
  - Configuration changes and backups 24
  - Firmware version control 25

Chapter 4: Accessing the Branch Gateway 27
- Accessing the Gateway 27
  - CLI access 27
- PIM access 32
- Avaya Aura® Communication Manager access 33
- Security overview 33
  - Login permissions 34
  - User account management 34
  - Service logins with ASG authentication 39
  - SSH protocol support 45
  - SCP protocol support 47
  - RADIUS authentication 48
- Special security features 50
  - The recovery password 50
  - Commands used to configure Telnet access 50
  - Gateway secret management 51
  - DoS attacks 52
  - Managed Security Services 55

Chapter 5: Basic device configuration 63

Basic device configuration 63
Defining an interface 63
Primary Management Interface (PMI) configuration 64
Example of defining a default gateway 67
Branch Gateway Controller configuration 67
DNS resolver 74
Device status viewing 81
Software and firmware management 83
Chapter 6: Standard Local Survivability (SLS) 101
Standard Local Survivability (SLS) 101
Media module compatibility with SLS 102
SLS features 102
Avaya telephones supported in SLS 103
Call processing functionality in SLS mode 104
Call processing functionality not supported by SLS 105
Provisioning data 106
PIM configuration data 107
SLS entry 107
SLS interaction with specific Branch Gateway features 109
SLS logging activities 116
SLS configuration 118
Chapter 7: Ethernet ports 199
Switch Ethernet port configuration 199
Ethernet ports on the Branch Gateway switch 199
Ethernet ports on the Branch Gateway router 199
Cables used for connecting devices to the fixed router 199
Roadmap for configuring switch Ethernet ports 200
Summary of switch Ethernet port configuration CLI commands 200
Configuring the WAN Ethernet port 202
DHCP client configuration 204
LLDP configuration 209
Chapter 8: System logging 215
System logging 215
Types of logging sinks 216
Syslog server configuration 216
Configuring a log file 220
Configuring a session log 223
Logging filter configuration 224
Summary of logging configuration CLI commands 229
Chapter 9: VoIP QoS 231
VoIP QoS 231
RTP and RTCP configuration 231
Header compression configuration 232
Commands used to configure QoS parameters 238
Weighted Fair VoIP Queuing 240
Priority queuing 242
Chapter 10: Modems and the Branch Gateway 245

Modems and the Branch Gateway ... 245
USB-modem interface configuration ... 245
Chapter 11: WAN interfaces ... 249
WAN interfaces ... 249
Configuring the initial WAN ... 249
WAN configuration and testing connectivity ... 253
Modem dial backup logging messages ... 269
Chapter 12: Emergency Transfer Relay (ETR) ... 297
Emergency Transfer Relay (ETR) ... 297
ETR state configuration ... 297
Summary of ETR commands ... 298
Chapter 13: SNMP ... 301
SNMP ... 301
Agent and manager communication ... 302
SNMP versions ... 302
SNMP trap configuration ... 307
Dynamic trap manager ... 311
SNMP configuration examples ... 312
Chapter 14: Contact closure ... 315
Contact closure ... 315
Configuring contact closure hardware ... 315
Software contact closure ... 316
Chapter 15: Announcement files ... 319
Announcement files ... 319
Announcement file operations ... 319
Chapter 16: Advanced switching ... 325
Advanced switching ... 325
VLAN configuration ... 325
Port redundancy ... 331
Port mirroring ... 334
Spanning tree ... 336
Port classification ... 341
Chapter 17: Monitoring applications ... 343
Monitoring applications ... 343
RMON ... 343
RTP statistics ... 346
Packet sniffing ... 380
Interface status reports ... 400
CNA test plugs ... 401
Echo cancellation ... 408
Integrated analog testing – Test and Heal ... 409
Service Level Agreement Monitor Agent ... 417
Chapter 18: The router ... 419
The router ... 419
Enabling and disabling the router ... 420
Interface configuration ... 420
Unnumbered IP interfaces ... 424

Routing sources ... 427
Routing table configuration ... 428
GRE tunneling ... 432
DHCP and BOOTP relay ... 442
DHCP server ... 445
Broadcast relay ... 454
ARP table ... 456
Proxy ARP ... 459
ICMP errors ... 459
RIP ... 460
OSPF ... 466
Route redistribution ... 470
VRRP ... 472
Fragmentation ... 475
Chapter 19: IPSec VPN ... 477
IPSec VPN ... 477
Overview of IPSec VPN configuration ... 478
Typical failover applications ... 526
Chapter 20: Policy lists ... 553
Policy lists ... 553
Types of policy lists ... 553
Policy list management ... 556
Policy list configuration ... 557
Policy list attachments ... 560
Device-wide policy lists ... 563
Defining global rules ... 563
Policy rule configuration ... 564
Composite operations ... 570
DSCP table ... 573
Policy list displays and tests ... 575
Summary of access control list commands ... 577
Summary of QoS list commands ... 579
Chapter 21: Policy-based routing ... 583
Policy-based routing ... 583
Applications for policy-based routing ... 584
Setting up policy-based routing ... 585
PBR rules ... 588
Next hop lists ... 590
Editing and deleting PBR lists ... 592
PBR list commands in context ... 593
Policy-based routing application example ... 594
Summary of policy-based routing commands ... 597
Chapter 22: Synchronization ... 601
Synchronization ... 601
Defining a stratum clock source ... 601
Setting the syncronization source ... 602
Disassociating a clock source ... 603

Enabling and disabling automatic failover and failback 603
Synchronization status 603
Appendix A: Traps and MIBs 607
Traps and MIBs 607
Branch Gateway traps 607
Branch Gateway MIB files 616
Index 669

Chapter 1: Introduction

Purpose

This book describes the procedure used in administering Branch Gateway.

Intended audience

The information in this book is intended for use by Avaya technicians, provisioning specialists, Business Partners, and customers.

Related resources

Documentation

Title	Description	Number
Installation		
Quick Start for Hardware Installation for the Avaya Branch Gateway G430	A concise installation guide covering assembly and basic configuration of the *G430*	03-603236
Installing and Upgrading the Avaya Branch Gateway G430	Describes how to install and upgrade the *G430*, prepare the *G430* for software configuration, and perform some basic configurations. This guide describes how to insert media modules and connect external devices to the *G4350* and media module ports.	03-603233
Administration		

Title	Description	Number
Administration for the Avaya Branch Gateway G430	Describes how to configure and manage the G430 after it is already installed. This guide contains detailed information about all the features of the G450 and how to implement them.	03-603228
Avaya Branch Gateway G430 CLI Reference	Describes the commands in the G430 CLI.	03-603234
Maintenance		
Maintenance Alarms for Avaya Aura® Communication Manager, Branch Gateways and Servers	Describes MOs and how to resolve alarms.	03-300430
Maintenance Commands for Avaya Aura® Communication Manager, Branch Gateways and Servers	Describes all the commands across platforms.	03-300431
Maintenance Procedures for Avaya Aura® Communication Manager, Branch Gateways and Servers	Describes maintenance procedures such as network recovery	03-300432
Implementation		
Operations Intelligence Suite Advanced Implementation Guide for SLA Mon	Describes installation and Configuration of Service Level Agreement Monitor	100167328

Training

The following courses are available on https://www.avaya-learning.com. To search for the course, in the **Search** field, enter the course code and click **Go** .

Course code	Course title
ATC00838VEN	Avaya Media Servers and Gateways Implementation Workshop
AVA00821H00	Avaya CM Architecture and Gateways: H.248, H.323, and Proprietary

Avaya Mentor videos

Avaya Mentor is an Avaya-run channel on YouTube that includes technical content on how to install, configure, and troubleshoot Avaya products.

Visit http://www.youtube.com/AvayaMentor 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.
- Click the name of a playlist to scroll through the posted videos.

Support

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

Warranty

Avaya provides a 90-day limited warranty on Branch Gateway. To understand the terms of the limited warranty, see the sales agreement or other applicable documentation. In addition, the standard warranty of Avaya and the details regarding support for Branch Gateway in the warranty period is available on the Avaya Support website at https://support.avaya.com under **Help & Policies> Policies & Legal > Warranty & Product Lifecycle**. See also **Help & Policies > Policies & Legal > License Terms**.

Chapter 2: Supported LAN deployments

Supported LAN deployments

Related topics:

Basic configuration on page 17
Port redundancy configuration on page 17
Port and switch redundancy configuration on page 18
RSTP configuration on page 18
RSTP and switch redundancy configuration on page 19

Basic configuration

The Branch Gateway can be deployed in the LAN with a basic configuration that includes no redundancy. The Branch Gateway is connected to an external LAN switch using one of the two Ethernet LAN ports located on the Gateway's front panel.



Figure 1: Basic LAN deployment

Port redundancy configuration

The Branch Gateway can be deployed in the LAN using port redundancy to provide redundancy. The Branch Gateway is connected to an external LAN switch using both of the Ethernet LAN ports located on the Gateway's front panel.

One of the Ethernet LAN ports is configured to be the active primary link, and the other Ethernet LAN port is configured to be on standby (disabled). For information on configuring the Ethernet LAN ports in a port redundancy pair, refer to Port redundancy on page 331.

When the Gateway senses a link down failure on the primary port, it automatically enables the secondary link. Both ports need to be administratively enabled on the LAN switch peer.

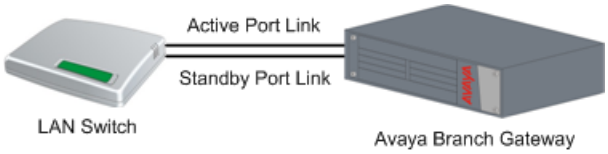


Figure 2: Port redundancy LAN deployment

Port and switch redundancy configuration

The Branch Gateway can be deployed in the LAN using port and switch redundancy to provide redundancy. The Branch Gateway is connected to two external LAN switches. Each of the Ethernet LAN ports located on the Branch Gateway's front panel is connected to one of the switches.

One of the Ethernet LAN ports is configured to be the active primary link, and the other Ethernet LAN port is configured to be on standby (disabled). For information on configuring the Ethernet LAN ports in a port redundancy pair, refer to Port redundancy on page 331.

When the Branch Gateway senses a link down failure on the primary port or failure of the switch to which the primary link is attached, it automatically enables the secondary link to the backup switch. Both ports need to be administratively enabled on their respective LAN switch peers.

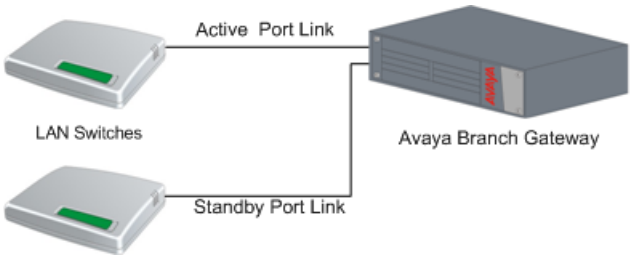


Figure 3: Port and switch redundancy LAN deployment

RSTP configuration

The Branch Gateway can be deployed in the LAN using RSTP to provide redundancy. The Branch Gateway is connected to an external LAN switch using both of the Ethernet LAN ports located on the Branch Gateway's front panel.

Spanning tree protocol blocks one of the links from the 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. For information on configuring spanning tree on the Ethernet LAN ports, refer to Spanning tree on page 336.

When the Branch Gateway senses a link down failure on the active port, it automatically enables the second link. Both ports need to be administratively enabled on the LAN switch peer.

The advantage of fast RSTP over port redundancy is that it controls the link state based on the best LAN topology using the links' cost. However, an RSTP convergence time penalty is incurred.

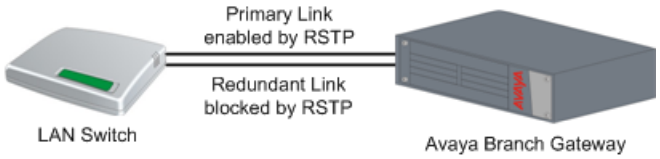


Figure 4: RSTP LAN deployment

RSTP and switch redundancy configuration

The Branch Gateway can be deployed in the LAN using RSTP and switch redundancy to provide redundancy. The Branch Gateway is connected to two external LAN switches. Each of the Ethernet LAN ports located on the Branch Gateway's front panel is connected to one of the switches.

Spanning tree protocol blocks one of the links from the 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. For information on configuring spanning tree on the Ethernet LAN ports, refer to Spanning tree on page 336.

When the Branch Gateway senses a link down failure on the active port or failure of the switch to which the active link is attached, it automatically enables the blocked link to the backup switch. Both ports need to be administratively enabled on the LAN switch peer.

The advantage of fast RSTP over port redundancy is that it controls the link state based on the best LAN topology using the links' cost. However, an RSTP convergence time penalty is incurred.

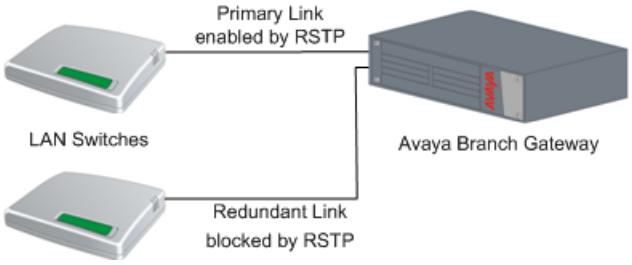


Figure 5: RSTP and switch redundancy LAN deployment

Chapter 3: Configuration overview

Configuration overview

A new Branch Gateway comes with default configuration settings. There are certain items that you must configure, according to your system specifications, before using the Branch Gateway. Configuration of other items depends on the specifications of your network.

A new Branch Gateway has two physical interfaces for management. These are the Services interface and the USB-modem interface.

You must also ensure that the Branch Gateway is properly configured for whichever methods you intend to use for accessing the Branch Gateway. For information on accessing the Branch Gateway, see Accessing the Branch Gateway on page 27.

Related topics:

About defining the Services interface on page 21
Defining the USB-modem interface on page 22
Other interfaces on page 22
Configuration using CLI on page 23
Configuration using GUI applications on page 23
Configuration changes and backups on page 24
Firmware version control on page 25

About defining the Services interface

No configuration of the Services interface is necessary. The Services interface has the fixed IP address 192.11.13.6. However, the console device you connect to the Services port requires a specific configuration of its network settings, as explained in Accessing the gateway through the Services port on page 30.

Defining the USB-modem interface

About this task

If you intend to use a USB modem to connect to the Branch Gateway, you should also assign an IP address to the USB-modem interface. It is not necessary to include a subnet mask.

Procedure

1. Enter **`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 assigns an IP address of 10.3.3.2 to 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 for 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 that the Branch Gateway uses to identify itself 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 the PMI. You can use any interface as the PMI. The PMI can be IPv4 (PMI4) or IPv6 (PMI6).

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.

For more information, see Defining an interface on page 63

Related topics:

Defining other interfaces on page 23

Defining other interfaces

Most Gateway configuration tasks are performed using the Branch Gateway CLI. Avaya also provides several GUI applications that are designed to perform the basic configuration tasks described in this section. Use the following steps to define your other interfaces.

1. Define a Primary Management IP address (PMI).
2. Register the Branch Gateway with an MGC.

Once you have performed these steps, the Branch Gateway is ready for use. Other configuration tasks may also have to be performed, but these steps depend on the individual specifications of your Branch Gateway and your network.

Related topics

- Configuration using GUI applications on page 23
- Primary Management Interface (PMI) configuration on page 64
- Gateway Controller configuration on page 67

Configuration using CLI

You can use the Branch Gateway CLI to manage the Branch Gateway. The CLI is a command prompt interface that enables you to type commands and view responses. For instructions on how to access the Branch Gateway CLI, see Methods to access the CLI on page 28.

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 the *Avaya Branch Gateway G430 CLI Reference*.

Configuration using GUI applications

Several Avaya GUI applications enable you to perform some configuration tasks on the Branch Gateway. Use these applications whenever possible, particularly for initial installation and provisioning.

Related topics:

The PIM on page 24
The Avaya Gxxx Manager on page 24

The PIM

The Avaya Provisioning and Installation Manager (PIM) is an application that allows the user to perform initial installation and provisioning of multiple Branch Gateway Gateways. It provides integrated network system views that ease centralized configuration tasks, especially provisioning and installing large numbers of Branch Gateways simultaneously. One of the primary functions of PIM is to provision and configure Standard Local Survivability (SLS). For instructions on how to access PIM, see PIM access on page 32. For instructions on configuring SLS, see Standard Local Survivability (SLS) on page 101.

The Avaya Gxxx Manager

You can also use the Avaya Gxxx Manager to configure most features of the Branch Gateway. The Avaya Gxxx Manager is a GUI application. You can access the Avaya Gxxx Manager from Avaya Integrated Management software or from a web browser. Most of the commands that are available through the Branch Gateway CLI are also available through the Avaya Gxxx Manager.

Note:

The Avaya Gxxx Manager supports SNMP over IPv4 only and only presents IPv4 information.

For more information about the Avaya G430 Manager, see *Avaya Integrated Management G430 Device Manager User Guide*.

Configuration changes and backups

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

- Running configuration
- Startup configuration

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

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.

Related topics:

Saving configuration changes and backing them up on page 25

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`**
   A copy of the running configuration becomes the new startup configuration.
2. Back up either the running configuration or the startup configuration to an FTP, TFTP or SCP server on your network, or to a USB flash drive.
   For more information, see Configuration file backup and restore on page 98

Firmware version control

Firmware is the software that runs the Branch Gateway. 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 redundancy of firmware. You can save an old version of the firmware in case you need to use it later. This is particularly important when uploading new versions.

Related topic

Software and firmware upgrades on page 83

Related topics:

Using an older firmware version on page 26

Using an older firmware version

About this task

Use this procedure if it becomes necessary to use an older firmware version.

Procedure

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

Chapter 4: Accessing the Branch Gateway

Accessing the Gateway

You can access the Branch Gateway using the CLI, the PIM, and the Avaya Aura® Communication Manager. You can manage login permissions by using and configuring usernames and passwords, and by configuring the Branch Gateway to use RADIUS authentication. There are special security features that enable and disable the recovery password, establish incoming and outgoing Telnet connections, and configure SYN cookies for preventing SYN attacks.

Related topics:

CLI access on page 27

CLI access

The CLI is a textual command prompt interface that you can use to configure the Branch Gateway and media modules.

Related topics:

Methods to access the CLI on page 28
Logging into the CLI on page 28
Disconnecting a Telnet session on page 28
CLI contexts on page 28
Using CLI help on page 29
CLI access using the local network on page 30
CLI access using a PC device on page 30
CLI access using modems on page 31
Accessing the CLI using a USB modem on page 31
The USB port settings on page 32

Methods to access the CLI

Methods to access the CLI include:

- SSH (Secure Shell) that enables you to establish a secure remote session over the network, Services port, or dial in modem (PPP). SSH is enabled by default.
- Telnet through the network, Services port, or dial in modem (PPP). Telnet is disabled by default.
- An SSH connection through a SAL Gateway to the S8300, then a Telnet connection to the gateway using IP address 127.1.1.11.

If the Branch Gateway is under service contract with Avaya Services, remote service providers can connect remotely to service the Branch Gateway with Telnet and SSH sessions. For higher security, you can configure the Branch Gateway to authenticate remote service logins using Access Security Gateway (ASG) authentication instead of password authentication.

Logging into the CLI

Procedure

1. Log in to the CLI with a username and password that your system administrator provides.
2. Use RADIUS authentication if your network has a RADIUS server.
   For more information, see Login permissions on page 34.

Disconnecting a Telnet session

About this task

If the normal Telnet logout does not work, disconnect a Telnet session by typing **<Ctrl>** +**]**

CLI contexts

The CLI is divided into various contexts from which sets of related commands can be entered. Contexts are nested in a hierarchy, with each context accessible from another context, called the parent context. The top level of the CLI tree is called the general context. Each command has a context in which the command must be used. You can only use a command in its proper context.

Related topics:

CLI contexts example on page 29

CLI contexts example

About this task

The following task provides an example of CLI contexts by describing how to configure the Loopback interface:

Procedure

1. Enter the Loopback interface context from general context.

   You can enter the Loopback interface context using the **`interface loopback 1`** command. Once you are in the Loopback interface context, you can enter Loopback interface commands.

2. Use the **`tree`** command to view the available commands in each context.

Using CLI help

About this task

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

Procedure

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

Specifically:

- To display a list of all commands in the current context that begin with this word or words type **`help`** or **`?`** before or after the first word or words of a command.

  For example, to display a list of IP commands available in general context, enter **`help ip`**, **`ip help`**, **`? ip`**, or **`ip ?`**.

- To display the command's syntax and parameters, and an example of the command type **`help`** or **`?`** before or after a full command.

  You must be in the command's context in order to use the **`help`** command to display information about the command.

Example

Example: In the following example, the user enters the vlan 1 interface context and displays help for 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

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

CLI access using a PC device

To access the CLI with a PC device, connect a PC device to the Services port.

Related topics:

Accessing the gateway through the Services port on page 30

Accessing the gateway through the Services port

Procedure

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

   Note:

   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 an equivalent, you will need to restore these entries to connect to other networks.
4. Configure the Internet browser settings of the PC device to disable the proxy server.
5. SSH to 192.11.13.6.

Result

Note:

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

CLI access using modems

You can use any standard SSH or Telnet program to access the CLI from a remote location. This is done by using a dialup PPP network connection from a modem at the remote location. You can use a USB modem connected to the USB port on the front panel of the Branch Gateway.

For more information, see Disconnecting a Telnet session on page 28.

Accessing the CLI using a USB modem

Procedure

1. Connect a modem to the USB port on the front panel of the Branch Gateway.

   Use a USB cable to connect the modem. The Branch Gateway supports the Multitech MultiModem USB MT5634ZBA-USB-V92, and the USRobotics USB modem model 5637.

2. Make sure the USB port is properly configured for modem use.

   For details, see USB-modem interface configuration on page 245.

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 RAS authentication. If your network has a RADIUS server, you can use RADIUS authentication for the PPP connection. For more information, see Login permissions on page 34.

4. Open any standard SSH/Telnet program on the remote computer.

   Note:

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

5. Open an SSH/Telnet session to the IP address of the USB port on the Branch Gateway.

To set the IP address of the USB port (i.e., the USB-modem interface), use the **`ip address`** command. For a list of similar commands, see Summary of CLI commands for configuring the USB port for modem use on page 246.

6. Configure the serial connection on the remote computer to match the configuration of the USB port on the Branch Gateway.

   For more information, see The USB port settings on page 328.

The USB port settings

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

PIM access

The Provisioning and Installation Manager (PIM) enables you to remotely configure devices, primarily Branch Gateways on a network-wide basis. PIM provides integrated network system views that ease centralized configuration tasks, especially provisioning and installing large numbers of gateways simultaneously.

One of PIM's primary functions is to provision and configure Standard Local Survivability (SLS) on the Branch Gateway. See Standard Local Survivability (SLS) on page 101.

PIM is launched from the Avaya Network Management Console. The Avaya Network Management Console is the central infrastructure application that discovers and monitors enabled network devices and runs Avaya Integrated Management applications.

PIM must be installed on the same Windows server as Avaya Network Management Console with System View and Avaya Secure Access Administration.

For detailed information about installing and launching PIM, see *Avaya Integrated Management Enterprise Network Management Installation and Upgrade*.

Avaya Aura® Communication Manager access

Note:

Avaya Site Administration (ASA) supports IPv6.

Use Avaya Aura® Communication Manager software to control telephone services that the Gateway provides. Run the Avaya Aura® Communication Manager software on a server. There might be several servers on your network that can control the Gateway. Access Avaya Aura® Communication Manager on any server that is a Media Gateway Controller (MGC) for the Gateway. For more information, see Media Gateway Controller configuration on page 67.

Access Avaya Aura® Communication Manager with any of the following tools:

Avaya Site Administration (ASA): ASA provides wizards and other tools that help you to use Avaya Aura® Communication Manager effectively. For more information, see *Administrator Guide for Avaya Aura® Communication Manager* .

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

Gateway CLI: See Accessing the registered MGC on page 72.

Security overview

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

In addition to its basic security mechanism, the Gateway supports secure data transfer via SSH and SCP.

The Gateway can be configured to work with an external RADIUS server to provide user authentication. When RADIUS authentication is enabled on the Gateway, the RADIUS server operates in conjunction with the Gateway security mechanism. When the user enters a username, the Gateway first searches its own database for the username. If the Gateway does not find the username in its own database, it establishes a connection with the RADIUS server, and the RADIUS server provides the necessary authentication services.

Related topics:

Login permissions on page 34
User account management on page 34
Service logins with ASG authentication on page 39

SSH protocol support on page 45
SCP protocol support on page 47
RADIUS authentication on page 48

Login permissions

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

User account management

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

- When you access the CLI. For more information, see Methods to access the CLI on page 28.
- When you access the CLI using a modem with dialup PPP. For more information, see CLI access using modems on page 31.
- When you open Avaya Gxxx Manager.

You can configure various password parameters to enhance your system security. Some parameters control password length and content, and some control lockout and expiry policies.

When you use Avaya Gxxx Manager or the CLI, your username determines 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 RADIUS authentication instead of a username and password. A RADIUS server provides centralized authentication service for many devices on a network.

Related topics:

Privilege level on page 35
Creating a username, password, and privledge level on page 35
Changing user privledges on page 36
Commands used for password length and contents on page 36
Commands used to manage password lockout and disabling on page 36
Password expiry management on page 37
Changing a password on page 37
Commands used to display user account information on page 37
User accounts CLI commands on page 38

Privilege level

When you open the Avaya Gxxx Manager or access CLI, you must enter a username. The username 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: You can use the Read-only privilege level to view configuration parameters.

Read-write: You can use the Read-write privilege level to view and change all configuration parameters except those related to security. For example, you cannot change a password with Read-write privilege level.

Admin: You can use Admin privilege level to view and change all configuration parameters, including parameters related to security. Use Admin privilege level only when you need to change configuration that is related to security, such as adding new user accounts and setting the device policy manager source.

The default username has the Admin privilege level. For security reasons, the network administrator usually changes the password of the default username. For more information about privilege levels, see *Avaya G430 CLI Reference*.

Creating a username, password, and privledge level

About this task

When you create a new user, you must define the user password and privilege level. 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*> **`password`** <*password for user*> **`access-type`** <*access type*>

Example

```
Gxxx-001(super)# username john password john7Long access-type read-write
```

Changing user privledges

About this task

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

Procedure

1. At the command prompt, type:
   no username <*the username*>
2. At the command prompt, type **username** <*the username*> **password** <*password for user*> **access-type** <*access type*>
   Example:

```
Gxxx-001(super)# username john password john7Long access-type read-write
```

Commands used for password length and contents

Use the following commands to control password length and the characters it must include:

- **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**

For more information about these commands, see User accounts CLI commands on page 38 or *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. Disabling an account is a strong measure since it requires administrator intervention to re-enable the account. An administrator must run the **username** command and re-configure 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 more information about these commands, see User accounts CLI commands on page 38 .

For information about parameters and default settings, see *Avaya G430 CLI Reference*.

Password expiry management

You can force all passwords to expire within a certain period of time after they were created. Accounts with expired passwords are locked and require an administrator to reset the account using the **username** command. However, a user can change the password before it 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 a password expiration policy is in effect, then starting from 10 days before password expiration, a warning appears every time you log on, informing you 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 **copy running-config startup-config** so that the new password takes effect.

Result

The new password you enter must match the password policies described in User accounts CLI commands on page 38.

Commands used to display user account information

- **show username**
- **show login authentication**

For more information about these commands, see User accounts CLI commands on page 38 .

For a full description of the commands and their output fields, see *Avaya G430 CLI Reference*.

User accounts CLI commands

All of the following commands manage user accounts. For more information about these commands, see *Avaya G430 CLI Reference*.

Command	Description
login authentication inactivity-period	Disable a local user account after an inactivity period of 2-365 days.
login authentication lockout	Lockout or disable a local user account after successive failed login attempts You can configure the lockout period to between 30-3600 seconds. Both the lockout and the disabling policies go into effect after a configured 1-10 successive failed login attempts.
login authentication min-password-digit-chars	Set the minimum number of digit characters that a password must contain
login authentication min-password-length	Set the minimum password length The minimum password length must be at least as great as 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 non-alphanumeric characters except for white characters (blank or tab), and a double quote ("), which is ascii character 34. The default is 0 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
password	Change the password of a user account

Command	Description
show login authentication	View the login authentication settings and information This includes information on 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

Service logins with ASG authentication

The gateway supports ASG authentication for remote service logins. Direct remote connection of services to the gateway is needed for gateways that are under service contract, do not have LSPs, and are controlled by external MGCs. ASG is a more secure authentication method than password authentication and does not require a static password.

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

ASG authentication is supported for remote services connecting to the gateway using Telnet or SSH protocols via any of the following:

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

When ASG authentication is enabled on the Gateway, the Gateway recognizes any login attempts using Avaya Services reserved usernames as service logins, and requests ASG authentication from the user, instead of a static user password.

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

When ASG authentication is enabled on the Gateway, all password user accounts with usernames similar to the reserved service logins are deactivated.

Related topics:

Enabling ASG authentication on page 40
Replacing the ASG authentication file on page 40
Examples of configuring ASG authentication on page 41

Examples for displaying ASG authentication information on page 43
ASG authentication CLI commands on page 43

Enabling ASG authentication

About this task

ASG authentication can be enabled and disabled on the Branch Gateway and requires an ASG authentication file. The ASG authentication file contains Avaya Services accounts for authenticating users at login as members of Avaya Services. The Branch Gateway is shipped with an ASG authentication file. For information about replacing the authentication file, refer to Replacing the ASG authentication file on page 40.

Procedure

1. For connection to Avaya Services using a modem dial-up, enable the RASaccess operation mode for modem operation using **`ppp authentication ras`**. The Branch Gateway must also be configured for remote modem access and enabled, as described in *Installing and Upgrading the Avaya Branch Gateway G430*.
2. For connection to Avaya Services using embedded VPN service, set up the VPN service for Services to connect.

Note:

By default, Avaya Services login access is enabled. If Avaya Services login access was blocked using **`no login authentication services-logins`**, you can reactivate it using **`login authentication services-logins`**.

Replacing the ASG authentication file

Before you begin

If there is a need to install an authentication file with a different ID, first delete the current authentication file using the command **`erase auth-file`**. This command requires Supervisor level access and can be used only when directly connecting to the Services port. If you do delete the authentication file and replace it with an authentication file with a new ID, the authentication file label on the gateway chassis must also be replaced.

About this task

In case of any problems with the ASG authentication file, you can download a newer authentication file from the Authentication File System (AFS). You cannot install an authentication file with a different authentication file ID to that of the authentication file currently installed in the gateway.

Procedure

1. Optionally display the current ASG authentication file version, using the **`show auth-file info`** command.
   For example:

   ```
   Gxxx-001(super)# show auth-file info
   Authentication File (AF) information:
   AF-ID :7000012345
   Date/time : 15:02:27 27-SEP-2005
   Major release : 4
   ```

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. Access the Internet and go to rfa.avaya.com.
4. Login using your SSO login and password.
   The AFS and RFA information home page appears.
5. Start the AFS application from the RFA information page.
   Follow the instructions outlined in the *Authentication File System (AFS) Guide* to create and download the authentication file.
6. Download the authentication file from an FTP, SCP or TFTP server or USB mass storage device to the Branch Gateway.
   The *filename* is the name of the authentication file, including the full path and *ip* is the IP address of the host. The **`source-usb-device`** is the source USB mass storage device and **`source-filename`** is the full name and path of the authentication file. The gateway prompts you for a username 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*
7. After the authentication file is downloaded, you can view the download status using **`show download auth-file status`**.

Examples of configuring ASG authentication

You can perform the following ASG configurations:

- Block Avaya Services login access, using **`no login authentication services-logins`**. This deactivates all Avaya Services logins, including local craft password-based

authenticated login. To reactivate, use **login authentication services-logins**.

- Set the time the gateway waits for user response to authentication requests before timing out a connection, using **login authentication response-time time**, where **time** is the time, in seconds, after which the gateway aborts the connection if no response is received.

  For example, to timeout connections if no response arrives within 180 seconds after an authentication request:

  ```
  Gxxx-001(super)# login authentication response-time 180
  ```

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

  - The response time interval between the username prompt and the username entry
  - The response time interval between the challenge prompt and the challenge response

- Deactivate password authentication and activate ASG authentication of Avaya Services local connections to the Services port. To do this, use **no login authentication local-craft-password**. To enable password authentication of Avaya Services local connections to the Services port, use **login authentication local-craft-password** (default).

- Set a policy for locking out access to the gateway after successive failed login attempts. To do this, use **login authentication lockout time attempt count**, where **time** is the interval of time for which lockout is enforced and **count** is a number of failed attempts after which lockout is enforced. Use **no login authentication lockout** to return the lockout time and lockout attempt threshold to their default values (180 and 3).

  For example, to lockout Avaya Services access to the device for 360 seconds following five failed login attempts:

  ```
  Gxxx-001(super)# login authentication lockout 360 attempt 5
  ```

  This lockout affects all users locally stored in the gateway, including locally defined user accounts and Avaya Services logins defined in the ASG authentication file. Remote users maintained centrally in a Radius server are not subject to the lockout sanction.

- Switch between modem operation modes, including rasaccess and ppp modes, using **ppp authentication {pap|chap|none|ras}**. ASG authentication is enabled when **ras** is selected. For example:

  ```
  Gxxx-001(super)# ppp authentication ras
  ```

Examples for displaying ASG authentication information

Procedure

1. Display login authentication settings and information, using **`show login authentication`**.
   For example:

```
Gxxx-001
(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
```

2. Display ASG authentication file information, using **`show auth-file info`**.
   For example:

```
Gxxx-001
(super)# show auth-file info
Authentication File (AF) information:
AF-ID :7000012345
Date/time : 15:02:27 27-SEP-2005
Major release : 4
```

3. Display all locally defined user accounts, including services accounts and account type information such as authentication method, using **`show username`**.
   For example:

```
Gxxx-001
(super)# show username
User account   Access level  Account type  Active  Authent. method
-----------  -----------   ----------     -----   --------------
sroot          dev          Services      yes      challenge
init           dev          Services      yes      challenge
inads          tech         Services      yes      challenge
craft          admin        Services      yes      challenge
dadmin         admin        local         yes      challenge
rasaccess      read-only    Services      yes      challenge
root           admin        local         yes      password
```

ASG authentication CLI commands

All of the following commands manage ASG authentication. For more information about these commands, see *Avaya G430 Branch Gateway CLI Reference*.

Command	Description
`copy auth-file ftp`	Upload the authentication file from the gateway to an FTP server

Command	Description
copy auth-file scp	Upload the authentication file from the gateway to an SCP server
copy auth-file tftp	Upload the authentication file from the gateway to a TFTP server
copy auth-file usb	Upload the authentication file from the gateway to a USB mass storage device
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
login authentication local-craft-password	Enable password authentication of Avaya Services local connections to the Services port with the "craft" login.
no login authentication local-craft-password	Disable password authentication. When password authentication is disabled, ASG authentication is activated.
login authentication response-time	Set the time the gateway waits for user response to authentication requests before timing out a connection
login authentication lockout	Set a policy for locking out access to the gateway after successive failed login attempts
login authentication services-logins	Activate all Avaya Services logins, including local login to the Services port with "craft" login.
no login authentication services-logins	Deactivate all Avaya Services logins.
ppp authentication	Set modem operation mode. Setting the mode to ras enables ASG authentication for Avaya Services remote logins through dial-up modem connection.
show auth-file info	Display ASG authentication file 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

Command	Description
show login authentication	Display login authentication settings and information
show upload auth-file status	Display upload status of ASG authentication file, after using **copy auth-file ftp|scp|tftp** to upload an authentication file from the gateway

SSH protocol support

Secure Shell (SSH) protocol is a security protocol that enables you to establish a remote session over a secured tunnel, also called a remote shell. 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 SCP file transfers. The Branch Gateway supports two concurrent SSH users.

Establishing an SSH session can be done by RSA authentication, or password authentication. To determine which of these ways is used on your Branch Gateway, enter **show ip ssh**.

Note:

SSH supports IPv4 and IPv6.

Related topics:

RSA authentication process on page 45
Password authentication process on page 46
Enabling SSH on the Gateway on page 46
Disabling SSH on the Gateway on page 46
Summary of SSH configuration commands on page 47

RSA authentication process

1. The Branch Gateway generates a key of variable length (512-2048 bits) using the DSA encryption method. This is the private key.
2. The Branch Gateway calculates an MD5 hash of the private key, called the public key (also called a fingerprint). The public key is always 16 bytes long. This public key is displayed.
3. The Branch Gateway sends the public key to the client computer. This public key is used by the client to encrypt the data it sends to the Branch Gateway. The Branch Gateway decrypts the data using the private key.
4. Both sides negotiate and must agree on the same chipper type. The Branch Gateway only supports 3DES-CBC encryption. The user on the client side accepts

the public key. The client maintains a cache containing a list of fingerprints per server IP address. If the information in this cache changes, the client notifies the user.

5. The client chooses a random number that is used to encrypt and decrypt the information sent.
6. This random number is sent to the Branch Gateway, after encryption based on the Branch Gateway's public key.
7. When the Branch Gateway receives the encrypted random number, it decrypts it using the private key. This random number is now used with the 3DES-CBC encryption method for all encryption and decryption of data. The public and private keys are no longer used.

Password authentication process

Before any data is transferred, the Branch Gateway requires the client to supply a username and password. This authenticates the user on the client side to the Branch Gateway.

Enabling SSH on the Gateway

About this task

To execute the SSH protocol, first assign the hostname identification.

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 dsa** command to generate an SSH host key pair.
3. Enter **ip ssh** to enable SSH authentication.
   SSH is enabled by default.

Disabling SSH on the 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 SSH configuration information and information about any active SSH sessions.

Summary of SSH configuration commands

For more information about these commands, see the *Avaya Branch Gateway G430 CLI Reference*.

Command	Description
crypto key generate dsa	Generate an SSH host key pair
disconnect ssh	Disconnect an existing SSH session
hostname	Assign hostname identification to the Branch Gateway
ip ssh	Enable or disable the Secure Shell (SSH) service
show ip ssh	Display general SSH information and information about the currently active connections that are using SSH

SCP protocol support

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

The process of establishing an SCP session is the same process as described in SSH protocol support on page 45, except that the roles of the Branch Gateway and the client computer are reversed.

To perform file transfers secured by SCP, the Branch Gateway launches a local SSH client using the CLI. This establishes a secured channel to the secured file server. The Branch Gateway authenticates itself to the server by providing a username and password. With a Windows-based SSH server (WinSSHD), the username 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.

Related topics:

Clearing the SSH of known host file content on page 48

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 http://www.avaya.com/support, and search for the document *Avaya RADIUS Configuration Overview*.

Related topics:

Using RADIUS authentication on page 48
RADIUS authentication configuration commands on page 49

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 the *Avaya Branch Gateway G430 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 enable and disable the recovery password, establish incoming and outgoing Telnet connections, copy gateway configurations while keeping configuration secrets, and configure SYN cookies for preventing SYN attacks.

Related topics:

The recovery password on page 50
Commands used to configure Telnet access on page 50
Gateway secret management on page 51
DoS attacks on page 52
Managed Security Services on page 55

The recovery password

The Branch Gateway includes a special recovery password. The purpose of the recovery password is to enable the system administrator to access the Branch Gateway in the event that the regular password is forgotten. You can only use the recovery password when accessing the Branch Gateway via a direct connection to the Services port. The username and password for the recovery password are:

username: **root**

password: **ggdaseuaimhrke**

Note:

After accessing the Branch Gateway using the recovery password, remember to define an Admin level user before exiting the Branch Gateway . See Creating a username, password, and privledge level on page 35.

You can use the **set terminal recovery password** command to enable or disable the recovery password option. Use this command only when accessing the Branch Gateway using a direct connection to the Services port.

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**

Related topics:

Telnet access configuration commands on page 51

Telnet access configuration commands

For more information about these commands, see the *Avaya Branch Gateway G430 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 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 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.

Related topics:

Configuring the Master Configuration Key on page 52

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.

Related topics:

SYN attack on page 53
SYN cookies on page 53
Configuring SYN cookies on page 54
Commands used to maintain SYN cookies on page 54
SYN cookies configuration commands on page 55

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 are able to 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 queues.
- 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.

Related topics:

SYN attack notification on page 54

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 SYN cookies configuration commands on page 55 .

For more information about these commands, see the *Avaya Branch Gateway G430 CLI Reference*.

SYN cookies configuration commands

For more information about these commands, see the *Avaya Branch Gateway G430 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.

Related topics:

MSS reporting mechanism on page 55
Configuring MSS on page 56
DoS attack classifications on page 57
Custom DoS classifications on page 58
Example of configuring MSS notifications using ACL rules on page 60
MSS configuration CLI commands on page 60

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. For general information about configuring and enabling

syslog messages and syslog message format, refer to Syslog server configuration on page 216.

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. For information about how to view syslog messages, see Viewing QoS traps, QoS fault traps, and QoS clear traps on page 364.

Note:

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

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 PPP interfaces.

Procedure

1. 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
Done!
```

```
//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
Done!
//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
```

3. 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 Avaya Aura® Communication Manager, 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

DoS Attack	Description
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.

Note:

For general information about configuring policy rules, refer to Policy lists on page 553.

Related topics:

Examples for defining a DoS class using ACLs on page 59

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. See Policy lists rule criteria on page 565.

  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!
```

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
Done!
//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
Done!
//Specify that the ip rule applies to ICMP packets
Gxxx-001(super-ACL 301/ip rule 1)# ip-protocol icmp
Done!
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
-----  --------  ---  ---------------  -----------  -----------  --------------
1      icmp    Src Any                           Any Type     Deny-Notify
       Any     Dst 255.255.255.255  Host         Any Code     No
Dos classification: smurf
Deflt  Any     Src Any                           Any          Permit
       Any     Dst Any                           Any          No
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
Done!
```

MSS configuration CLI commands

For more information about these commands, see the *Avaya Branch Gateway G430 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

Command	Description
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.
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

Chapter 5: Basic device configuration

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

Related topics:

Defining an interface on page 63
Primary Management Interface (PMI) configuration on page 64
Example of defining a default gateway on page 67
Branch Gateway Controller configuration on page 67
DNS resolver on page 74
Device status viewing on page 81
Software and firmware management on page 83

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
```

For more information on the various types of interfaces, see Router interface concepts on page 421.

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 on page 420. For interface configuration examples, see Configuration example on page 264.

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.

Related topics:

Setting the PMI of the Branch Gateway on page 65
Active and configured PMI on page 66
PMI configuration CLI commands on page 66

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 the *Avaya Branch Gateway G430 CLI Reference*.

Root level command	Command	Description
interface (fastethernet|tunnel| vlan| loopback| dialer)		Enter configuration mode for the FastEthernet, Tunnel, VLAN, Loopback, or Dialer interface
	pmi **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
	no pmi no pmi6	
set system contact		Set the contact information for this Branch Gateway system

Root level command	Command	Description
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 **ip default-gateway** 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

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

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

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

Related topics:

Locating the Branch Gateway serial number on page 68

Supported S8XXX servers on page 68
MGC list configuration on page 69
About setting reset times on page 71
Example for setting reset times on page 72
Accessing the registered MGC on page 72
ICC or Survivable Remote Server monitoring on page 73
Summary of MGC list configuration commands on page 73

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

Supported S8XXX servers

The MGCs supported by the Branch Gateway include both ECCs and ICCs. The Branch Gateway supports the following MGCs:

Table 1: MGCs supported by the Branch Gateways

MGCs	Type	Usage
Avaya S8300D Server	Media module	ICC, ECC or LSP
Avaya S8800 Server	External	ECC
Dell R610	External	ECC

See Chapter 2: Optional components for information about the S8300D Server module.

MGC list configuration

The Branch Gateway must be registered with an MGC in order to provide telephone service. You can set the Branch Gateway's MGC, and show the current MGC list used to determine the results.

Related topics:

[The Branch Gateway's MGC settings](#) on page 69
[Example of setting the Branch Gateway's MGC](#) on page 69
[Results from the set mgc list command](#) on page 70
[Showing the current MGC list](#) on page 70
[Removing MGCs from the MGC list](#) on page 71
[Changing the MGC list](#) on page 71

The Branch Gateway's MGC settings

Use the **`set mgc list`** command to set the Branch Gateway's 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. The Branch Gateway searches for the primary MGC first. If it cannot connect to the primary MGC, it searches for the next MGC on the list, and so on. If there are both IPv4 and IPv6 addresses in the same index on the MGC list, the IPv6 address is preferred.

This allows you to select the destination address; the source address is selected according to the destination address, e.g., if the first address in the mgc list is an IPv6 address and the GW has both a IPv4 and a IPv6 address then the gateway selects its IPv6 address as the source address.

When SLS is enabled, the MGC list includes the SLS module as a fifth entry on the MGC list. For details about SLS, see [Standard Local Survivability (SLS)](#) on page 101.

Note:

If the MGC is an S87XX server, the first server on the list will normally be the primary C-LAN board connected to the server. If the MGC is an S8400 or S85XX, the first server on the list will be either the primary C-LAN board connected to the server, or an Ethernet port on the server that has been enabled for processor Ethernet connections. If the MGC is an S8300, the first server on the list will be the IP address of the S8300. The remaining servers will be either alternate C-LAN boards connected to the S8400, S85XX, or S87XX servers, or an S8300 configured as an LSP, or the port enabled as the Ethernet processor port on an S85XX configured as an LSP.

Example of setting the Branch Gateway's 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
Registered	Indicates whether or not the Branch Gateway is registered with an 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 the Branch Gateway and the MGC is up or down
H248 Link Error Code	If there is a communication failure between the Branch Gateway and the MGC, this field displays the error code
PRIMARY MGC HOST	IPv4 and IPv6 addresses of the primary MGC host
SECONDARY MGC HOST	IPv4 and IPv6 addresses of the seconday MGC hosts

Showing the current MGC list

About this task

This command shows the IP addresses of the MGCs on the MGC list. It also shows whether or not SLS is enabled.

Procedure

To show the current MGC list, use the **show mgc list** command.

Example

```
Gxxx-001(super)# sh mgc list

PRIMARY MGC HOST, Primary Search Time : 1 min(s)
IPv4 Address          IPv6 Address
```

```
-------------------- ----------------------------------------------
-- Not Available --  100:0:0:0:0:0:0:803

SECONDARY MGC HOST
IPv4 Address         IPv6 Address
-------------------- ----------------------------------------------
-- Not Available --  -- Not Available --
-- Not Available --  -- Not Available --
-- Not Available --  -- Not Available --

sls disabled

Done!
```

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.

Result

Note:

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 the Branch Gateway and its registered MGC is lost, the 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 or not 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 Avaya Aura® Communication Manager 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
```

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 the *Avaya Branch Gateway G430 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

Command	Description
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. For more information about VPNs on the Branch Gateway, see IPSec VPN on page 477.

Related topics:

DNS resolver features on page 74
Typical DNS resolver application – VPN failover on page 75
Configuring DNS resolver on page 76
Using DNS resolver to resolve a hostname on page 79
DNS resolver maintenance on page 79
DNS resolver configuration commands on page 79

DNS resolver features

The 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. For more information on DHCP Client, see Configuring the DHCP client on page 205.

Note:

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

- FastEthernet with PPPoE
- Dialer interface

The most common application of this configuration is for connecting the 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.

Typical DNS resolver application – VPN failover

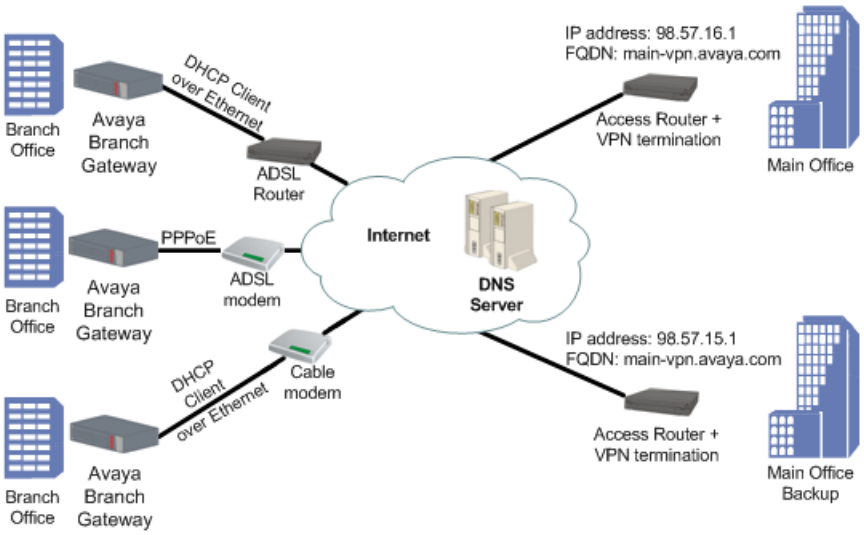
In this typical application, the DNS resolver feature is used to provide a VPN failover mechanism between two main offices. The failover mechanism is implemented as follows.

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.

This typical application is described in full in Failover using DNS on page 532.



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 on page 0 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 on page 0 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!
   ```

9. 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 on page 205.

- 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
```

Figure 6: DNS resolver configuration workflow

Related topics:

DNS resolver configuration example on page 78

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”
Done!
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

Done!
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
Done!
Gxxx-001(config)# ip domain timeout 5
Done!
```

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

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.

Related topics:

Examples of viewing DNS resolver logging on page 79

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
   Done!
   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
   Done!
   CLI-Notification: write: set logging session condition DNSC Info
   ```

Note:

You can also enable logging messages to a log file or a Syslog server. For a full description of logging on the Branch Gateway, see System logging on page 215.

DNS resolver configuration commands

For more information about these commands, see the *Avaya Branch Gateway G430 CLI Reference*.

Root level command	Command	Description
clear ip domain statistics		Clear the DNS resolver's statistics counters
interface {dialer| FastEthernet| USB-modem}		Enter the interface configuration mode for a Dialer, 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
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 G430 Branch Gateway CLI Reference*.

Related topics:

[The show mm command](#) on page 81
[The show mm and show mg list config commands](#) on page 81
[Device status commands](#) on page 82

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 the *Avaya Branch Gateway G430 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

Software and firmware management

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

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

Related topics:

File transfer on page 83
Software and firmware upgrades on page 83
Software and firmware upgrades using FTP/TFTP on page 85
Example of an upgrade using FTP/TFTP on page 85
Upgrading software and firmware using a USB mass storage device on page 86

File transfer

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

- Install software and firmware upgrades on the Branch Gateway
- Install firmware upgrades on media modules
- Back up and restore configuration settings

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

Note:

If you use an FTP server, the 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 the Branch Gateway. Software used to control the Branch Gateway itself and media modules installed on the Branch Gateway is called firmware. Use a

USB device or the FTP or TFTP protocol to download a new version of software or firmware. You can upgrade the following types of software and firmware:

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

Note:

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

For details, see *Installing and Upgrading the Avaya G430 Branch Gateway*

Related topics:

Firmware bank management on page 84
Displaying firmware versions in the banks on page 84
Bank management changes on page 84
Loading firmware from the non-default bank on page 85

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 FTP/TFTP

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

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

Example of an upgrade using FTP/TFTP

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
```

Note:

When downloading firmware from the S8300, use only the file name, without the directory path, in the command line. Otherwise, the procedure will fail. For instance, in the example above, you must use the following command:

When downloading firmware from the S8300 using TFTP, you may need to enable the TFTP service in the Set LAN Security parameters of your web server.

Example

The following example downloads a firmware version with the path and file name `C:\gxxx.net` from an FTP server with the IP address 149.49.134.153 to Bank A of the Branch Gateway.

```
copy ftp SW_imageA C:\gxxx.net 149.49.134.153
```

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 the Branch Gateway USB port.
4. Copy the software or firmware files to the Branch Gateway using one of the following commands:
   - **`copy usb SW_imageA`**
   - **`copy usb SW_imageB`**
   - **`copy usb EW_archive`**
   - **`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`**

5. Use the **show download software status** command to display the status of the firmware download process.

Related topics:

Upgrading firmware using the USB mass storage device restore command on page 87

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. Back up the Branch Gateway by entering **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, with a directory structure as detailed in Sample backup directory after backup on page 92.
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 subdirectory.
   d. Copy IP phone firmware files to the IPPHONE subdirectory.
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.

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
- auth-file. Authentication file
- phone-scriptA. Phone script bank A in the Branch Gateway's TFTP directory
- phone-scriptB. Phone script bank B in the Branch Gateway's TFTP directory
- 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 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
- auth-file. Authentication file
- 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
- auth-file. Authentication file
- 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 G ateway to a TFTP server, where **file** can be any of the following:

- announcement-file. Announcements files
- capture-file. The packet sniffing buffer
- auth-file. Authentication file
- capture-file. The packet sniffing buffer

- cdr-file. A Call Detail Recording (CDR) file
- dhcp-binding. The DHCP binding file

Software and firmware management commands

For more information about these commands, see the *Avaya Branch Gateway G430 CLI Reference*.

Command	Description
copy file ftp	Upload a specific file from the Branch Gateway to an FTP server
copy file scp	Upload a specific file from the Branch Gateway to an SCP server
copy file tftp	Upload a specific file from the Branch Gateway to a TFTP server
copy file usb	Upload a specific file from the Branch Gateway to the USB mass storage device
copy ftp EW_archive	Upgrade the Java applet for Branch Gateway software from an FTP server
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 the Branch Gateway firmware into Bank A from an FTP server
copy ftp SW_imageB	Upgrade the Branch Gateway firmware into Bank B from an FTP server
copy tftp EW_archive	Upgrade the Java applet for Avaya Gxxx Manager software from a TFTP server
copy tftp module	Upgrade the firmware on a media module from a TFTP server
copy tftp SW_imageA	Upgrade the Branch Gateway firmware into Bank A from a TFTP server
copy tftp SW_imageB	Upgrade the Branch Gateway firmware into Bank B from a TFTP server
copy usb announcement-file	Upgrade announcements files from the USB mass storage device
copy usb auth-file	Upgrade the authorization file from the USB mass storage device
copy usb EW_archive	Upgrade the Java applet for Avaya Gxxx Manager software from the USB mass storage device

Command	Description
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 usb SW_image	Upgrade the Branch Gateway firmware into Bank A or into Bank B, from the USB mass storage device
dir	List all files in the USB mass storage device connected to the Branch Gateway
set boot bank	Set the default bank from which firmware is loaded during startup
show boot bank	Display the bank from which the 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

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. The Avaya Branch Gateway also supports USB 2.0 high speed (480 Mbits/sec) for faster file transfer between the 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 a 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 method, in which files are copied and restored individually.

A single CLI command backs up all the administration and configuration files of a Branch Gateway onto a USB mass storage device. Another single command restores all of the backed up files. If you need to completely replicate a Branch Gateway, you can also download the 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 the Branch Gateway. Refer to Upgrading software and firmware using a USB mass storage device on page 86 and Software and firmware uploads from the Branch Gateway.

Tip:

Use a USB mass storage device with LED indication.

Related topics:

Backing up administration and configuration files using a USB mass-storage device on page 91
Sample backup directory after backup on page 92
Restoring backed up configuration and administration files to a Branch Gateway using a USB mass-storage device on page 93
Replicating a Branch Gateway using a USB mass-storage device on page 93
Sample backup directory after replication on page 96
Replacing/adding/upgrading media modules using a USB mass-storage device on page 97
USB backup, restore, and replication commands on page 97

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 Gatewa 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-25-Nov-2005			Backup directory name
		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 a Branch Gateway using a USB mass-storage device

Procedure

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

   Refer to Backing up administration and configuration files using a USB mass-storage device on page 91.

2. Connect the USB mass-storage device to a 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.

Result

Note:

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

Replicating a Branch Gateway using a USB mass-storage device

About this task

The following procedure is useful for replicating a 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, detailed in Sample backup directory after backup on page 92, to enable a successful restore.

Procedure

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

   Refer to Backing up administration and configuration files using a USB mass-storage device on page 91.

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.

   To do so:

   a. Download the Branch Gateway firmware from the Avaya support Website (http://www.avaya.com/support) to an FTP/TFTP server.
   b. Download the Branch Gateway firmware from the FTP/TFTP server to the new Branch Gateway.

      Assuming that Bank A holds the older firmware version, enter **`copy ftp sw_imageA`** *filename ip*, where *filename* is the full path and file name of the firmware file, and *ip* is the IP address of the FTP server. Alternatively, enter **`copy tftp sw_imageA`** *filename ip* if you are downloading from a TFTP server.

6. If the new Branch Gateway firmware version is 26.x.y or above, add a Branch Gateway firmware to the USB mass-storage device, as follows:

   a. From the 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 the Branch Gateway firmware file to the root backup directory in the USB mass-storage device.

7. Add the firmware files of the media modules to the USB mass-storage device, as follows:

   a. From the 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 subdirectory 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 the Avaya support Website, download to your PC the firmware files (booter and application) of up to two supported IP phones, as well as the [1] or [2] 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.

[1] 46xxupgrade.txt
[2] 46xxupgrade.scr

Place them in the IPPHONE subdirectory 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.

9. You can optionally restore or add the Device Manager, as follows:
   a. From the 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 Avaya Aura® Communication Manager.

    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.

Sample backup directory after replication

After replicating an 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-25-Nov-2005			Backup directory name
		readme.txt	File with backup info
		startup_config.cfg	Configuration file
		audio.bin	Customer-specific VoIP parameters
		auth-file.cfg	Authentication file
		gxxx_sw_24_21_1.bin	Branch Gateway image
		gxxx_emweb_3_0_5.bin	Embedded web image
	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 the Branch Gateway by entering **`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, with a directory structure as detailed in Sample backup directory after backup on page 92.

2. From the 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 an 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 the Branch Gateway.

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

Result

Note:

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

USB backup, restore, and replication commands

For more information about these commands, see the *Avaya Branch Gateway G430 CLI Reference*.

Command	Description
`backup config usb`	Back up the Branch Gateway configuration to a USB mass-storage

Command	Description
copy ftp sw_imageA	Download a software image from an FTP server into Bank A
copy tftp sw_imageA	Download a software image from a TFTP server into Bank A
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
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 the Branch Gateway. You can use configuration files to back up and restore the configuration of the 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 the Branch Gateway. For more information about running configuration and startup configuration, see Configuration changes and backups on page 24.

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. For more information, see Gateway secret management on page 51.

You can:

- Use the FTP/TFTP/SCP copy commands to transfer a configuration file between the Branch Gateway and a server on the network.
- Use a USB mass-storage device connected to a Branch Gateway USB port to upload or download the startup configuration file of the 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 the Branch Gateway (refer to Backup and restores using a USB mass-storage device on page 90).

Related topics:

Configuration file backup and restore commands on page 99

Configuration file backup and restore commands

For more information about these commands, see the *Avaya Branch Gateway G430 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 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 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
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)

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 Avaya Aura® Communication Manager translations (survivable ARS analysis and configuration data). This data set is compiled and distributed to a group of devices using the Provisioning and Installation Manager (PIM). In the absence of the PIM, the data set can be configured manually from individual Branch Gateways using CLI commands. For instructions on configuring SLS, see SLS configuration rules on page 120.

Related topics:

Media module compatibility with SLS on page 102
SLS features on page 102
Avaya telephones supported in SLS on page 103
Call processing functionality in SLS mode on page 104
Call processing functionality not supported by SLS on page 105
Provisioning data on page 106
PIM configuration data on page 107
SLS entry on page 107
SLS interaction with specific Branch Gateway features on page 109
SLS logging activities on page 116
SLS configuration on page 118

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
MM721	Vintage 1
MM722	Vintage 7

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

Module name	CLI interface name
1603	4610
1608	4610
1616	4620
9610, FW V2.0 +	4606[3]
9620, FW V2.0 +	4610*
9630, FW V2.0 +	4620*
9640, FW V2.0 +	4620*
9650, FW V2.0 +	4620*

Call processing functionality in SLS mode

In survivable mode, SLS provides only a limited subset of Avaya Aura® Communication Manager call processing functionality:

- Limited call routing through a Survivable ARS Analysis Table (in the PIM application or 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.
- Communication Manager Feature Access Codes for ARS, contact closure, and Hold
- Acts as an H.323 Gatekeeper that enables IP endpoints to register simultaneously

[3] For R4.0, the firmware must be build 26_39 or newer. For R5.0, the firmware must be build 27_27 or newer.

- Direct Inward Dialing
- Multiple call appearances
- Hold and Call Transfer functions
- Contact closure feature
- Call Detail Recording (CDR, see SLS logging activities on page 116)
- 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

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:

- Avaya Aura® Communication Manager 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
- Avaya Aura® Communication Manager provisioning information for the options in the station and trunk media modules is sent through the CCMS channel
- Provisioning and Installation Manager (PIM) queries Avaya Aura® Communication Manager for station/trunk configuration and dial plan routing administration data through SNMP. Alternatively, the provisioning may be entered manually via an SNMP MIB browser or via the local Branch Gateway's CLI interface.

Related topics:

Standard Local Survivability data sources and communication paths on page 106

Standard Local Survivability data sources and communication paths

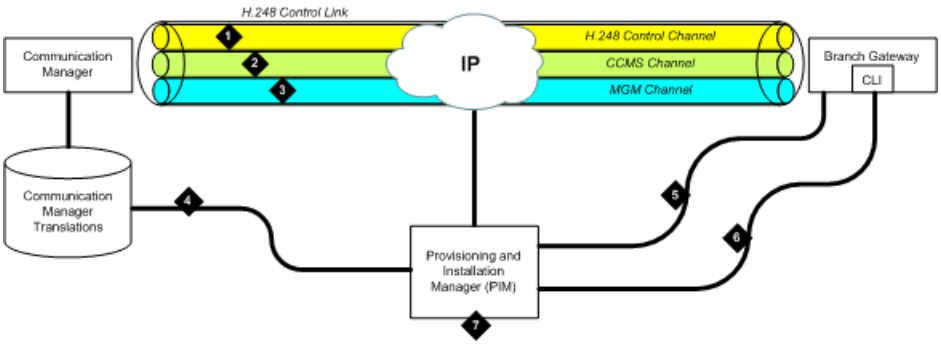


Table 3: Figure notes:

1. 248 call signaling and configuration data
2. CCMS messages through Clear Channel
3. Branch Gateway Maintenance Channel
4. PIM extracts Communication Manager translation subset through OSSI
5. PIM data set and SLS MIB delivered to the Branch Gateway through SNMP

6. Security codes (passwords) sent over SSH connection to CLI
7. Provisioning and Installation Manager (PIM) for remotely provisioning Branch Gateways, network-wide. PIM is installed on an enterprise management server, not on the primary Communication Manager server.

NOTE: The SLS data must be configured manually in the Branch Gateway if the PIM is not available.

The required Communication Manager translations for SLS include fields on the Station and Branch Gateway screens. See Configuring Communication Manager for SLS on page 120 for more information about the information types and how to administer Communication Manager for SLS.

PIM configuration data

SLS also requires PIM configuration data, some of which the Branch Gateway extracts from the Avaya Aura® Communication Manager translations. PIM aggregates the required data and copies the provisioning data over a secure communication path to non-volatile RAM (NVRAM) on the Branch Gateway. After the initial data collection, PIM retains a copy of the data set for each Branch Gateway. This set is compared with subsequent data sets to determine if anything has changed:

- If the data set changes, the newer data set is pushed down to the Branch Gateway
- If the data set does not change, the data set in NVRAM remains unchanged

Users can schedule when to collect and push data, perform scheduled and manual backups, and enable and disable SLS, as well as display (but not change) the data to ensure correct information. See Using PIM to manage SLS administration on the gateway on page 133.

If PIM is unavailable, the SLS data set can be manually configured in the Branch Gateway CLI. For information on configuring SLS, both manually and via PIM, see SLS configuration rules on page 120.

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.

Related topics:

Unregistered state on page 108
Setup state process on page 108
Registered state process on page 108
Teardown state on page 109

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.
3. 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.
3. 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.

Related topics:

Teardown state process on page 109

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.

Related topics:

Direct Inward Dialing in SLS mode on page 110
Multiple call appearances in SLS mode on page 110
Hold in SLS mode on page 111
DCP and IP phones on page 111
Using the Flash button on page 112
Using the switchhook button on page 112
Call Transfer in SLS mode on page 113
Using contact closure in SLS mode on page 114
Administering IP Softphone in SLS mode on page 116

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, Communication Manager 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 on page 111 and Analog phones on page 111 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

Related topics:

Analog telephones on page 111

Analog telephones

Newer analog telephones (for example, Avaya 62*xx* 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.
2. 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 on page 0 .

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)

Related topics:

Transferring a call on DCP and IP phones on page 113
Transferring an established call from an analog phone on page 114

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.

Note:

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 0 .
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 0 .
   - 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. For more information, see Example of CDR log entries and format on page 117.

   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 topics:

Contact closure / SLS feature interactions on page 115

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.

Note:

For more information on contact closure, refer to Contact closure on page 315.

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 Communication Manager administrative SAT interface.

   For instructions on accessing the Avaya Aura® Communication Manager through the Avaya Branch Gateway, see Accessing the registered MGC on page 72.
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.

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 of time.

- Contact closure

Related topics:

Example of CDR log entries and format on page 117
Example of CDR log with contact closure on page 118

Example of CDR log entries and format

```
Gxxx-SLS(super)# show logging cdr file content
02/18/2005,10:46:35:CDR-Informational: 10:46 00:00 A 700 50029555 52001 v301
02/18/2005,10:45:46:CDR-Informational: 10:45 00:00 A 700 50029 52001 v301
02/18/2005,10:45:14:CDR-Informational: 10:45 00:00 A 700 52 52001 v301
02/18/2005,10:44:35:CDR-Informational: 10:44 00:00 A 700 445200 52001 v301
02/10/2005,13:20:23:CDR-Informational: 13:20 00:00 A 700 50029 52001 v301
02/10/2005,13:20:15:CDR-Informational: 13:20 00:00 A 700 50029 52000 v301
02/10/2005,13:20:05:CDR-Informational: 13:20 00:00 A 700 44 52000 v301
02/10/2005,13:19:59:CDR-Informational: 13:19 00:00 A 700 44500 52000 v301
```

An interpretation of the first entry is:

- **02/18/2005:** 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
07/27/2005,03:59:24:(0 0 0:15:5)CDR-Informational: July 27 03:59 B 15840 PULSE 003
2
```

An interpretation of this entry is:

- Date (07/27/2005) 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

Related topics:

SLS configuration rules on page 120
Configuring Communication Manager for SLS on page 120
Inherited Class of Restriction (COR) permissions on page 123
Station screen field descriptions for the Branch Gateway on page 124
Using PIM to manage SLS administration on the Branch Gateway on page 133
SLS ARS Entry page field descriptions on page 135
PIM Device Profile Wizard buttons on page 137
Enabling SLS on page 137
Disabling SLS on page 138

Activating changes in SLS on page 138
Prerequisites for using the CLI to manually configure SLS administration on the Branch Gateway on page 138
SLS data set preparation on page 139
SLS capacities on page 139
Collecting analog stations data on page 140
Collecting DCP stations data on page 141
Collecting IP stations data on page 142
Collecting trunk groups data on page 143
Trunk Group screen field descriptions on page 145
Collecting DS1 trunks data on page 147
DS1 circuit pack field descriptions on page 147
Collecting signaling groups data on page 152
Signaling Group field descriptions on page 152
Collecting administered ISDN-BRI trunks data on page 153
ISDN-BRI Trunk field descriptions on page 154
Collecting Feature Access Codes data on page 156
Feature Access Code field descriptions on page 157
Collecting system parameters data on page 158
Codecs supported in SLS on page 159
General system parameters field descriptions on page 159
Collecting ARS dial patterns data on page 159
ARS Dial Patterns field descriptions on page 160
Collecting Incoming Call Handling data on page 161
Incoming call handling data field descriptions on page 161
Configuration of the SLS data through the CLI on page 162
Creating the SLS administration data set on the Branch Gateway on page 163
Administering station parameters on page 165
Class values in SLS station context on page 168
Module-port values in SLS station configuration mode on page 168
Administering DS1 parameters on page 169
ISDN Layer 3 country codes on page 171
ISDN Layer 3 country protocols for ISDN Primary Rate service on page 172
Administering BRI parameters on page 173
Trunk group assignment on page 175
Administering trunk-group parameters on page 176
Maximum number of members in a trunk group on page 181
SLS group type assignments on page 181
Module-port values in SLS trunk-group context for analog trunks on page 182
Trunk port values in SLS trunk-group context for digital trunks on page 182
Administering signaling-group parameters on page 183

Administering dial-pattern parameters on page 184
Administering incoming-routing parameters on page 185
Summary of SLS configuration commands on page 187

SLS configuration rules

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

- Avaya Aura® Communication Manager must be configured for SLS and Auto Fallback. For instructions on configuring SLS in Avaya Aura® Communication Manager, see Configuring Communication Manager for SLS on page 120.
- Provisioning data from the PIM tool must be gathered from Avaya Aura® Communication Manager and delivered to the Branch Gateway using PIM. For instructions on gathering and delivering the provisioning data, see Using PIM to manage SLS administration on the gateway on page 133.

  If PIM is not available, the Branch Gateway can be manually configured for SLS and Auto Fallback using the CLI. See Using the CLI to manually configure SLS administration on the gateway on page 138.
- SLS must be enabled on the Branch Gateway. See Enabling SLS on page 137.
- To activate any saved changes within SLS, the disable and enable SLS commands must be used together. See Activating changes in SLS on page 138.

Configuring Communication Manager for SLS

About this task

You must configure the Avaya Aura® Communication Manager for SLS whether you will be using PIM provisioning or manual CLI entry of SLS administration. Perform the configuration during the initial administration of the host Communication Manager server.

Procedure

1. Access theCommunication Manager administrative SAT interface.

   For instructions on accessing the Avaya Aura® Communication Manager through the Branch Gateway, see Accessing the registered MGC on page 72.
2. At the SAT, enter **`change node-names ip`** to display the IP Node Names screen.
   For example:

```
change ip-codec-set-1                                          Page   1 of   3
                                IP NODE NAMES
    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 Communication Manager (**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 (see Step 2 on page 163 of Configuring the SLS data through the CLI on page 162).
    - **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 150.

    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**

      Inherited Class of Restriction (COR) permissions on page 123 shows the hierarchical relationship among the calling-restriction categories.
    - **Survivable Trunk Dest**
    -
14. Submit the screen.

Inherited Class of Restriction (COR) permissions

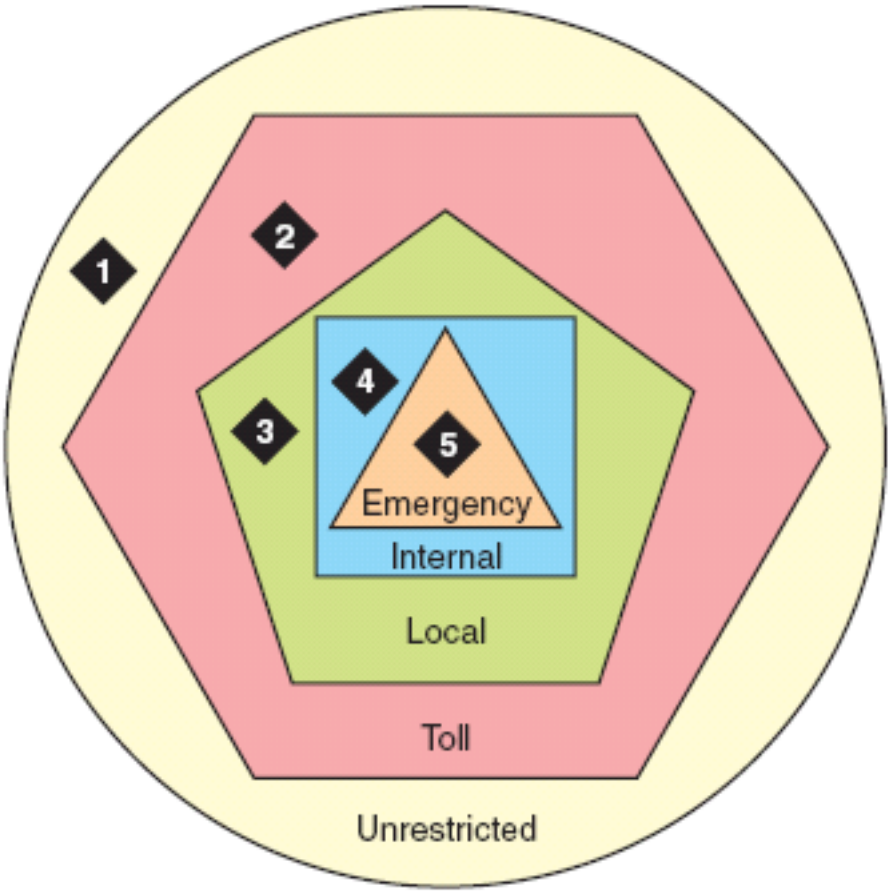


Table 4: Figure notes:

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:
   - **locl:** (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

Related topics:

Security Code on page 124
Type on page 125
Port on page 130
Survivable GK Node Name on page 131
Survivable COR on page 131
Survivable Trunk Dest on page 132
Switchhook Flash on page 132
Expansion Module on page 132
Name on page 132

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

The type of telephone. A station type must be administered for each station added to the system.

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

Note:

Analog telephones administered with hardware to a virtual extension cannot be changed if TTI is enabled for the system. For more information, go to the Avaya Support website at http://support.avaya.com for current documentation, product notices, knowledge articles.

Telephone type	Model	Administer 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 w/Caller ID	CallrID
	7101A, 7102A	7101A
	7103A Programmable and Original	7103A
	7104A	7104A
	8110	8110
	DS1FD	DS1FD
	7302H, 7303H	7303S
	VRU (voice response unit) with C&D tones	VRU
	VRU without C&D tones	2500
Single-line DS1/DSO (Lineside T1/ DS1)	DS1 device without forward disconnect	ops
	VRU with forward disconnect without C&D tones	ds1fd or ds1sa
	VRU with forward disconnect without C&D tones	VRUFD or VRUSA

Telephone type	Model	Administer as
Terminals	510D	510
	515BCT	515
Multi-appearance hybrid	7303S	7303S, 7313H
	7305H	7305S
	7305S	7305S, 7316H, 7317H
	7309H	7309H, 7313H
	7313H	7313H
	7314H	7314H
	7315H	7315H
	7316H	7316H
	7317H	7317H
Multi-appearance digital	2402	2402
	2410	2410
	2420	2420
	6402	6402
	6402D	6402D
	6408	6408
	6408+	6408+
	6408D	6408D
	6408D+	6408D+
	6416D+	6416D+
	6424D+	6424D+
	7401D	7401D
	7401+	7401+
	7403D	7403D
Multi-appearance digital	7404D	7404D
	7405D	7405D
	7406D	7406D
	7406+	7406+
	7407D	7407D
	7407+	7407+

Telephone type	Model	Administer as
	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
IP Telephone	4601+ **Note:** When adding a new 4601 IP telephone, you must use the 4601+ station type. This station type enables the Automatic Callback feature.	4601+
	4602+ **Note:** When adding a new 4602 IP telephone, you must use the 4602+ station type. This station	4602+

Telephone type	Model	Administer as
	type enables the Automatic Callback feature.	
	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
SIP IP Telephone	• 4602SIP with SIP firmware • 4610SIP with SIP firmware • 4620SIP with SIP firmware • 4620SIP CC (Call Center) • SIP Softphone/Avaya one-X Desktop • Toshiba SP-1020A **Note:** Any model telephone that has SIP firmware and is being used for SIP networking must be administered as a 4620SIP telephone, 96xxSIP telephone, or 16CC SIP telephone.	4620SIP

Telephone type	Model	Administer as
	Note: Communication Manager does not support 1616SIP CC and 4620SIP CC telephones from Release 6.2 and later.	
	Avaya one-X (tm) Deskphone 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	Road-warrior application	H.323 or DCP type
	Native H.323	H.323
	Single-connect	H.323 or DCP type
ISDN-BRI station	—	asai
	Any NI-BRI (N1 and N2) telephone	NI-BRI
	7505D	7505D
	7506D	7506D
	7507D	7507D
	8503D	8503D
	8510T	8510T
	8520T	8520T
Personal computer	6300/7300	PC
(voice/data)	6538/9	Constellation
Test Line	ATMS	105TL

Telephone type	Model	Administer as
No hardware assigned at the time of administration.		• XDID (use when Communication Manager later assigns a DID number to this station) • XDIDVIP (use when the administrator later assigns a DID number to this station) virtual (use to map this and other extensions to one physical telephone)
Key telephone system interface	—	K2500
ASAI	asai link computer telephony adjunct link	asai adjlk
AWOH	any digital set	same as “Multi-appearance Digital”
	CTI station	CTI
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

Valid Entry	Usage
	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.
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 46*xx* or 96*xx* 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. This field is used by PIM module of the Integrated Management to communicate with the Communication Manager administration tables and obtain the class of service information. PIM module builds a managed database to send for Standard Local Survivability (SLS) on the Branch Gateways.

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.

Valid Entries	Usage
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. This field is used by the PIM module of the Integrated Management to successfully interrogate the Communication Manager administration tables and obtain the class of service information. PIM module builds a managed database to send for SLS on the Branch Gateways.

Available for all analog and IP station types.

Valid Entry	Usage
y	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
y	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 Unicode Display” in *Administering Avaya Aura® Communication Manager*.

Note:

Avaya BRI stations support only ASCII characters. Non-ASCII characters, such as Eurofont or Kanafont, are displayed incorrectly on a BRI station.

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.

Using PIM to manage SLS administration on the Branch Gateway

Before you begin

Before enabling SLS, you must gather provisioning data from PIM and deliver it to the Branch Gateway. Run PIM’s Device Profile Wizard to perform this task. The Device Profile Wizard gathers a subset of the Communication Manager translations (dial plan analysis and destination routing instructions) and delivers them to the Branch Gateway. If PIM is not available, this translation subset (the SLS data set) can be created manually, using the procedure described in Using the CLI to manually configure SLS administration on the gateway on page 138.

About this task

PIM must be installed on and launched from the Avaya Network Management Console. For information about PIM, see PIM access on page 32.

Procedure

1. Ensure that the Network Management Console (NMC) has discovered the Branch Gateway.
2. Before PIM’s automatic scheduled SLS updates can work as expected, set the device parameters for both the server and the Branch Gateway in the NMC:
   - **Server**. Communication Manager login and password

     Note:

     The server must be the first listing in NMC’s discovery output. If an Survivable Core Server node is discovered and listed prior to the main server, the main server’s login/password will not permit access to the Survivable Core Server node.

- **Gateway**. SNMPv1/v3 access parameters
- **Gateway**. NMC has discovered the Branch Gateway's IP address

3. Make sure the Communication Manager has been configured for SLS as described in Configuring Communication Manager for SLS on page 120.
4. Click the **Device Profiles** icon/link in the top-level toolbar of the main PIM window.

   Alternatively, select **PIM Objects** > **Device Profiles** from the left panel.
5. Click the **New** icon on the **Device Profile list** page that appears in the right panel of the main PIM window.

   If this is not a new profile, open the existing profile from the left panel or from the **Device Profile list** page.
6. Proceed through the Device Profile Wizard to the Details page.

   Set the **CM version** field to 4.0.
7. Proceed through the Device Profile Wizard to the SLS / ARS page and perform the following:
   a. Select the **Enable the SLS feature on this device?** checkbox to enable SLS on the Branch Gateway.
      A cleared checkbox means that SLS is disabled.
   b. Select the **Perform scheduled SLS updates on this device?** checkbox to send the SLS administration data set to the Branch Gateway according to the settings on the SLS Update Schedule screen.
8. Optionally click the following buttons:
   - **View Extract**
   - **Perform Extract**
   - **Actions**
9. If this Branch Gateway has not been previously provisioned, click **Add ARS Entry** to open the ARS Entry page.
10. Use the SLS Update Schedule page to administer up to six SLS updates per day.
    a. Check the Enable SLS Updates box.
    b. Set as many as six Daily Updates.

       Note:

       The Daily Updates must be at least four hours apart.
    c. Click **Submit** .
11. Use the **Backup/Restore** page to backup the PIM database backup schedule.

Note:

Step 11 on page 0 backs up the PIM database. Avaya encourages users to set a PIM backup schedule or /policy independent of the SLS implementation.

If you require the use of the Incoming Call Handling Treatment option for adding or deleting the incoming dial pattern on incoming trunk calls, this route pattern must be modified using the CLI. There are NO equivalent commands in the PIM wizard screens.

SLS ARS Entry page field descriptions

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

Related topics:

Dialed String on page 135
Min on page 135
Max on page 135
Del on page 135
Replacement String on page 135
Call Type (ARS only) on page 136
Trunk Group on page 137
Permit / Deny on page 137

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 enter the minimum number of user-dialed digits that the system collects to match to the dialed string.

Max

Use this field to enter the maximum number of user-dialed digits that the system collects to match to the dialed string.

Del

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

Replacement String

Use this field to enter the digits that replace the deleted portion of the dialed number.

Valid Entry	Usage
blank	Use this option to delete the digits, without replacement. This is the default option.
0 to 9, *	Use this option to enter the digit string. You can enter up to 18 digits.
#	Use this option to indicate end-of-dialing used at the end of the digit string.

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
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
op	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 Communication Manager server.

Permit / Deny

Indicates whether the call should be permitted or denied.

PIM Device Profile Wizard buttons

Button	Description
View Extract	Displays the current SLS administration data set for this Branch Gateway.
Perform Extract	Extracts the SLS information from the controlling Communication Manager server for this Branch Gateway
Actions	Enables you to edit or delete a previously-administered entry: • The paper/pencil icon is the **edit** icon that opens the ARS Entry page. • The trash can icon is the **delete** icon that removes the ARS Entry from the table. The Add ARS Entry option may be used to create or edit a maximum of 30 ARS dial pattern entries.

Enabling SLS

Procedure

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

Note:

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

About this task

.

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

Use PIM to configure the SLS data. However, if PIM is unavailable, you can also configure the SLS data from the Branch Gateway itself.

Note:

Do *not* run two SLS data update sessions concurrently. The SLS data can be administered locally using CLI, and centrally using PIM or an 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 an 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.

- Communication Manager Release 4.1 is running on the host server
- PIM or configuration of the Branch Gateway through its CLI
- The Branch Gateway is registered with Avaya Aura® Communication Manager
- The SLS is enabled on the Branch Gateway through its CLI
- S8300 is not serving as an Survivable Remote Server
- Branch Gateway is not subtending to another external server (including Survivable Core Server or another Survivable Remote Server in another gateway)

SLS data set preparation

It is recommended to plan the SLS coverage and gather information from Avaya Aura® Communication Manager 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 Communication Manager 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 Communication Manager 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
G430	150

You can collect the Communication Manager data using the Communication Manager administrative SAT interface. For instructions on accessing the Avaya Aura® Communication Manager through the Branch Gateway, see Accessing the registered MGC on page 72.

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.
5. Once you know the extension, enter **`display station`** *extension* to display the Station screen for this extension.
   Use Collecting DCP stations data on page 141 as a reference.
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

   For more information about these fields, see Station screen field descriptions for Media Gateway on page 124.

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. Once 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. 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
   - 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 Media Gateway on page 124.

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 0 .
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

    For more information about these fields, see Station screen field descriptions for Media Gateway on page 124.

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 SLS group type assignments on page 181 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 Communication Manager 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.

   Refer to Module-port values in SLS trunk-group context for analog trunks on page 182.

5. Identify the BRI trunk ports.

   Refer to Trunk port values in SLS trunk-group context for digital trunks on page 182.

6. Identify the digital DS1 trunk ports.

   Refer to Trunk port values in SLS trunk-group context for digital trunks on page 182.

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

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 **Dial Access?** 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 **Digit Treatment** field is set to insert1, insert2, insert3, or insert4
Trunk Type	Depends on trunk signaling type: • Analog trunks: - Loop-start - Ground-start

Name	Description
	- 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 included in the SLS data set.

DS1 circuit pack field descriptions

Related topics:

Name on page 148
Bit Rate on page 148
Signaling Mode on page 148
Channel Numbering on page 149

Connect on page 149
Interface on page 150
Interface on page 150
Side on page 150
Country Protocol on page 150
Protocol Version on page 151
DCP/ANALOG Bearer Capability on page 151
ITN-C7 Long Timers on page 152

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.

Note:

Avaya BRI stations support only ASCII characters. Non-ASCII characters, such as Eurofont or Kanafont, are displayed incorrectly on a BRI station.

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.

Valid Entry	Usage
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, Avaya 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 S8*XXX* 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

Controls how a server running Communication Manager resolves glare at layer 3 over an ISDN-PRI link in QSIG private networks. Available if the **Interface** type is peer-master or peer-slave.

⚠ Caution:

It is critical that administration on this server correctly pairs with the administration of the far-end switch/server. If the far-end is administered as the “b” side, this field should be set to “a” regardless of whether the layer 2 designation is peer-master or peer-slave, and vice versa.

Valid Entry	Usage
a	The **Interface** is peer-master. In other words, this server overrides the far-end when glare occurs.
b	The **Interface** is peer-slave . In other words, this server 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 **Signaling Mode** 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** typeis 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 S8*XXX* 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
y	Increases the length of the long timers.
n	Uses the default long timers.

Collecting signaling groups data

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

Related topics:

Trunk Group for Channel Selection on page 153

Associated Signaling on page 153
Primary D-channel on page 153
Trunk Board on page 153
Interface Id on page 153

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
y	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

Related topics:

Name on page 154
ISDN-BRI Trunk/Interface on page 155
ISDN-BRI Trunk/Side on page 155
ISDN-BRI Trunk/Country Protocol on page 155
ISDN-BRI Trunk/DCP/Analog Bearer Capability on page 155
Companding Mode on page 155
TEI on page 155
Directory Number on page 155
SPID on page 155
Endpt Init on page 155
Layer 1 Stable on page 155

Name

The name used to identify the circuit pack. Accepts up to 15 alphanumeric characters.

Note:

Avaya BRI stations support only ASCII characters. Non-ASCII characters, such as Eurofont or Kanafont, are displayed incorrectly on a BRI station.

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
y	Requires that an **SPID** 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
y	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 0 .
   - 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 0 .
   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 0 .

Feature Access Code field descriptions

Related topics:

Contact Closure Open Code on page 157
Contact Closure Close Code on page 157
Contact Closure Pulse Code on page 157
Auto Route Selection (ARS) Access Code 1 on page 157
Auto Route Selection (ARS) Access Code 2 on page 158
ARS FAC on page 158
CAS Remote Hold/Answer Hold-Unhold Access Code on page 158

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® Communication Manager Screen Reference.

Related topics:

Date Format on Terminals on page 159
Max Survivable IP Ext on page 159

Date Format on Terminals

Applies to 64*xx* and 24*xx* DCP terminals, and to 46*xx* 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 Communication Manager, 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 159. 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

Related topics:

Dialed String on page 135
Min on page 135
Max on page 135
No Deleted Digits on page 160
General system parameters/Inserted Digits on page 160

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 enter the minimum number of user-dialed digits that the system collects to match to the dialed string.

Max

Use this field to enter the maximum number of user-dialed digits that the system collects to match to 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 Communication Manager, 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

Related topics:

Called Number on page 161
Called Len on page 162
Del on page 162
Insert on page 162

Called Number

Valid Entry	Usage
1 to 16	The number of leading digits received for an incoming call.
blank	Used as a “wildcard”, so that any number associated with the specified service or feature can match in this field.

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 **Called Party IE**, such as in Japan.
blank	When **Called Number** has also been set to blank, so that any length of digits associated with the **Called Party IE** of the Incoming SETUP message matches this field.

Del

Valid Entry	Usage
1 to 21 blank	The number of leading digits to be deleted from the incoming **Called Party Number**. Calls of a particular type can be administered to be routed to a single destination by deleting all incoming digits and then administering the **Insert** 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 sub-context 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 sub-context 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-routingtgnum mode pattern 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. See Summary of SLS configuration commands on page 187 for a complete hierarchical listing of all SLS CLI commands.

Note:

Review Summary of SLS configuration commands on page 187 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

Procedure

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** command.

   Note:

   The Branch Gateway’s administered name must match the name in the Communication Manager administration.
3. At the 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. Enter **set pim-lockout yes** to prevent Provisioning and Installation Manager (PIM) updates while you are working on SLS administration of the Branch Gateway.
5. 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 150.
6. Use the **set date-format** command to set a date format for the SLS data set.

7. 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.
8. Administer the slot configuration information by entering **set slot-config slot-number board-type**, where **slot-number** is the slot where the Media Module is located and **board-type** is the Media Module type.

   See Media module compatibility with SLS on page 102
9. Administer the station information.

   See Administering station parameters on page 165.
10. Administer DS1 trunks as required.

    Refer to Administering DS1 parameters on page 169.
11. Administer BRI links as required.

    Refer to Administering BRI parameters on page 173.
12. Administer the trunk groups.

    Refer to Administering trunk-group parameters on page 176. Note that you can add members to the trunk group only after you administer the signaling group information.
13. Administer the signaling groups.

    Refer to Administering signaling-group parameters on page 183.
14. Administer ARS dial patterns for outgoing calls.

    Refer to Administering dial-pattern parameters on page 184.
15. Administer digit treatment for incoming routed calls.

    Refer to Administering incoming-routing parameters on page 185.
16. 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**.
17. 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

  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.

18. Enter **set pim-lockout no** to allow Provisioning and Installation Manager (PIM) updates, since you finished SLS administration of the Branch Gateway.
19. 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.
20. 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.
21. At the Branch Gateway command prompt, enter **copy running-config startup-config** to save the changes.

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 13 digit numeric string that may begin with 0, and **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 0), enter **set type model**, where **model** is a value from Class values in SLS station context on page 168.
   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 0), enter **set port module-port** for this station, where **module-port** is a value in Module-port values in SLS station configuration mode on page 168.

   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 0), 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** to set the class of restriction (COR) for this extension, where **cor** 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. See Inherited Class

of Restriction (COR) permissions on page 123 for the hierarchical relationship among the COR permissions.

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 0), 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 previously-administered 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 Communication Manager.

   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 0) to have an expansion module, enter **set expansion-module yes**.
8. For analog phones (set in Step 1 on page 0) that you want SLS to recognize the switchhook flash signal (that offers subsequent transfer features), enter **set swhook-flash yes**.
9. Enter **set name name** to identify the user name for the station.

   Use the 1 to 27 character name as specified on Communication Manager. 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 y           n           -         ********
            ip station registered 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.

Class values in SLS station context

analog	dcp	ip
analog2500[4]	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	
	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

[4] Since there is just one entry, the model is optional; analog2500 is the default value.

Gateway	Media module	Analog station ports*	DCP
	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 slot-address**.

   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 Communication Manager (**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:
• **network. If the Branch Gateway is connected to a host computer and encounters glare, it overrides the far-end** • **user. If the Branch Gateway is connected to a public network and encounters glare, it releases the circuit**	• peerMaster. SLS overrides the other end when glare occurs • peerSlave. SLS releases the 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), enter **set side side** to specify the glare mode: either a or b.
9. 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 171:
10. 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 (see ISDN Layer 3 country protocols for ISDN Primary Rate service on page 172).

Verify that the protocol version matches the country specified in **set country-protocol** (set in Step 9 on page 0).

11. 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
12. 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
13. 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
14. 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 country1   a speech
ulaw  no
```

15. Enter **exit** to leave the ds1 context in SLS.

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) National ISDN-1 Nortel mode (also known as DMS) Telecordia (NI-2)	a b c d
Country 2 (Australia)	Australia National PRI ETSI	a b

Country code	Description	Possible Values
	invalid invalid	c d
Country 10 (United Kingdom)	DASS ETSI invalid invalid	a b c d
Country 12 (France)	French National PRI ETSI invalid invalid	a b c d
Country 13 (Germany)	German National PRI ETSI invalid invalid	a b c d
ETSI	Full message set, including RESTART No RESTART message invalid invalid	a b c 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 Communication Manager (**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:
• **network. If the Branch Gateway is connected to a host computer and encounters glare, it overrides the far-end**	• peerMaster. SLS overrides the other end when glare occurs • peerSlave. SLS releases the circuit when glare occurs

• **user. If the Branch Gateway is connected to a public network and encounters glare, it releases the circuit**	

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 on page 0), enter **set side side** to specify the glare mode: either a or b.
5. 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 the values listed in ISDN Layer 3 country codes on page 171.
6. If the BRI 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
7. 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
8. 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
9. 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.
10. 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.
11. Enter **set spid-a number** to assign an SPID to the B1 channel of the BRI link.
12. 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.

13. 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.
14. 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.
15. Enter **`show`** to check the BRI administration.
    The report lists the BRI parameters. For example:

```
Name = BRI-SLS1
BRI   Interface    Side   Country   Bearer   Compand   Endpt-Init   Layer1-
Stable
---   ---------    ----   --------  ------   -------   ----------
-------------
v301      user      a   country1  speech     ulaw         yes           yes
Dir-NumberA Dir-NumberB Spid-A          Spid-B
----------- ----------- -------------- --------------
 3033234567  3033234568 30332345671111 30332345681111
```

16. 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 SLS group type assignments on page 181.

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-<tgnum>`. If you want to remove the trunk group from the SLS administration, enter **exit** to leave the second-level 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.

   For more information, see Maximum number of members in a trunk group on page 181.

   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.

6. For a non-ISDN digital trunk (t1-inband or e1-inband), enter **set supervision sup-type** 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 Communication Manager (**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:

```
Group Type       Dial   Tac  Supervision         Treat   Insert
----- ---------- ------ ---- ------------------- ------- ------
    1        bri      -  *99                  -       -      -
    Name = Willow Street 2
Ports = v201,v202,v217,v218
Codeset  Codeset  Channel    Digit          Japan  Send Send   Number Trunk
Display  National Preference Handling       Discon Name Number Format Hunt
----- ---------- ---------- ----------- -------- ------- ------ ------
------
codeset6 codeset6 exclusive  enbloc-enbloc   no     yes  yes    public
ascend
```

    The following example shows twelve port members assigned as t1-inband signaling:

```
Group Type       Dial   Tac  Supervision         Treat   Insert
----- ---------- ------ ---- ------------------- ------- ------
```

```
    1   t1inband   dtmf  *96      wink/immediate       -      -
    Name = Willow Street 2
Ports = v201,v202,v203,v204,v205,v206,v207,v208,v209,v210,v211,v212
Incoming-Dest Incoming-Dial Trunk-Hunt
------------- ------------- ----------
            -             no     ascend
```

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
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)

Group type	Media module	Number of ports/channels	Description of trunks that may be assigned
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 `sls-sig-group <sgnum>`. If you want to remove the signaling group from the SLS administration, enter **exit** to leave the second-level sig-group context and return to the (super-sls)# context, and then enter **clear sig-group sgnum**.
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.

   Note:

   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 trunk-group

- 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
-
```

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.
   For more information, see Available call types on page 185.
   Each level of call includes the previous level's dialing privileges. For example, **locl** has the calling privileges of **iop**, **intl**, etc.
   See Inherited Class of Restriction (COR) permissions on page 123 for an illustration of the relationship between the various dial types and the COR permissions.
3. Enter **set max-length length** to define the maximum length of the dialed string.
   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:

```
                      Min/Max          Trunk   Delete/Insert
Dialed-String/Deny    Length   Type    Group   Digits
------------------    ------   ----    -----   ----------------------
         5381000/n       9/9   locl        2   1/303
         5385000/n       9/9   locl        3   1/720
```

10. Enter **`exit`** to leave the dial-pattern context in SLS.

Related topics:

Available call types on page 185

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 calls

svc: 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.

Note:

Since the PIM application does not automatically extract this information from the Communication Manager SAT screen for Incoming-Digit-Treatment-Handling, you must enter this SLS information using the Branch Gateway CLI interface.

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. Enter **set match-pattern pattern** to define the beginning digit pattern of an incoming alphanumeric dial string to be matched against.

3. Enter **set length length** to define the length of the dialed string.

4. 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.

5. Optional. 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 that this action takes place after the deletion task has been completed for the enbloc-receiving mode.

6. Enter **exit** to leave the incoming-routing context in SLS.

7. 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 the *Avaya Branch Gateway G430 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
		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

Root Level Commands	First Level Context Commands	Second Level Context Commands	Description
			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 has been 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
	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

Root Level Commands	First Level Context Commands	Second Level Context Commands	Description
	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

Root Level Commands	First Level Context Commands	Second Level Context Commands	Description
		set min-length	Establish the minimum length of the dialed string in SLS
		set tgnum	Designate the trunk-group number in SLS
		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

Root Level Commands	First Level Context Commands	Second Level Context Commands	Description
		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
		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

Root Level Commands	First Level Context Commands	Second Level Context Commands	Description
	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 pim-lockout		Prevent or enable PIM updates while working on SLS administration of the Branch Gateway
	set slot-config		Define the slot and the board type in the Branch Gateway for SLS
	show attendant		Display the administered attendant provisioning
	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

Root Level Commands	First Level Context Commands	Second Level Context Commands	Description
	show ip-codec-set		List the codec set entries for SLS
	show last-pim-update		Display when the last PIM update of SLS data occurred
	show max-ip-registrations		Display the maximum IP registration administration in the SLS data set
	show pim-lockout		Display the current status of the setting for the PIM lockout feature
	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
		set trunk-group-chan-select	Specify the trunk-group number that can accept incoming calls in cases where the **Information**

Root Level Commands	First Level Context Commands	Second Level Context Commands	Description
			Channel Selection 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 **scocs** service declared in the Network Services Facility information element
		set channel-preference	Define how the **Channel Identification IE** 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

Root Level Commands	First Level Context Commands	Second Level Context Commands	Description
		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
		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 in-band 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

Root Level Commands	First Level Context Commands	Second Level Context Commands	Description
		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
		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: Ethernet ports

Switch Ethernet port configuration

Ethernet ports on the Branch Gateway switch

The switch on the Branch Gateway has 10/100 Mbps fixed switch ports on the front panel (ports 10/3 and 10/4).

Ethernet ports on the Branch Gateway router

The router on the Branch Gateway has a 10/100 Mbps fixed router port on the front panel (port 10/2).

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. For more information, see Advanced switching on page 325.
- VoIP queuing. To configure VoIP queuing on a switch port, configure a VLAN for the port. Then configure VoIP queuing on the VLAN. For more information about VoIP queuing, see Commands used to configure QoS parameters on page 238.
- 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. For more information on policy lists, see Policy lists on page 553.
- SNMP Link Up and Link Down traps. For more information, see SNMP trap configuration on page 307.

Summary of switch Ethernet port configuration CLI commands

For more information about these commands, see the *Avaya Branch Gateway G430 CLI Reference*.

Command	Description
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
set port negotiation	Enable or disable auto-negotiation on the port

Command	Description
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 or 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 This command applies to the Fast Ethernet 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 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

Command	Description
show port flowcontrol	Display port flow control information

Configuring the WAN Ethernet port

Procedure

1. Use the **interface fastethernet 10/2** command to enter the context of the port interface.
2. Perform basic configuration of the interface.
   For more information, see Interface configuration on page 420.
3. Use the Ethernet WAN port configuration commands in the context of the port interface.
   See Summary of WAN Ethernet port configuration CLI commands on page 203.

Related topics:

Roadmap for configuring additional features on the WAN Ethernet port on page 202
WAN Ethernet port traffic shaping on page 202
About backup interfaces on page 203
Summary of WAN Ethernet port configuration CLI commands on page 203

Roadmap for configuring additional features on the WAN Ethernet port

- Primary Management Interface (PMI). For more information, see Primary Management Interface (PMI) configuration on page 64.
- Advanced router features. For more information, see The router on page 477.
- VoIP queuing. For more information, see Commands used to configure QoS parameters on page 238.
- Access control policy lists and QoS policy lists. For more information, see Policy lists on page 553.
- SNMP Link Up and Link Down traps. For more information, see SNMP trap configuration on page 307.

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.

For information on traffic shaping in general, see Commands used to configure QoS parameters on page 238.

About backup interfaces

You can configure backup relations between a pair of any Layer 2 interfaces, except the VLAN interface. For instructions on how to configure backup interfaces, see Backup interfaces on page 254.

Summary of WAN Ethernet port configuration CLI commands

For more information about these commands, see the *Avaya Branch Gateway G430 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.

Root level command	Command	Description
	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

The Branch Gateway can be configured to function as a DHCP (Dynamic Host Configuration Protocol) client.

DHCP client enables the Branch Gateway to receive an IP address from a DHCP server, according to the DHCP client-server protocol. The DHCP server grants the Branch Gateway DHCP client an IP address for a fixed amount of time, called the lease. After the lease expires, the Branch Gateway DHCP client is required to stop using the IP address. The Branch Gateway DHCP client periodically sends requests to the server to renew or extend the lease.

In addition to receiving an IP address, an 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:

The 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 the Branch Gateway as a DHCP client. At the same time, you can activate the DHCP server on the Branch Gateway for use by clients, such as, IP phones and PCs connected to the LAN ports. The DHCP server on the Branch Gateway does *not* serve Internet devices connected over the WAN Fast Ethernet ports. For information on configuring the Branch Gateway as a DHCP server, see DHCP server on page 445.

Note:

The DHCP client only supports IPv4.

Related topics:

DHCP client applications on page 205
Configuring the DHCP client on page 205
Examples of DHCP lease release and renew on page 207
Commands used for DHCP client maintenance on page 207

Examples of configuring DHCP client logging messages on page 208
Summary of DHCP client configuration CLI commands on page 208

DHCP client applications

The typical application of DHCP client in the 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.

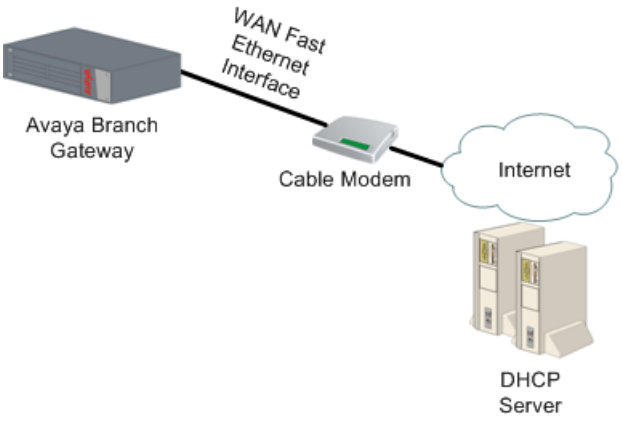


Figure 7: Fixed connection to broadband Internet using a Branch Gateway as DHCP client

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 information on the specific options, see Summary of DHCP Server commands on page 452.

  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.

   To define an object tracker, see Object tracking provisioning on page 284.

   For an example of how to track the DHCP client default route, see Typical application – tracking the DHCP client default route on page 293.

   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.

Examples of DHCP lease release and renew

- The **release dhcp** command example:

```
Gxxx-001(super)# release dhcp FastEthernet 10/2
Done!
```

- The **renew dhcp** command example:

```
Gxxx-001(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 Summary of DHCP client configuration CLI commands on page 208 or *Avaya G430 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 Summary of DHCP client configuration CLI commands on page 208 or the *Avaya Branch Gateway G430 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 full description of logging on the Branch Gateway, see System logging on page 215.

For a description of these commands, see Summary of DHCP client configuration CLI commands on page 208 or *Avaya G430 Branch Gateway CLI Reference*.

Summary of DHCP client configuration CLI commands

For more information about these commands, see the *Avaya Branch Gateways G250 and G350 CLI Reference*.

For more information about these commands, see the *Avaya Branch Gateway G430 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
	`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

Root level command	Command	Description
	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.

Related topics:

Supported TLVs on page 210
Configuring LLDP on page 211
Summary of LLDP configuration CLI commands on page 212

Supported TLVs

Related topics:

Mandatory TLVs on page 210
Optional TLVs on page 210
Optional 802.1 TLVs on page 211

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 lldp 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 lldp`** 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 lldp 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 lldp 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 lldp 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 lldp re-init-delay**. The default is 2 seconds.

5. Verify LLDP advertisements using the **show lldp** command.

Related topics:

Supported ports for LLDP on page 212

Supported ports for LLDP

You can configure only ports 10/3 and 10/4 to support LLDP.

Summary of LLDP configuration CLI commands

For more information about these commands, see the *Avaya Branch Gateways G250 and G350 CLI Reference*.

For more information about these commands, see the *Avaya Branch Gateway G430 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

Command	Description
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 lldp	Display the LLDP information received on each port
show lldp config	Display the global LLDP configuration
show port lldp 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

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 entering **`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 the sink receives (see Logging filter configuration on page 224).

The logging facility logs configuration commands entered through the CLI or through SNMP, as well as system traps and informative messages concerning the behavior of various processes. However, a user enabling the log will only see entered commands with a user-level no higher than the user's privileges. For example, a user with read-only privileges will not see entered commands having a read-write user level. In addition, the log does not display entered information of a confidential nature, such as, passwords and VPN pre-shared-keys.

Related topics:

Types of logging sinks on page 216
Syslog server configuration on page 216
Configuring a log file on page 220
Configuring a session log on page 223
Logging filter configuration on page 224
Summary of logging configuration CLI commands on page 229

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 messages.
Log file	Logging data is saved in the flash memory. These compressed, cyclic files serve as the system logging database.
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.

Related topics:

Defining Syslog servers on page 216
Disabling Syslog servers on page 218
Deleting Syslog servers on page 218
Displaying the status of the Syslog server on page 219
Syslog sink default settings on page 219
Syslog message format on page 219
Commands used to copy a syslog file on page 220

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.

For example:

```
Gxxx-001(super)# set logging server 147.2.3.66
Done!
```

or

```
Gxxx-001(super)# set logging server 2001:db8:2179::1
Done!
```

2. 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!
   ```

3. 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
   - lpr. 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 (see Logging filter configuration on page 224).

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:

```
Gxxx-001(super)# show logging server condition 147.2.3.66
*****************************************************
*** Message logging configuration of SYSLOG   sink ***
Sink Is Enabled
Sink default severity: Warning
Server name: 147.2.3.66
Server facility: auth
Server access level: read-only
```

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 the Branch Gateway to another location using FTP, SCP, or TFTP, 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`**

For a description of these commands, see Summary of logging configuration CLI commands on page 229 .

For more information about these commands, see the *Avaya Branch Gateways G250 and G350 CLI Reference*.

For more information about these commands, see the *Avaya Branch Gateway G430 CLI Reference*.

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.

See Logging filter configuration on page 224.

Related topics:

Disabling logging system messages to a log file on page 221
Deleting current log file and opening an empty log file on page 221
Log file message format on page 222

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!
```

Related topics:

Example display of log file messages on page 221
Example display of conditions defined for the file output sink on page 222

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

```
Gxxx-001
(super)# show logging file content
<190>Apr 21 16:28:32 149.49.77.11 -NoTag: -NoUTC 2009 055 1
mediagateway.g430 | 0 coldStart[BOOT-Informational: System boot up
from cold reset, ID=N/A
<187>Apr 21 16:28:32 149.49.77.11 -NoTag: -NoUTC 2009 525 1
mediagateway.g430 | 0 MSY-TRPMAJNA[VOICE-Error: No Call Controller
Found, ID=N/A
<190>Apr 21 14:30:25 149.49.77.11 -NoTag: -NoUTC 2009 965 1
```

```
mediagateway.g430 | 0 BOOT MESSAGE[BOOT-Informational: Booting from
bank B with firmware version 29.22.50, ID=N/A
<190>Apr 21 14:30:25 149.49.77.11 -NoTag: -NoUTC 2009 965 1
mediagateway.g430 | 0 coldStart[BOOT-Informational: System boot up
from cold reset, ID=N/A
<187>Apr 21 14:30:25 149.49.77.11 -NoTag: -NoUTC 2009 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

```
Gxxx-001
(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:

```
01/18/2005,10:55:09:CLI-Notification: root:   set port disable 10/6
01/18/2005,10:49:03: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

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.

2. Optionally, define filters to limit the types of messages received (see Logging filter configuration on page 224).

Related topics:

Example discontinuation of the display of system messages on page 223
Example display of session logging configuration on page 223
Session logging message format on page 224

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

```
Gxxx-001
(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

```
Gxxx-001
(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:

```
01/18/2005,10:49:03:SWITCHFABRIC-Notification: Port Connection Lost on Module 10
port 5 was cleared

01/18/2005,10:55:09: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.

Related topics:

Commands used to set the logging filters on page 225
Severity levels on page 225
Default sink severity levels on page 226
Application filtering on page 226
Syslog server example on page 228
Log file example on page 228

Session log example on page 228

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). For the list of applications see Application filtering on page 226.
  - **severity** is the minimum severity to log for the specified application (use none to disable logging messages for the specified application). For a list of the severity levels and the default severity settings, see Severity levels on page 225.
  - **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
critical	2	Critical condition

Severity level	Code	Description
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
cna-tp	CNA test plugs
config	Configuration changes
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)

Application	Description
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
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.

```
Gxxx-001(super)# set logging session enable
Done!
Gxxx-001(super)# set logging session condition all Error
Done!
Gxxx-001(super)# set logging session condition ISAKMP Informational
```

```
Done!
Gxxx-001(super)# show logging session condition
*****************************************************
*** Message logging configuration of CLI sink ***
Sink Is Enabled
Sink default severity: Error
Application          ! Severity Override
-----------------------------------------
ISAKMP               ! Informational
```

Summary of logging configuration CLI commands

For more information about these commands, see the *Avaya Branch Gateways G250 and G350 CLI Reference*.

For more information about these commands, see the *Avaya Branch Gateway G430 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
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

Command	Description
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: VoIP QoS

VoIP QoS

The 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. For more information about configuring RTP and RTCP on the Branch Gateway, see RTP and RTCP configuration on page 231.

You can use many types of telephones and trunks that do not directly support VoIP. The Branch Gateway translates voice and signalling data between VoIP and the system used by the telephones and trunks.

Related topics:

RTP and RTCP configuration on page 231
Header compression configuration on page 232
Commands used to configure QoS parameters on page 238
Weighted Fair VoIP Queuing on page 240
Priority queuing on page 242

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.

Related topics:

Header compression configuration options on page 232
Header compression support by interface on page 233
Configuring IPHC on page 233
Summary of IPHC header compression CLI commands on page 234
Configuring VJ header compression on page 236
Commands used to display and clear header compression statistics on page 238

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
Dialer	IPHC and VJ

Note:

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
Done!
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
Done!
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
Done!
Gxxx-001(config-if:Serial 4/1:1)# ip rtp port-range 40000 50000
Done!
```

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 header-compression**.

Summary of IPHC header compression CLI commands

For more information about these commands, see the *Avaya Branch Gateways G250 and G350 CLI Reference*.

For more information about these commands, see the *Avaya Branch Gateway G430 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

Root level command	First level command	Description
		enter an interface type and number. Clearing the statistics does not cause renegotiation of parameters.
interface (dialer)		Enter the Dialer 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.
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-		Display a subset of header compression statistics in the form of a table

Root level command	First level command	Description
compression brief		
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
   Done!
   ```

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.

   Note:

   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 header-compression** command in the interface context.

Related topics:

Summary of Van Jacobson header compression CLI commands on page 237

Summary of Van Jacobson header compression CLI commands

For more information about these commands, see the *Avaya Branch Gateways G250 and G350 CLI Reference*.

For more information about these commands, see the *Avaya Branch Gateway G430 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
interface (dialer)		Enter the Dialer 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 the *Avaya Branch Gateways G250 and G350 CLI Reference*.

For more information about these commands, see the *Avaya Branch Gateway G430 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

The 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 Summary of QoS, RSVP, and RTCP configuration CLI commands on page 239.

For more information about these commands, see the *Avaya Branch Gateways G250 and G350 CLI Reference*.

For more information about these commands, see the *Avaya Branch Gateway G430 CLI Reference*.

Related topics:

Commands used to configure RTCP QoS parameters on page 239
Commands used to configure RSVP parameters on page 239
Summary of QoS, RSVP, and RTCP configuration CLI commands on page 239

Commands used to configure RTCP QoS parameters

Use the following commands to set the RTCP QoS parameters.

- **`set qos rtcp`**.
- **`show qos-rtcp`**

Avaya Branch Gateways G250 and G350 CLI Reference

For more information about these commands, see Summary of QoS, RSVP, and RTCP configuration CLI commands on page 239, or the

Avaya Branch Gateway G430 CLI Reference

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`**

Avaya Branch Gateways G250 and G350 CLI Reference

For more information about these commands, see Summary of QoS, RSVP, and RTCP configuration CLI commands on page 239, or

Avaya Branch Gateway G430 CLI Reference

Avaya Branch Gateway G450 CLI Reference

Summary of QoS, RSVP, and RTCP configuration CLI commands

For more information about these commands, see the *Avaya Branch Gateways G250 and G350 CLI Reference*.

For more information about these commands, see the *Avaya Branch Gateway G430 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).
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.WFVQ is the default queuing mode for 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.

Related topics:

Summary of WFVQ configuration CLI commands on page 241

Summary of WFVQ configuration CLI commands

For more information about these commands, see the *Avaya Branch Gateways G250 and G350 CLI Reference*.

For more information about these commands, see the *Avaya Branch Gateway G430 CLI Reference*.

Root level command	Command	Description
interface (fastethernet | dialer)		Enter the 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.
	priority-queue	Enable or disable priority queuing mode in a FastEthernet interface. If you disable priority queuing, WFVQ is re-enabled.
	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 re-enabled.
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:

- FastEthernet (L2, L2-L3) - when Traffic Shaping is 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.

Related topics:

Summary of priority queueing configuration CLI commands on page 242

Summary of priority queueing configuration CLI commands

For more information about these commands, see the *Avaya Branch Gateways G250 and G350 CLI Reference*.

For more information about these commands, see the *Avaya Branch Gateway G430 CLI Reference*.

Root level command	Command	Description
interface (fastethernet | dialer)		Enter the FastEthernet, or Dialer interface configuration context
	priority-queue	Enable or disable priority queuing mode in a FastEthernet interface. By default, priority queuing is off, and WFVQ is enabled on 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

Root level command	Command	Description
		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 the Branch Gateway

Modems and the Branch Gateway

You can connect a USB modem to the Branch Gateway. A USB modem must be connected to the USB port on the Branch Gateway chassis.

The USB port requires configuration for modem use.

For more information about these commands, see the *Avaya Branch Gateways G250 and G350 CLI Reference*.

For more information about these commands, see the *Avaya Branch Gateway G430 CLI Reference*.

Note:

If you have an Avaya Service contract, no configuration of the USB port is necessary for Services personnel to remotely access the Branch Gateway through a USB modem.

Related topics:

USB-modem interface configuration on page 245

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

Related topics:

Example of IP address to USB port assignment on page 246
The ppp authentication command parameters on page 246
Summary of CLI commands for configuring the USB port for modem use on page 246

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:

```
Gxxx-001
(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

Summary of CLI commands for configuring the USB port for modem use

For more information about these commands, see the *Avaya Branch Gateways G250 and G350 CLI Reference*.

For more information about these commands, see the *Avaya Branch Gateway G430 CLI Reference*.

Root level command	Command	Description
interface usb-modem		Enter USB-modem interface configuration context
	async modem-init-string	Change the default modem initialization string

Root level command	Command	Description
	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. See The ppp authentication command parameters on page 246.
	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
	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.

Chapter 11: WAN interfaces

WAN interfaces

You can use a Fast Ethernet port on the Branch Gateway chassis as the endpoint for a WAN line by configuring the FastEthernet interface for PPP over Ethernet (PPPoE). The Branch Gateway serves as a router, as well as the endpoint, for the WAN line. For more information about routing, see The router on page 477.

Related topics:

Configuring the initial WAN on page 249

Configuring the initial WAN

Procedure

1. Use the Fast Ethernet port on the G430 chassis as the endpoint for a WAN line by configuring this interface for PPPoE.
   See Configuring PPPoE on page 250.
2. Test the WAN configuration.
   See WAN configuration and testing connectivity.
3. Enter **`copy running-config startup-config`** to save the configuration.

Related topics:

PPPoE overview on page 249

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.

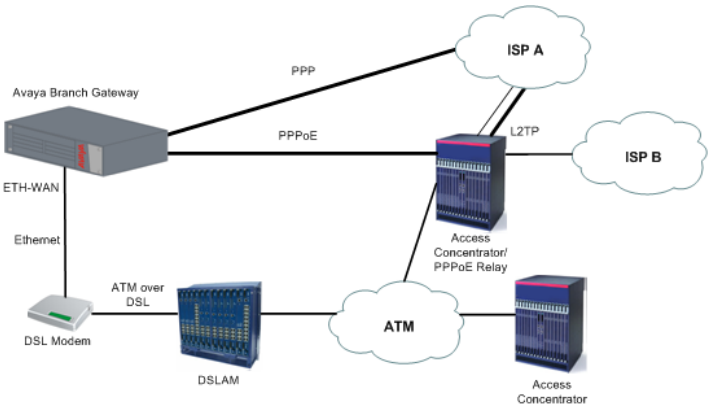


Figure 8: Typical PPPoE Network Topology

Related topics:

[Configuring PPPoE](#) on page 250
[Summary of PPPoE commands](#) on page 251

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. See [Dynamic CAC](#) on page 278.
   - The interface is not part of a primary-backup interface pair. See [Backup interfaces](#) on page 254.

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 (see DHCP client configuration on page 204).

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 123456
     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 123456
     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.

Summary of PPPoE commands

For more information about these commands, see the *Avaya Branch Gateways G250 and G350 CLI Reference*.

For more information about these commands, see the *Avaya Branch Gateway G430 CLI Reference*.

Root level command	Command	Description
interface fastethernet		Enter the FastEthernet interface context
	encapsulation pppoe	Change the encapsulation to PPPoE
	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

Root level command	Command	Description
	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
	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

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 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 traffic-shape** command to view 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 to another node on the network. Each node is periodically pinged and checked if an answer was received. This checks host reachability and network connectivity.

Summary of WAN configuration verification commands

For more information about these commands, see the *Avaya Branch Gateways G250 and G350 CLI Reference*.

For more information about these commands, see the *Avaya Branch Gateway G430 CLI Reference*.

Command	Description
ping	Check host reachability and network connectivity
show interfaces	Display interface configuration and statistics for a particular interface or all interfaces
show ip interface	Display information about an IP interface
show traffic-shape	Display traffic shaping configuration information

Backup interfaces

You can configure backup relations between a pair of any Layer 2 interfaces, except the VLAN interface. A backup interface is activated when the primary interface fails. The backup interface is deactivated when the primary interface is restored. A Dialer interface, FastEthernet interface, GRE tunnel interface, or Loopback interface can serve as a backup interface to a FastEthernet interface, GRE tunnel interface, or Loopback interface on the same module.

Note:

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 expiration of the leases on its IP address or no reception of an IP address does not cause activation of the backup interface.

Related topics:

Backup delay configuration on page 254
Interface backup relations rules on page 255
Summary of backup interfaces commands on page 255

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.

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 the *Avaya Branch Gateways G250 and G350 CLI Reference*.

For more information about these commands, see the *Avaya Branch Gateway G430 CLI Reference*.

Root level command	Command	Description
interface (fastethernet| loopback| tunnel)		Enter FastEthernet,Loopback, 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 the Branch Gateway to utilize a modem to provide redundant connectivity between a 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 the 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), the 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, Avaya Aura® Communication Manager 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 Dynamic CAC in the Branch Gateway, see Dynamic CAC on page 278. 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 the Branch Gateway and the Remote Access Server (RAS). For information on

ACL and QoS lists, see Policy lists on page 553. For information on WFQ, see Weighted Fair VoIP Queuing on page 240.

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 the Branch Gateway's 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. For more information about backup interfaces, see Backup interfaces on page 254.

Note:

You can only backup one interface with modem dialer backup.

Using the Branch Gateway's 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 the Branch Gateway.

The workaround is to use the Branch Gateway's 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. For more information about object tracking, see Object tracking on page 280.

Modem dial backup uses a modem connected directly to the Branch Gateway's USB or Console port. The modem can also be used to access the Branch Gateway CLI from a remote

location. The modem cannot do both at the same time. For information about remote access to the Branch Gateway via modem, see CLI access using modems on page 31.

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. For information about unnumbered IP interfaces, see Unnumbered IP interfaces on page 424.

Note:

Modem dial backup has complex interactions with other configuration modules within the 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. See Modem dial backup interactions with other features on page 262 for brief discussions of the various features required for an effective backup scenario for your VoIP installation.

Note:

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 topics:

Typical installations on page 258
Prerequisites for configuring modem dial backup on page 259
Configuring modem dial backup on page 259
Modem dial backup interactions with other features on page 262
Configuration example on page 264
Modem dial backup maintenance on page 268

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: MultimodemUSB (MT5634ZBA-USB), or USRobotics USB modem (5637)
- RAS properties:
  - A dialer string
  - Authentication parameters (username, password, PAP/CHAP)
  - IP addressing (static, dynamic, or unnumbered)
  - Routing (static, RIP, or OSPF)
  - IPSec VPN, with all necessary parameters configured

Note:

Make sure policy is configured properly at the RAS server to ensure that signaling has priority over regular traffic.

For modem configuration instructions, see Modems and the Branch Gateway.

Configuring modem dial backup

Procedure

1. From the general context, use the **`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 5555555
   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 123456
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:

```
G430-001(if:Tunnel 1)# backup interface dialer 1
Done!
```

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. For more information on the **backup interface** command, see Backup interfaces on page 254.
- 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. For more information on configuring PPP authentication and encryption, see PPPoE overview on page 249. For more information on heading compression, see Header compression configuration on page 232.
- It is recommended to filter traffic through the Dialer interface to permit only those packets necessary for continued interaction with the Avaya Aura® Communication Manager server. Filtering can be accomplished using access control lists, which specify traffic permissible through a selected interface. For more information on configuring access control lists, see Policy lists on page 553.
- 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 Avaya Aura® Communication Manager 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 Avaya Aura® Communication Manager server by forcing voice calls to and from the branch office to use the PSTN for bearer traffic. For more information on configuring Dynamic CAC, see Dynamic CAC on page 278. 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. For information on dynamic IP addressing, see Dynamic local peer IP on page 506. For information on configuring unnumbered IP, see Unnumbered IP interfaces on page 424.
- 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. For more information about object tracking, see Object tracking on page 280.

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.

Note:

Refer to www.multitech.com for a listing of modem AT commands used to configure the modem directly.

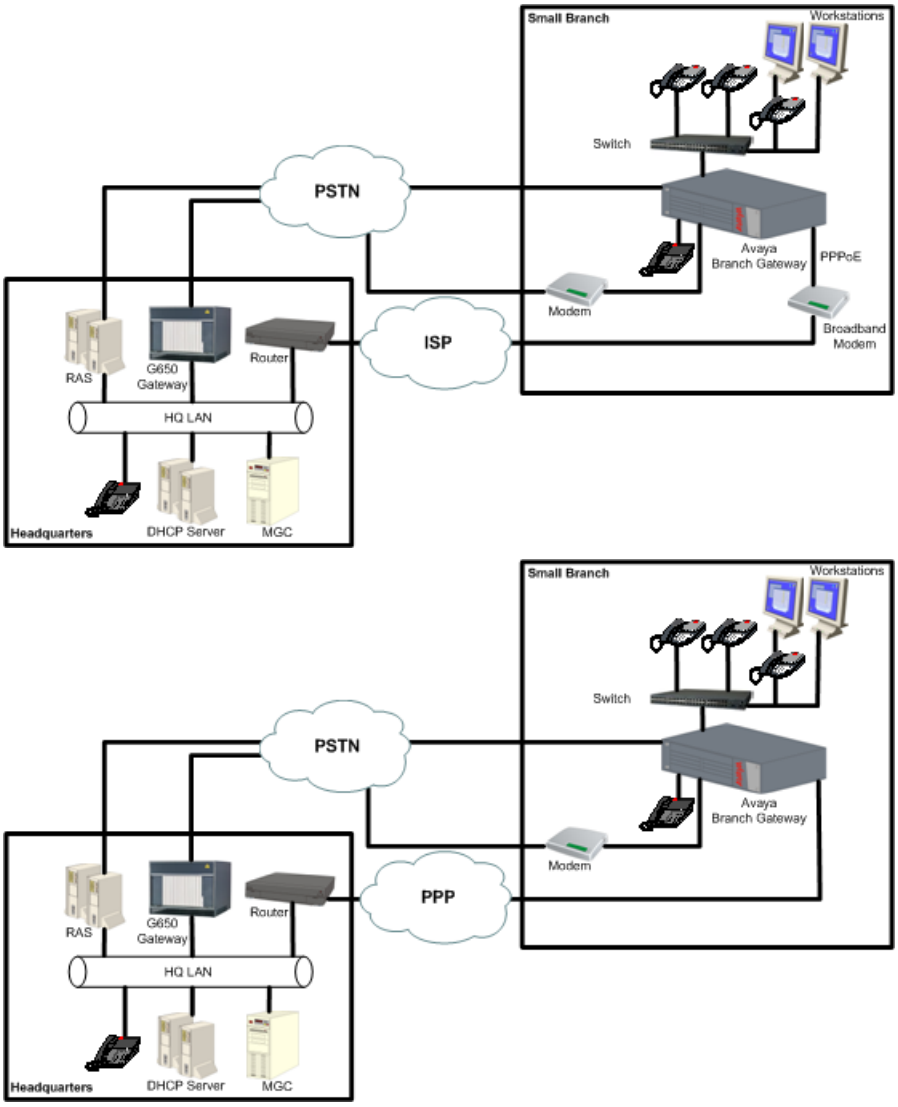
Configuration example

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 broadband link connected to the WAN FastEthernet 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.



Related topics:

[Command sequence](#) on page 265
[Command sequence explanation](#) on page 266

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”
Done!
```

```
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”
Done!
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
Done!
Gxxx-001(super-if:Dialer 1)# dialer string 2 7325213412
Done!
Gxxx-001(super-if:Dialer 1)# dialer modem-interface usb-modem
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
G430-001(super)# interface usb-modem
Gxxx-001(super-if:USB-Modem)# ppp authentication none
Done!
Gxxx-001(super-if:USB-Modem)# no shutdown
Done!
Gxxx-001(super-if:USB-Modem)# exit
Gxxx-001(super)#
Step 12
Gxxx-001(super)# interface fastethernet 10/2
Gxxx-001(if:fastEthernet 10/2)# backup interface Dialer 1
Done!
Gxxx-001(if:fastEthernet 10/2)# 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
Done
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.

2. 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. For more information on configuring access control lists, see Policy lists on page 553.

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 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 USB port to support the modem with the **`interface usb-modem`** command.

    For more information on configuring the USB-modem interface to support modems, see Modems and the Branch Gateway on page 245.

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 FastEthernet 10/2, the primary WAN connection to the headquarters network. The Dialer activates in the event of a failure of the FastEthernet port and all permitted traffic transverses the Dialer interface.

    For more information on backing up WAN interfaces, see Backup interfaces on page 254.

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. For more information on configuring OSPF routing, see OSPF on page 466.

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.

Related topics:

Commands used to activate session logging on page 268
Severity levels of the logging session on page 269

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 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. For more information on logging configuration, see System logging on page 215.

Note:

Syslog and log file logging are also available. See System logging on page 215.

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>	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>	Informational	In a modem dial backup scenario, the event triggering the Dialer interface is a failure of	None required.

Log Message	Severity	Possible cause	Action
		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.	
Dialer 1 string <string_ID> <dialer_string>	Informational	The value of <*string_ID*> is equal to the ID of the string configured using the dialer string command. The value of <*dialer_string*> 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	None required.

Log Message	Severity	Possible cause	Action
		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.	
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.	Troubleshooting steps: • Check modem cable connection to port. • Check modem cable connection to modem. • Check power to modem.

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 - Unplugged	Warning	This message is generated when a modem cable is connected to the USB port, but no modem is detected.	Troubleshooting steps: • Check modem cable connection to modem and to USB port and re-seat if necessary.

Log Message	Severity	Possible cause	Action
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.
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.

Log Message	Severity	Possible cause	Action
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 the *Avaya Branch Gateways G250 and G350 CLI Reference*.

For more information about these commands, see the *Avaya Branch Gateway G430 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

Root level command	Command	Description
	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
	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
interface (fastethernet | loopback| tunnel)		Enter the FastEthernet, Loopback, 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 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 on page 583.

Note:

ICMP keepalive has been replaced by the object tracking feature that supports keepalive probes over WAN, FastEthernet, Loopback, PPPoE, and Dialer PPP interfaces. ICMP keepalive is still supported for backward compatibility. For information about object tracking, see Object tracking on page 280.

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.

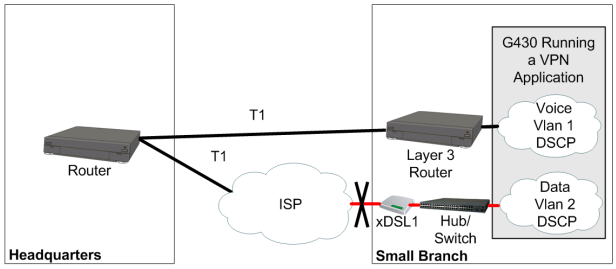


Figure 9: Branch Gateway with T1 and xDSL lines

For example, your branch office might have a G430 that connects to an external router that connects to Headquarters over a T1 line and through 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. For details, see GRE tunneling on page 432.

Note:

For details on DHCP Client see DHCP client configuration on page 204.

Related topics:

Command used for enabling the ICMP keepalive feature on page 276

Commands used to define the ICMP keepalive parameters on page 276
Example of configuring ICMP keepalive on page 276
Summary of ICMP keepalive configuration commands on page 277

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 these commands, see Summary of ICMP keepalive configuration commands *on page 277* or

Avaya Branch Gateway G430 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 Summary of ICMP keepalive configuration commands on page 277

For more information about these commands, see the *Avaya Branch Gateway G430 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 the *Avaya Branch Gateways G250 and G350 CLI Reference*.

For more information about these commands, see the *Avaya Branch Gateway G430 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.
	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 Avaya Aura® Communication Manager 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
- 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.

Related topics:

Dynamic CAC tasks on page 278
Summary of dynamic CAC configuration commands on page 279

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 Avaya Aura® Communication Manager. For details, see *Administrator Guide for Avaya Aura® Communication Manager*.

For more information about these commands, see Summary of dynamic CAC configuration commands *on page 279* or *Avaya Branch Gateway G430 CLI Reference* .

Summary of dynamic CAC configuration commands

For more information about these commands, see the *Avaya G430 CLI Reference*.

Root level command	Command	Description
interface (dialer| loopback| fastethernet|tunnel| vlan)		Enter theDialer, 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: • **bbl**. 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.
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.

Related topics:

Configuring object tracking on page 280
Tasks for maintaining object tracking on page 286
Typical object tracking applications on page 289
Summary of object tracking configuration commands on page 293

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 G430 CLI Reference*.

   Note:

   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. For more information on DHCP Client see DHCP client configuration on page 204.

Related topics:

Configuring RTR on page 281
Object tracking provisioning on page 284

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 on page 0 to 7 on page 0 .

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.

Related topics:

Configuring a simple object tracker on page 284
Configuring a track list on page 284
Object tracking configuration workflow on page 285

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”
   Done!
   ```

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”
Done!
```

```
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 Summary of object tracking configuration commands on page 293 or the *Avaya Branch Gateway G430 CLI Reference*

Related topics:

Viewing RTR and object trackers logging on page 286
Example of tracking a single remote device on page 287
Example of tracking a group of devices on page 288

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

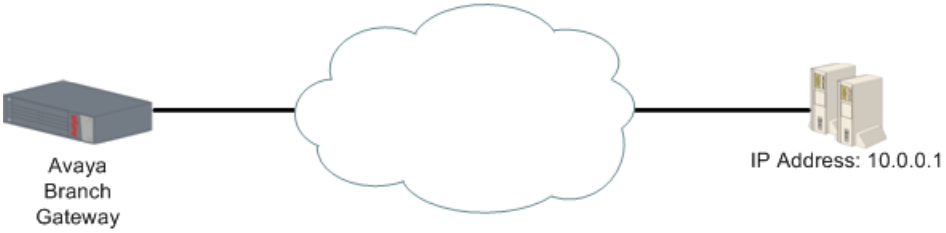


Figure 10: Tracking a single remote device

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

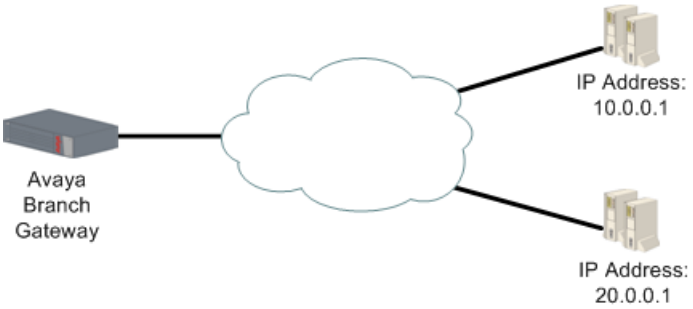


Figure 11: Tracking multiple remote devices

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. See Typical application – VPN failover using object tracking on page 289.
- Trigger the failover mechanism for interfaces. See Typical application – backup for the WAN FastEthernet interface on page 290, and Typical application – interface backup via policy-based routing on page 291.
- Track the state of a route: a static route, a PBR next hop, or the DHCP client default route. For an example of how to track the DHCP client default route, see Typical application – tracking the DHCP client default route on page 293.

Related topics:

Typical application – VPN failover using object tracking on page 289
Typical application – backup for the WAN FastEthernet interface on page 290
Typical application – interface backup using policy-based routing on page 291
Typical application – tracking the DHCP client default route on page 293

Typical application – VPN failover using object tracking

In this application, the 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, the Branch Gateway can failover to a backup gateway, and attempt to establish a VPN connection to it.

A typical application of this type is described in full in Failover using a peer-group on page 538.

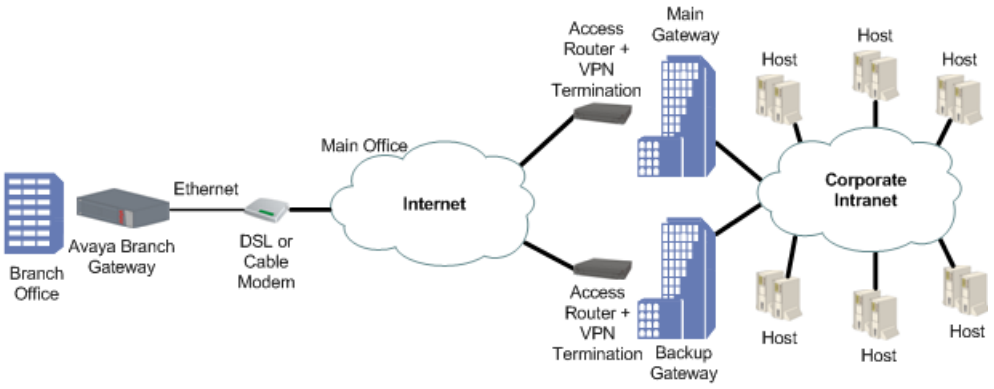


Figure 12: Failover VPN topology using object tracking

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.

Related topics:

Configuring the backup mechanism on page 290

Configuring the backup mechanism

Procedure

1. 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.
5. Define Loopback 1 as a backup interface for the WAN FastEthernet interface.

   Thus, when the track list is down the Loopback interface will be up until the track list is up again.

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 loopback 1 interface
!
interface loopback 1
ip address 10.0.0.1        255.0.0.0
 exit
!
! Assign the loopback 1 interface to be the backup interface for
! interface WAN FastEthernet 10/2.
!
interface fastethernet 10/2
    backup interface loopback 1
    backup delay 0 60
    exit
```

Typical application – interface backup using policy-based routing

In the previous typical application (see Typical application – backup for the WAN FastEthernet interface on page 290), 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 a VLAN interface used to connect the Branch Gateway to an external router. 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 VLAN interface used to connect the Branch Gateway to an external router. 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
!
interface Vlan 2
    ip address 149.49.43.254   255.255.255.0
      exit
!
! Configure next hop list 10 with interface fastethernet 10/2 as the
! first next hop, and the VLAN interface used to connet to the external
! router as the second next hop.
!
ip next-hop-list 10
    next-hop-interface 1 FastEthernet 10/2
        next-hop-ip 2 149.49.43.1
exit
```

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 the *Avaya Branch Gateways G250 and G350 CLI Reference*.

For more information about these commands, see the *Avaya Branch Gateway G430 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.

Root level command	First level command	Second level command	Description
	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
		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

Chapter 12: Emergency Transfer Relay (ETR)

Emergency Transfer Relay (ETR)

The ETR feature provides basic telephone services in the event of system failure, such as a power outage or a failed connection to the MGC. ETR services are offered on installed MM714B media modules. When ETR is activated, the G430 connects the MM714B's trunk port 5 to line port 4. All calls are then 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 do not start to operate until the active call ends.

You can install an MM714B media module in any slot (1-3, 5-8).When ETR is active and the Branch Gateway has power, the ETR LED is lit.

Related topics:

ETR state configuration on page 297
Summary of ETR commands on page 298

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.

Related topics:

Activating ETR manually on page 297
Deactivating ETR manually on page 298
Restoring ETR to automatic activation on page 298

Activating ETR manually

About this task

Use this command only for testing.

Procedure

Enter **set etr 3 manual-on**

Deactivating ETR manually

Procedure

Enter **set etr 3 manual-off**.

Result

ETR does not become active in the event of a link failure.

Restoring ETR to automatic activation

Procedure

Enter **set etr 3 auto**Enter **set etr 10 auto**

If the system fails, the trunk and port in the MM714B 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 the *Avaya Branch Gateways G250 and G350 CLI Reference*.

For more information about these commands, see the *Avaya Branch Gateway G430 CLI Reference*.

Command	Description
set etr	Enable or disable ETR mode on the Branch Gateway chassis or on an MM714B media module, or enable the gateway to control ETR mode automatically.

Command	Description
show etr	Display the status of ETR mode. This information includes the following: • Admin state (auto, manual-off, or manual-on) • Module status (in service, out of service, or out of service waiting for off-hook) • Trunk number of the trunk connected to ETR • Line number of the line connected to ETR • Line status (off hook or on hook)

Chapter 13: SNMP

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.

Related topics:

Agent and manager communication on page 302
SNMP versions on page 302
SNMP trap configuration on page 307
Dynamic trap manager on page 311
SNMP configuration examples on page 312

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.

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 G250, G350, 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.

Related topics:

SNMPv1 on page 303
SNMPv2c on page 303
SNMPv3 on page 304
Users on page 304
Groups on page 305
Views on page 306

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.

Related topics:

SNMP security levels on page 304
snmp-server user command on page 305

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 privacy protocol, and the user's privacy password if you enable DES 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.

Related topics:

Pre-configured SNMP groups on page 306
snmp-server group command on page 306

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		v3configVie w
v3AdminView G	v3 (USM)	AuthPriv	iso	iso	iso
v3ReadWriteG	v3 (USM)	AuthNoPriv	v3configView	v3configView	v3configVie w

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. For a list of MIBs and their OIDs, see Media Gateway MIB files on page 616.

Related topics:

SNMPv3 view creation on page 307

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.

Related topics:

snmp-server host command parameters on page 308
Notification types on page 308
Summary of SNMP trap configuration commands on page 309
Summary of SNMP access configuration commands on page 310

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. For a list of possible notification types, see Notification types on page 308

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
- **l3-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 the *Avaya Branch Gateways G250 and G350 CLI Reference*.

For more information about these commands, see the *Avaya Branch Gateway G430 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

Root level command	Command	Description
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 the *Avaya Branch Gateways G250 and G350 CLI Reference*.

For more information about these commands, see the *Avaya Branch Gateway G430 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

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.

Note:

The dynamic trap manager is created by default and cannot be removed.

Related topics:

Dynamic trap manager parameters on page 312
Summary of dynamic trap manager configuration commands on page 312

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. For a list of possible notification types, see Notification types on page 308.

Summary of dynamic trap manager configuration commands

For more information about these commands, see the *Avaya Branch Gateways G250 and G350 CLI Reference*.

For more information about these commands, see the *Avaya Branch Gateway G430 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:

```
Gxxx-001(super)# show snmp
Authentication trap disabled
Community-Access     Community-String
----------------     ----------------
read-only            *****
```

```
read-write           *****
SNMPv3 Notification Status
----------------------------
Traps: Enabled
Informs: Enabled         Retries: 3   Timeout: 3 seconds
SNMP-Rec-Address Model  Level   Notification   Trap/Inform   User name
---------------- -----  ------   ------------   -----------  ----------
149.49.70.137     v1     noauth   all              trap       ReadCommN
 UDP port: 162 DM
```

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
Done!
```

The following example creates a read-only user:

```
Gxxx-001# snmp-server user joseph ReadOnlyG v3 auth md5 katmandu priv des56
ktamatan
```

The following example creates a read-write user:

```
Gxxx-001# snmp-server user johnny ReadWriteG v3 auth md5 katmandu priv des56 ktamatan
```

The following example creates an admin user:

```
Gxxx-001# snmp-server user johnny v3AdminG v3 auth md5 katmandu priv des56 ktamatan
```

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: Contact closure

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 Avaya Aura® Communication Manager software. For more information, see Branch Gateway Controller configuration on page 67.

It is recommended that you use an Avaya Partner Contact Closure Adjunct™ for contact closure. For more information, see *Overview for the Avaya Branch Gateway G430*. An Avaya Partner Contact Closure Adjunct™ 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 the Avaya Aura® Communication Manager. For more information, see *Administrator Guide for Avaya Aura® Communication Manager*.

Related topics:

Configuring contact closure hardware on page 315

Configuring contact closure hardware

Procedure

Connect an Avaya Partner Contact Closure Adjunct™ 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™.

For information on contact closure specifications, see *Overview for the Avaya Branch Gateway G430*.

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™ 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™ 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™. 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™. 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™ box.

```
Gxxx-001(super)# show contact-closure
MODULE   PORT   RELAY   ADMIN             PULSE DURATION (secs)   STATUS
-------  -----  ------  ----------------  ---------------------   ------
10       2      1       mgc               5 secs                  off
10       2      2       mgc               3 secs                  off
```

Summary of contact closure commands

For more information about these commands, see the *Avaya Branch Gateway G430 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 15: Announcement files

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 15 announcements can be played simultaneously, and one port may be used for recording. Recording, storing, and playing announcement files is controlled by Communication Manager.

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

Announcement file operations

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

Procedure

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

Procedure

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 announcment 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
```

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:

```
Gxxx-001(super)# show announcements files
Mode: FTP-SERVER/SCP-CLIENT
```

```
ID   File              Description  Size (Bytes) Date
---- ---------------- ------------ ------------ -----------------
5     46xxupgrade.scr  Announcement1  4000        09:54:55 04 APR 2005
8     4601dbte1_82.bin Announcement2  8000        09:55:55 04 APR 2005
9     4602dbte1_82.bin Announcement3  16000       09:56:55 04 APR 2005
Nv-Ram:
Total bytes used: 28000
Total bytes free: 7344800
Total bytes capacity(fixed) 7372800
```

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:

```
Gxxx-001(super)# show download announcement-file status
Module #9
===========
Module           : 9
Source file      : hellosource.wav
Destination file : hellodestination.wav
Host             : 135.64.102.64
Running state    : Idle
Failure display  : (null)
Last warning     : No-warning
Bytes Downloaded  : 7825
===========
```

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 the *Avaya Branch Gateways G250 and G350 CLI Reference*.

For more information about these commands, see the *Avaya Branch Gateway G430 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 the Branch Gateway announcement directory
copy scp announcement-file	Download an announcement file from a remote SCP server to the Branch Gateway announcement directory
copy usb announcement-file	Download an announcement file from a USB mass storage device to the Branch Gateway announcement directory
erase announcement-file	Erase an announcement file from the Branch Gateway announcement directory
rename announcement-file	Rename an announcement file in the Branch Gateway announcement directory
show announcements files	Display the announcements files stored in the 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

Chapter 16: Advanced switching

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.

Related topics:

VLAN configuration on page 325
Port redundancy on page 331
Port mirroring on page 334
Spanning tree on page 336
Port classification on page 341

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.

Related topics:

VLAN Tagging on page 326
Multi VLAN binding on page 326
Gateway VLAN table on page 327
Ingress VLAN Security on page 327
ICC-VLAN on page 328
Configuring ICC-VLAN on page 328
VLAN configuration examples on page 328
Summary of VLAN commands on page 330

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, the 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 figure on page 327 shows these binding modes.

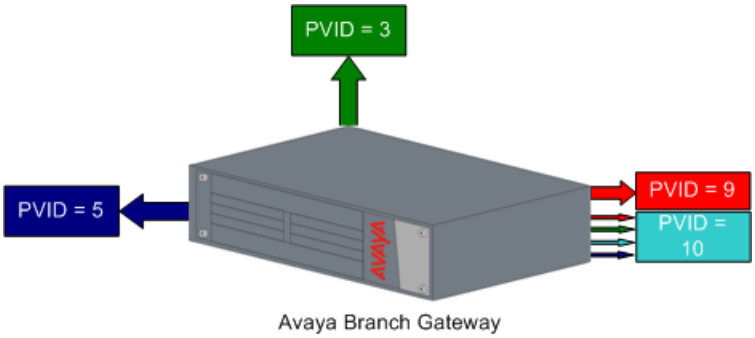


Figure 13: Multi VLAN Binding

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 eight 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

Before you begin

About this task

You muse 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:

```
Gxxx-001(super)# show trunk
Port   Mode Binding mode              Native VLAN
------ ----- ------------------------ -----------
10/3   dot1q bound to configured VLANs 54
```

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 the *Avaya Branch Gateways G250 and G350 CLI Reference*.

For more information about these commands, see the *Avaya Branch Gateway G430 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

Root level command	First level Command	Description
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
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.

You can configure up to 25 pairs of ports per chassis. Each pair contains a primary and secondary port. You can configure any type of Ethernet port to be redundant to any other. You can configure redundant ports from among the Ethernet LAN port on the Branch Gateway front panel and the Ethernet ports (1 to 24) and the Gigabit Ethernet port (51) on the MM314 Media

Module or the Ethernet ports (1-40) and the Gigabit Ethernet port (51) on the MM316 Media Module.

Related topics:

Secondary port activation on page 332
Switchback on page 332
Enabling and disabling redundancy pairs on page 332
Defining or removing redundancy pairs on page 333
Configuring time constants on page 333
Displaying port redundancy schemes on page 333
Port redundancy configuration examples on page 333
Summary of port redundancy commands on page 334

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 redundancy-intervals`** 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.

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:

```
G430-001(super)# set port redundancy 10/3 10/4 on 1
Monitor: Port 10/4 is redundant to port 10/3.
Port redundancy is active - entry is effective immediately
```

The following example deletes a port redundancy pair:

```
G430-001
(super)# set port redundancy 10/3 10/4 off
Entry Monitor removed: Port 10/4 is not redundant to port 10/3
```

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:

```
G430-001
(super)# show port redundancyRedundancy Name     Primary Port        Secondary
Port      Status
-----------------   --------------      ----------------    --------
Monitor             10/3            10/4            primary
Minimum Time between Switchovers: 60
Switchback interval: 30
```

Summary of port redundancy commands

For more information about these commands, see the *Avaya Branch Gateways G250 and G350 CLI Reference*.

For more information about these commands, see the *Avaya Branch Gateway G430 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.

Related topics:

Port mirroring configuration examples on page 335
Summary of port mirroring commands on page 335

Port mirroring configuration examples

The following example creates a port mirroring pair in the Branch Gateway:

```
G430-001(super)# set port mirror source-port 10/3 mirror-port 10/4 sampling always
direction rx
Mirroring rx packets from port 10/3 to port 10/4 is enabled
```

The following example displays port mirroring information for the Branch Gateway:

```
G430-001(super)# show port mirror
port mirroring
Mirroring both Rx and Tx packets from port 10/3 to port 10/4 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 the *Avaya Branch Gateways G250 and G350 CLI Reference*.

For more information about these commands, see the *Avaya Branch Gateway G430 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

- **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.

Related topics:

Spanning tree protocol on page 336
Spanning tree per port on page 337
Rapid Spanning Tree Protocol (RSTP) on page 337
Spanning tree configuration examples on page 339
Summary of spanning tree commands on page 340

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 media-dependent 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

Related topics:

Port roles on page 337
RSTP port types on page 338

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
Designated Root Priority: 32768
Designated Root Cost: 0
Designated Root Port: No root port, Bridge is Designated root
Root Max Age: 20   Hello Time: 2
Root Forward Delay: 15
Bridge ID MAC ADDR: 00-04-0d-ea-b0-2d
Bridge ID priority: 32768
Bridge Max Age: 20        Bridge Hello Time: 2
Bridge Forward Delay: 15  Tx Hold Count 3
Spanning Tree Version is rapid spanning tree
Spanning Tree Default Path Costs is according to common spanning tree
Port   State         Cost       Priority
------ ------------ ---------- ------------
10/3 not-connected 4          128
10/4 not-connected 4          128
```

Summary of spanning tree commands

For more information about these commands, see the *Avaya Branch Gateways G250 and G350 CLI Reference*.

For more information about these commands, see the *Avaya Branch Gateway G430 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 the Branch Gateway

Command	Description
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
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.

Related topics:

Port classification configuration examples on page 341
Summary of port classification commands on page 342

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:

```
G430-001(super)# show port classification
Port      Port Classification
--------  ------------------------
```

```
10/3      valuable
10/4      regular
```

Summary of port classification commands

For more information about these commands, see the *Avaya Branch Gateways G250 and G350 CLI Reference*.

For more information about these commands, see the *Avaya Branch Gateway G430 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 17: Monitoring applications

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.

Related topics:

RMON on page 343
RTP statistics on page 346
Packet sniffing on page 380
Interface status reports on page 400
CNA test plugs on page 401
Echo cancellation on page 408
Integrated analog testing – Test and Heal on page 409
Service Level Agreement Monitor Agent on page 417

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.

Related topics:

[RMON configuration examples](#) on page 344
[Summary of RMON commands](#) on page 345

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 the *Avaya Branch Gateways G250 and G350 CLI Reference*.

For more information about these commands, see the *Avaya Branch Gateway G430 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

About this task

The RTP statistics application collects data and statistics for RTP sessions (streams) from the 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.

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 Avaya 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 the Branch Gateway's firmware, and does not require any dedicated hardware. For information about configuring VMON in Avaya Aura® Communication Manager, see *Administrator Guide for Avaya Aura® Communication Manager*.

Note:

The Branch Gateway performs traceroutes whenever RTP statistics is enabled.

The RTP statistics application provides the following functionality:

Procedure

1. Collects QoS data from the 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 the 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.

Related topics:

Configuring the RTP statistics application on page 347
RTP statistics output on page 356
RTP statistics examples on page 370
Summary of RTP statistics commands on page 379

Configuring the RTP statistics application

About this task

To configure the RTP statistics application, work through the following sections, in order:

Procedure

1. Viewing RTP statistics thresholds on page 348
2. RTP statistics thresholds on page 350
3. RTP statistics application on page 351
4. Viewing application configuration on page 352
5. QoS traps on page 353
6. QoS fault and clear traps on page 354
7. The trap rate limiter on page 355

Related topics:

Viewing RTP statistics thresholds on page 348
RTP statistics thresholds on page 350

RTP statistics application on page 351
Viewing application configuration on page 352
QoS traps on page 353
QoS fault and clear traps on page 354
Configuring QoS fault and clear traps on page 355
The trap rate limiter on page 355
Configuring the trap rate limiter on page 355

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 Avaya Aura® Communication Manager, 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® Communication Manager*.

Related topics:

Thresholds types on page 348
Viewing the configured thresholds on page 349
QoS metrics on page 349

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.

Note:

All CLI commands described in this section are available in the general context of the CLI.

Viewing the configured thresholds

Enter **show rtp-stat thresholds**. For example:

```
Gxxx-001(super)# show rtp-stat thresholds
Item                  Threshold      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
Codec RTT	An estimation of the overall Round Trip Time (RTT) on the voice-channel, including the network delay and internal delays. RTT is the time taken for a message to get to the remote peer and back to the local receiver.	Each time an RTCP packet is received
Echo Return Loss	The echo cancellation loss on the TDM bus	Every RTCP interval
Loss	The estimated network RTP packet loss. 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**.	Every RTCP interval

Metric	Description	Evaluation time
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

RTP statistics thresholds

About this task

RTP statistics thresholds should be configured so that incrementation of QoS event counters coincides with real detectable bad QoS in your network. Optimal values are different for each network. Configure any thresholds that are not already configured as you require them. See Viewing RTP statistics thresholds on page 348.

For a description of each metric, see QoS metrics on page 349. 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. For example, the Codec RTT metric indicates the overall delay experienced by the user. If you configure a meaningful threshold on the Codec RTT metric, metrics such as Local Jitter, Remote Jitter, and rtt metrics may help you identify causes when Codec RTT exceeds its threshold.

Related topics:

Configuring RTP statistics thresholds on page 350

Configuring RTP statistics thresholds

Procedure

1. Use the **`rtp-stat thresholds`** command to set thresholds on QoS indicators. For example:

```
Gxxx-001(super)# rtp-stat thresholds echo-return-loss 5
Done!
```

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. Use 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.

RTP statistics application

About this task

When you enable the RTP statistics application on the Branch Gateway, the application starts to collect QoS data from the VoIP engines and stores the data in the Branch Gateway RAM, which holds a limited history of RTP session entries. The VoIP engine also starts to perform and report UDP traceroutes.

Session data and automatic session traceroute results can be viewed using the CLI.

Related topics:

Enabling the RTP statistics application on page 351
Resetting the RTP statistics application on page 351

Enabling the RTP statistics application

Procedure

Enter **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)
```

Resetting the RTP statistics application

Procedure

Enter **rtp-stat clear**.

All counters are reset and the RTP statistics history is erased.

Viewing application configuration

Viewing the application configuration helps you 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.

Enter **`show rtp-stat config`**. For example:

```
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
```

Related topics:

RTP statistics application output field descriptions on page 352

RTP statistics application output field descriptions

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.

Name	Description
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:	
Size	The maximum number of RTP session entries held in the session table in the Branch 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.

QoS traps

About this task

You can configure the application to automatically generate QoS traps via 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. For example, if the event threshold for packet loss is 2, the application generates a trap at the termination of any session in which packet-loss was sampled over its threshold twice or more during the session.

⚠ 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.

Related topics:

Enabling QoS traps on page 354

Enabling QoS traps

1. View the RTP statistic thresholds and modify their configurations as necessary. See Viewing RTP statistics thresholds on page 348 and RTP statistics thresholds on page 350.
2. If you need to modify the minimum statistic window, use the **rtp-stat min-stat-win** command. For example:

   ```
   Gxxx-001(super)# rtp-stat min-stat-win 50
   Done!
   ```

   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**. For example:

   ```
   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**. For more information about the dynamic trap manager, see Dynamic trap manager on page 311.
4. Enter **rtp-stat qos-trap** to enable the traps, if not already enabled. For example:

   ```
   Gxxx-001# rtp-stat qos-trap
   The RTP statistics QoS trap is enabled
   ```

   QoS traps are now enabled.

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.

Related topics:

Viewing RTP statistics summary reports on page 356
RTP statistics summary reports output field descriptions on page 356
Viewing RTP session statistics on page 357
Detailed CLI output per RTP session on page 359
Viewing QoS traps, QoS fault traps, and QoS clear traps on page 364
Example of QoS trap output on page 364
QoS Trap output fields on page 365
Example of QoS fault and clear trap output on page 368
QoS fault and clear trap output fields on page 368
Viewing automatic traceroute results on page 369
RTP traceroute results output on page 370

Viewing RTP statistics summary reports

RTP statistics summary reports display QoS trap statistics for the VoIP engine(s).

Enter **`show rtp-stat summary`**. For example:

```
Gxxx-001(super)# show rtp-stat summary
Total QoS traps: 23
QoS traps Drop : 0
Qos Fault
Engine                              Active   Total    Mean      Tx
ID   Description     Uptime         Session  Session  Duration  TTL
---  --------------  -----------    -------  -------  --------  ----
000        internal  04,18:15:15     2/1      35/24   01:04:44    64
```

RTP statistics summary reports output field descriptions

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

Field	Description
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 354.
Engine ID	The ID of the VoIP engine. Since the Branch 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:

```
Gxxx-001(super)# show rtp-stat sessions last 5
ID    QoS Start date and time End Time Type     Destination
----- --- ------------------- -------- ------- ---------------
00031     2004-10-20,10:51:36 10:59:07  G729    135.8.76.64
00032  *  2004-10-20,10:53:42 10:57:36  G723    135.8.76.107
00033  *  2004-10-20,10:58:21 10:59:06  G723    135.8.76.107
```

```
00034     2004-10-20,11:08:40        -  G729    135.8.76.64
00035  *  2004-10-20,11:09:07        -  G723    135.8.76.107
```

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: 35[1]
Status: Terminated[2]
, QOS: Faulted[3]
, EngineId: 0[4]
Start-Time: 2004-10-20[5]
,11:09:07[6]
, End-Time: 2004-10-20,11:13:40[7]
Duration: 00:04:33[8]
CName: gwp@135.8.118.252[9]
Phone: 69:2011[10]
Local-Address: 135.8.118.252:2061[11]
 SSRC 154611212[12]
Remote-Address: 135.8.76.107:2061[13]
 SSRC 2989801899 (0)[14]
Samples: 54[15]
 (5 sec)[16]
Codec:
G723[17]
 62B[18]
 30mS[19]
 Off[20]
, Silence-suppression(Tx/Rx) Disabled[21]
/Not-Supported[22]
,
Play-Time 272.610sec[23]
, Loss 0.0%[24]
 #1[25]
, Avg-Loss 0.1%[26]
, RTT 741mS[27]
 #38[28]
,
Avg-RTT 570mS[29]
, JBuf-under/overruns 0.1%[30]
/0.0%[31]
, Jbuf-Delay 22mS[32]
,
Max-Jbuf-Delay 60mS[33]
Received-RTP:
Packets 9236[34]
, Loss 0.0%[35]
 #0[36]
, Avg-Loss 0.0%[37]
, RTT 604mS[38]
 #38[39]
, Avg-RTT
376mS[40]
, Jitter 0mS[41]
 #0[42]
, Avg-Jitter 0mS[43]
, TTL(last/min/max) 63/63/63[44]
,
Duplicates 0[45]
, Seq-Fall 0[46]
```

```
, DSCP 46[47]
, L2Pri 12[48]
, RTCP 54[49]
Transmitted-RTP:
VLAN 1[50]
, DSCP 184[51]
, L2Pri 6[52]
, RTCP 62[53]
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[63]
, 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: • OK. There are no QoS problems in the session. • Faulted. There are QoS problems in the session.	QOS: Faulted
EngineId	4	The ID of the VoIP engine. The Branch Gateway has one VoIP engine.	EngineId: 0
Start-Time	5	The date of the RTP session	2004-10-20
	6	The start time of the RTP session	Start-Time: 2004-10-20,11:09:07

Field	Label	Description	From the CLI example
End-Time	7	The end time of the RTP session	End-Time: 2004-10-20,11:13:40
Duration	8	The duration of the RTP session	Duration: 00:04:33
CName	9	format: gwt@<*MGP-address*>	CName: gwp@135.8.118.252
Phone	10	The local extension number and conference ID in format <*conference ID*>:<*extension number*>. 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 Avaya Aura® Communication Manager only if VMON is configured. • If you are not running VMON, you can cause Avaya Aura® Communication Manager to send the phone data by configuring a dummy RTCP-server for the region, with a 'localhost' IP address (127.x.x.x).	Phone: 69:2011
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[15] (5 sec)
	16	The sampling interval	Samples: 54 (5 sec)[16]
Codec:	17	The codec used for the session	G723

Field	Label	Description	From the CLI example
	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[21]/Not-Supported
	22	The transmitted silence suppression method	Silence-suppression(Tx/Rx) Disabled/Not-Supported[22]
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%[24] #1
#codec-loss-events	25	The codec loss event counter	Loss 0.0% #1[25]
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[27] #38
#rtt-events	28	The codec RTT event counter	RTT 741mS #38[28]
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%[30]/0.0%
	31	The estimated percentage contribution of jitter-buffer overruns to the average codec loss	JBuf-under/overruns 0.1%/0.0%[31]
Jbuf-delay	32	The last jitter buffer delay	Jbuf-Delay 22mS

Field	Label	Description	From the CLI example
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 loss%	35	The last sampled value of network RTP packet loss	Loss 0.0%[35] #0
#loss-events	36	The network RTP packet loss event counter	Loss 0.0% #0[36]
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[38] #38
#rtt-events	39	The network RTT event counter	RTT 604mS #38[39]
Avg-RTT	40	The average of all network RTT values during the session	Avg-RTT 376mS
Jitter jitter ms	41	The network jitter at the RTP receiver. Combined with long RTT, a large jitter value may indicate WAN congestion.	Jitter 0mS[41] #0
#jitter-event	42	The RTP receiver network jitter event counter	Jitter 0mS #0[42]
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	Seq-Fall 0

Field	Label	Description	From the CLI example
		be caused by switching to a backup WAN interface or route flaps.	
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 items are calculated and evaluated upon reception of RTCP messages)			
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%[54] #0
#rem-loss-ev	55	The number of samples that were over the rem-loss threshold	Loss 0.0% #0[55]
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[57] #0
#rem-jitter-ev	58	The number of samples that were over the remote jitter threshold	Jitter 0mS #0[58]
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[60] #1

Field	Label	Description	From the CLI example
#loss-ev	61	A counter that increments each time the echo-cancellation loss is sampled below its threshold	Loss 45dB #1[61]
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.
6. 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[1]
 11:13:40[2]
 LZ-SIT-SR1 snmptrapd[9407]: 135.8.118.252[3]
 [135.8.118.252]: Trap
sysUpTime.0 = Timeticks: (43147723) 4 days, 23:51:17.23[4]
```

```
, snmpTrapOID.0 = OID: av
RtpQoSTrap[5]
, avRtpSessionLocAddrV4.0 = IpAddress: 135.8.118.252[6]
,
avRtpSessionRemAddrV4.0 = IpAddress: 135.8.76.107[7]
, avRtpSessionDuration.0 =
INTEGER: 273[8]
, avRtpSessionCname.0 = STRING: gwp@135.8.118.252[9]
,
avRtpSessionPhone.0 = STRING: 69:2011[10]
, avRtpSessionSeverity.0 = INTEGER:
warning(4), avRtpSessionDebugStr.0 = STRING: Id{35

}[11]
;
Traps{24[12]
/0[13]
};Stats{S 54[14]
 RTCP 54[15]
 RX 9236[16]
};Codec{g723[17]
 62B[18]
 encryptionOff[19]

SSup disabled[20]
/disabled[21]
 Loss 0.1%[22]
 #1[23]
 RTT 570mS[24]
 #38[25]
 Jbuf
0.1%[26]
/0.0%[27]
};Net{Loss 0.0%[28]
 #0[29]
 RTT 376mS[30]
 #38[31]
 Jtr #0[32]
 TTL 63-63[33]
 Dup 0[34]

Fall 0[35]
};Rem{Loss 0.0%[36]
 #0[37]
 Jtr #0[38]
} EC{Loss 45dB[39]
}
```

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

Label	Description	From the trap example
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: avRtpQoSTrap
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*>	avRtpSessionCname.0 = STRING: gwp@135.8.118.252
10	The local extension number and conference ID in format <conference ID>:<extension number>. 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 Avaya Aura® Communication Manager if VMON is configured. • If you are not running VMON, you can cause Avaya Aura® Communication Manager to send the phone string data by configuring a dummy RTCP-server for the region, with a 'localhost' IP address (127.x.x.x).	avRtpSessionPhone.0 = STRING: 69:2011
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[11]/0}
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[12]}
14	The number of times the application sampled the VoIP engine (RTP receiver) statistics	Stats{S 54}

Label	Description	From the trap example
15	The total number of received RTCP packets	Stats{S 54 RTCP 54[14] RX 9236}
16	The total number of received RTP packets	Stats{S 54 RTCP 54 RX 9236[15]}
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[19]/disabled
21	The transmitted silence suppression method	SSup disabled/disabled[20]
22	The average of all codec loss values sampled during the session	Loss 0.1%[21] #1
23	The codec loss event counter	Loss 0.1% #1[22]
24	The average of all codec round trip time values sampled during the session	RTT 570mS[23] #38
25	The codec round trip time event counter	RTT 570mS #38[24]
26	The percentage contribution of jitter-buffer underruns to the average codec loss	Jbuf 0.1%[25]/0.0%
27	The percentage contribution of jitter-buffer overruns to the average codec loss	Jbuf 0.1%/0.0%[26]
28	The average of all network RTP packet loss values sampled during the session	Loss 0.0%[27] #0
29	The network RTP packet loss event counter	Loss 0.0% #0[28]
30	The average of all network RTT values during the session	RTT 376mS[29] #38
31	The network RTT event counter	RTT 376mS #38[30]
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
36	The average network loss experienced by the remote RTP receiver	Rem{Loss 0.0%[36] #0 Jtr #0}

Label	Description	From the trap example
37	A counter that increments each time the remote loss is sampled over its threshold	Rem{Loss 0.0% #0[37] 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[38]}
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[2]
 LZ-SIT-SR1 snmptrapd[9407]: 135.8.118.252
[135.8.118.252]: TrapsysUpTime.0 = Timeticks: (43131114) 4 days,
23:48:31.14[3]
, snmpTrapOID.0 = OID: avRtpQoSFault[4]
, avRtpQoSFaultTh.0 =
INTEGER: 1[5]
, avRtpQoSClearTh.0 = INTEGER: 0[6]
Oct 20[1]
 11:13:40[2]
 LZ-SIT-SR1 snmptrapd[9407]: 135.8.118.252
[135.8.118.252]: TrapsysUpTime.0 = Timeticks: (43147723) 4 days,
23:51:17.23[3]
, snmpTrapOID.0 = OID: avRtpQoSClear[4]
, avRtpQoSFaultTh.0 =
INTEGER: 1[5]
, 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.

For example:

```
Gxxx-001(super)# show rtp-stat traceroute destination-ip 10.2.5.0
255.255.255.0
Session ID: 1234
From: 123.21.11.5, To: 10.2.4.15, At: 2004-12-26,12:21:55
TTL HOP ADDRESS       DELAY
--- ---------------  --------
 1  123.21.11.1         2ms
 2  212.201.233.102     65ms
 3  213.21.51.12        110ms
 4  10.2.4.15            175ms
Session ID: 1234
From: 123.21.11.5, To: 10.2.4.5, At: 2004-12-26,13:30:15
```

Result

Note:

The traceroute results are displayed with the most recent first.

RTP traceroute results output

Name	Description
Session ID	The RTP statistics index for the RTP session
From	The IP address of the Branch Gateway
To	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

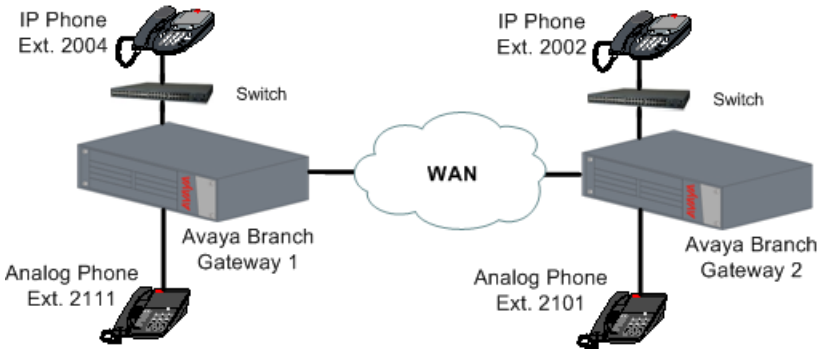
This section includes an example of configuring the RTP statistics application for a sample network. In addition, there are some example calls between various types of phones.

Related topics:

Four telephones in a sample network on page 370
A remote call from analog to IP telephone on page 373
A local call between an IP and an analog telephone on page 374
A remote call from IP telephone to IP telephone on page 375
A conference call on page 377

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.



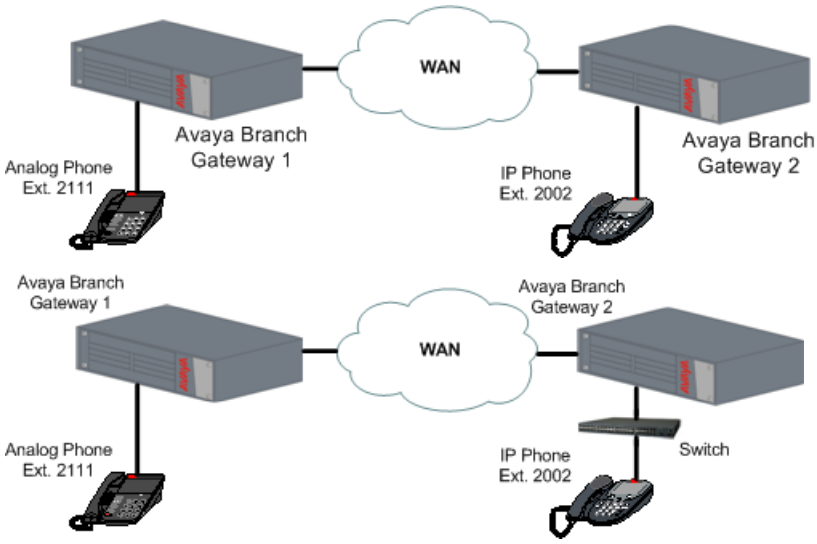
At the site of local Branch Gateway 1 – the administrator enabled and configured the RTP-MIB application as follows:

```
//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
Item                          Threshold             Event Threshold
--------------------         ------------          -----------------
Codec Loss                       0.0%                    1
Average Codec Loss               1.0%                    N/A
Codec RTT                        5 mS                    1
Echo Return Loss                 1 dB                    1
Loss                             1.0%                    1
Average Loss                     1.0%                    N/A
Remote Loss                      1.0%                    1
Average Remote Loss              1.0%                    N/A
RTT                              13mS                    1
Local Jitter                     1mS                     1
Remote Jitter                    1mS                     1
SSRC Changes                     N/A                     1
//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
--------------------         -------------         -----------------
Codec Loss                       6.0%                    1
Average Codec Loss               0.0%                    N/A
Codec RTT                        700mS                   1
Echo Return Loss                 5dB                     0
Loss                             6.0%                    0
Average Loss                     0.0%                    N/A
Remote Loss                      6.0%                    0
Average Remote Loss              0.0%                    N/A
RTT                              500mS                   0
Local Jitter                     70mS                    0
Remote Jitter                    70mS                    0
SSRC Changes                     N/A                     0
//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
```

A remote call from analog to IP telephone

At 00:39 on December 7, 2004, a call is placed from analog extension 2111 to IP phone extension 2002 in the network described in Four telephones in a sample network on page 370.



The RTP statistics application is configured as described in Four telephones in a sample network on page 370. The callers complain after the call that there were QoS problems during the call. The administrator investigates as follows:

```
//to see if the RTP statistics application registered QoS problems for the call:
Gxxx-001 (super)# show rtp sessions
ID    QoS Start date and time End Time Type        Destination
----- --- ------------------- -------- ---------- ---------------
00001  *1
  2004-12-07,00:39:26 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: Faulted2
, EngineId: 0
Start-Time: 2004-12-07,00:39:26, End-Time: 2004-12-07,00:41:01
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% #153
, 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% #94
, 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% #145
```

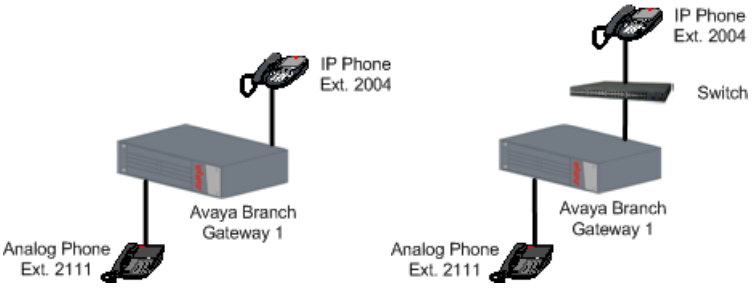
```
, Avg-Loss 8.9%, Jitter 33mS #0, Avg-Jitter 26mS
Echo-Cancellation:
Loss 49dB #0, Len 32mS
RSVP:
Status Disabled, Failures 0
```

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 there were QoS faults [2]
- QoS faults that can be seen in the output are:
  - The codec loss event counter indicates that codec loss went over its threshold 15 times [3]
  - The received-RTP packet loss event counter indicates that packet loss went over its threshold nine times [4]
  - The remote packet loss event counter indicates that remote packet loss went over its threshold 14 times [5]

A local call between an IP and an analog telephone

A local call is placed at 00:57 between IP telephone extension 2004 and analog telephone extension 2111 in the network described in Four telephones in a sample network on page 370. The call is finished at 00:59:19.



After the call is ended, 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
ID    QoS[1]
 Start date and time End Time  Type       Destination
----- --- ------------------- -------- ---------  ------------
00001     2004-12-07,00:57:13 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: Ok[2]
, EngineId: 0
Start-Time: 2004-12-07,00:57:13, End-Time: 2004-12-07,00:59:19
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)
```

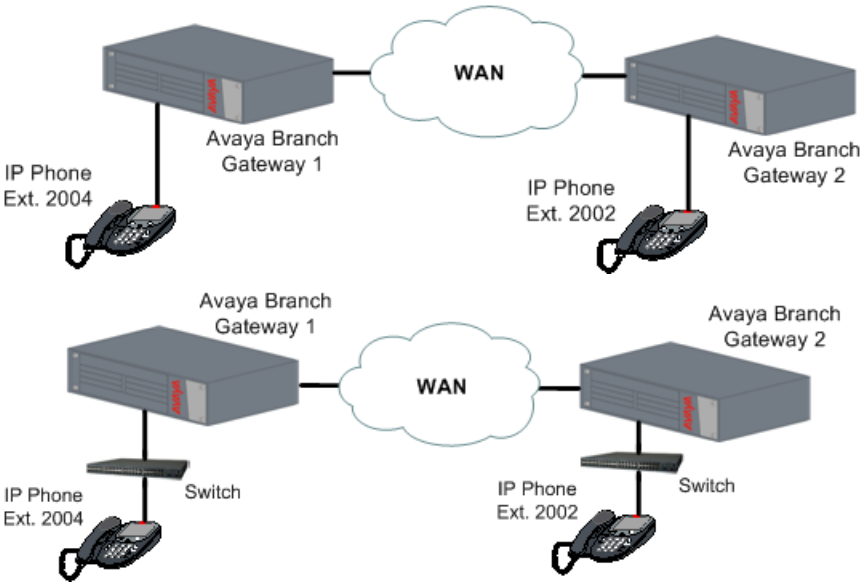
```
Codec:
G711U 200B 20mS Off, Silence-suppression(Tx/Rx) Disabled/Disabled, Play-Time 130
.080sec, Loss 0.0% #0[3]
, Avg-Loss 0.0%[4]
, RTT 83mS #0[5]
, Avg-RTT 108mS[6]
,
JBuf-under/overruns 0.0%/0.0%, Jbuf-Delay 5mS, Max-Jbuf-Delay 27mS
Received-RTP:
Packets 6503, Loss 0.0% #0[7]
, Avg-Loss 0.0%[8]
, RTT 0mS #0[9]
, Avg-RTT 0mS[10]
, Jitter 0mS
#0[11]
, Avg-Jitter 0mS[12]
, 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 10mS #0[15]
, Avg-Jitter 10mS[16]
Echo-Cancellation:
Loss 49dB #0[17]
, Len 32mS
RSVP:
Status Disabled, Failures 0
```

A few points to note:

- The QoS column in the `show rtp sessions` output has no asterisk (*), showing that no metrics went over 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]

A remote call from IP telephone to IP telephone

An unshuffled call is placed from IP telephone extension 2004 to IP telephone extension 2002 in the network described in Four telephones in a sample network on page 370.



After the call is ended, the following commands are run:

```
//to display the RTP sessions:
Gxxx-001 (super)# show rtp sessions
ID    QoS Start date and time End Time    Type       Destination
----- --- ------------------- -------- ------------- --------------
00011     2004-12-07,00:57:13 00:59:19    G711U      30.30.30.2
00012  *  2004-12-07,00:39:26 00:41:01    G711U      20.20.20.2
00013  *  2004-12-07,01:02:45 01:05:15    G711U      20.20.20.2
00014     2004-12-07,01:02:50 01:05:15    G711U      30.30.30.2
```

Sessions 13 and 14 both belong to the call, since two VoIP channels are used by an unshuffled call between two IP telephones: one channel between each telephone and the Branch Gateway VoIP 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: 2004-12-07,01:02:45, End-Time: 2004-12-07,01:05:15
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)
Codec:
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
```

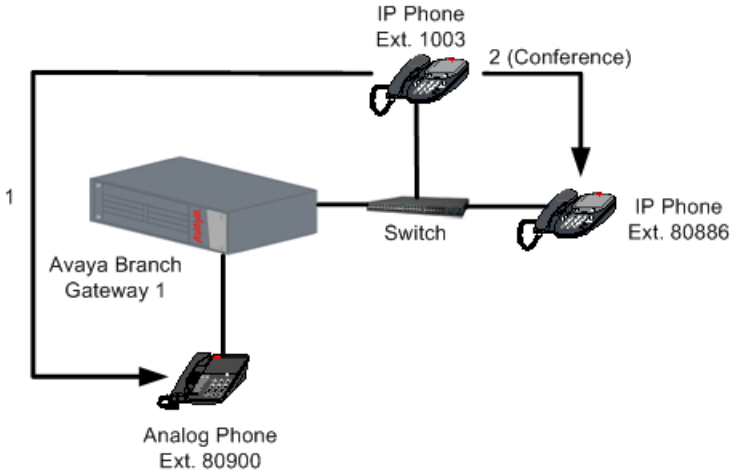
```
Echo-Cancellation:
Loss 49dB #0, Len 32mS
RSVP:
Status Disabled, Failures 0
```

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: 2004-12-07,01:02:50, End-Time: 2004-12-07,01:05:15
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
```

A conference call

A conference call is placed between IP telephone extension 1003, analog telephone extension 80900, and IP telephone extension 80886. The call is established by calling from extension 1003 to extension 80900, and then using the conference function on extension 1003 to add 80886.



During the call, the following commands are run:

```
//to display the RTP sessions:
Gxxx-001(super)# show rtp sessions
ID    QoS Start date and time End Time Type            Destination
----- --- ------------------ -------- -------------- --------------
00001     2004-12-23,09:55:17        -           G729 16.16.16.101
00002     2004-12-23,09:55:20        -          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: 2004-12-23,09:55:17, End-Time: -
Duration: 00:00:48
CName: gwp@33.33.33.33
Phone: 140[1]
: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 0mS, 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: 2004-12-23,09:55:20, End-Time: -
Duration: 00:00:50
CName: gwp@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
```

The conference ID that appears in the Phone string for session 1 and for session 2 is identical, which identifies the two sessions as belonging to the same conference call [1] [2].

Summary of RTP statistics commands

For more information about these commands, see the *Avaya Branch Gateways G250 and G350 CLI Reference*.

For more information about these commands, see the *Avaya Branch Gateway G430 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
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 http://www.ethereal.com).

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.

Related topics:

What can be captured on page 380
Roadmap for configuring packet sniffing on page 381
Configuring capture lists on page 383
Analyzing captured packets on page 393
About simulating packets on page 397
Summary of packet sniffing commands on page 397

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 381 for a description of how to configure packet sniffing and analyze the resulting capture file.

Related topics:

Streams that can always be captured on page 381

Streams that can never be captured on page 381
Streams that can sometimes be captured on page 381

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 382.
2. Limiting packet sniffing to specific interfaces on page 382 (if necessary).
3. Applying a capture list on page 390 that specifies which packets to capture.
4. Rule criteria for a capture list on page 383.
5. Viewing the capture list on page 390.
6. Applying a capture list on page 390.

7. Configuring packet sniffing settings on page 391.
8. Starting the packet sniffing service on page 392.

Related topics:

Enabling and disabling packet sniffing on page 382
Limiting packet sniffing to specific interfaces on page 382
Capture lists on page 382

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 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 500 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.

Related topics:

Rule criteria for a capture list on page 383
Configuring rule criteria for a capture list on page 384
Viewing the capture list on page 390
Applying a capture list on page 390
Configuring packet sniffing settings on page 391
Starting the packet sniffing service on page 392

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)#
```

Related topics:

Rule applications on page 385
Rule criteria commands on page 385
Applying rules to packets with DSCP values on page 385
Applying rules to packets with IP protocols on page 386
Applying rules to source or destination IP address on page 386
IP range criteria on page 387
Commands used to specify a range of source and destination ports on page 387
Port name or number range criteria on page 388
Applying rules to ICMP on page 388
Fragment command on page 389
Capture list example on page 389

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 G430 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 **lt**, 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 135.122.50.149 255.255.255.254 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
Done!
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
Done!
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
Done!
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
Done!
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
Done!
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-001# show ip capture-list 511
Index Name                            Owner
----- ------------------------------- -------------------------
511   list #511                        other
Index Protocol     IP               Wildcard        Port         Operation
      DSCP
----- -------- --- ---------------- --------------- ------------
-------------
10     tcp     Src  Any                             Any         No-Capture
       Any     Dst  Any                             eq Telnet
15     tcp     Src  Any                             eq Telnet   No-Capture
       Any     Dst  Any                             Any
20     tcp     Src  135.122.50.171  Host             Any         Capture
       Any     Dst  135.122.50.128  0.0.0.31         Any
30     Any     Src  135.122.50.128  0.0.0.31         Any
       Any     Dst  135.122.50.171  Host             Any
Deflt  Any     Src  Any                             Any         No-Capture
       Any     Dst  Any                             Any
Index Name                  Trust
----- --------------------- ------------
0     Capture               No
1     No-Capture            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
   Done!
   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.

Tip:

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

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

Note:

The capture start command resets the buffer before starting the sniffer.

Note:

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.

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)#
```

Related topics:

Decrypted IPSec VPN packets on page 393

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.

Related topics:

Stopping the packet sniffing service on page 393
Viewing packet sniffing information on page 393
Uploading the capture file on page 394
Capture file analysis on page 396

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 19/06/2004-13:57:40
Capture stop time 19/06/2004-13:58:23
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    .......@..B.....
00000010:0800 0604 0001 0040 0da9 4201 9531 4e7a    .......@..B..1Nz
00000020:0000 0000 0000 9531 4e7a 0000 0000 0000    .......1Nz......
00000030:0000 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    .......@..TU....
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.

Related topics:

Uploading the capture file to a remote server or USB mass storage device on page 395
Uploading the capture file to an S8300 Server on page 395

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`**
- **`coyy capture-file usb`**

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 G430*.
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 tcpdump, 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 http://www.ethereal.com.

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 Interface identification on page 396.

Related topics:

Interface identification on page 396

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
-----------------  ---------------------------------------------------
00:00:01:00:00:01  Decrypted IPSec packet
00:00:0a:00:0a:02  interface fastethernet 10/3
00:00:0c:a0:b0:01  interface vlan 1

00:00:31:00:00:01  interface dialer 1
```

About simulating packets

Capture lists support the IP simulate command. Refer to Simulating packets on page 576.

Summary of packet sniffing commands

For more information about these commands, see the *Avaya Branch Gateways G250 and G350 CLI Reference*.

For more information about these commands, see the *Avaya Branch Gateway G430 CLI Reference*.

Root level command	First level command	Second level command	Description
capture buffer-mode			Set the capture buffer to cyclic mode

Root level command	First level command	Second level command	Description
capture buffer-size			Change the size of the capture file
capture filter-group			Activate a capture list
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
ip capture-list			Enter the capture list configuration context, create a

Root level command	First level command	Second level command	Description
			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
		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

Root level command	First level command	Second level command	Description
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 ICMP keepalive on page 274.

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)
```

Related topics:

Reporting of interface status on page 400
Summary of interface status commands on page 401

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

Port status	Keepalive status	Show interfaces output	Administrative state	Operational state	Extended operational state
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 the *Avaya Branch Gateways G250 and G350 CLI Reference*.

For more information about these commands, see the *Avaya Branch Gateway G430 CLI Reference*.

Summary of interface status commands

For more information about these commands, see the *Avaya Branch Gateways G250 and G350 CLI Reference*.

For more information about these commands, see the *Avaya Branch Gateway G430 CLI Reference*.

Command	Description
show interfaces	Display interface information

CNA test plugs

The Converged Network Analyzer (CNA) is a distributed system for real-time monitoring of IP networks, using active measurements. The CNA supports various network tests including connectivity tests with pings, topology tests with traceroute, and QoS tests with synthetic RTP streams. Within a CNA system, test plugs are the entities that execute the tests, according to instructions from CNA schedulers, and return the results. For more information about

administrating the CNA system, see *IM R3.0 Converged Network Analyzer (CNA) Configuration*.

Related topics:

CNA test plug functionality on page 402
Configuring the Branch Gateway test plug for registration on page 403
CNA test plug configuration example on page 405
Resetting the CNA test plug counters on page 407
Summary of CNA test plug commands on page 407

CNA test plug functionality

When activated, test plugs present themselves to the CNA system in a process called “registration”. During registration, a test plug uses a fingerprint certificate to authenticate the CNA scheduler, and publishes its IP address and active ports.

The schedulers are software components running on single board computers called “chatterboxes”. Schedulers are responsible for initiating tests, coordinating tests, and collecting the test results.

For redundancy and load sharing, CNA systems usually include multiple chatterboxes and, therefore, multiple schedulers. However, since the schedulers distribute test plug registration parameters among themselves, a test plug only has to register with a single scheduler. Test plug administrators typically configure multiple schedulers addresses, for redundancy.

You can configure a list of up to five scheduler IP addresses. The test plug attempts to register with the first scheduler on the list first, and then moves down the list as necessary if the registration is unsuccessful.

When the test plug registers with a scheduler, the test plug provides the scheduler with its IP address, and two UDP port numbers, called the control port and the RTP echo port. The test plug IP address is the IP address of the interface on which the PMI is configured.

Related topics:

Test plug actions on page 402
CNA tests on page 403

Test plug actions

Once registered, the test plug listens for test requests on the control port. When the test plug receives an authenticated and validly formatted test request from the scheduler, the test plug performs the following:

- Injects any one of the tests specified in the test request into the network
- Performs the specified test using the parameter values passed in the test request
- Upon successful completion of the test, sends the test results to the analyzer of the chatterbox whose IP address is designated in the test request

CNA tests

The Branch Gateway test plug supports all of the following CNA tests:

Traceroute: Measures per-hop round-trip delays to a target IP address by sending a sequence of hop-limited UDP messages, each with a Time To Live (TTL) value that is one greater than that of the preceding message.

Real Time Protocol (RTP): Measures delay, packet loss, and jitter to another test plug by sending a simulated RTP stream that is echoed back.

Ping: Sends an ICMP echo message to a target IP address, and reports whether or not a response was returned.

Transmission Control Protocol (TCP) Connect: Attempts to establish a TCP connection to a specified port at a target IP address, and reports whether the attempt succeeded or failed and the time taken by the TCP packet to reach its destination.

Merge: Chatter test that is used, transparently to the user, to identify a single device with multiple IP addresses and to merge its multiple appearances into one in the network topology map.

When the test plug receives a request to run an RTP test, the test plug uses a UDP port called the RTP test port to send an RTP stream to another test plug. The test plug listens on the RTP echo port for RTP streams sent by other test plugs running RTP tests. All the UDP ports have default values, which can be overridden using CLI commands. The defaults are:

UDP Port	Default value
Control port	8889
RTP echo port	8888
RTP test port	8887

Any changes you make to the test plug configuration, such as changing scheduler addresses or port numbers, only take effect when you cause the test plug to disconnect from the scheduler and register again.

Configuring the Branch Gateway test plug for registration

About this task

From the Branch Gateway CLI, you can configure the Branch Gateway test plug to register with a CNA scheduler.

Procedure

1. Use the **`cna-testplug`** command to enter the testplug context.

For example:

```
Gxxx-001# cna-testplug 1
Gxxx-001(cna-testplug 1)#
```

2. Use the **scheduler** command to configure one or more CNA scheduler IP addresses.

   You can configure up to five scheduler addresses. The test plug attempts to register with a scheduler according to its place on the list. By default, no schedulers are configured. At least one scheduler must be configured for registration to be possible.

3. Use the **fingerprint** command to enter the certificate fingerprint, provided by your administrator.

   The fingerprint is used by the CNA test plug to authenticate the CNA scheduler.

4. Perform the following configurations as necessary:

   - Use the **control-port** command to configure the control port. The default control port number is 8889.
   - Use the **rtp-echo-port** command to configure the RTP echo port. The default RTP echo port number is 8888.
   - Use the **rtp-test-port** command to configure the RTP test port. The default RTP test port number is 8887.
   - Use the **test-rate-limit** command to configure the CNA test rate limiter. The default test rate is 60 tests every 10 seconds.

5. If necessary, use the **no shutdown** command to enable the test plug.

   By default, the test plug is enabled.

6. When the test plug configurations are complete, use the **exit** command to exit the testplug context.

   From the general context, you can enter **show cna testplug** to display the test plug configuration.

7. From the general context, enter **cna-testplug-service** to enable the test plug service.
   For example:

```
Gxxx-001# cna-testplug-service
The Converged Network Analyzer test plug is enabled.
```

Note:

The **cna-testplug-service** command requires admin access level.

Result

The test plug attempts to register with the first scheduler on the scheduler list. You can use the **show cna testplug** command to see if the test plug is registered and to view test plug statistics counters.

CNA test plug configuration example

The following example includes displaying default test plug configuration, configuring the test plug, enabling the test plug service, and displaying test plug configuration and counters.

```
//to display default test plug configuration before performing any
//configuration:
Gxxx-001(super)# show cna testplug

CNA testplug 1 is administratively down, test-plug status is unregistered
Address 149.49.75.178, bind to PMI, ID 00:04:0d:6d:30:48
Scheduler list:
Ports: Control 8889,  RTP-test 8888,  RTP-echo 8887
Test rate limiter: Maximum 60 tests in 10 seconds
Last Test: none
Test                 Count        Failed       Cancelled
----------           ------       ------       ---------
traceroute           0            0            0
rtp                  0            0            0
ping                 0            0            0
tcpconnect           0            0            0
merge                0            0            0
//to enter the test plug context:
Gxxx-001(super)# cna testplug 1

//to configure entries 3 and 1 on the scheduler list:
Gxxx-001(super-cna testplug 1)# scheduler 3 135.64.102.76

Done!
Gxxx-001(super-cna testplug 1)# scheduler 1 1.1.1.1

Done!
//to change the configuration of scheduler 1:
Gxxx-001(super-cna testplug 1)# scheduler 1 1.1.1.2

Done!
//to exit the test plug context:
Gxxx-001(super-cna testplug 1)# exit

//to display test plug configuration:
Gxxx-001(super)# show cna testplug

CNA testplug 1 is administratively down, test-plug status is unregistered
Address 149.49.75.178, bind to PMI, ID 00:04:0d:6d:30:48
Scheduler list:
        1: 1.1.1.2:50002
        3: 135.64.102.76:50002
Ports: Control 8889,  RTP-test 8888,  RTP-echo 8887
Test rate limiter: Maximum 60 tests in 10 seconds
Last Test: none
Test                 Count        Failed       Cancelled
----------           ------       ------       ---------
traceroute           0            0            0
```

```
rtp                  0            0            0
ping                 0            0            0
tcpconnect           0            0            0
merge                0            0            0
//to reenter the test plug context:
Gxxx-001(super)# cna testplug 1

//to delete scheduler 1:
Gxxx-001(super-cna testplug 1)# no scheduler 1

Done!
//to exit the test plug context:
Gxxx-001(super-cna testplug 1)# exit

//to show that scheduler 1 is no longer configured:
Gxxx-001(super)# show cna testplug

CNA testplug 1 is administratively down, test-plug status is unregistered
Address 149.49.75.178, bind to PMI, ID 00:04:0d:6d:30:48
Scheduler list:
        3: 135.64.102.76:50002
Ports: Control 8889,  RTP-test 8888,  RTP-echo 8887
Test rate limiter: Maximum 60 tests in 10 seconds
Last Test: none
Test                 Count        Failed       Cancelled
----------           ------       ------       ---------
traceroute           0            0            0
rtp                  0            0            0
ping                 0            0            0
tcpconnect           0            0            0
merge                0            0            0
//to enable the test plug service:
Gxxx-001(super)# cna testplug-service

Done!
//to display test plug configuration and counters after some running time:
Gxxx-001(super)# show cna testplug

CNA testplug 1 is up, test-plug status is running a test
Address 149.49.75.178, bind to PMI, ID 00:04:0d:6d:30:48
Scheduler list:
        3: 135.64.102.76:50002
Ports: Control 8889,  RTP-test 8888,  RTP-echo 8887
Test rate limiter: Maximum 60 tests in 10 seconds
Last Test: traceroute to 135.64.103.107
Result:
ip1=149.49.75.178 ip2=135.64.103.107 ttl_len = 4
Test                 Count        Failed       Cancelled
----------           ------       ------       ---------
traceroute           4            0            0
rtp                  3            0            0
ping                 2            0            0
tcpconnect           4            0            0
merge                0            0            0
```

Resetting the CNA test plug counters

Procedure

In the CNA testplug context, enter **clear counters**.

```
Gxxx-001(cna-testplug 1)# clear counters
```

All CNA test plug counters are cleared.

Summary of CNA test plug commands

For more information about these commands, see the *Avaya Branch Gateways G250 and G350 CLI Reference*.

For more information about these commands, see the *Avaya Branch Gateway G430 CLI Reference*.

Root level command	Command	Description
cna testplug		Enter the **CNA testplug** configuration context
	clear counters	Clear the CNA test plug counters
	control-port	Set or reset the UDP port on which the CNA test plug listens for test requests from schedulers
	fingerprint	Configure the certificate fingerprint used by the CNA test plug to authenticate the scheduler
	rtp-echo-port	Set or reset the UDP port used by the CNA test plug to listen for RTP streams sent by other test plugs running RTP tests
	rtp-test-port	Set or reset the UDP port used by the CNA test plug to send an RTP stream to another test plug in an RTP test
	scheduler	Add a scheduler's IP address to the list of schedulers with which the test plug can attempt to register
	shutdown	Disable the CNA test plug

Root level command	Command	Description
	test-rate-limit	Configure the CNA test rate limiter
cna-testplug-service		Enable or disable the CNA test plug service on the Branch Gateway
show cna testplug		Display CNA test plug configuration and statistics

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 Communication Manager 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.

Related topics:

Summary of echo cancellation commands on page 409

Summary of echo cancellation commands

For more information about these commands, see the *Avaya Branch Gateways G250 and G350 CLI Reference*.

For more information about these commands, see the *Avaya Branch Gateway G430 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 analog	Configure echo cancellation on analog lines and trunks 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.

Related topics:

Hardware support for integrated analog testing on page 410
Types of tests on page 410
Types of test lines on page 411
Setting up a test profile on page 412
Displaying and clearing profiles on page 413
Launching and cancelling a test on page 413
Displaying test results on page 414
Healing trunks on page 414
Displaying corrections on page 415
Summary of integrated analog testing commands on page 415

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 Types of test lines on page 411.
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.

  Note:

  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 will fail if the port specified for the test is in use for a call, unless you specified **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 Communication Manager before the test is launched.

Result

Note:

As soon as **launch** is issued, the results of previous measurements on the port are cleared.

You can use the **cancel** command to abort an analog test that is currently running.

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 the *Avaya Branch Gateways G250 and G350 CLI Reference*.

For more information about these commands, see the *Avaya Branch Gateway G430 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

Root Level Commands	First level command	Second level command	Description
		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
		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, receive-gain, and transmit-gain corrections applied to each port
	show profile		Display the details of a test profile

Root Level Commands	First level command	Second level command	Description
	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
	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.
	set sla-monitor		Enables or disables the SLA Monitor Agent.
	set sla-capturemode		Defines the degree of data captured by the SLA Monitor Agent. By default, the capture mode is set to “without-payload”.

Chapter 18: The router

The router

The Branch Gateway has an internal router. You can configure the following routing features on the router:

Note:

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 Routing sources on page 427 for an explanation of the priority considerations employed by the Branch Gateway to determine the next hop source.

Related topics:

Enabling and disabling the router on page 420
Interface configuration on page 420
Unnumbered IP interfaces on page 424

Routing sources on page 427
Routing table configuration on page 428
GRE tunneling on page 432
DHCP and BOOTP relay on page 442
DHCP server on page 445
Broadcast relay on page 454
ARP table on page 456
Proxy ARP on page 459
ICMP errors on page 459
RIP on page 460
OSPF on page 466
Route redistribution on page 470
VRRP on page 472
Fragmentation on page 475

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.

Related topics:

Router interface concepts on page 421
Configuring an IP interface on page 422
Interface configuration examples on page 422
Summary of basic interface configuration commands on page 423

Router interface concepts

The router in the Branch Gateway includes the following interface categories:

- Physical
- Layer 2 virtual
- Layer 3 routing

Related topics:

Physical router interfaces on page 421
Layer 2 virtual interfaces on page 421
Layer 2 logical interfaces on page 422

Physical router interfaces

The physical interfaces of the Branch Gateway router include:

FastEthernet Interface: The 10/3 Fast Ethernet port on the front panel of the Branch Gateway provides 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 250.

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 GRE tunneling on page 432.

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 eight VLANs that can be configured over their internal switching interface connections.

Dialer Interface: The Dialer interface is used for the modem dial-backup feature. Refer to Modem dial backup on page 256.

Note:

One or more IP interfaces can be defined over each 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 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 the *Avaya Branch Gateways G250 and G350 CLI Reference*.

For more information about these commands, see the *Avaya Branch Gateway G430 CLI Reference*.

Root level command	Command	Description
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 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

Root level command	Command	Description
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 Modem dial backup on page 256. 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 topics:

Unnumbered IP on an interface configuration on page 425
Configuring IP on an interface configuration on page 425
Unnumbered IP examples on page 425
Summary of unnumbered IP interface configuration commands on page 426

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
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
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 the *Avaya Branch Gateways G250 and G350 CLI Reference*.

For more information about these commands, see the *Avaya Branch Gateway G430 CLI Reference*.

Root level command	Command	Description
interface (dialer| fastethernet| serial| tunnel) interface (dialer|		Enter the **Dialer**, **FastEthernet**, **Serial**, or **Tunnel** interface context Enter the **Dialer**, **FastEthernet**, or **Tunnel** interface context

Root level command	Command	Description
fastethernet|tunnel)		
	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 428.
- For information about configuring OSPF, see OSPF on page 466.
- For information about configuring RIP, see RIP on page 460.
- For information about configuring DHCP client, see DHCP client configuration on page 204.

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 **`ip admin-state down`** command. For more information, see Permanent static route on page 430. 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 280.

Static routes can be advertised by routing protocols, such as RIP and OSPF. For more information, see Route redistribution on page 470. Static routes also support load-balancing similar to OSPF.

Related topics:

Next hops on page 429
Static route types on page 429
Configuring multiple next hops on page 429
Deleting a route and its next hops on page 430

Permanent static route on page 430
Discard routes on page 431
Summary of routing table commands on page 431

Next hops

Static routes can be configured with the following as next hops:

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**

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 FastEthernet 10/2 permanent** creates a permanent static route to the network 193.168.10.0 24 via the FastEthernet 10/2 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 Layer 2 interfaces that participate in a Primary-Backup pair.

For more information on Backup interfaces, see Backup interfaces on page 254.

Note:

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*>**null0** CLI command.

Note:

You cannot configure tracking on a discard route.

Example

For example, the command **ip route 134.66.0.0 16 Null0** configures the network 134.66.0.0 16 as a discard route

Summary of routing table commands

For more information about these commands, see the *Avaya Branch Gateways G250 and G350 CLI Reference*.

For more information about these commands, see the *Avaya Branch Gateway G430 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
ip route	Establish a static route

Command	Description
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 254.

For an example of a GRE tunneling application, see GRE tunnel application example on page 439.

Related topics:

Packet routing to a GRE tunnel on page 433
Prevention of nested tunneling in GRE tunnels on page 433
Optional GRE tunnel features on page 436
Setting up a GRE tunnel on page 438
GRE tunnel application example on page 439
Summary of GRE tunneling commands on page 441

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 Routing table configuration on page 428.
- 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 on page 583.

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.

Related topics:

[Reasons for nested tunneling in a GRE tunnel](#) on page 434
[Nested tunneling example](#) on page 435
[Recommendations on avoiding nested tunneling](#) on page 435

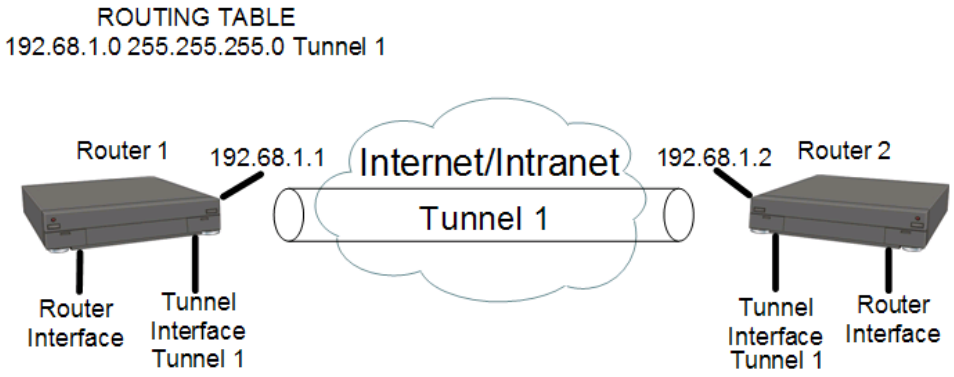
Reasons for nested tunneling in a GRE tunnel

- 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
Done!
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
Done!
Gxxx-001(super-if:Tunnel 3)# exit
Gxxx-001(super)# ip route 1.0.0.1 tunnel 2
Done!
Gxxx-001(super)# ip route 2.0.0.1 tunnel 3
Done!
Gxxx-001(super)# ip route 3.0.0.1 tunnel 1
Done!
```

Using the network shown in [Nested tunneling example](#) on page 435 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 Figure on page 435 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 Nested tunneling example on page 435 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.

Related topics:

Keepalive feature on page 436
Enabling the keepalive feature on page 436
Keepalive command parameters on page 437
Dynamic MTU discovery on page 437
Enabling and deactivating dynamic MTU discovery on page 437
tunnel path-mtu-discovery parameters on page 437

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 Fragmentation on page 475.

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 436.

   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 Dynamic MTU discovery on page 437.

   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 Optional GRE tunnel features on page 436. For a list of additional GRE tunnel CLI commands, refer to Summary of GRE tunneling commands on page 441.

GRE tunnel application example

This section provides an example of a GRE tunnel application and its configuration.

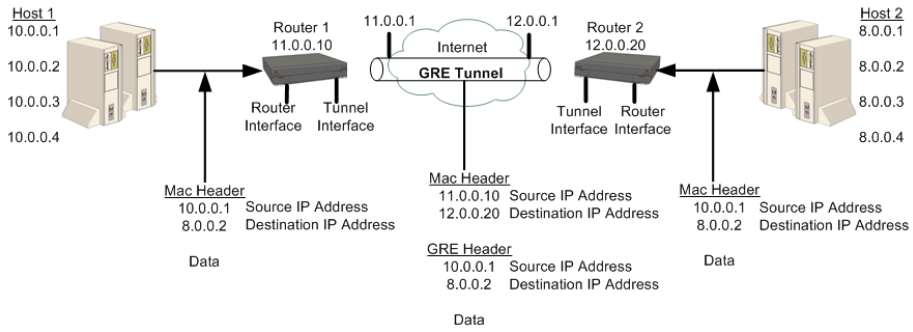


Figure 14: Simple GRE tunneling application example

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
Done!
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
Done!
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
Done!
```

```
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 the *Avaya Branch Gateways G250 and G350 CLI Reference*.

For more information about these commands, see the *Avaya Branch Gateway G430 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

Root level command	Command	Description
	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.
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 DHCP server on page 445. For information about configuring DHCP client on the Branch Gateway, see DHCP client configuration on page 204.

Related topics:

DHCP on page 443
BOOTP on page 443
DHCP/BOOTP relay on page 443
Summary of DHCP and BOOTP relay commands on page 444

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 the *Avaya Branch Gateways G250 and G350 CLI Reference*.

For more information about these commands, see the *Avaya Branch Gateway G430 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

Root level command	Command	Description
		A maximum of two servers can be added to a single interface. You must be in an interface context to use this command
	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 256 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.

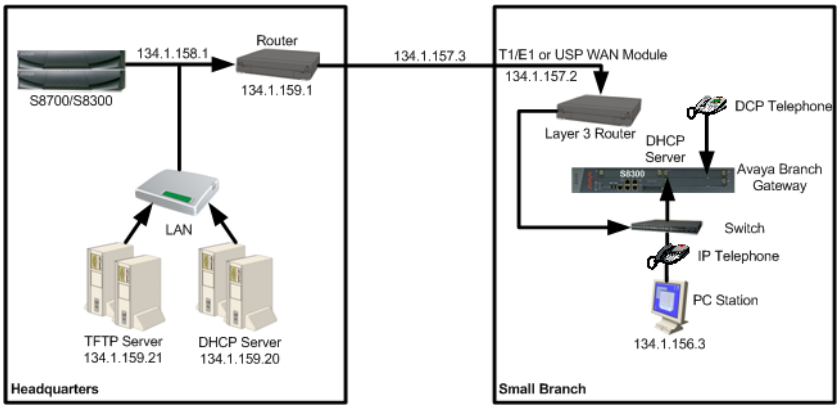
The Branch Gateway can function as a DHCP server or as a DHCP client, or both simultaneously. For information about configuring DHCP client on the Branch Gateway, see DHCP client configuration on page 204.

Related topics:

Typical DHCP server application on page 446
Configuring the DHCP server on page 447
Deleting an IP address binding on page 449
DHCP pool configuration examples on page 450
Commands for displaying DHCP server information on page 451
Summary of DHCP Server commands on page 452

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 448 and, for vendor specific options, Configuring vendor-specific options on page 449.
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.

Related topics:

Configuring options on page 448
Common user-configurable DHCP options on page 449
Configuring vendor-specific options on page 449

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 449. Some options are configured with specific CLI commands that are also listed in Common user-configurable DHCP options on page 449. 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 449 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
Done!
Gxxx-001(super-DHCP 1)# end-ip-addr 135.64.20.30
Done!
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”
Done!
Gxxx-001(super-DHCP 1/option 176)# value ascii “MCIPADD=10.10.2.140,
MCPORT=1719, TFTPSRVR=10.10.5.188”
Done!
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
Done!
Gxxx-001(super-DHCP 2)# subnet-mask 255.255.255.0
Done!
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
Done!
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/”
Done!
```

```
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”
Done!
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
Done!
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 Summary of DHCP Server commands on page 452 or the *Avaya Branch Gateway G430 CLI Reference*.

Summary of DHCP Server commands

For more information about these commands, see the *Avaya Branch Gateways G250 and G350 CLI Reference*.

For more information about these commands, see the *Avaya Branch Gateway G430 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

Root level command	First level command	Second level command	Description
	end-ip-addr		Set the end IP address of the range of available IP addresses that the DHCP server may assign to clients
	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

Root level command	First level command	Second level command	Description
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, and DHCP and BOOTP client broadcast.

For more information about DHCP and BOOTP client broadcast, see DHCP and BOOTP relay on page 442.

Related topics:

Directed broadcast forwarding on page 454
NetBIOS rebroadcast on page 455
Summary of broadcast relay commands on page 455

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 the *Avaya Branch Gateways G250 and G350 CLI Reference*.

For more information about these commands, see the *Avaya Branch Gateway G430 CLI Reference*.

Root level command	Command	Description
interface (dialer| fastethernet| tunnel| vlan)		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

Related topics:

Overview of ARP on page 456
Static and dynamic table entries on page 456
Adding static ARP table entries on page 457
Changing an entry in the ARP table on page 458
Summary of ARP table commands on page 458

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.

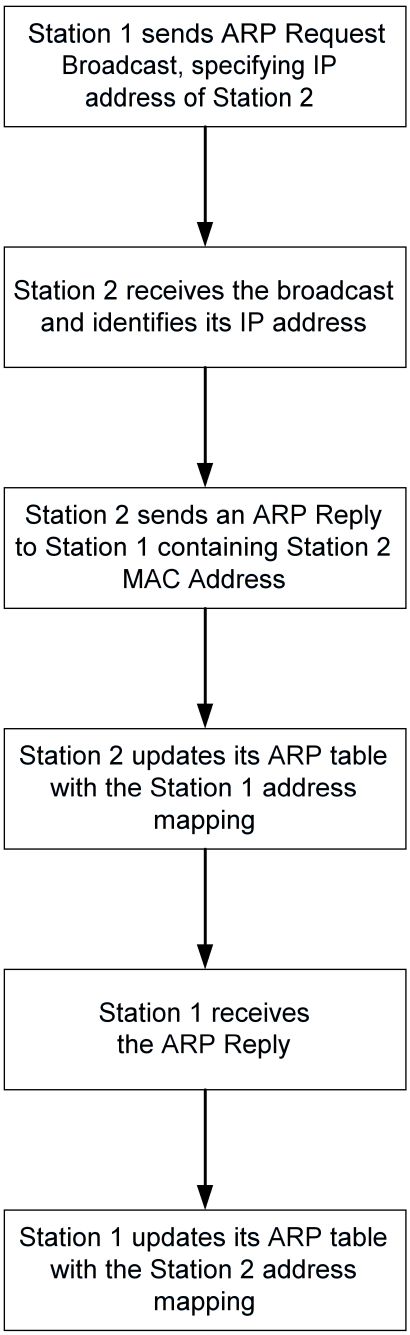
Static and dynamic table entries

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
```

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 the *Avaya Branch Gateways G250 and G350 CLI Reference*.

For more information about these commands, see the *Avaya Branch Gateway G430 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

Command	Description
show ip reverse-arp	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.

Related topics:

Summary of Proxy ARP commands on page 459

Summary of Proxy ARP commands

For more information about these commands, see the *Avaya Branch Gateways G250 and G350 CLI Reference*.

For more information about these commands, see the *Avaya Branch Gateway G430 CLI Reference*.

Root level command	Command	Description
interface (fastethernet|vlan)		Enter the FastEthernet or VLAN interface context
	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.

Related topics:

Summary of ICMP errors commands on page 460

Summary of ICMP errors commands

For more information about these commands, see the *Avaya Branch Gateways G250 and G350 CLI Reference*.

For more information about these commands, see the *Avaya Branch Gateway G430 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 OSPF on page 466.

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 Route redistribution on page 470.

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 461
- RIPv2 on page 461

Related topics:

RIPv1 on page 461
RIPv2 on page 461
RIPv1 vs. RIPv2 on page 461
Prevention of routing loops in RIP on page 462
Commands used to prevent routing loops in RIP on page 462

RIP distribution access lists on page 462
Configuring a distribution access list example on page 463
RIP limitations on page 463
Summary of RIP commands on page 464

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 461.

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 Commands used to prevent routing loops in RIP on page 462

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 the *Avaya Branch Gateways G250 and G350 CLI Reference*.

For more information about these commands, see the *Avaya Branch Gateway G430 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-list		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
interface (dialer|fastethernet|loopback|vlan|tunnel)		Enter the Dialer, FastEthernet, Loopback, 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

Root level command	Command	Description
	no ip rip authentication mode	Restore the default value, none
	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

Root level command	Command	Description
	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
	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 460.

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 Route redistribution on page 470.

Related topics:

OSPF dynamic Cost on page 467
OSPF limitations on page 467
Summary of OSPF commands on page 468

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 the *Avaya Branch Gateways G250 and G350 CLI Reference*.

For more information about these commands, see the *Avaya Branch Gateway G430 CLI Reference*.

Root level command	Command	Description
interface (dialer fastethernet| loopback|tunnel| vlan)		Enter the Dialer, FastEthernet, Loopback, 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	Specify the time interval between hello packets sent by the router
	no ip ospf hello-interval	Set the hello-interval to its default value
	ip ospf message-digest-key	Specify the message-digest key for the interface and enable OSPF MD5 authentication

Root level command	Command	Description
	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.

Related topics:

Export default metric on page 471
Summary of route redistribution commands on page 471

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 the *Avaya Branch Gateways G250 and G350 CLI Reference*.

For more information about these commands, see the *Avaya Branch Gateway G430 CLI Reference*.

Root level command	Command	Description
`router ospf`		Enable OSPF and enter the router configuration context

Root level command	Command	Description
	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.

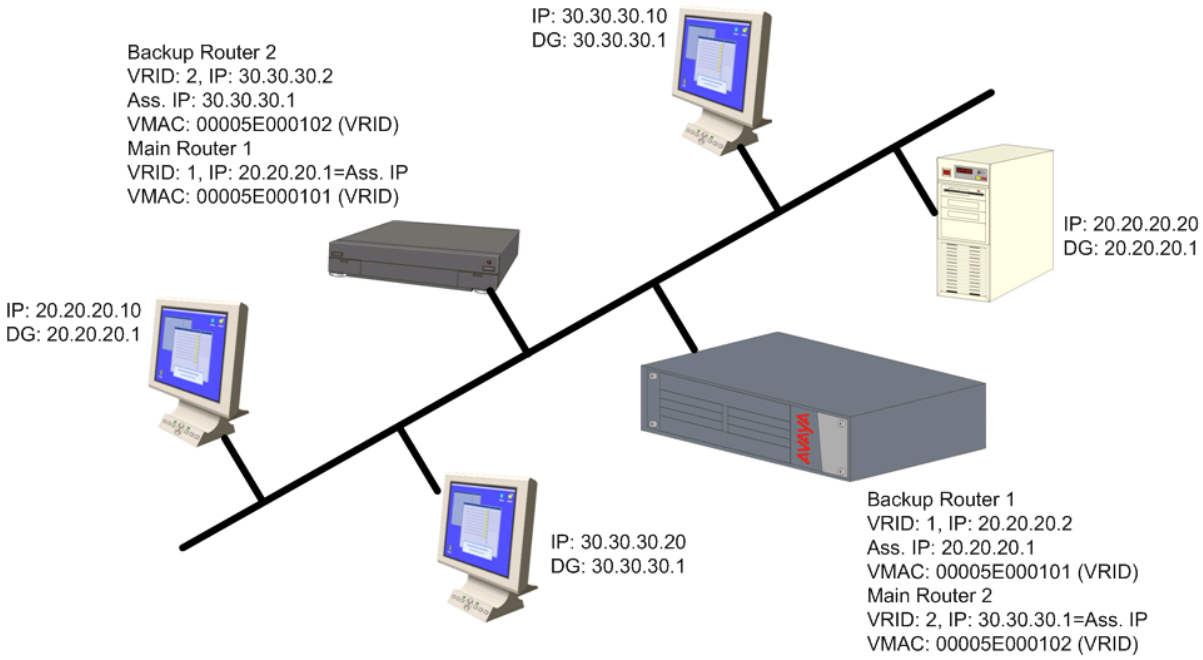
You can activate VRRP on an interface using a single command while allowing for the necessary fine-tuning of the many VRRP parameters. For a detailed description of VRRP, see VRRP standards and published literature.

Related topics:

[VRRP configuration example](#) on page 473
[Summary of VRRP commands](#) on page 474

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 the *Avaya Branch Gateways G250 and G350 CLI Reference*.

For more information about these commands, see the *Avaya Branch Gateway G430 CLI Reference*.

Root level command	Command	Description
interface (fastethernet |vlan)		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)

Root level command	Command	Description
	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.
	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

The 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.

Related topics:

Summary of fragmentation commands on page 476

Summary of fragmentation commands

For more information about these commands, see the *Avaya Branch Gateways G250 and G350 CLI Reference*.

For more information about these commands, see the *Avaya Branch Gateway G430 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
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 19: IPSec VPN

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.

Note:

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.

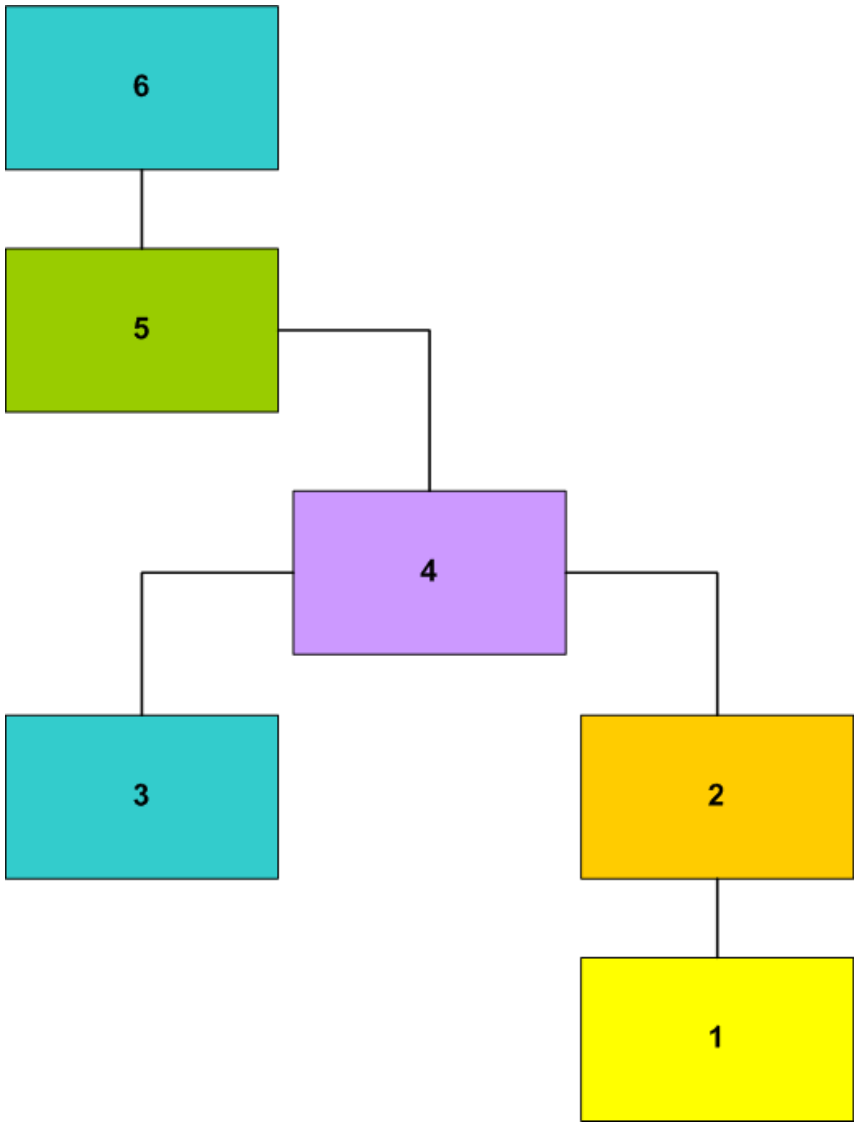


Table 5: Figure notes:

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

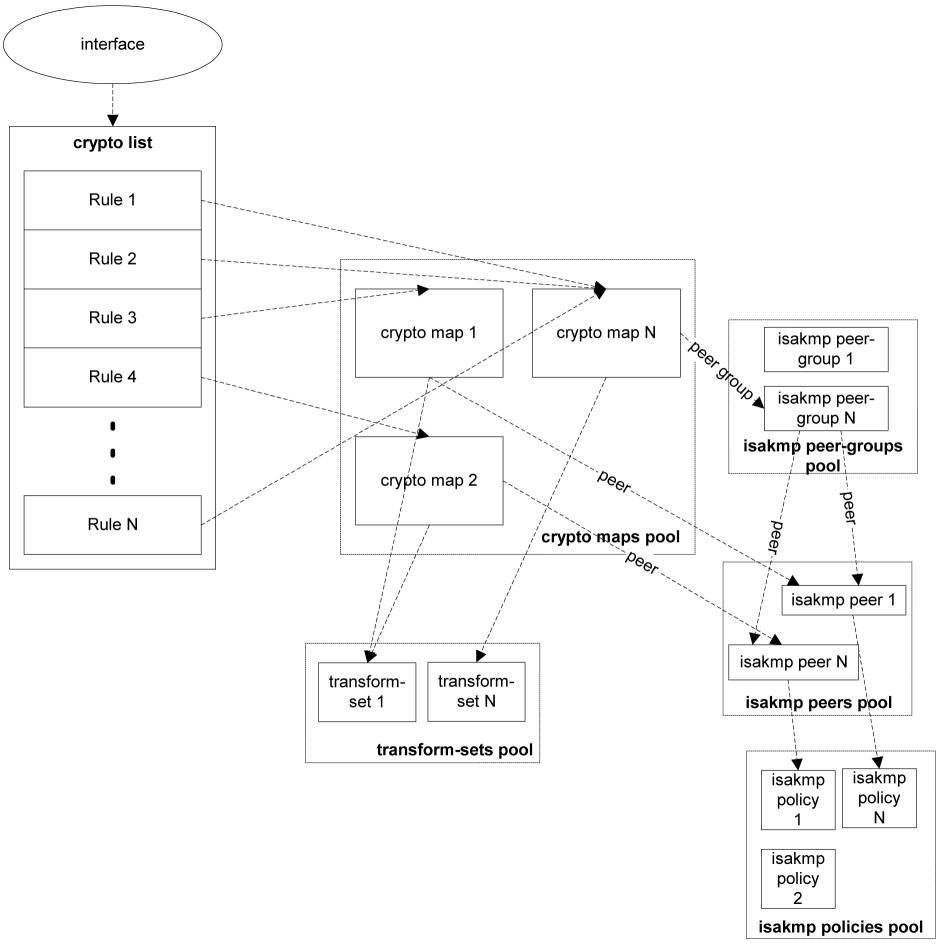
Transform-sets: Define parameters for IKE phase 2 negotiation

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 Site-to-site IPSec VPN on page 482.

Note:

You must configure VPN in the order shown in the summary. Commands appearing in bold are mandatory.

- ISAKMP policy – crypto isakmp policy on page 483
  - description
  - authentication pre-share
  - encryption
  - hash

- group
- lifetime

• IPSEC transform-set – crypto ipsec transform-set on page 485

- set pfs
- set security-association lifetime seconds
- set security-association lifetime kilobytes
- mode (tunnel/transport)

• ISAKMP peer – crypto isakmp peer on page 486

- description
- **isakmp-policy**
- **pre-shared-key**
- initiate mode
- self-identity
- keepalive
- keepalive-track
- continuous-channel

• *(Optional)* ISAKMP peer group – crypto isakmp peer-group on page 489

- description
- set peer

• Crypto map – crypto map on page 490

- description
- **set transform-set**
- **set peer** *or* **set peer-group**
- set dscp
- continuous-channel

• IP crypto list – ip crypto-list on page 492

- **local-address**
- **ip-rule**
  - description
  - **source-ip**
  - **destination-ip**
  - **protect crypto map**

- ip-protocol
- tcp
- udp
- icmp
- dscp
- fragment

- Access control list – ip access-control-list on page 495
- global parameters on page 495
  - crypto isakmp invalid-spi-recovery
  - crypto ipsec nat-transparency udp-encapsulation
  - crypto isakmp nat keepalive
- assigning a crypto-list to an interface on page 497
  - 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 Configuring global parameters on page 495).

Note:

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.

Related topics:

VPN peer coordination on page 483
Configuring ISAKMP policies on page 483
Configuring transform-sets on page 485
Configuring ISAKMP peer information on page 486

Configuring an ISAKMP peer-group on page 489
Configuring crypto maps on page 490
Configuring crypto lists on page 492
Access control lists on page 495
Configuring global parameters on page 495
Assigning a crypto list to an interface on page 497

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.

Note:

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 Configuring ISAKMP policies on page 483)
- The IKE phase 2 parameters (as defined in the transform-set, see Configuring transform-sets on page 485)
- The ISAKMP peer parameters (see Configuring ISAKMP peer information on page 486)
- Which packets should be secured (as defined in the crypto list, see Configuring crypto lists on page 492)
- The peer addresses. For each peer, the local address entered in the crypto list (see Configuring crypto lists on page 492) should match the ISAKMP peer address in the other peer (see Configuring ISAKMP peer information on page 486).
- NAT Traversal, if your installation includes one or more NAT devices between the local and remote VPN peers. See Configuring global parameters on page 495.

See Configuring IPSec VPN logging on page 500 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.

Note:

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.

   Note:

   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 DNS resolver on page 74.

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.

   Important:

   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
Done!
```

   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
Done!
```

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 506.

For example:

```
Gxxx-001(config-peer:149.49.70.1)# initiate mode aggressive
Done!
```

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 509.

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 506.

   For example:

   ```
   Gxxx-001(config-peer:149.49.70.1)# self-identity address
   Done!
   ```

   ```
   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
   Done!
   ```

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 280.

For example:

```
Gxxx-001(config-peer:149.49.70.1)# keepalive-track 5
Done!
```

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 **`continuous-channel`** 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 509.

    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 peer-group 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 526.

Note:

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 486).

   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 0 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 Continuous channel on page 509.

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
Done!
```

```
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 506.

3. Specify the name of the crypto list using the **name** command.
   For example:

```
Gxxx-001(Crypto 901)# name “Public Network via ADSL”
Done!
```

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 Configuring crypto maps on page 490.

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.

6. 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 on page 0 to 6 on page 0 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#
```

Related topics:

Deactivating crypto lists to modify IPSec VPN parameters on page 494
Changing parameters of a crypto list. on page 495

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:

   ```
   G430-001# interface fastethernet 10/2
   G430-001(if:FastEthernet 10/2)# no ip crypto-group
   Done!
   ```

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:

   ```
   G430-001# interface fastethernet 10/2
   G430-001(if:FastEthernet 10/2)# ip crypto-group 901
   Done!
   ```

Changing parameters of a crypto list.

Procedure

1. Use the **ip policy-list-copyold listnew list** command
2. Edit the new list
3. 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 501.

Configuring global parameters

Related topics:

Enabling invalid SPI recovery on page 496

NAT Traversal on page 496

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 496

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 re-enable 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.

Related topics:

Configuring NAT Traversal on page 497

Configuring NAT Traversal

Procedure

1. Enable NAT Traversal by entering **crypto ipsec nat-transparency udp-encapsulation**.
   For example:

   ```
   Gxxx-001# crypto ipsec nat-tranparency 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 492)
  - 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 Dynamic local peer IP on page 506

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 pre-fragmented 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 Summary of VPN commands on page 547 or *Avaya Branch Gateway G430 CLI Reference*.

Related topics:

Commands used to display an IPSec VPN configuration on page 499
Commands used to display IPSec VPN status on page 499
Clearing both ISAKMP connection and IPSec SAs on page 500
Configuring IPSec VPN logging on page 500

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 547

For a full description of the commands and their output fields, see *Avaya Branch Gateway G430 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 547 .

For a full description of the commands and their output fields, see *Avaya Branch Gateway G430 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 System logging on page 215.

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
SA:
   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.

Related topics:

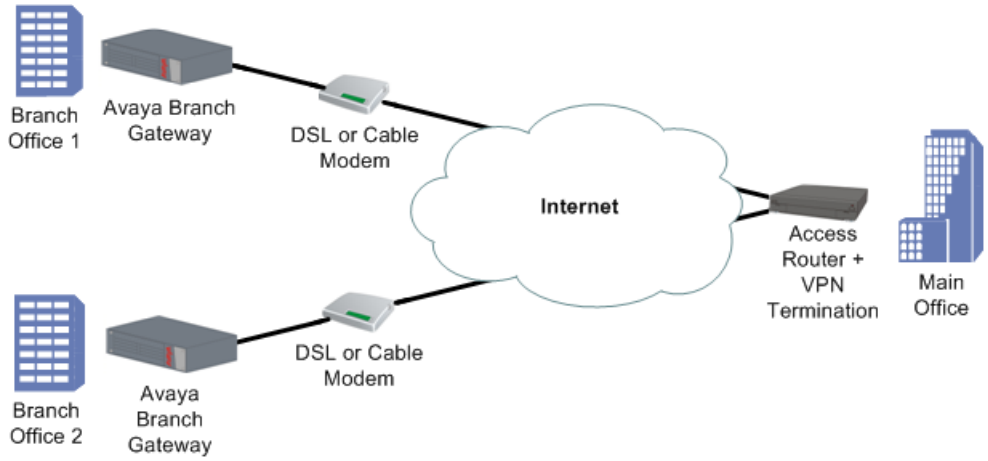
Simple VPN topology – VPN hub and spokes on page 501
Full or partial mesh on page 510
Full or partial mesh diagram on page 511
Full solution: hub and spoke with VPN on page 520
Full solution: hub-and-spoke with VPN for data and VoIP control backup on page 521

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



Related topics:

Configuring the simple VPN topology on page 502
Simple VPN topology on page 503
Simple VPN topology example on page 503
Dynamic local peer IP on page 506
Continuous channel on page 509
Enabling continuous channel on page 509

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 Simple VPN topology on page 503 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)

Note:

For information about using access control lists, see Policy lists on page 553.

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

                       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 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
                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
               exit
      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
      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        901
```

```
         ip access-group      301 in
         ip access-group      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 509).
- Maintain a steady transmission of traffic by sending GRE keepalives or employing object tracking.

Related topics:

Prerequisites for dynamic local peer IP on page 507
Configuring dynamic local peer IP on a PPPoE interface on page 507
Configuring dynamic local peer IP for a DHCP Client on page 508

Prerequisites for dynamic local peer IP

- Specify IKE aggressive mode with the **initiate mode aggressive** command when entering the ISAKMP peer information (see Configuring ISAKMP peer information on page 486).

```
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 Configuring ISAKMP peer information on page 486). 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 Configuring crypto lists on page 492). 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!
```

Note:

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 Configuring PPPoE on page 250.

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.
   b. 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 Policy rule configuration on page 564).
   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
Done!
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
Done!
Gxxx-001(config-ACL 301/ip rule 25)# destination-ip any
Done!
Gxxx-001(config-ACL 301/ip rule 25)# ip-protocol udp
Done!
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
Done!
Gxxx-001(config-ACL 301/ip rule 25)# composite-operation permit
Done!
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
Done!
Gxxx-001(config-ACL 302/ip rule 25)# udp source-port eq bootpc
Done!
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
Done!
```

```
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
Done!
```

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
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 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 204.

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

1. To set continuous channel for IKE phase 1, enter **continuous-channel** when configuring the crypto ISAKMP peer information (see Configuring ISAKMP peer information on page 486).

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 490.

   For example:

```
Gxxx-001# crypto map 1
Gxxx-001(config-crypto:1)# continuous-channel
Done!
```

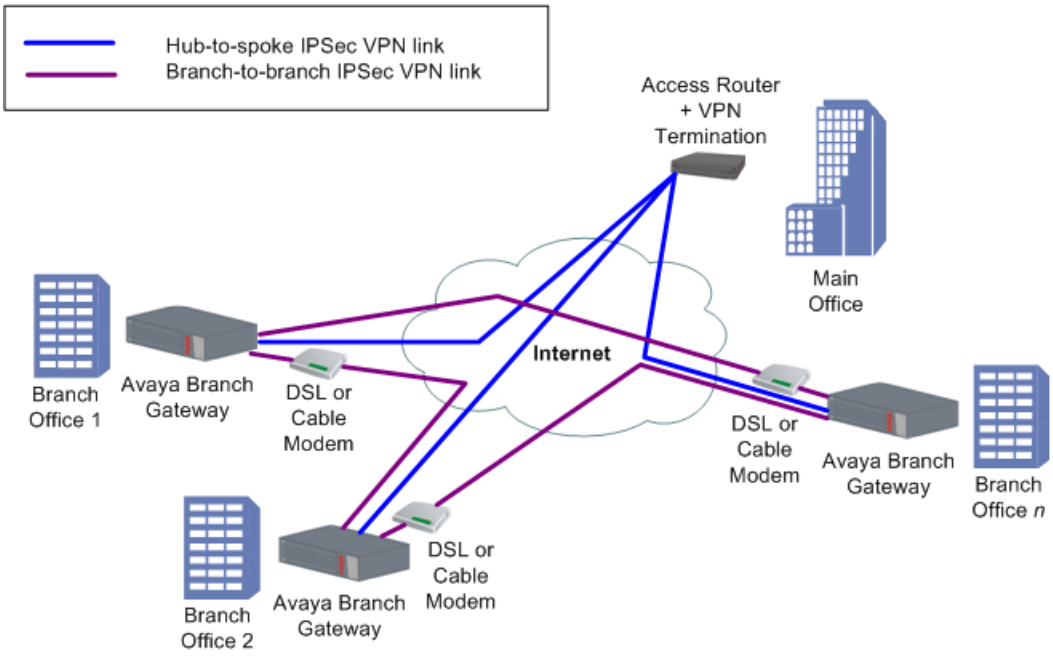
Full or partial mesh

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



Related topics:

[Configuring the mesh VPN topology](#) on page 511
[Mesh VPN topology – Branch Office 1](#) on page 512
[Mesh VPN topology – Branch Office 2](#) on page 513
[Mesh VPN topology example](#) on page 514
[Branch Office 1 configuration](#) on page 514
[Branch Office 2 configuration](#) on page 517

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 [Configure Branch Office 2 as follows:](#) on page 0 for configuration settings.

Note:

For information about using access control lists, see Policy lists on page 553.

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 Mesh VPN topology – Branch Office 2 on page 513 for configuration settings.

Note:

For information about using access control lists, see Policy lists on page 553.

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

Traffic direction	ACL parameter	ACL value	Description
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 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	-

Traffic direction	ACL parameter	ACL value	Description
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

                  Address>
        pre-shared-key  <secret key>
        isakmp-policy 1
        exit
crypto isakmp peer address <Second Branch Office Public Internet Static

                 IP Address>
        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
```

```
          Subnet1 Mask>
               protect crypto map 2
               exit

      ip-rule 2
               source-ip <Branch Subnet2> <Branch Subnet2 Mask>
               destination-ip   <Second Branch Subnet1> <Second Branch

          Subnet1 Mask>
               protect crypto map 2
               exit
      ip-rule 3
               source-ip <Branch Subnet1> <Branch Subnet1 Mask>
               destination-ip   <Second Branch Subnet2> <Second Branch

          Subnet2 Mask>
               protect crypto map 2
               exit
      ip-rule 4

               source-ip <Branch Subnet2> <Branch Subnet2 Mask>
               destination-ip   <Second Branch Subnet2> <Second Branch

          Subnet2 Mask>
               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
               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 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
                exit
      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
      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        901
         ip access-group      301 in
         ip access-group      302 out
         exit
ip default-gateway  FastEthernet 10/3 high
```

Note:

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

                     Address>
         pre-shared-key  <secret key>
         isakmp-policy 1
         exit
crypto isakmp peer address <First Branch Office Public Internet Static IP

                   Address>
         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>
      ip-rule 1

                source-ip <Branch Subnet1> <Branch Subnet1 Mask>
```

```
               destination-ip <First Branch Subnet1> <Second Branch

            Subnet1 Mask>
               protect crypto map 2
               exit
      ip-rule 2
               source-ip <Branch Subnet2> <Branch Subnet2 Mask>
               destination-ip <First Branch Subnet1> <Second Branch

            Subnet1 Mask>
               protect crypto map 2
               exit
      ip-rule 3
               source-ip <Branch Subnet1> <Branch Subnet1 Mask>
               destination-ip <First Branch Subnet2> <Second Branch

            Subnet2 Mask>
               protect crypto map 2
               exit
      ip-rule 4

               source-ip <Branch Subnet2> <Branch Subnet2 Mask>
               destination-ip <First Branch Subnet2> <Second Branch

            Subnet2 Mask>
               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
               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 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
              exit
    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
      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        901
         ip access-group      301 in
         ip access-group      302 out
exit
ip default-gateway  FastEthernet 10/3 high
```

Note:

The highlighted commands are the CLI commands that add the mesh capabilities to the simple hub and spokes configuration.

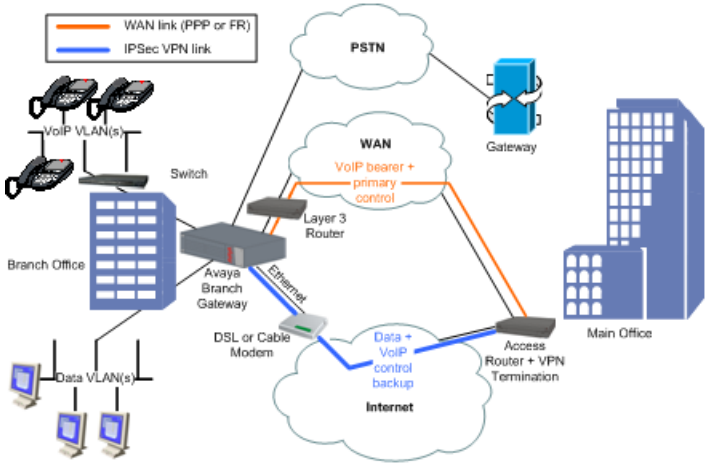
Full solution: hub and spoke with VPN

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, through an external layer 3 router in the branch, to the Main Office for VoIP bearer and as primary VoIP control connection. The layer 3 router is connected to the G430 through a dedicated VLAN interface.
- 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



Related topics:

[Configuring hub-and-spoke with VPN for data and VoIP control backup](#) on page 521
[Hub-and-spoke with VPN](#) on page 522
[Hub-and-spoke with VPN example](#) on page 523

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 [Configuring hub-and-spoke with VPN for data and VoIP control backup](#) on page 521 for configuration settings.

     Note:

     For information about using access control lists, see [Policy lists](#) on page 553.

   - 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

Note:

For information about PBR, see Policy-based routing on page 583.

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

                      Address>
   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

                         Mask>
               composite-operation  Permit
               exit
      ip-rule 50
               source-ip any
               destination-ip <Branch voice Subnet> <Branch voice Subnet

                         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
               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
      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 vlan 3 description “External_router_connection”    ip address
<external router IP address> <external router 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
     ip access-group      301 in
     ip access-group      302 out
     exit
     ip next-hop-list 1    next-hop-ip 1 <external layer 3 router IP address>
    exit
ip next-hop-list 2
    next-hop-interface 1 FastEthernet 10/3    next-hop-ip 2 <external layer 3 router
IP address>
    exit
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
  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 Failover using GRE on page 527), 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 Failover using DNS on page 532). 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 Failover using a peer-group on page 538):
  - 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

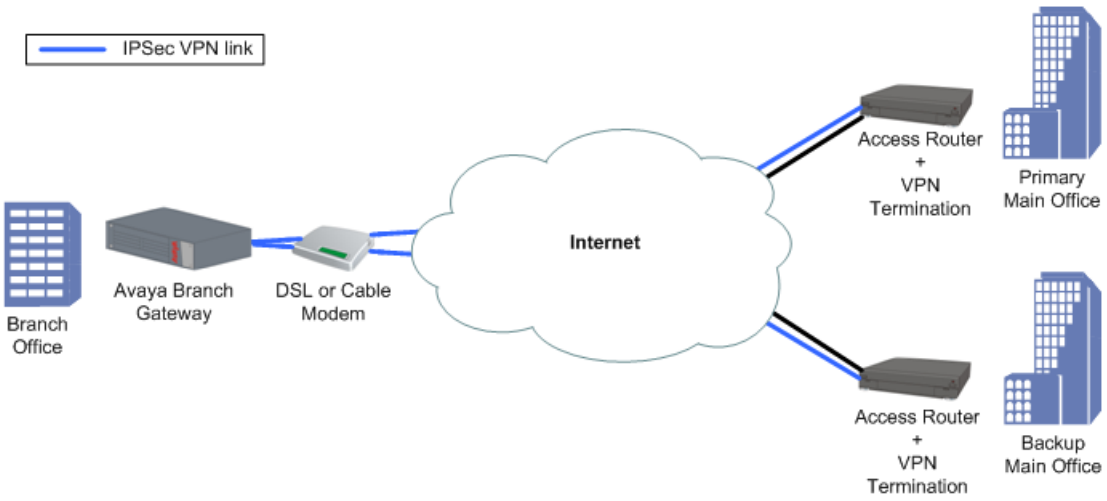
The two GRE tunnels can then be used for branch to Primary/Backup Main Office in either Redundancy or Load sharing mode:

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 VPN hub redundancy and load sharing topologies on page 529 for configuration settings.

      For information about using access control lists, see Policy lists on page 553.
   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
    exit
crypto isakmp peer address <Primary Main Office Internet public Static IP

                      Address>
   pre-shared-key  <key1>
   isakmp-policy 1
   exit
crypto isakmp peer address <Backup Main Office Internet public Static

                IP Address>
   pre-shared-key  <key2>
   isakmp-policy 1
```

```
   exit
crypto ipsec transform-set ts1 esp-3des esp-sha-hmac
   exit
crypto map 1
    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>
ip-rule 1
         source-ip host <Branch GRE Tunnel end point IP Address>
         destination-ip host <Primary Main Office GRE Tunnel end point IP

                        Address>
protect crypto map 1
         exit
ip-rule 2
         source-ip host <Branch GRE Tunnel end point IP Address>
         destination-ip host <Backup Main Office GRE Tunnel end point

                 IP Address>
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 Address>
               ip-protocol icmp
               composite-operation  Permit
               exit
      ip-rule 60
```

```
               source-ip any
               destination-ip any
                        composite-operation  Permit
               exit
      ip-rule 70
               source-ip host <Backup Main Office GRE Tunnel end point

                 IP Address>
               destination-ip host <Branch GRE Tunnel end point IP

              Address>
               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
               source-ip host <Branch GRE Tunnel end point IP Address>
               destination-ip host <Primary Main Office GRE Tunnel end

           point IP Address>
               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 IP Address>
               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
     ip access-group      301 in
     ip access-group      302 out
     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

               Address>
    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

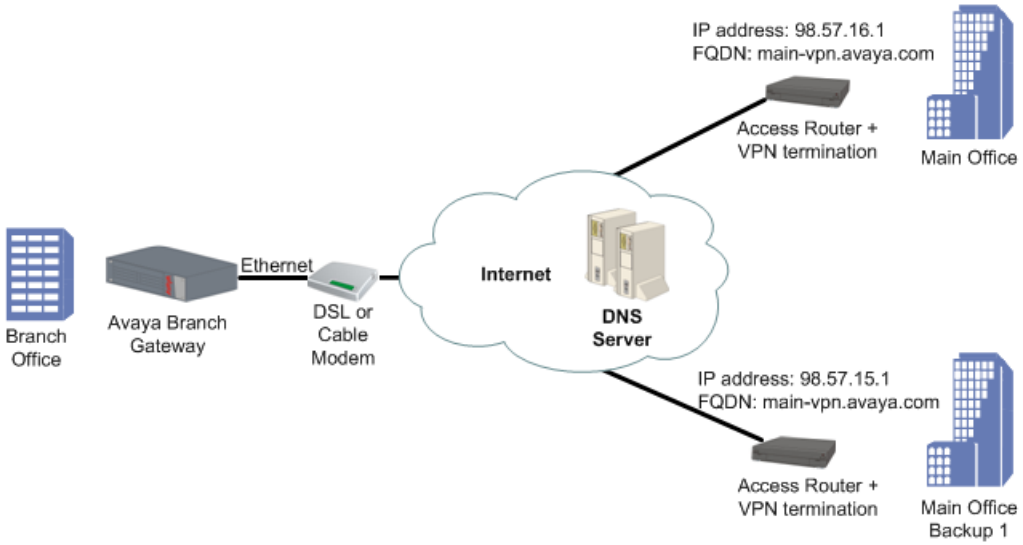
            Address>
   ip address 20.20.20.1 255.255.255.252
   exit
ip route <Primary Main Offfice GRE Tunnel end point IP Address>
                                                          255.255.255.255
FastEthernet 10/3 high
ip route <Backup Main Offfice GRE Tunnel end point IP Address>
                                                          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 74.

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.

5. 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 non-secure 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
   exit
!
! 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
   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 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
      source-ip      10.0.20.0 0.0.0.255
      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
      ip-protocol          udp
      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
```

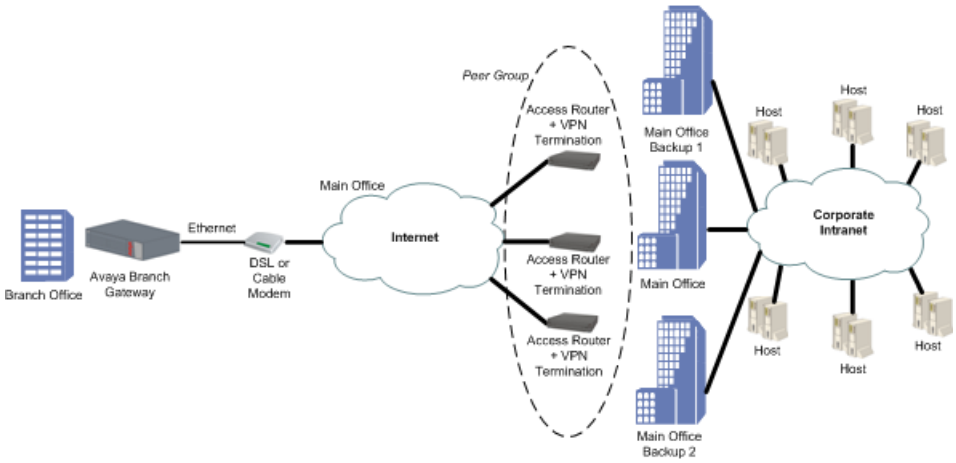
```
      destination-ip any
      ip-protocol     udp
      udp destination-port eq Ike-nat-t
      composite-operation permit
      exit
   ip-rule 12
      source-ip any
      destination-ip any
      ip-protocol     udp
      udp destination-port eq Ike-nat-t-vsu
      composite-operation permit
      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
      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          udp
      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
      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
!
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 Object tracking on page 280.

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 non-secure 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
   exit
!
! 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
rtr 2
   type echo protocol ipIcmpEcho <host2 IP>
   exit
rtr-schedule 2 start-time now life forever
rtr 3
   type echo protocol ipIcmpEcho <host3 IP>
   exit
rtr-schedule 3 start-time now life forever
rtr 4
   type echo protocol ipIcmpEcho <host4 IP>
   exit
rtr-schedule 4 start-time now life forever
```

```
rtr 5
   type echo protocol ipIcmpEcho <host5 IP>
   exit
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
   exit
```

```
! 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
      source-ip      10.0.20.0 0.0.0.255
      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          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       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 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            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
!
interface fastethernet 10/3
   ip crypto-group 901
   ip access-group 301 in
   ip access-group 302 out
   exit
```

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	
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 peer		
a.) VPN IKE (Control) Phase 1 Parameters		
— 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 Parameters		

Parameter	Possible values	Actual value
— 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	
— 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		

Parameter	Possible values	Actual value
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 G430 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

Root level command	First level command	Second level command	Description
	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
	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

Root level command	First level command	Second level command	Description
			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
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.

Root level command	First level command	Second level command	Description
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
interface (fastethernet | dialer|vlan)			Enter the FastEthernet, Dialer, 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
		destination-ip	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 sa			Display the IPSec SA database and related runtime, statistical, and configuration information **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 sa			Display the ISAKMP SA database status
show crypto map			Display all or specific crypto map configurations

Root level command	First level command	Second level command	Description
show ip active-lists			Display information about a specific policy list or all lists
show ip crypto-list			Display all or specific crypto list configurations

Chapter 20: Policy lists

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.

Related topics:

Types of policy lists on page 553
Policy list management on page 556
Policy list configuration on page 557
Policy list attachments on page 560
Device-wide policy lists on page 563
Defining global rules on page 563
Policy rule configuration on page 564
Composite operations on page 570
DSCP table on page 573
Policy list displays and tests on page 575
Summary of access control list commands on page 577
Summary of QoS list commands on page 579

Types of policy lists

There are various policy lists on the Branch Gateway, including access control lists, QoS lists, and Policy-based routing.

Related topics:

About access control lists on page 554
QoS lists on page 555

QoS list parts on page 555
Allowed values on QoS fields on page 556
Use of policy-based routing on page 556

About access control lists

Access lists have the following parts:

Global rules: A set of rules that are executed before the list is evaluated.

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. See Composite operations on page 570.

Related topics:

Access control list rule specifications on page 554
Network security using access control lists on page 554

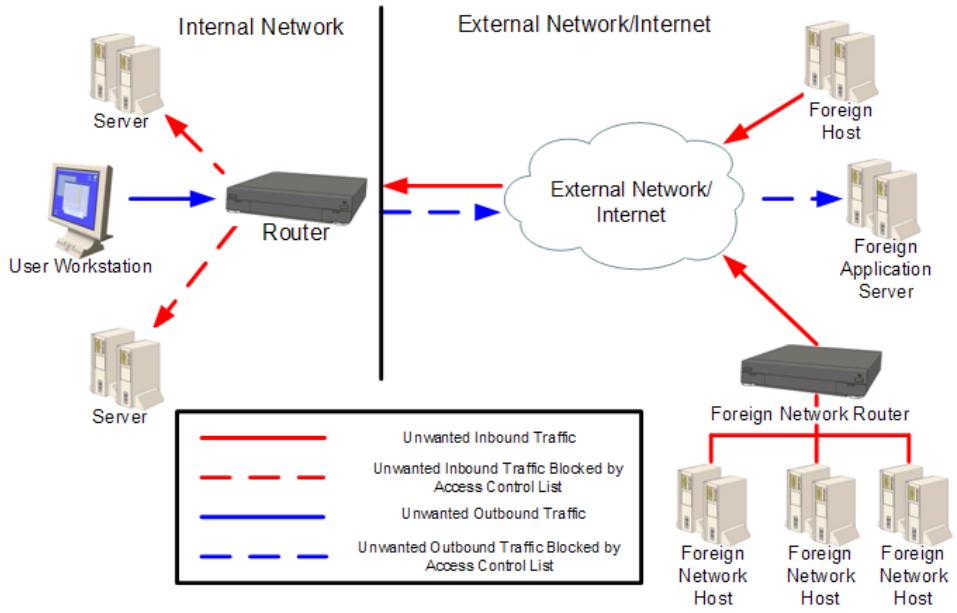
Access control list rule specifications

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 556.

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 570.

DSCP map: A table that contains DSCP code points and match action pairs. Match actions are pointers to the composite operation table. Refer to DSCP table on page 573.

Allowed values on QoS fields

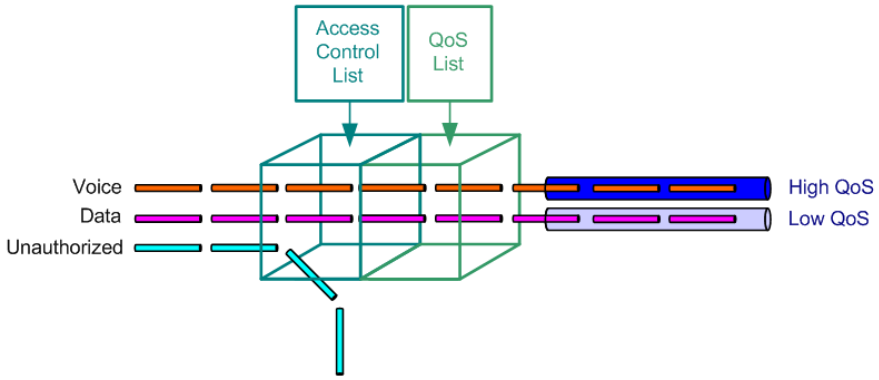
Layer	QoS field	Allowed values
2	802.1p	0–7
3	DSCP	0–63

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 on page 583.

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.

Related topics:

Creating or editing a policy list on page 557
Creating a list based on an existing list on page 558
Defining list identification attributes on page 558
Policy list attributes on page 559
Default actions on page 559
Deleting a policy list on page 559

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 Policy rule configuration on page 564
   - Configure composite operations - see Composite operations on page 570
   - Configure DSCP mapping (QoS lists only) - see DSCP table on page 573

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# <*listnumber*>.
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 qos-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.

Related topics:

[Packets entering the interface](#) on page 560
[Packets exiting the interface](#) on page 560
[Policy lists to packets](#) on page 561
[Policy list attachment configuration](#) on page 561
[Attaching policy lists and access control lists](#) on page 561
[Attaching policy lists and QoS lists](#) on page 562
[Removing a list](#) on page 562

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

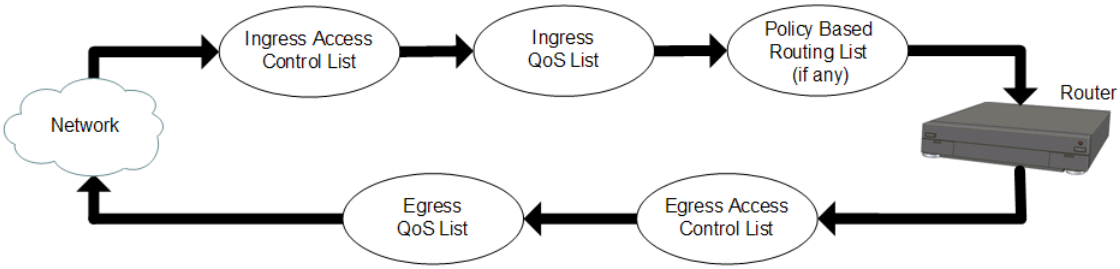
When a packet exits the Branch Gateway through an interface, the Branch Gateway applies the policy lists in the following order:

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 560.

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:
    a. Apply the ingress policy lists that are attached to the interface
    b. Apply the device-wide ingress policy lists
- Outgoing packets:
    a. Apply the device-wide egress policy lists
    b. 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 Policy rule configuration on page 564.

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.

Related topics:

Editing and creating rules on page 565
Policy lists rule criteria on page 565

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 non-fragment packets
- Layer 3 rules that do not include the fragment criteria apply to initial fragments and non-fragment 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

Related topics:

Specifying IP protocol on page 566
Specifying a range of IP addresses on page 566
Specifying source and destination port range on page 567
Applying the rule to ICMP type and code on page 568
Specifying TCP establish bit on page 569

Specifying fragments on page 569
Specifying DSCP on page 569
Composite operation instructions on page 570

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 Summary of access control list commands on page 577, Summary of QoS list commands on page 579, 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 **lt** (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 lt 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 Adding composite operation to an ip rule on page 573.

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.

Related topics:

Pre-configured composite operations for access control lists on page 570
Pre-configured composite operations for QoS lists on page 571
Configuring composite operations on page 572
Adding composite operation to an IP rule on page 573
Composite operation example on page 573

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

No	Name	Access	Notify	Reset Connection
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 pre-configured 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] composite-operation** 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 573.

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 qos-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 Pre-configured composite operations for QoS lists on page 571.

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.

Related topics:

Changing an entry in the DSCP table on page 574

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)# 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.

Related topics:

Policy list commands in context on page 575
Simulating packets on page 576
Simulated packet properties on page 577

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 qos-list/dscp-table context:
  - **show dscp-table**. Displays the parameters of the current DSCP table entry
- In ip qos-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 G430 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 G430 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
	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

Root level command	Command	Command	Description
	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

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 G430 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

Root level command	Command	Command	Description
		name	Assign a name to the current DSCP table entry
		show dscp-table	Display the parameters of the current DSCP table entry
	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

Root level command	Command	Command	Description
		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
	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 21: 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 561.

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 274.

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.

Related topics:

Applications for policy-based routing on page 584
Setting up policy-based routing on page 585
PBR rules on page 588
Next hop lists on page 590
Editing and deleting PBR lists on page 592
PBR list commands in context on page 593
Policy-based routing application example on page 594
Summary of policy-based routing commands on page 597

Applications for policy-based routing

The most common application for policy-based routing is to provide for separate routing of voice and data traffic. It can also be used as a means to provide backup routes for defined traffic types.

Related topics:

Separate routing of voice and data traffic on page 584
Backup interface definition on page 585

Separate routing of voice and data traffic

Although there are many possible applications for policy-based routing, the most common application is to create separate routing for voice and data traffic.

For example, the application shown in the following figure uses the DSCP field to identify VoIP control packets (DSCP = 34, 41), VoIP Bearer RESV packets (DSCP = 43, 44), and VoIP Bearer packets (DSCP = 46). Policy-based routing sends these packets over the T1 WAN line, and sends other packets over the Internet. This saves bandwidth on the more expensive external Serial interface.

Note:

When using a broadband modem (either xDSL or cable), run the VPN application.

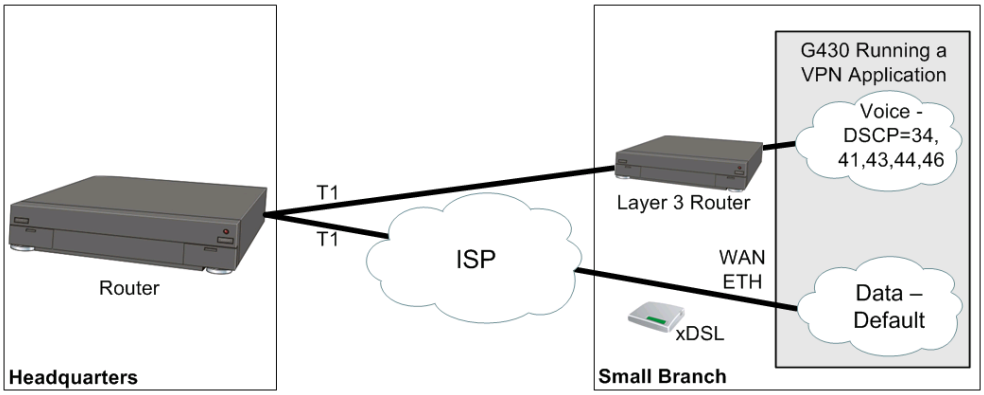


Figure 15: Policy-based routing – Voice/Data division by DSCP

Backup interface definition

You can utilize policy-based routing to define backup routes for defined classes of traffic. If the first route on the next hop list fails, the packets are routed to a subsequent hop. When necessary, you can use the NULL interface to drop packets when the primary next hop fails.

Example

Voice packets are usually sent over a WAN line, and not the Internet. You can configure a PBR list to drop voice packets when the WAN line is down.

Setting up policy-based routing

About this task

For a full example of a policy-based routing configuration, see Policy-based routing application example on page 594.

Procedure

1. Define PBR lists.
   - In general context, enter **`ip pbr-list`** followed by a list number in the range 800 to 899. For example:

```
Gxxx-001(super)# ip pbr-list 802
Gxxx-001(super-PBR 802)#
```

- To assign a name to the list, use the **name** command, followed by a text string, in the PBR list context. The default name is **list** #<*list number*>. For example:

```
Gxxx-001(super-PBR 802)# name voice
Done!
Gxxx-001(super-PBR 802)#
```

- To assign an owner to the list, use the **owner** command, followed by a text string, in the PBR list context. The default owner is other. For example:

```
Gxxx-001(super-PBR 802)# owner tom
Done!
Gxxx-001(super-PBR 802)#
```

2. Define PBR rules.

   In the PBR list context, enter **ip-rule**, followed by the number of the rule, to define a rule for the PBR list. Repeat this command to define additional rules. A rule contains: (i) criteria that is matched against the packet, and (ii) a next hop list. When a packet matches the criteria specified in the rule, the rule's next hop list determines how the packet is routed. Each PBR list can have up to 1,500 rules. The first rule that matches the packet determines the packet's routing.

   It is important to include a destination address, or range of addresses, in PBR rules to better classify the traffic to be routed. For an illustration, see Policy-based routing application example on page 594.

   Note:

   Leave a gap between rule numbers, in order to leave room for inserting additional rules at a later time. For example, ip-rule 10, ip-rule 20, ip-rule 30.

   The following example creates rule 1, which routes packets going to IP address 149.49.43.210 with a DSCP value of 34 according to next hop list 1. The next step explains how to define a next hop list. For additional details about PBR rules, see PBR rules on page 588.

```
Gxxx-001(super-PBR 802)# ip-rule 1
Gxxx-001(super-PBR 802/ip rule 1)# next-hop list 1
Done!
Gxxx-001(super-PBR 802/ip rule 1)# destination-ip host 149.49.43.210
Done!
Gxxx-001(super-PBR 802/ip rule 1)# dscp 43
Done!
Gxxx-001(super-PBR 802/ip rule 1)#
```

   Note:

   Rules do not include a default next hop list. Thus, if you do not include a next hop list in the rule, the packet is routed according to destination-based routing, that is, the ordinary routing that would apply without policy-based routing.

3. Define next hop lists.

   Enter **exit** twice to return to general context. In general context, define all the next hop lists that you have used in PBR rules.

Note:

You can also perform this step before defining PBR lists and rules.

Enter **ip next-hop-list**, followed by the number of the list, to define a next hop list. In the next hop list context, use the following commands to define the next hops in the list:

- Enter **next-hop-ip**, followed by the index number of the entry in the next hop list, to define an IP address as a next hop. You can optionally apply tracking to monitor the route.
- Enter **next-hop-interface**, followed by the index number of the entry in the next hop list, to define an interface as a next hop. You can optionally apply tracking to monitor the route.

You can also use the **name** command to assign a name to the next hop list.

Note:

You cannot use a FastEthernet Interface as an entry on a next hop list unless the interface was previously configured to use **PPPoE** encapsulation, or was configured as a DHCP client. See Configuring PPPoE on page 250, and DHCP client configuration on page 204.

A next hop list can include the value NULL0. When the next hop is NULL0, the Branch Gateway drops the packet. However, you cannot apply tracking to NULL0.

The following example creates next hop list 1, named “Data to HQ”, with the following entries:

- The first entry is the FastEthernet 10/2 interface. Object tracker 3 is applied to monitor the route. For details about configuring the object tracker see Object tracking on page 280.
- The second entry is IP address 172.16.1.221. This is the IP address of the external Layer 3 router connected to the Branch Gateway.
- The third entry is NULL0, which means the packet is dropped

```
Gxxx-001(super)# ip next-hop-list 1
Gxxx-001(super-next hop list 1)#name “Data_to_HQ”
Done!
Gxxx-001(super-next hop list 1)#next-hop-interface 1 FastEthernet 10/2
track 3
Done!
Gxxx-001(super-next hop list 1)#next-hop-ip 2 172.16.1.221
Done!
Gxxx-001(super-next hop list 1)#next-hop-interface 3 Null0
Done!
Gxxx-001(super-next hop list 1)#
```

For additional details about next hop lists, see Next hop lists on page 590.

This example demonstrates a case where the data traffic is sent over the WAN FastEthernet Interface through the Internet.

When the track detects that this next hop is not valid, traffic is routed over the external Serial interface connected to the external Layer 3 router.

4. Apply the PBR list to an interface.

   Enter **exit** to return to general context. From general context, enter the interface to which you want to apply the PBR list. In the interface context, enter **ip pbr-group**, followed by the number of the PBR list, to attach the list to the interface. The list will be applied to packets entering the interface.

   The following example applies PBR list 802 to VLAN 2.

   ```
   Gxxx-001(super)# interface vlan 2
   Gxxx-001(super-if:VLAN 2)# ip pbr-group 802
   Done!
   Gxxx-001(super-if:VLAN 2)#
   ```

5. Apply the PBR list to the Loopback interface.
   The following example applies PBR list 802 to the Loopback interface.

   ```
   Gxxx-001(super)# interface Loopback 1
   Gxxx-001(super-if:Loopback 1)# ip pbr-group 802
   Done!
   Gxxx-001(super-if:Loopback 1)# exit
   Gxxx-001(super)#
   ```

6. Enter **copy running-config startup-config**.
   This saves the new policy-based routing configuration in the startup configuration file.

PBR rules

Each PBR list can have up to 1,500 rules. The first rule that matches the packet specifies the next hop list for the packet. If no rule matches the packet, the packet is routed according to the default rule.

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, 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

- Fragments
- DSCP field

Note:

The fragment criteria is used for non-initial fragments only. You cannot specify TCP/UDP ports or ICMP code/type for a rule when using the **`fragment`** command.

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.

Note:

When you use destination and source ports in a PBR rule, policy-based routing does not catch fragments.

Note:

It is recommended to leave a gap between rule numbers, in order to leave room for inserting additional rules at a later time. For example, ip-rule 10, ip-rule 20, ip-rule 30.

Related topics:

Modifying rules on page 589
PBR rule criteria on page 590

Modifying rules

About this task

To modify a policy-based routing rule, you must enter the context of the rule and redefine the rule criteria.

Procedure

1. Enter the context of the PBR list to which the rule belongs.
2. Enter **`ip-rule`** followed by the number of the rule you want to modify.
   For example, to create rule 1, enter **`ip-rule 1`**.

   To view the rules that belong to a PBR list, enter the list's context and then enter **`show ip-rule`**.

PBR rule criteria

The rule criteria for PBR rules are largely the same as the rule criteria for other policy list rules. Refer to Policy lists rule criteria on page 565 for an explanation of the rule criteria, including explanations and examples of the commands used to set the criteria.

Unlike other policy lists, PBR lists do not use composite operations. Thus, there is no **composite-operation** command in the context of a PBR rule. Instead, PBR lists use next hop lists. For an explanation of next hop lists, see Next hop lists on page 590.

Enter **next-hop list**, followed by the list number of a next hop list, to specify a next hop list for the Branch Gateway to apply to packets that match the rule. You can specify Destination Based Routing instead of a next hop list, in which case the Branch Gateway applies destination-based routing to a packet when the packet matches the rule.

If the next hop list specified in the rule does not exist, the Branch Gateway applies destination-based routing to packets that match the rule.

Next hop lists

PBR rules include a next hop list. When the rule matches a packet, the Branch Gateway routes the packet according to the specified next hop list.

Each next hop list can include up to 20 entries. An entry in a next hop list can be either an IP address or an interface. The Branch Gateway attempts to route the packet to the first available destination on the next hop list. If every destination on the list is unavailable, the Branch Gateway routes the packet according to destination-based routing.

Related topics:

Modifying next hop lists on page 590

Modifying next hop lists

Procedure

1. To modify a next hop list, you must enter the context of the next hop list.

   To enter a next hop list context, enter **ip next-hop-list** followed by the number of the list you want to edit.

   For example, to modify next hop list 1, enter **ip next-hop-list 1**.

2. To show the next hops in an existing list, enter the context of the next hop list and enter **show next-hop**.

Related topics:

Adding entries to a next hop list on page 591
Deleting an entry from a next hop list on page 591
Canceling tracking and keeping the next hop on page 591
Changing the object tracker and keeping the next hop on page 592

Adding entries to a next hop list

Procedure

1. Enter the context of the next hop list.
2. Use one of the following commands:
   - To enter an IP address as a next hop, enter **next-hop-ip**, followed by the index number of the entry and the IP address. You can optionally apply tracking to monitor the route. For example, the command **next-hop-ip 2 149.49.200.2 track 3** sets the IP address 149.49.200.2 as the second entry on the next hop list and applies object tracker 3 to monitor the route.
   - To enter an interface as a next hop, enter **next-hop-interface**, followed by the index number of the entry and the name of the interface. You can optionally apply tracking to monitor the route, except for the NULL0.

   For example, the command **next-hop-interface 3 fastethernet 10/2** sets FastEthernet 10/2 as the third entry on the next hop list.

Deleting an entry from a next hop list

Procedure

1. Enter the context of the next hop list.
2. Use one of the following commands:
   - To delete an IP address, enter **no next-hop-ip**, followed by the index number of the entry you want to delete. For example, the command **no next-hop-ip 2** deletes the second entry from the next hop list.
   - To delete an interface, enter **no next-hop-interface**, followed by the index number of the entry you want to delete. For example, the command **no next-hop-interface 3** deletes the third entry from the next hop list.

Canceling tracking and keeping the next hop

Procedure

1. Enter the context of the next hop list.

2. Use the **next-hop-ip** or **next-hop-interface** command again, without the **track** keyword.

Changing the object tracker and keeping the next hop

Procedure

1. Enter the context of the next hop list.
2. Use the **next-hop-ip** or **next-hop-interface** command again, with the **track** keyword followed by the new track index.

Editing and deleting PBR lists

About this task

You cannot delete or modify a PBR list when it is attached to an interface. In order to delete or modify a PBR list, you must first remove the list from the interface. You can then delete or modify the list. After modifying the list, you can reattach the list to the interface.

Procedure

1. To remove a list from an interface, use the **no** form of the **ip pbr-group** command in the interface context.
   The following example removes the PBR list from the VLAN 2 interface.

```
Gxxx-001(super)# interface vlan 1
Gxxx-001(super-if:VLAN 1)# no ip pbr-group
Done!
Gxxx-001(super-if:VLAN 1)#
```

2. To modify a PBR list, enter **ip pbr-list**, followed by the number of the list you want to modify, to enter the list context.

   Redefine the parameters of the list.

3. To delete a PBR list, enter **exit** to return to general context and enter **no ip pbr-list** followed by the number of the list you want to delete.

PBR list commands in context

When viewing information about PBR lists and their components, the following commands produce different results in different contexts.

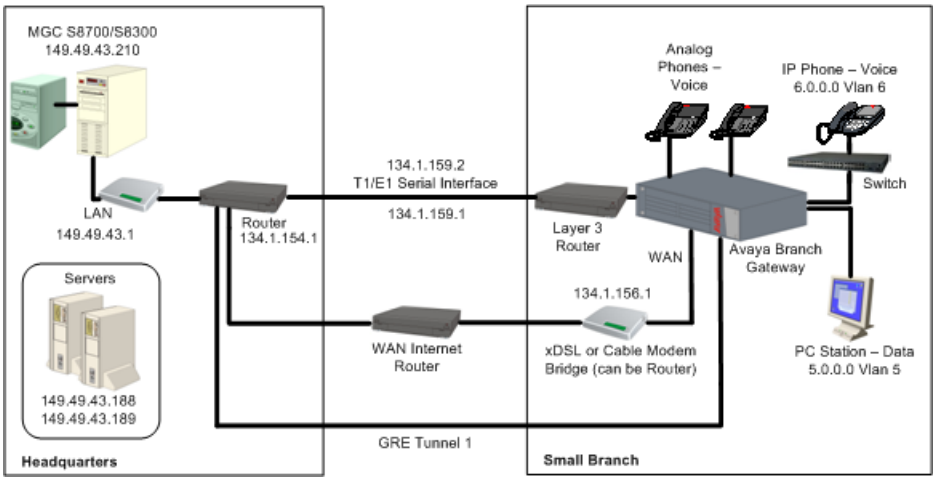
- In general context:
  - **show ip active-pbr-lists**. Displays details about a specified PBR list, or about all active PBR lists, according to the interfaces on which the lists are active
  - **show ip pbr-list**. Displays a list of all configured PBR lists, with their list numbers and names and their owners
  - **show ip pbr-list list number**. Displays the list number and name of the specified PBR list
  - **show ip pbr-list all detailed**. Displays all the parameters of all configured PBR lists
  - **show ip pbr-list list number detailed**. Displays all the parameters of the specified PBR list
  - **show ip active-lists**. Displays a list of each Branch Gateway interface to which a PBR list is attached, along with the number and name of the PBR list
  - **show ip active-lists list number**. Displays a list of each Branch Gateway interface to which the specified PBR list is attached, along with the number and name of the PBR list
  - **show ip next-hop-list all**. Displays the number and name of all next hop lists
  - **show ip next-hop-list list number**. Displays the number and name of the specified next hop list
- In PBR list context:
  - **show list**. Displays all the parameters of the current PBR list
  - **show ip-rule**. Displays the parameters of all rules configured for the current list
  - **show ip-rule rule number**. Displays the parameters of the specified rule
- In next hop list context:
  - **show next-hop**. Displays the next hop entries in the current next hop list and their current status

Policy-based routing application example

The following example creates a policy-based routing scheme in which:

- Voice traffic is routed over an external Serial interface using an external Layer 3 router connected to the gateway. If the interface is down, the traffic is dropped.
- Data traffic is routed over a GRE tunnel. If the tunnel is down, the traffic is routed over the external Serial interface. If both interfaces are down, the traffic is dropped.

The following figure illustrates the sample application described below.



This example includes a voice VLAN (6) and a data VLAN (5). The PMI is on VLAN 6. The Branch Gateway is managed by a remote Media Gateway Controller (MGC) with the IP address 149.49.43.210. The Branch Gateway also includes a local S8300 in LSP mode.

IP phones are located on the same subnet as the PMI. Therefore, there is no routing between the PMI and the IP phones.

In this example, the object of policy-based routing is to route all voice traffic over the E1/T1 line, which is more expensive but provides the superior QoS necessary for voice traffic. Remaining traffic is to be routed over the more inexpensive Internet connection.

It is assumed that the IP phones on VLAN 6 establish connections with other IP phones on the same subnet, sending signalling packets to the MGC, and bearer packets directly to other IP phones or to the Branch Gateway.

The policy-based routing configuring starts with PBR list 801. This list requires all voice packets addressed to the MGC (149.49.43.210) with DSCP values that indicate voice transmission (34, 41, 43, 44, and 46) to be routed according to next hop list 1. This list directs packets to the T1/E1 interface. If that interface is down, the packets are dropped.

In this example, it is important to include the destination IP address in each rule. This is because without the destination address, calls from IP phones on VLAN 6 to a Softphone on VLAN 5

will be routed by the PBR list to the E1/T1 line, rather than being sent directly to VLAN 5 via the Branch Gateway.

Related topics:

Configuration for the sample policy-based routing application on page 595
Packet simulation in PBR on page 597

Configuration for the sample policy-based routing application

```
Gxxx-001(super)# ip pbr-list 801
Gxxx-001(super-PBR 801)# name “Voice”
Done!
Gxxx-001(super-PBR 801)# ip-rule 1
Gxxx-001(super-PBR 801/ip rule 1)# next-hop list 1
Done!
Gxxx-001(super-PBR 801/ip rule 1)# destination-ip 149.49.123.0 0.0.0.255
Done!
Gxxx-001(super-PBR 801/ip rule 1)# dscp 34
Done!
Gxxx-001(super-PBR 801/ip rule 1)# exit
Gxxx-001(super-PBR 801)# ip-rule 10
Gxxx-001(super-PBR 801/ip rule 10)# next-hop list 1
Done!
Gxxx-001(super-PBR 801/ip rule 10)# destination-ip 149.49.123.0 0.0.0.255
Done!
Gxxx-001(super-PBR 801/ip rule 10)# dscp 41
Done!
Gxxx-001(super-PBR 801/ip rule 10)# exit
Done!
Gxxx-001(super-PBR 801/ip rule 20)# destination-ip 149.49.123.0 0.0.0.255
Done!
Gxxx-001(super-PBR 801/ip rule 20)# dscp 43
Done!
Gxxx-001(super-PBR 801/ip rule 20)# exit
Gxxx-001(super-PBR 801)# ip-rule 30
Gxxx-001(super-PBR 801/ip rule 30)# next-hop list 1
Done!
Gxxx-001(super-PBR 801/ip rule 30)# destination-ip 149.49.123.0 0.0.0.255
Done!
Gxxx-001(super-PBR 801/ip rule 30)# dscp 44
Done!
Gxxx-001(super-PBR 801/ip rule 30)# exit
Gxxx-001(super-PBR 801)# ip-rule 40
Gxxx-001(super-PBR 801/ip rule 40)# next-hop list 1
Done!
Gxxx-001(super-PBR 801/ip rule 40)# destination-ip 149.49.123.0 0.0.0.255
Done!
Gxxx-001(super-PBR 801/ip rule 40)# dscp 46
Done!
Gxxx-001(super-PBR 801/ip rule 40)# exit
Gxxx-001(super-PBR 801)# exit
Gxxx-001(super)#
```

The next group of commands configures next hop list 1, which was included in the rules configured above. Next hop list 1 sends packets that match the rule in which it is included to the IP address of the Layer 3 router. If that interface is not available, the next hop list requires the packet to be dropped (Null0). This is because the QoS on the Internet interface is not

adequate for voice packets. It would also be possible to include one or more backup interfaces in this next hop list.

```
Gxxx-001(super)# ip next-hop-list 1
Gxxx-001(super-next hop list 1)#name “Voice-To_HQ”
Done!
Gxxx-001(super-next hop list 1)#next-hop-ip 1 <external Layer 3 router IP address>
Done!
Gxxx-001(super-next hop list 1)#next-hop-interface 2 Null0
Done!
Gxxx-001(super-next hop list 1)#exit
Gxxx-001(super)#
```

The next set of commands applies the PBR list to the voice VLAN (6).

```
Gxxx-001(super)# interface vlan 6
Gxxx-001(super-if:VLAN 6)# ip pbr-group 801
Done!
Gxxx-001(super-if:VLAN 6)# exit
Gxxx-001(super)#
```

The next set of commands applies the PBR list to the Loopback interface. This is necessary to ensure that voice packets generated by the Branch Gateway itself are routed via the external E1/T1 line installed on the external Layer 3 router. The Loopback interface is a logical interface that is always up. Packets sent from the Branch Gateway, such as signaling packets, are sent via the Loopback interface. In this example, applying PBR list 801 to the Loopback interface ensures that signaling packets originating from voice traffic are sent via the T1/E1 line.

```
Gxxx-001(super)# interface Loopback 1
Gxxx-001(super-if:Loopback 1)# ip pbr-group 801
Done!
Gxxx-001(super-if:Loopback 1)# exit
Gxxx-001(super)#
```

The next set of commands defines a new PBR list (802). This list will be applied to the data interface (VLAN 5). The purpose of this is to route data traffic through interfaces other than the E1/T1 interface, so that this traffic will not interface with voice traffic.

```
Gxxx-001(super)# ip pbr-list 802
Gxxx-001(super-PBR 802)# name “Data_To_HQ”
Done!
Gxxx-001(super-PBR 802)# ip-rule 1
Gxxx-001(super-PBR 802/ip rule 1)# next-hop list 2
Done!
Gxxx-001(super-PBR 802/ip rule 1)# ip-protocol tcp
Done!
Gxxx-001(super-PBR 802/ip rule 1)# destination-ip host 149.49.43.189
Done!
Gxxx-001(super-PBR 802/ip rule 1)# exit
Gxxx-001(super-PBR 802)# exit
```

The next set of commands creates next hop list 2. This next hop list routes traffic to the GRE tunnel (Tunnel 1). If the GRE tunnel is not available, then the next hop list checks the next entry on the list and routes the traffic to the external E1/T1 interface. If neither interface is available, the traffic is dropped. This allows data traffic to use the E1/T1 interface, but only when the GRE tunnel is not available. Alternatively, the list can be configured without the external E1/T1 interface, preventing data traffic from using the external E1/T1 interface at all.

```
G430-001(super)# ip next-hop-list 2
G430-001(super-next hop list 2)#name “Data-To_HQ”
```

```
Done!
G430-001(super-next hop list 2)#next-hop-interface 1 Tunnel 1
Done!
G430-001(super-next hop list 2)#next-hop-ip 2 <external Layer 3 router IP address>
Done!
G430-001(super-next hop list 2)#next-hop-interface 3 Null0
Done!
G430-001(super-next hop list 2)#exit
G430-001(super)#
```

Finally, the next set of commands applies the PBR list to the data VLAN (5).

```
Gxxx-001(super)# interface vlan 5
Gxxx-001(super-if:VLAN 6)# ip pbr-group 802
Done!
Gxxx-001(super-if:VLAN 6)# exit
Gxxx-001(super)#
```

In this example you can add a track on GRE Tunnel 1 in order to detect whether this next hop is valid or not (for more information on object tracking, refer to Object tracking on page 280). Note that the GRE tunnel itself has keepalive and can detect the status of the interface and, therefore, modify the next hop status.

Packet simulation in PBR

Policy-based routing supports the **`ip simulate`** command for testing policies. Refer to Simulating packets on page 576.

Summary of policy-based routing commands

For more information about these commands, see the *Avaya Branch Gateway G430 CLI Reference*.

Root level command	First level command	Second level command	Description
`ip next-hop-list`			Enter the context of the specified next hop list. If the list does not exist, it is created.
	`next-hop-interface`		Add the specified interface to the next hop path for this next-hop list
	`next-hop-ip`		Add the specified ip address to the next hop path for this next-hop list
	`show next-hop`		Display the next-hop entries in the current list

Root level command	First level command	Second level command	Description
interface			Enter the interface configuration mode for a Dialer, Loopback, Fast Ethernet, Tunnel or VLAN interface
	ip pbr-group		Apply the specified PBR list to the current interface. The PBR list is applied to ingress packets only.
ip pbr-list			Enter the context of the specified PBR list. If the list does not exist, it is created.
	cookie		Set the cookie for the current list
	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.
		destination-ip	Specify the destination IP address of packets to which the current rule applies
		dscp	Specify the DSCP value that is set by the current policy operation
		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
		next-hop	Specify the next-hop policy to use when the current rule is applied
		show ip next-hop-list	Display the details of the next-hop list or of all next-hop lists
		show ip-rule	Display the attributes of a specific rule or all rules
		source-ip	Apply the current rule to packets from the specified source IP address

Root level command	First level command	Second level command	Description
		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 specified list or operation
	owner		Specify the owner of the current list
	show ip-rule		Display the attributes of a specific rule or all rules
	show list		Display information about the specified list
show ip active-lists			Display information about a specific policy list or all lists
show ip active-pbr- lists			Display details about a specific PBR list or all PBR lists
show ip pbr-list			Display information about the specified PBR list

Chapter 22: Synchronization

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. If no MM710 is 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 Communication Manager's SAT Administration forms to administer Synchronization over IP.

Related topics:

Defining a stratum clock source on page 601
Setting the syncronization source on page 602
Disassociating a clock source on page 603
Enabling and disabling automatic failover and failback on page 603
Synchronization status on page 603

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 syncronization 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 additional 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 S8300 Server.

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

Related topics:

Displaying synchronization status on page 604
Summary of synchronization commands on page 604

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

```
Gxxx-???(super)# sh sync timing
SYNCHRONIZATION CONTROL: --- Local ---

SOURCE     MM or VoIP           STATUS                   FAILURE
---------  -------------------  -----------------------  ---------------
Primary                         Not Configured
Secondary                       Not Configured
Local      v0                   Active                   None

Active Source: v0               Sync Source Switching: Enabled

Done!
```

Summary of synchronization commands

For more information about these commands, see *Avaya Branch Gateway G430 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

Command	Description
show sync timing	Display the status of the primary, secondary, and local clock sources

Appendix A: Traps and MIBs

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 implementation.
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

Name	Parameters (MIB variables)	Class	Msg Facility	Severity	Trap Name/ Mnemonic	Format	Description
							and the entity's implementation intact.
LinkUp	ifIndex, ifAdminStatus, ifOperStatus	STD	System	Warning	LinkUp	Agent Interface Up (linkUp Trap) enterprise: $E ($e) on interface $1	A linkUp trap indicates that the entity 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, ifAdminStatus, ifOperStatus	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

Name	Parameters (MIB variables)	Class	Msg Facility	Severity	Trap Name/ Mnemonic	Format	Description
							the agent's configuration. 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_Authen_Failure		P330	SECURITY	Notification	authenticFailure	Incorrect Community Name (authentication Failure Trap) enterprise: $E ($e) args($#):$*	An authentication failure trap indicates that the protocol is not properly authenticated.
risingAlarm	alarmIndex, alarmVariable, alarmSampleType, alarmValue, alarmRisingThreshold	RMON	THRESHOLD	Warning	risingAlarm	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
fallingAlarm	alarmIndex, alarmVariable,	RMON	THRESHOLD	Warning	fallingAlarm	Falling Alarm: $2 fell below threshold	The SNMP trap that is generated when an alarm

Name	Parameters (MIB variables)	Class	Msg Facility	Severity	Trap Name/ Mnemonic	Format	Description
	alarmSampleType, alarmValue, alarmRisingThreshold, alarmFallingThreshold					$5; value = $4. (Sample type = $3; alarm index = $1)	entry crosses its falling threshold and generates an event that is configured for sending SNMP traps
deleteSWRedundancy Trap	softRedundancyStatus	P330	SWITCH FABRIC	Info	deleteSWRedundancyTrap	Software Redundancy $1 definition deleted	The trap notifies the manager of the deletion of the specified redundant link, which is identified by the softRedundancyId. It is enabled/ disabled by chLntAgConfigChangeTraps.
createSWRedundancy Trap	softRedundancyStatus	P330	SWITCH FABRIC	Info	createSWRedundancyTrap	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 softRedundancyId defines the instances of the above-

Name	Parameters (MIB variables)	Class	Msg Facility	Severity	Trap Name/ Mnemonic	Format	Description
							mentioned variables. The trap is enabled/ disabled by chLntAgConfig ChangeTraps.
lseIntPort CAMLast Change Trap	lseIntPort CAMLast Change	P330	SWITCH FABRIC	Info	lseIntPort CAMLast Change Trap	CAM Change at $1	This trap reports of the occurred configuration changes. It is enabled/ disabled by chLntAgCAMC hangeTraps.
duplicateI P Trap	ipNetToM ediaPhys Address, ipNetToM ediaNetA ddress	P330	ROUTER	Warni ng	duplicate IPTrap	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.
lntPolicy ChangeEv ent	ipPolicy Activation EntID, ipPolicy Activation List, ipPolicy Activation if Index, ipPolicy Activation Sub Context	P330	POLICY	Info	lntPolicy ChangeE vent	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.

Name	Parameters (MIB variables)	Class	Msg Facility	Severity	Trap Name/ Mnemonic	Format	Description
IntPolicyAccessControlViolationFlt	ipPolicyAccessControlViolationEnt ID, ipPolicyAccessControlViolationSrcAddr, ipPolicyAccessControlViolationDst Addr, ipPolicyAccessControlViolationProtocol, ipPolicyAccessControlViolationL4SrcPort, ipPolicyAccessControlViolationL4DstPort, ipPolicyAccessControlViolationEstablished, ipPolicyRuleID, ipPolicyRule ListID, ipPolicyAccessControlViolationIfIndex, ipPolicy	P330	POLICY	Warning	IntPolicyAccessControlViolationFlt	IP PolicyAccess Control violation, if-index$9 ip-protocol=$4 src-ip=$2 dst-ip=$3 src-port=$5 dst-port=$6 rule-id=$8 rule-list=$$9	This trap reports to the Management station on IP PolicyAccess Control violation. The trap includes in its varbind information about the slot where the event occurred. The id of the rule that was violated in the current rules table, and the quintuplet that identifies the faulty packet. A management application would display this trap and the relevant information in a log entry. This trap will not be sent at intervals smaller than one minute for identical information in the varbinds list variables.

Name	Parameters (MIB variables)	Class	Msg Facility	Severity	Trap Name/ Mnemonic	Format	Description
	AccessControl ViolationSub Ctxt, ipPolicy AccessControl ViolationTime						
DormantPort Fault	genPortSWRdFault, genPortGroup 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.
DormantPort Ok	genPortSWRdFault, genPortGroup Id, genPortId	P330	SWITCH FABRIC	Notification	Dormant PortOk	Dormant Port Connection Returned to Normal on Module $2 Port $3;	This trap reports the return of connection on a dormant port.
InlinePwr Flt	genGroup FaultMask, genGroup Id, genGroup BUPSActivity Status	P330	POE	Error	InlinePwr Flt	Module $2 Inline Power Supply failure	This trap reports the failure of an inline power supply.
InlinePwr FltOK	genGroup FaultMask, genGroup Id, genGroup BUPSActivity Status	P330	POE	Notification	InlinePwr FltOK	Module $2 Inline Power Supply failure was cleared	This trap reports the correction of a failure on an inline power supply.
WanPhysical AlarmOn	ifIndex, ifAdminStatus, ifOperStatus, ifName,	WAN	WAN	Critical	Wan Physical AlarmOn	Cable Problem on port $4	An E1/T1/serial cable was disconnected.

Name	Parameters (MIB variables)	Class	Msg Facility	Severity	Trap Name/ Mnemonic	Format	Description
	ifAlias, dsx1LineStatus						
wanPhysicalAlarmOff	ifIndex, ifAdminStatus, ifOperStatus, ifName, ifAlias, dsx1LineStatus	WAN	WAN	Notification	wanPhysicalAlarmOff	Cable Problem on port $4 was cleared	An E1/T1/serial cable was reconnected.
wanLocalAlarmOn	ifIndex, ifAdminStatus, ifOperStatus, ifName, ifAlias, dsx1LineStatus	WAN	WAN	Error	wanLocalAlarmOn	Local Alarm on interface $4	Local alarms, such as LOS.
wanLocalAlarmOff	ifIndex, ifAdminStatus, ifOperStatus, ifName, ifAlias, dsx1LineStatus	WAN	WAN	Notification	wanLocalAlarmOff	Local Alarm on interface $4 was cleared	Local alarms, such as LOS, was cleared.
wanRemoteAlarmOn	ifIndex, ifAdminStatus, ifOperStatus, ifName, ifAlias, dsx1LineStatus	WAN	WAN	Error	wanRemoteAlarmOn	Remote Alarm on interface $4	Remote alarms, such as AIS.
wanRemoteAlarmOff	ifIndex, ifAdminStatus, ifOperStatus,	WAN	WAN	Notification	wanRemoteAlarmOff	Remote Alarm on interface $4 was cleared	Remote alarms, such as AIS, was cleared.

Name	Parameters (MIB variables)	Class	Msg Facility	Severity	Trap Name/ Mnemonic	Format	Description
	ifName, ifAlias, dsx1LineStatus						
wanMinorAlarmOn	ifIndex, ifAdminStatus, ifOperStatus, ifName, ifAlias, dsx1LineStatus	WAN	WAN	Warning	wanMinorAlarmOn	Minor Alarm on interface $4	Low BER.
wanMinorAlarm Off	ifIndex, ifAdminStatus, ifOperStatus, ifName, ifAlias, dsx1LineStatus	WAN	WAN	Notification	wanMinorAlarmOff	Minor Alarm on interface $4 was cleared	Normal BER.
AvEntFanFlt	entPhysicalIndex, entPhysicalDescr, entPhySensorValue, avEntPhySensorLoWarning	AVAYA-ENTITY	TEMP		AvEntFan Flt	Fan $2 is Faulty	This trap reports a faulty fan.
AvEntFanOk	entPhysicalIndex, entPhysicalDescr, entPhySensor Value, avEntPhySensorLoWarning	AVAYA-ENTITY	TEMP	Notification	AvEntFanOk	Fan $2 is OK	This trap reports the return to function of a faulty fan.

Name	Parameters (MIB variables)	Class	Msg Facility	Severity	Trap Name/ Mnemonic	Format	Description
avEntAmbientTempFlt	entPhysical Index, entPhysical Descr, entPhySensor Value, avEntPhySensorHiWarning, entPhysical ParentRelPos	AVAYA-ENTITY	TEMP		avEnt AmbientTempFlt	Ambient Temperature fault ($3)	This trap reports that the ambient temperature in the device is not within the acceptable temperature range for the device.
avEntAmbientTempOk	entPhysical Index, entPhysical Descr, entPhySensor Value, avEntPhySensorHiWarning, entPhysical ParentRelPos	AVAYA-ENTITY	TEMP	Notification	avEnt AmbientTempOk	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
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

MIB File	MIB Module Supported by Branch Gateway
ENTITY-SENSOR-MIB.my	ENTITY-SENSOR-MIB
RSTP-MIB.my	RSTP-MIB
APPLIC-MIB.MY	APPLIC-MIB
DS1-MIB.my	DS1-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
DS0BUNDLE-MIB.my	DS0BUNDLE-MIB
RFC1406-MIB.my	RFC1406-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

Related topics:

MIB files in the Load.MIB file on page 619
MIB files in the RFC1315-MIB.my file on page 620
MIB files in the Q-BRIDGE-MIB.my file on page 621
MIB files in the ENTITY-MIB.my file on page 622
MIB files in the IP-FORWARD-MIB.my file on page 623
MIB files in the VRRP-MIB.my file on page 623
MIB files in the UTILIZATION-MANAGEMENT-MIB.my file on page 624
MIB files in the ENTITY-SENSOR-MIB.my file on page 625
MIB files in the RSTP-MIB.my file on page 625
MIB files in the APPLIC-MIB.my file on page 626
MIB files in the DS1-MIB.my file on page 626
MIB files in the PPP-IP-NCP-MIB.my file on page 628
MIB files in the RFC1213-MIB.my file on page 629
MIB files in the AVAYA-ENTITY-MIB.my file on page 632
MIB files in the Rnd-MIB.my file on page 632
MIB files in the XSWITCH-MIB.my file on page 633
MIB files in the CROUTE-MIB.my file on page 634
MIB files in the RS-232-MIB.my file on page 636
MIB files in the RIPv2-MIB.my file on page 638
MIB files in the IF-MIB.my file on page 638
MIB files in the DS0BUNDLE-MIB.my file on page 640
MIB files in the RFC1406-MIB.my file on page 640
MIB files in the DS0-MIB.my file on page 642
MIB files in the POLICY-MIB.my file on page 642
MIB files in the BRIDGE-MIB.my file on page 648
MIB files in the CONFIG-MIB.my file on page 649
MIB files in the G700-MG-MIB.my file on page 652
MIB files in the FRAME-RELAY-DTE-MIB.my file on page 656
MIB files in the IP-MIB.my file on page 657
MIB files in the Load12-MIB.my file on page 659
MIB files in the PPP-LCP-MIB.my file on page 660
MIB files in the WAN-MIB.my file on page 661
MIB files in the SNMPv2-MIB.my file on page 662
MIB files in the OSPF-MIB.my file on page 664
MIB files in the TUNNEL-MIB.my file on page 666

MIB files 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

Object	OID
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 files 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
frDlcmiIfIndex	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
frCircuitIfIndex	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

Object	OID
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
frErrIfIndex	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 files 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
dot1qVlanFdbId	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

Object	OID
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 files 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	1.3.6.1.2.1.47.1.1.1.1.1
entPhysicalDescr	1.3.6.1.2.1.47.1.1.1.1.2
entPhysicalVendorType	1.3.6.1.2.1.47.1.1.1.1.3
entPhysicalContainedIn	1.3.6.1.2.1.47.1.1.1.1.4
entPhysicalClass	1.3.6.1.2.1.47.1.1.1.1.5
entPhysicalParentRelPos	1.3.6.1.2.1.47.1.1.1.1.6
entPhysicalName	1.3.6.1.2.1.47.1.1.1.1.7
entPhysicalHardwareRev	1.3.6.1.2.1.47.1.1.1.1.8
entPhysicalFirmwareRev	1.3.6.1.2.1.47.1.1.1.1.9
entPhysicalSoftwareRev	1.3.6.1.2.1.47.1.1.1.1.10
entPhysicalSerialNum	1.3.6.1.2.1.47.1.1.1.1.11
entPhysicalMfgName	1.3.6.1.2.1.47.1.1.1.1.12
entPhysicalModelName	1.3.6.1.2.1.47.1.1.1.1.13
entPhysicalAlias	1.3.6.1.2.1.47.1.1.1.1.14
entPhysicalAssetID	1.3.6.1.2.1.47.1.1.1.1.15
entPhysicalIsFRU	1.3.6.1.2.1.47.1.1.1.1.16

MIB files 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 files 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
vrrpOperVrId	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

Object	OID
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 files 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 the Branch Gateway and their OIDs:

Object	OID
genCpuIndex	1.3.6.1.4.1.6889.2.1.11.1.1.1.1.1
genCpuUtilizationEnableMonitoring	1.3.6.1.4.1.6889.2.1.11.1.1.1.1.2
genCpuUtilizationEnableEventGeneration	1.3.6.1.4.1.6889.2.1.11.1.1.1.1.3
genCpuUtilizationHighThreshold	1.3.6.1.4.1.6889.2.1.11.1.1.1.1.4
genCpuAverageUtilization	1.3.6.1.4.1.6889.2.1.11.1.1.1.1.5
genCpuCurrentUtilization	1.3.6.1.4.1.6889.2.1.11.1.1.1.1.6
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

Object	OID
genMemUtilizationDynAllocMemMaxUsed	1.3.6.1.4.1.6889.2.1.11.1.2.3.2
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 files 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 files 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

Object	OID
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 files 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
lseIntPortGroupId	1.3.6.1.4.1.81.19.1.2.1.1.1
lseIntPortId	1.3.6.1.4.1.81.19.1.2.1.1.2
lseIntPortCAMLastChange	1.3.6.1.4.1.81.19.1.2.1.1.39
lseIntPortMACAddGroupId	1.3.6.1.4.1.81.19.1.2.2.1.1.1
lseIntPortMACAddPortId	1.3.6.1.4.1.81.19.1.2.2.1.1.2
lseIntPortMACAddLAId	1.3.6.1.4.1.81.19.1.2.2.1.1.3
lseIntPortMACAddList	1.3.6.1.4.1.81.19.1.2.2.1.1.4

MIB files 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 the Branch Gateway and their OIDs:

Object	OID
dsx1LineIndex	1.3.6.1.2.1.10.18.6.1.1
dsx1IfIndex	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

Object	OID
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
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

Object	OID
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 files 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 the Branch Gateway and their OIDs:

Object	OID
pppIpOperStatus	1.3.6.1.2.1.10.23.3.1.1.1
pppIpLocalToRemoteCompressionProtocol	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
pppIpRemoteMaxSlotId	1.3.6.1.2.1.10.23.3.1.1.4
pppIpLocalMaxSlotId	1.3.6.1.2.1.10.23.3.1.1.5
pppIpConfigAdminStatus	1.3.6.1.2.1.10.23.3.2.1.1
pppIpConfigCompression	1.3.6.1.2.1.10.23.3.2.1.2

MIB files 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
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
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
ifInUnknownProtos	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

Object	OID
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
ipRouteIfIndex	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
ipNetToMediaIfIndex	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

Object	OID
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
snmpEnableAuthenTraps	1.3.6.1.2.1.11.30

MIB files 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 files 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

Object	OID
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 files 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
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 files 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 the 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
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

Object	OID
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
relayVlIndex	1.3.6.1.4.1.81.31.1.6.1.1
relayVlPrimaryServerAddr	1.3.6.1.4.1.81.31.1.6.1.2
relayVlSeconderyServerAddr	1.3.6.1.4.1.81.31.1.6.1.3
relayVlStatus	1.3.6.1.4.1.81.31.1.6.1.4
relayVlRelayAddr	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
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

Object	OID
ipVRRPAdminStatus	1.3.6.1.4.1.81.31.1.14.1
iphcIfIndex	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
ospfXtndIfIpAddress	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 files 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

Object	OID
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 files 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
rip2IfStatAddress	1.3.6.1.2.1.23.2.1.1
rip2IfStatRcvBadPackets	1.3.6.1.2.1.23.2.1.2
rip2IfStatRcvBadRoutes	1.3.6.1.2.1.23.2.1.3
rip2IfStatSentUpdates	1.3.6.1.2.1.23.2.1.4
rip2IfStatStatus	1.3.6.1.2.1.23.2.1.5
rip2IfConfAddress	1.3.6.1.2.1.23.3.1.1
rip2IfConfDomain	1.3.6.1.2.1.23.3.1.2
rip2IfConfAuthType	1.3.6.1.2.1.23.3.1.3
rip2IfConfAuthKey	1.3.6.1.2.1.23.3.1.4
rip2IfConfSend	1.3.6.1.2.1.23.3.1.5
rip2IfConfReceive	1.3.6.1.2.1.23.3.1.6
rip2IfConfDefaultMetric	1.3.6.1.2.1.23.3.1.7
rip2IfConfStatus	1.3.6.1.2.1.23.3.1.8
rip2IfConfSrcAddress	1.3.6.1.2.1.23.3.1.9

MIB files 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

Object	OID
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
ifInUnknownProtos	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	1.3.6.1.2.1.31.1.1.1.1
ifInMulticastPkts	1.3.6.1.2.1.31.1.1.1.2
ifInBroadcastPkts	1.3.6.1.2.1.31.1.1.1.3
ifOutMulticastPkts	1.3.6.1.2.1.31.1.1.1.4
ifOutBroadcastPkts	1.3.6.1.2.1.31.1.1.1.5
ifHCInOctets	1.3.6.1.2.1.31.1.1.1.6
ifHCInUcastPkts	1.3.6.1.2.1.31.1.1.1.7
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	1.3.6.1.2.1.31.1.1.1.10
ifHCOutUcastPkts	1.3.6.1.2.1.31.1.1.1.11
ifHCOutMulticastPkts	1.3.6.1.2.1.31.1.1.1.12
ifHCOutBroadcastPkts	1.3.6.1.2.1.31.1.1.1.13

Object	OID
ifLinkUpDownTrapEnable	1.3.6.1.2.1.31.1.1.1.14
ifHighSpeed	1.3.6.1.2.1.31.1.1.1.15
ifPromiscuousMode	1.3.6.1.2.1.31.1.1.1.16
ifConnectorPresent	1.3.6.1.2.1.31.1.1.1.17
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 files 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 the Branch Gateway and their OIDs:

Object	OID
dsx0BundleIndex	1.3.6.1.2.1.10.82.3.1.1
dsx0BundleIfIndex	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 files 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 the Branch Gateway and their OIDs:

Object	OID
dsx1LineIndex	1.3.6.1.2.1.10.18.6.1.1
dsx1IfIndex	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

Object	OID
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
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

Object	OID
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 files 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
dsx0IdleCode	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 files 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 the 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

Object	OID
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
ipPolicyRuleApplicabilityStatus	1.3.6.1.4.1.81.36.2.1.16
ipPolicyRuleApplicabilityType	1.3.6.1.4.1.81.36.2.1.17

Object	OID
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

Object	OID
ipPolicyQueryListID	1.3.6.1.4.1.81.36.5.1.2
ipPolicyQuerySrcAddr	1.3.6.1.4.1.81.36.5.1.3
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

Object	OID
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
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

Object	OID
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	
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
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 files 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 the 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
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

Object	OID
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 files 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 the 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
chLntAgPermMngrId	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
chLntAgMngrTraps	1.3.6.1.4.1.81.7.9.3.2.1.3
chLntAgTrapsPermMngrId	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

Object	OID
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
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

Object	OID
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
genPortType	1.3.6.1.4.1.81.9.1.1.4
genPortDescr	1.3.6.1.4.1.81.9.1.1.5

Object	OID
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
softRedundancyId	1.3.6.1.4.1.81.11.1.1.1
softRedundancyName	1.3.6.1.4.1.81.11.1.1.2
softRedundancyGroupId1	1.3.6.1.4.1.81.11.1.1.3
softRedundancyPortId1	1.3.6.1.4.1.81.11.1.1.4
softRedundancyGroupId2	1.3.6.1.4.1.81.11.1.1.5
softRedundancyPortId2	1.3.6.1.4.1.81.11.1.1.6
softRedundancyStatus	1.3.6.1.4.1.81.11.1.1.7
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 files 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

Object	OID
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
cmgHardwareStatusMask	1.3.6.1.4.1.6889.2.9.1.1.10.13
cmgModuleSlot	1.3.6.1.4.1.6889.2.9.1.1.11.1.1.1
cmgModuleType	1.3.6.1.4.1.6889.2.9.1.1.11.1.1.2
cmgModuleDescription	1.3.6.1.4.1.6889.2.9.1.1.11.1.1.3
cmgModuleName	1.3.6.1.4.1.6889.2.9.1.1.11.1.1.4
cmgModuleSerialNumber	1.3.6.1.4.1.6889.2.9.1.1.11.1.1.5
cmgModuleHWVintage	1.3.6.1.4.1.6889.2.9.1.1.11.1.1.6
cmgModuleHWSuffix	1.3.6.1.4.1.6889.2.9.1.1.11.1.1.7
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	1.3.6.1.4.1.6889.2.9.1.1.11.1.1.11
cmgModuleReset	1.3.6.1.4.1.6889.2.9.1.1.11.1.1.12
cmgModuleNumberOfChannels	1.3.6.1.4.1.6889.2.9.1.1.11.1.1.13
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
cmgCurrentIpAddress	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

Object	OID
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
cmgDhcpControllerHosts	1.3.6.1.4.1.6889.2.9.1.3.7
cmgPrimarySearchTime	
cmgTotalSearchTime	
cmgTransitionPoint	
cmgVoipEngineUseDhcp	1.3.6.1.4.1.6889.2.9.1.4.1
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

Object	OID
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
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
cmgVoipStaticIpAddress	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
cmgTrapManagerAddress	
cmgTrapManagerControl	
cmgTrapManagerMask	

Object	OID
cmgTrapManagerRowStatus	
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

MIB files 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
frDlcmiIfIndex	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
frCircuitIfIndex	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

Object	OID
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
frCircuitLogicalIfIndex	1.3.6.1.2.1.10.32.2.1.20
frCircuitRowStatus	1.3.6.1.2.1.10.32.2.1.21
frErrIfIndex	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 files 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 the 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
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
ipNetToMediaIfIndex	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 files in the Load12-MIB.my file

The following table provides a list of the MIBs in the Load12-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
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

Object	OID
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 files 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 the Branch Gateway and their OIDs:

Object	OID
pppLinkStatusPhysicalIndex	1.3.6.1.2.1.10.23.1.1.1.1.1
pppLinkStatusBadAddresses	1.3.6.1.2.1.10.23.1.1.1.1.2
pppLinkStatusBadControls	1.3.6.1.2.1.10.23.1.1.1.1.3
pppLinkStatusPacketTooLongs	1.3.6.1.2.1.10.23.1.1.1.1.4
pppLinkStatusBadFCSs	1.3.6.1.2.1.10.23.1.1.1.1.5
pppLinkStatusLocalMRU	1.3.6.1.2.1.10.23.1.1.1.1.6
pppLinkStatusRemoteMRU	1.3.6.1.2.1.10.23.1.1.1.1.7
pppLinkStatusLocalToPeerACCMap	1.3.6.1.2.1.10.23.1.1.1.1.8
pppLinkStatusPeerToLocalACCMap	1.3.6.1.2.1.10.23.1.1.1.1.9
pppLinkStatusLocalToRemoteACCompression	1.3.6.1.2.1.10.23.1.1.1.1.12
pppLinkStatusRemoteToLocalACCompression	1.3.6.1.2.1.10.23.1.1.1.1.13
pppLinkStatusTransmitFcsSize	1.3.6.1.2.1.10.23.1.1.1.1.14
pppLinkStatusReceiveFcsSize	1.3.6.1.2.1.10.23.1.1.1.1.15
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 files 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

Object	OID
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
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
frStaticCircuitSubIfIndex	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
frSubIfDlcmiIndex	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 files 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

Object	OID
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
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 files 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
ospfAreaId	1.3.6.1.2.1.14.2.1.1
ospfAuthType	1.3.6.1.2.1.14.2.1.2
ospfImportAsExtern	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
ospfLsdbAreaId	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

Object	OID
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
ospfIfIpAddress	1.3.6.1.2.1.14.7.1.1
ospfAddressLessIf	1.3.6.1.2.1.14.7.1.2
ospfIfAreaId	1.3.6.1.2.1.14.7.1.3
ospfIfType	1.3.6.1.2.1.14.7.1.4
ospfIfAdminStat	1.3.6.1.2.1.14.7.1.5
ospfIfRtrPriority	1.3.6.1.2.1.14.7.1.6
ospfIfTransitDelay	1.3.6.1.2.1.14.7.1.7
ospfIfRetransInterval	1.3.6.1.2.1.14.7.1.8
ospfIfHelloInterval	1.3.6.1.2.1.14.7.1.9
ospfIfRtrDeadInterval	1.3.6.1.2.1.14.7.1.10
ospfIfPollInterval	1.3.6.1.2.1.14.7.1.11
ospfIfState	1.3.6.1.2.1.14.7.1.12
ospfIfDesignatedRouter	1.3.6.1.2.1.14.7.1.13
ospfIfBackupDesignatedRouter	1.3.6.1.2.1.14.7.1.14
ospfIfEvents	1.3.6.1.2.1.14.7.1.15
ospfIfAuthKey	1.3.6.1.2.1.14.7.1.16
ospfIfStatus	1.3.6.1.2.1.14.7.1.17
ospfIfMulticastForwarding	1.3.6.1.2.1.14.7.1.18
ospfIfDemand	1.3.6.1.2.1.14.7.1.19
ospfIfAuthType	1.3.6.1.2.1.14.7.1.20
ospfIfMetricIpAddress	1.3.6.1.2.1.14.8.1.1
ospfIfMetricAddressLessIf	1.3.6.1.2.1.14.8.1.2
ospfIfMetricTOS	1.3.6.1.2.1.14.8.1.3
ospfIfMetricValue	1.3.6.1.2.1.14.8.1.4
ospfIfMetricStatus	1.3.6.1.2.1.14.8.1.5
ospfNbrIpAddr	1.3.6.1.2.1.14.10.1.1

Object	OID
ospfNbrAddressLessIndex	1.3.6.1.2.1.14.10.1.2
ospfNbrRtrId	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 files 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
tunnelIfLocalAddress	1.3.6.1.2.1.10.131.1.1.1.1.1
tunnelIfRemoteAddress	1.3.6.1.2.1.10.131.1.1.1.1.2
tunnelIfEncapsMethod	1.3.6.1.2.1.10.131.1.1.1.1.3
tunnelIfTOS	1.3.6.1.2.1.10.131.1.1.1.1.4
tunnelIfHopLimit	1.3.6.1.2.1.10.131.1.1.1.1.5
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

Object	OID
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
ipTunnelIfIndex	1.3.6.1.4.1.81.31.8.1.1.1
ipTunnelIfChecksum	1.3.6.1.4.1.81.31.8.1.1.2
ipTunnelIfKey	1.3.6.1.4.1.81.31.8.1.1.3
ipTunnelIfkeyMode	1.3.6.1.4.1.81.31.8.1.1.4
ipTunnelIfAgingTimer	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
ipTunnelIfKeepaliveRate	1.3.6.1.4.1.81.31.8.1.1.8
ipTunnelIfKeepaliveRetries	1.3.6.1.4.1.81.31.8.1.1.9

Index

A

Access Code 2 158
Access control list 577
  CLI commands 577
Access control list rule specifications 554
Access control lists, see Policy 554
Access Security Gateway (ASG) authentication 39
Access through Services port 30
access-control-list 266
Accessing 31–33
  Avaya Aura Communication Manager 33
  MGC 33
  PIM 32
  via modem 31
Accessing the Branch Gateway 27
Active PMI 66
add nfas-interface 183, 187
add port 176, 187
Address Resolution Protocol table 456
Administration for the Avaya Branch Gateway G430s 13
analog telephones 111
analog-test 412, 415
Announcement files 319, 324
  CLI commands 324
  managing and transferring using SCP 319
area 468
arp 456–458
ARP table 456, 458
  changing an entry 458
  CLI commands 458
  description 456
  dynamic entries 456
  static entries 456
ARP table entries 457
arp timeout 458
ARS 157
ARS Dial Patterns 160
ARS dial patterns data 159
ARS FAC 158
ASG authentication 39
ASG commands 43
Associated Signaling 153
async-limit-string 246
async-reset-modem 246
Authenticating 39
  Service logins 39
authentication 547
Auto Fallback in SLS 102
Auto Route Selection (ARS) Access Code 1 157
automatic failover and failback 603
automatically activating ETR 298
autoneg 203
Autonomous System Boundary Router 467
Avaya Aura Communication Manager 33, 120
  accessing 33
  configuring for SLS 120
  functions 33
Avaya Aura™ Communication Manager 120
  configuring for SLS 120
Avaya courses 14
Avaya G250/G350/G450 Manager User Guide 13
Avaya G430 CLI Reference 13
Avaya G430 Manager User Guide 13
Avaya Mentor videos 15
Avaya Services 39
  authenticating logins with ASG 39
Avaya Site Administration 33
Avaya Voice Announcement Manager (VAM) 319

B

Backing up the Branch Gateway 91
  using the Branch Gateway USB port 91
backup config usb 91, 97
backup control for data and VoIP 521
backup delay 254, 255
backup interface 255, 259, 262, 266, 273
Backup interfaces 203, 254–256, 278, 432, 585
  CLI commands 255
  configuring 254
  defining through policy-based routing 585
  dynamic bandwidth reporting 278
  GRE tunnels as 432
  limitations 254
  modem dial backup, Modem dial backup 256
  modem dial backup, see Modem dial backup 256
  overview 203
backup mechanism configuration 290
backup peer mechanism 526
Backup service 297
bandwidth 467, 468
Bandwidth 232, 278, 467

dynamic reporting 278
manual adjustment 467
reducing via header compression 232
used to calculate Cost 467
Basic 17
LAN deployment 17
Bit Rate 148
bootfile 452
BOOTP 443
description 443
BOOTP relay 442
BOOTstrap Protocol 443
see BOOTP 443
BPDU 336, 337
Branch Gateway access 27
Branch Office 1 configuration 514
Branch Office 2 configuration 517
bri 173, 187
Bridge Protocol Data Units 336
see BPDU 336
Bridges 336, 337
direct handshaking 337
loops 336
Broadcast relay 454, 455
CLI commands 455
description 454
directed broadcast forwarding 454
NetBIOS rebroadcast 455

C

CAC-BL 278
Call admission control 278
Dynamic CAC 278
Call admission control, see Dynamic CAC 278
call types 185
Called Len 162
Called Number 161
cancel 413, 415
capture buffer mode 391
capture buffer-mode 397
capture buffer-size 397
capture filter-group 390, 392
capture interface 382, 391
capture max-frame-size 391
capture start 392
capture stop 393
captured packets 393
CAS Remote Hold/Answer Hold-Unhold Access Code 158
CDR, SLS information 116
Challenge Handshake Authentication Protocol 246
Changing crypto list parameters 495
Channel Numbering 149
CHAP 246
Class values in SLS station context 168
class-identifier 449, 452
clear arp-cache 458
clear attendant 187
clear bri 173, 187
clear capture-buffer 391
clear counter 407
clear counters 407
clear crypto isakmp 500, 547
clear crypto sa 547
clear crypto sa all 500
clear crypto sa counters 499, 547
clear dial-pattern 184, 187
clear ds1 ..... 169, 187
clear dynamic-trap-manager 312
clear extension 187
clear fac 187
clear fragment 476
clear incoming-routing 187
clear ip dhcp-client statistics 207, 208
clear ip dhcp-server binding 449, 452
clear ip dhcp-server statistics 452
clear ip domain statistics 79
clear ip route 431
clear ip rtp header-compression 234, 238
clear ip tcp header-compression 234, 237, 238
clear logging file 221, 229
clear logging server 218
clear mgc list 71, 73
clear port mirror 335
clear port static-vlan 330
clear profile 413, 415
clear radius authentication server 49
clear rmon statistics 345
clear sig-group 183, 187
clear slot-config 187
clear ssh-client known-hosts 48
clear station 187
clear survivable-config 187
clear sync interface 602–604
clear tac 187
clear tcp syn-cookies 54
clear tcp syn-cookies counters 55
clear trunk-group 176, 187
clear vlan 327, 330
CLI 23, 28–31, 81, 84, 85, 98, 100
accessing from local network 30
accessing from remote location 31

accessing with modem 31
contexts 28
contexts example 29
listing files 100
managing configuration files 98
managing firmware banks 84
online help 29
upgrading firmware using FTP/TFTP 85
using to configure the system 23
viewing device status 81
CLI access 27
CLI access using a PC device 30
CLI documentation 13
CLI output per RTP session 359
client identifier 447
client identifiers 452
CNA test plugs 401–403, 405, 407
CLI commands 407
configuration example 405
configuring for registration 403
functionality 402
overview 401
CNA tests 403
cna-testplug 403, 407
cna-testplug-service 403, 407
Codec 238
Codecs in SLS 159
command sequence 265
Commands 43, 52, 71, 138, 162, 233, 236, 246, 253, 286, 306, 352, 355, 357, 382, 389, 393, 395, 397, 423, 437, 468, 497, 569, 590
bri 162
capture filter-group 397
capture interface 397
capture ipsec 397
capture max-frame-size 397
capture start 397
capture stop 397
capture-service 382, 397
clear capture-buffer 397
composite-operation, packet sniffing 397
cookie, capture list 397
copy auth-file ftp 43
copy auth-file scp 43
copy auth-file tftp 43
copy auth-file usb 43
copy capture-file ftp 395, 397
copy capture-file scp 395, 397
copy capture-file tftp 395, 397
copy capture-file usb 395, 397
copy ftp auth-file 43
copy running-config startup-config 52
copy scp auth-file 43
copy tftp auth-file 43
copy usb auth-file 43
crypto ipsec df-bit 497
destination-ip, packet sniffing 397
dial-pattern 162
ds1 162
dscp, packet sniffing 397
dscp, policy lists 569
erase auth-file 43
fragment, packet sniffing 389, 397
icmp 397
incoming-routing 162
interface console 423
interface dialer 423
interface fastethernet, interface configuration 423
interface loopback 423
interface serial, interface configuration 423
interface tunnel 423
interface usb-modem 423
interface vlan 423
ip admin-state 423
ip broadcast-address 423
ip capture-list 397
ip next-hop-list 590
ip rtp compression-connections 233
ip rtp header-compression 233, 236
ip rtp max-period 233
ip rtp max-time 233
ip rtp non-tcp-mode 233
ip rtp port-range 233
ip tcp compression-connections 233, 236
ip tcp header-compression 233, 236
ip-protocol, packet sniffing 397
ip-rule, packet sniffing 397
key config-key password-encryption 52
login authentication local-craft-password 43
login authentication lockout 43
login authentication response-time 43
login authentication services-logins 43
name, packet sniffing 397
owner, packet sniffing 397
ping 253
ppp authentication, ASG authentication 43
rtp-stat qos-trap-rate-limit 355
set logging session, object tracking 286
set mgc list 71
set sls 138
show auth-file info 43
show auth-file status 43

show capture 393, 397
show capture-buffer hex 393, 397
show controllers 253
show frame-relay fragment 253
show frame-relay lmi 253
show frame-relay map 253
show frame-relay pvc 253
show frame-relay traffic 253
show interfaces, WAN configuration 253
show ip capture-list 397
show ip interface 253
show ip interface brief 423
show login authentication 43
show map-class frame-relay 253
show next-hop 590
show rtp-stat config 352
show rtp-stat detailed 357
show rtp-stat sessions 357
show running-config 253
show startup-config 253
show traffic-shape 253
show upload auth-file status 43
show upload status 397
sig-group 162
sls 162
snmp-server view 306
source-ip, packet sniffing 397
station 162
tcp destination-port 397
tcp source-port 397
trunk-group 162
tunnel path-mtu-discovery 437
udp destination-port 397
udp source-port 397
communication methods for agents and managers on SNMP 302
composite operations 570
Composite operations 570, 572, 573
adding to IP rule 573
configuring 572
deleting from IP rule 573
example 573
pre-configured for access control lists 570
composite-operation 573
IP rule configuration 573
composite-operation, access control list 577
composite-operation, DSCP table 574, 579
composite-operation, MSS configuration 59
composite-operation, QoS list 572, 579
Computer, connecting to fixed router port 199
conference call 377
Configuration 21–24, 63, 64, 69, 98, 202, 205, 211, 231, 232, 245, 253, 311, 325
defining an interface 63
DHCP client 205
dynamic trap manager 311
header compression 232
installation and setup 21
LLDP 211
managing configuration files 98
MGC list 69
modem 245
primary management interface 64
RTCP 231
RTP 231
running configuration 24
saving configuration changes 24
startup 253
startup configuration 24
switching 325
using GUI applications 22, 23
using the CLI 23
WAN ethernet port 202
Configuration file 99
CLI commands 99
Configured PMI 66
Connect 149
Console port 266
associating with Dialer interface 266
contact closure 115
Contact closure 114, 315–317
activating when access code dialed 316
closure modes 316
configuring software 316
deactivating manually 316
displaying status 317
overview 315
relay control methods 315
setting manually 316
setting pulse duration 316
using in SLS mode 114
Contact Closure Close Code 157
Contact closure configuration 318
CLI commands 318
Contact Closure Open Code 157
Contact Closure Pulse Code 157
Contexts 28
Contexts example 29
Continuous channel in VPN 509
continuous-channel 486, 490, 509, 547
control-port 403, 407
cookie, access control list 577

cookie, capture list 383
cookie, policy list 558
cookie, QoS list 579
copy announcement-file ftp 88, 89, 319, 320, 324
copy announcement-file scp 88, 89, 319, 324
copy announcement-file usb 87, 89, 321, 324
copy auth-file ftp 40, 88, 89
copy auth-file scp 40, 88, 89
copy auth-file tftp 40
copy auth-file usb 40, 87, 89
copy capture-file ftp 88, 89
copy capture-file scp 88, 89
copy capture-file usb 87, 89
copy cdr-file ftp 88, 89
copy cdr-file scp 88, 89
copy cdr-file usb 87, 89
copy dhcp-binding ftp 88, 89
copy dhcp-binding scp 88, 89
copy dhcp-binding usb 87, 89
copy file usb 87
copy ftp announcement-file 320, 324
copy ftp auth-file 40
copy ftp EW_archive 89
copy ftp module 85, 89
copy ftp startup-config 99
copy ftp sw_imageA 93, 97
copy ftp SW_imageA 89
copy ftp SW_imageB 89
copy license-file usb 87, 89
copy phone-script usb 87, 89
copy running-config ftp 99
copy running-config scp 99
copy running-config startup-config 54
copy running-config tftp 99
copy scp announcement-file 319, 320, 324
copy scp auth-file 40
copy scp startup-config 99
copy startup-config ftp 99
copy startup-config scp 99
copy startup-config tftp 99
copy startup-config usb 87, 89, 99
copy syslog-file ftp 220, 229
copy syslog-file scp 220, 229
copy syslog-file tftp 229
copy syslog-file usb 87, 89, 220, 229
copy tftp auth-file 40
copy tftp EW_archive 89
copy tftp module 89
copy tftp startup-config 99
copy tftp sw_imageA 93, 97
copy tftp SW_imageA 89
copy tftp SW_imageB 89
copy usb 86
copy usb announcement-file 89, 321, 324
copy usb auth-file 40, 89
copy usb EW_archive 89
copy usb modules 89
copy usb phone-image 89
copy usb phone-script 89
copy usb startup-config 89, 99
copy usb SW_image 89
cos 572, 579
Cost 467
Country Protocol 150
crypto ipsec df-bit 547
crypto ipsec minimal pmtu 497
crypto ipsec minimal-pmtu 547
crypto ipsec nat-transparency udp-encapsulation 497, 547
crypto ipsec transform-set 485, 533, 539, 547
crypto isakmp invalid-spi-recovery 496, 547
crypto isakmp nat keepalive 497, 547
crypto isakmp peer 486, 533, 539, 547
crypto isakmp peer-group 489, 539, 547
crypto isakmp policy 533, 539, 547
crypto isakmp suggest-key 547
crypto ispec nat-transparency udp-encapsulation 547
crypto ispec transform-set 547
crypto key generate 46, 47
crypto list 479
  overview 479
Crypto list 492, 494
  configuring 492
  deactivating 494
crypto list parameters 495
  changing 495
crypto map 490, 533, 539, 547
Crypto map 479, 490
  configuring 490
  overview 479
crypto-group 497
cyrpto isakmp policy 483

D

data and VoIP control backup 521
Date Format on Terminals 159
DCP stations data 141
DCP telephones 111
DCP/ANALOG Bearer Capability 151
decrypted IPSec VPN packets 393
Default gateway 67

defining ... 67
default sink severity levels ... 226
default-metric ... 464, 468, 471
default-router ... 449
default-routers ... 452
defining other interfaces ... 23
Del ... 135, 162
AAR and ARS Digit Conversion Table ... 135
Incoming Call Handling Treatment ... 162
DeMilitarized Zone ... 421
see DMZ ... 421
Denial of Service reporting ... 55
Deployments ... 17–19
basic ... 17
port redundancy ... 17, 18
RSTP ... 18
RSTP and switch redundancy ... 19
switch redundancy ... 18
description, crypto list rule ... 547
description, crypto map ... 547
description, DNS servers list ... 79
description, ISAKMP peer ... 486, 547
description, ISAKMP peer-group ... 547
description, ISAKMP policy ... 483, 547
description, object tracker ... 293
description, policy rule ... 565
destination-ip ... 386
packet sniffing ... 386
destination-ip, access control list ... 577
destination-ip, crypto list rule ... 492, 547
destination-ip, MSS configuration ... 59
destination-ip, policy list ... 566
destination-ip, QoS list ... 579
Device status ... 81, 82
CLI commands ... 82
viewing ... 81
DHCP ... 443
BOOTP relay ... 443
description ... 443
DHCP and BOOTP relay ... 444
CLI commands ... 444
DHCP client ... 204, 205, 207, 208
applications ... 205
CLI commands ... 208
CLI logging, enabling ... 208
CLI logging, setting logging session conditions ... 208
CLI logging, viewing ... 208
configuring ... 205
determining DHCP option requests ... 205
displaying configuration ... 207
displaying parameters ... 205
enabling ... 205
interface fastethernet, DHCP client ... 205
ip address dhcp ... 205
ip dhcp client client-id ... 205
ip dhcp client hostname ... 205
ip dhcp client lease ... 205
ip dhcp client request ... 205
ip dhcp client route track ... 205
lease, releasing ... 207
lease, renewing ... 207
maintaining ... 207
overview ... 204
setting the client identifier ... 205
setting the client lease ... 205
setting the hostname ... 205
show ip dhcp-client ... 205
DHCP Client configuration ... 508
DHCP options ... 448
DHCP relay ... 442
DHCP server ... 445, 446, 448–450, 452
CLI commands ... 452
configuration examples ... 450
configuring DHCP options ... 448
configuring vendor-specific options ... 449
overview ... 445
typical application ... 446
Diagnosing ... 343
and monitoring the network ... 343
Dial On Demand Routing (DDR) ... 256
dial-pattern ... 184, 187
Dialed String ... 135, 161
AAR and ARS Digit Analysis Table ... 135, 161
AAR and ARS Digit Conversion Table ... 135, 161
dialer interface ... 268
Dialer interface ... 256, 259, 262, 266, 268, 273, 424
activating with object tracking ... 262
as backup for Loopback interface ... 256
as backup for WAN interface ... 256
assigning access control list to ... 266
assigning to Console port ... 266
authentication method ... 259
CHAP authentication ... 259
CLI commands ... 273
configuring ... 259
configuring as backup ... 259
configuring backup routing ... 259
dynamic IP ... 262
dynamic routing ... 256
giving priority to VoIP ... 256
logging ... 268
setting IP address ... 259

static routing 256
unnumbered IP 256, 262, 424
verifying connection 259
Dialer Messages 269
dialer modem-interface 266, 273
dialer order 259, 273
dialer persistent 259, 273
dialer persistent delay 259, 266, 273
dialer persistent initial delay 259, 266, 273
dialer persistent max-attempts 259, 273
dialer persistent re-enable 259, 273
dialer string 259, 266, 273
Dialer strings 259
dialer wait-for-ipcp 259, 273
dir 89, 97, 100
Directed broadcast forwarding 454
Directory Number 155
Discard routes 431
disconnect ssh 46, 47
displaying DHCP server information 451
Distribution access lists 462
distribution list 463
distribution-list 464
DMZ 421
DNS resolver 74–76, 78, 79
CLI commands 79
configuration example 78
features 74
maintaining 79
overview 74
typical application 75
when not necessary 76
DNS servers 205, 250
requesting list of DNS servers during a PPP/IPCP session 250
requesting list of DNS servers from a DHCP server 205
dns-server 449, 452
Documentation 13
Administration for the Avaya Branch Gateway G430s 13
Avaya G430 CLI Reference 13
Avaya G430 Manager User Guide 13
Installing and Upgrading the Avaya Branch Gateway G430 13
Maintenance Alarms for Avaya Aura Communication Manager, Branch Gateways and Servers 13
Maintenance Commands for Avaya Aura Communication Manager, Branch Gateways and Servers 13
Maintenance Procedures for Avaya Aura Communication Manager, Branch Gateways and Servers 13
Quick Start for Hardware Installation for the Avaya Branch Gateway G430 13
domain-name 449, 452
lease 449
DoS reporting 55
dos-classification 59
downloading announcement files 320
ds1 187
DSA encryption 45
dscp 385
packet sniffing 385
DSCP 281, 490, 569, 584
as access control list rule criteria 569
as policy-based routing rule criteria 569
as QoS list rule criteria 569
in RTR probes 281
in VPN packets 490
routing based on 584
DSCP table 573
Policy 573
DSCP table, see Policy 573
dscp-table 574, 579
dscp, access control list 577
dscp, object tracking 281, 293
dscp, QoS list 572, 579
duplex 203
Dynamic CAC 256, 262, 278, 279
and modem dial backup 256, 262
CLI commands 279
description 278
Dynamic CAC tasks 278
Dynamic Host Configuration Protocol 443
see DHCP 443
Dynamic IP 262, 506, 507
configuring 507
Dialer interface 262
overview 506
dynamic local peer IP 508
dynamic MTU discovery 437
Dynamic routes 470
redistributing 470
Dynamic trap manager 311, 312
CLI commands 312
configuring 311
dynamic trap manager parameters 312
dynamic-cac 279

E

E1/T1 lines 249
  connecting to WAN media module 249
Echo cancellation 408, 409
  CLI commands 409
  overview 408
ECMP 467
Emergency Transfer Relay 297
  see ETR 297
encapsulation pppoe 250, 251
Encrypting gateway secrets 51
encryption 483, 547
end-ip-addr 447, 452
Endpt Init 155
erase announcement-file 321, 322, 324
erase auth-file 40
Ethernet ports 199, 200, 202, 331
  CLI commands 200
  configuring switch port 200
  connecting devices to 199
  list of 199
  port redundancy 331
  WAN Ethernet port 202
  WAN Ethernet port, see WAN Ethernet port 202
Ethernet ports on the router 199
ETR 297, 298
  CLI commands 298
  deactivating 298
  description 297
  LED 297
  manual activation 297
  setting state 297
  trunk-to-port latchings 297
ETR automatic activation 298
exit 65
Expansion Module 132

F

FAC data 156
fail-retries 281, 293
failback 603
failover 603
Fair VoIP queue 240
fair-queue-limit 241
fair-voip-queue 241
Fast Ethernet interface 249
  configuring PPPoE 249
Fast Ethernet port 202, 277, 421
  configuring interface 202
  firewall connected 421
  VPN connected 421
FastEthernet interface 274, 278
  checking status 274
  dynamic bandwidth reporting 278
  ICMP keepalive 274
FastEthernet Interface 421
  described 421
File transfer 83
  FTP or TFTP 83
File transfer, see FTP or TFTP 83
fingerprint 403, 407
FIPS 429
  adding next hops 429
  next hops static routes 429
Firewall 421
Firmware 25, 83–86, 89
  CLI commands 89
  firmware bank defaults 84
  firmware banks 25
  load with ASB button 85
  managing firmware banks 84
  redundancy 84
  upgrade overview 83
  upgrading using FTP/TFTP 85
  upgrading using USB mass storage device 86
  version control 25
firmware versions in the banks displays 84
Fixed analog trunk port 297
fragment chain 476
fragment size 476
fragment timeout 476
fragment, access control list 569, 577
fragment, QoS list 579
Fragmentation 437, 475, 476
  CLI commands 476
  description 475
  GRE tunneling 437
Frame relay 253
  displaying configuration 253
Frame relay encapsulation 255, 422
  down status 255
  supported on Serial interfaces 422
Frame relay traffic shaping 253
  displaying configuration 253
frequency 281, 293
FTP 83
FTP/TFTP used for upgrades 85

G

General context 28

General context example 29
Generic Routing Encapsulation 432
GRE tunneling 432
Generic Routing Encapsulation, see GRE tunneling 432
Gigabit Ethernet port 331
port redundancy 331
global parameters 495
GRE tunneling 278, 421, 432, 433, 436–438, 441, 590
applications 432
as next hop 590
checking tunnel status 436, 438
CLI commands 441
compared to VPN 432
dynamic bandwidth reporting 278
dynamic MTU discovery 437
optional features 436
overview 421, 432
preventing recursive routing 433
routing packets to tunnel 433
group 483, 547
GUI tools, configuring the system with 22, 23

H

hash 483, 547
Header compression 232–234, 236–238
clearing rtp header compression statistics 238
clearing tcp header compression statistics 238
decompression 232
IPCH method - RTP and TCP header compression, CLI commands 234
IPCH method - RTP and TCP header compression, disabling 233
IPCH method - RTP and TCP header compression, enabling 233
IPCH method - RTP and TCP header compression, overview 232
IPHC method - RTP and TCP header compression, configuring UDP ports range 233
methods 232
overview 232
show ip rtp header-compression 238
show ip tcp header-compression 238
showing rtp header compression statistics 238
showing tcp header compression statistics 238
supported methods per interface type 232
transmission rate 232
Van Jacobson Method - TCP header compression, CLI commands 237
Van Jacobson Method - TCP header compression, configuring 236
Van Jacobson Method - TCP header compression, disabling 236
Van Jacobson Method - TCP header compression, enabling 236
Van Jacobson Method - TCP header compression, overview 232
help 29
Help 29
CLI 29
commands 29
High Preference static routes 429
hostname 46, 47
hub-and-spoke with VPN 521

I

icc-vlan 328, 330
ICC-VLAN 328
configuring 328
Configuring 328
icc-vlan 328
ICC-VLAN 328
icmp 388, 568, 577, 579
ICMP errors 459, 460
CLI commands 460
ICMP keepalive 274, 277, 583
and policy-based routing 583
CLI commands 277
ICMP keepalive feature, enabling 276
IGAR 256, 262, 278
IKE 477
phase 1 477
phase 2 477
incoming call handling data 161
incoming-routing 185, 187
Ingress Access Control List 583
Ingress QoS List 583
initiate mode 486, 547
Insert 162
Incoming Call Handling Treatment 162
Installing and Upgrading the Avaya Branch Gateway G430 13
Integrated analog testing 409–415
CLI commands 415
displaying corrections 415
displaying test results 414
healing trunks 414
overview 409
profiles, clearing 413
profiles, configuring 412
profiles, displaying 413

test cancelling ... 413
test launching ... 413
test lines ... 411
types of tests ... 410
Inter-Gateway Alternate Routing ... 278
IGAR ... 278
Inter-Gateway Alternate Routing, see IGAR ... 278
interface ... 63, 65, 273
Interface ... 150, 151
Interface configuration ... 423
CLI commands ... 423
interface console ... 266
interface dialer ... 259, 266, 273
interface fastethernet, DHCP and BOOTP relay ... 444
interface fastethernet, DHCP client ... 208
interface fastethernet, PPPoE ... 250
interface fastethernet, WAN Ethernet port ... 202, 203
interface Loopback ... 266
Interface status ... 401
CLI commands ... 401
interface tunnel ... 438, 441
interface usb-modem ... 245, 246
interface vlan ... 326, 330
Interfaces ... 63, 203, 253, 278, 400, 420–422, 428, 467, 583, 585
adjusting bandwidth ... 467
applying PBR lists ... 585
assigning Cost ... 467
assigning IP addresses ... 63
backup ... 203
configuration ... 420
configuration examples ... 422
defining ... 63
disabling ... 428
displaying information ... 253
displaying status ... 400
dynamic bandwidth reporting ... 278
fastethernet ... 421
GRE tunnel, GRE tunneling ... 421
GRE tunnel, see GRE tunneling ... 421
IP ... 422
IP, see IP interfaces ... 422
Layer 2 ... 421, 428
logical ... 422
Loopback ... 421, 583, 585
physical ... 421
Serial ... 422
setting load calculation intervals ... 63
switching ... 421, 422
testing configuration ... 253
USP WAN ... 421
virtual ... 421
WAN ... 421
Internet Key Exchange (IKE) ... 477
invalid SPI recovery ... 496
ip access group ... 561
ip access-control-list ... 59, 495, 557, 577
ip access-group ... 266, 508, 577
IP address ... 22, 205, 250, 422, 456
assigning to USB port ... 22
defining ... 422
obtaining via DHCP ... 205
obtaining via PPP/IPCP negotiation ... 250
storing in ARP table ... 456
ip address dhcp ... 76, 208
ip address negotiated ... 250, 251, 259, 273, 507
ip address, dialer interface ... 259, 273
ip address, interface configuration ... 63, 422
ip address, PPPoE ... 250, 251
ip address, USB port ... 246
ip bootp-dhcp network ... 444
ip bootp-dhcp relay ... 444
ip bootp-dhcp server ... 444
ip capture-list ... 383
ip crypto list ... 492
ip crypto-group ... 494, 509, 547
ip crypto-list ... 547
ip default-gateway ... 67, 273, 431
ip default-gateway dialer ... 259
ip dhcp activate pool ... 447, 452
ip dhcp client client-id ... 208
ip dhcp client hostname ... 208
ip dhcp client lease ... 208
ip dhcp client request ... 208, 533
ip dhcp client route track ... 208
ip dhcp ping packets ... 452
ip dhcp ping timeout ... 452
ip dhcp pool ... 447
ip dhcp pools ... 452
ip dhcp-server ... 447, 452
ip directed-broadcast ... 454, 455
ip distribution access-default-action ... 463, 464
ip distribution access-list ... 463, 464
ip distribution access-list-cookie ... 464
ip distribution access-list-copy ... 464
ip distribution access-list-name ... 464
ip distribution access-list-owner ... 464
ip domain list ... 76, 79
ip domain lookup ... 76, 79
ip domain name-server-list ... 76, 79
ip domain retry ... 76, 79
ip domain timeout ... 76, 79

ip icmp-errors 460
IP interfaces 422
ip max-arp-entries 458
ip netbios-rebroadcast 455
ip netmask-format 431
ip next-hop-list 585
ip ospf authentication 468
ip ospf authentication-key 468
ip ospf cost 467, 468
ip ospf dead-interval 468
ip ospf hello-interval 468
ip ospf message-digest-key 468
ip ospf network point-to-multipoint 468
ip ospf priority 468
ip ospf router-id 468
ip pbr-group 585
ip pbr-list 585, 592
ip peer address 246
ip policy-list-copy 494, 557, 558, 577, 579
ip proxy-arp 459
ip qos-group 561, 562, 579
ip qos-list 557, 579
ip redirects 431
ip rip authentications key 464
ip rip authentications mode 464
ip rip default-route-mode 464
ip rip poison-reverse 462, 464
ip rip rip-version 464
ip rip send-receive-mode 464
ip rip split-horizon 462, 464
ip route 429–431
ip routing 419, 420, 431
ip rtp compression-connections 234
ip rtp header-compression 234
ip rtp max-period 234
ip rtp max-time 234
ip rtp non-tcp-mode 234
ip rtp port-range 234
ip rule 565
IP Security 477
  VPN 477
IP Security, see VPN 477
ip show rule 565
ip simulate 576, 577, 579
ip ssh 46, 47
IP stations data 142
ip tcp compression-connections 234, 237
ip tcp header-compression 237
IP telephones 111
ip telnet 50, 51
ip telnet-client 50, 51
ip telnet-services 51
ip unnumbered 259, 266, 425
IP unnumbered interface configuration 426
  CLI commands 426
ip vrrp 474
ip vrrp address 474
ip vrrp auth-key 474
ip vrrp override addr owner 474
ip vrrp preempt 474
ip vrrp primary 474
ip vrrp priority 474
ip vrrp timer 474
ip-fragments-in 563, 577
ip-option-in 563, 577
ip-protocol 386
  packet sniffing 386
ip-protocol, access control list 577
ip-protocol, MSS configuration 59
ip-protocol, policy list 566
ip-protocol, QoS list 579
ip-rule, access control list 577
ip-rule, crypto list 492
ip-rule, MSS configuration 59
ip-rule, packet sniffing 382, 383
ip-rule, policy based routing 585, 589
ip-rule, QoS list 579
ip-rule, VPN 547
IPSec VPN 477
IPSec VPN configuration display 499
IPSec VPN packets decryption 393
IPSec VPN, see VPN 477
ISAKMP 483, 486, 489
  peer-group configuration 489
  policies 483
  VPN peer configuration 486
isakmp policy 486
isakmp-policy 547
ITN-C7 Long Timers 152

K

keepalive 250, 251, 436, 438, 441, 486, 547
keepalive feature 436
keepalive ICMP 274
  ICMP keepalive 274
keepalive ICMP, see ICMP keepalive 274
keepalive-icmp 276, 277
keepalive-icmp failure-retries 276, 277
keepalive-icmp interval 276, 277
keepalive-icmp source-address 276, 277
keepalive-icmp success-retries 276, 277
keepalive-icmp timeout 276, 277

keepalive-track 203, 250, 251, 486, 547
configuring in VPN 486
configuring on PPPoE interface 250
Keepalive, GRE tunnel 436
key config-key password-encryption 97

L

LAN 421
launch 413, 415
Layer 1 Stable 155
Layer 2 interfaces 428
Layer 2 logical interfaces 422
Layer 2 virtual interfaces 421
lease 447, 452
LEDs, ETR 297
legal notice 2
lifetime 483, 547
Link Layer Discovery Protocol 209
LLDP 209
Link Layer Discovery Protocol, see LLDP 209
Link-state algorithm 466
List rule specification for access control 554
Listing files 100
LLDP 209–212
802.1 TLVs (optional) 210
CLI commands 212
configuration 211
enabling 211
mandatory TLVs 210
optional TLVs 210
overview 209
setting additional TLVs 211
setting port status 211
supported ports 212
supported TLVs 210
verify advertisements 211
Load balancing 467, 472
ECMP 467
VRRP 472
load sharing topologies 528
load-interval 63
local calls between IP and analog telephones 374
local-address 492, 547
Log file 220
see Logging 220
log file messages 221
Logging 215, 216, 218–226, 228, 229, 268, 286, 500
CLI commands 229
configuring and enabling the log file 220
configuring session log 223
configuring Syslog server 216
copying the Syslog file 220
default severity levels 225
defining filters 224
deleting log file 221
deleting Syslog server 218
Dialer interface 268
disabling log file 221
disabling session log 223
disabling Syslog server 216
displaying log file contents 221
displaying Syslog server status 219
enabling session log 223
enabling Syslog server 216
filtering by application 226
introduction 215
limiting Syslog access 216
log file 215, 216
log file example 228
log file filter contents 225
log file message format 222
modem dial backup 268
object trackers 286
object tracking 286
overview 215
RTR 286
saving settings 215
session log 215, 216, 223
session log example 228
session log message format 224
setting filters 225
sinks 215, 216
specifying Syslog output facility 216
Syslog default settings 219
Syslog server 215, 216
Syslog server example 228
Syslog server message format 219
VPN 500
Logging session 223
Logging 223
Logging session, see Logging 223
Logical interfaces 422
login authentication 41
login authentication inactivity-period 36, 38
login authentication local-craft-password 41
login authentication lockout 36, 38, 41
login authentication min-password-digit-chars 36, 38
login authentication min-password-length 36, 38
login authentication min-password-lower-chars 36, 38
login authentication min-password-special-chars 36, 38
login authentication min-password-upper-chars 36, 38
login authentication password-expire 37, 38

login authentication response-time 41
Loopback interface 256, 421, 583, 585
Loops 336, 433, 462
defined 336
preventing in GRE tunneling 433
preventing in RIP 462
Low preference static routes 429

M

MAC addresses, storing in ARP table 456
Managed Security Services 55
MSS 55
Managed Security Services, see MSS 55
Manuals 13
Administration for the Avaya Branch Gateway G430s 13
Administration for the Avaya Branch Gateway G450s 13
Avaya G430 CLI Reference 13
Avaya G430 Manager User Guide 13
Installing and Upgrading the Avaya Branch Gateway G430 13
Maintenance Alarms for Avaya Aura Communication Manager, Branch Gateways and Servers 13
Maintenance Commands for Avaya Aura Communication Manager, Branch Gateways and Servers 13
Maintenance Procedures for Avaya Aura Communication Manager, Branch Gateways and Servers 13
Quick Start for Hardware Installation for the Avaya Branch Gateway G430 13
Master Configuration Key 52, 55
CLI commands 55
configuring 52
MCG 73
CLI commands 73
MCK (Master Configuration Key) 51
Media Gateway Controller (MGC) 22
Media modules 97, 249, 421
adding, using a USB mass-storage device 97
MM340 ..... 249, 421
MM342 ..... 249, 421
upgrading, using a USB mass-storage device 97
WAN 249
mesh VPN topology configuration 511
Metrics 471
MGC 33, 67, 69–73, 256, 278
accessing 33
accessing the registered MGC 72
changing the list 71
checking connectivity with 256
clearing the list 71
displaying the list 70
monitoring the ICC 73
monitoring the Survivable Remote Server 73
overview 67
reporting bandwidth to 278
running Avaya Aura Communication Manager 33
setting reset times 71
setting the list 69
MGC (Media Gateway Controller) 68
supported servers 68
MGC list 107
SLS entry 107
MIB files 616
Min 135, 160
AAR and ARS Digit Analysis Table 135, 160
AAR and ARS Digit Conversion Table 135, 160
MM340 media module 421
E1/T1 WAN interface 421
MM342 media module 421
USP WAN interface 421
mode 485, 547
Modem 31, 245, 256
configuring 245
connecting to USB port 31
dial backup, Modem dial backup 256
dial backup, see Modem dial backup 256
USB 245
Modem dial backup 256, 258, 259, 262, 264, 268
activating with object tracking 262
and dynamic CAC 256, 262
as backup interface 256
authentication method 259
bandwidth available for 256
CHAP authentication 259
configuration example 264
configuring backup routing 259
entering dialer strings 259
feature interactions 262
logging 268
overview 256
policy lists and 256
prerequisites 259
RAS configuration 259
typical installations 258
using VPN 256
Weighted Fair Queuing and 256
Monitoring applications 343
configuring 343
MSS 55–58, 60

CLI commands 60
configuring 56
example 60
Overview 55
predefined DoS classes 57
reporting mechanism 55
user-defined DoS classes 58
mtu 250, 251

N

Name 132, 148, 154
DS1 Circuit Pack 148
ISDN BRI Trunk Circuit Pack 154
Station 132
name server 76
name-server 79
name, access control list 577
name, crypto list 492
name, DHCP option 448, 449, 452
name, DHCP server 447, 452
name, DHCP vendor specific option 449, 452
name, packet sniffing 383
name, policy based routing 585
name, policy list 558
name, QoS list 572, 579
NAT Traversal 496
configuring 496
overview 496
Nested tunneling 433
NetBIOS 455
network 468
Network monitoring 343
applications 343
Next hop lists 585, 590
applying to policy-based routing rules 590
backup routes 585
editing 590
entries 590
overview 590
Next hops 429
FIPS 429
Next hops, see FIPS 429
next-hop 281, 293, 590
next-hop-interface 585, 591, 592
next-hop-ip 591, 592
next-hop-list 585
next-server 452
nslookup 79

O

object 284, 293
object tracker 284
object tracker changes 592
object tracking 284
configuration workflow 284
Object tracking 205, 256, 262, 280, 281, 284, 286, 289–291, 293, 428, 585
activating Dialer interface 262
applying to DHCP client 205
applying to PBR next-hops 585
applying to static routes 428
backup for the FastEthernet interface 290
CLI commands 293
configuration 280
enabling logging 286
interface backup using policy-based routing 291
maintenance 286
object tracker configuration 284
overview 280
RTR configuration 281
verifying MGC connectivity 256
viewing log messages 286
VPN failover 289
Open Shortest Path First protocol 466
see OSPF 466
option 448, 452
OSPF 258, 428, 460, 466–468, 470, 471
advertising static routes 428
CLI commands 468
compared to RIP 460, 466
default metric 471
description 466
dynamic Cost 467
limitations 467
modem dial backup and 258
shortest-path-first algorithm 466
using with RIP 470
OSPF Autonomous System Boundary Router 467
owner, access control list 577
owner, packet sniffing 383
owner, policy based routing 585
owner, policy list 558
owner, QoS list 579

P

Packet sniffing 380–386, 388–397
analyzing capture file 396
analyzing captured packets 393
applying a capture-list 390
applying rules to an address range 386
applying rules to packets with DSCP values 385

applying rules to packets with ip protocols 386
capture list examples 389
clearing the capture buffer 391
CLI commands 397
configuring 381
creating capture-list 382
defining rule criteria 383
disabling 382
enabling 382
enabling the service 392
excepting protocols from rules 386
identifying the interface 396
information, viewing 393
overview 380
packets captured 380
reducing the size of the capture file 391
rule criteria commands 384
scp file upload limit 395
service, starting 392
service, stopping 393
setting buffers 391
setting capture list context 382, 383
setting capture list parameters 383
setting max frame size 391
settings 391
simulating packets 397
specifying and excluding ICMP type and code .. 388
specifying bugger size 391
specifying capture actions 382
specifying interfaces 382
streams that always be captured 381
streams that can be captured 380
streams that can never be captured 381
uploading capture file 394
uploading capture files to remote servers or USB storage device 395
uploading capture files to the S8300 395
viewing the capture-list 390
viewing, captured packet hex dump 393
with conditional capture requirements 381
Packets, simulating 576
Policy 576
Packets, simulating, see Policy 576
passive-interfaces 468
password 38
Password authentication process 46
Password Authentication Protocol 246
password changes 37
Passwords 33–37, 50
creating by the admin 35
disabling 36
displaying password information 37
managing 34
managing contents 36
managing expiry 37
managing length 36
managing lockout 36
overview 33
recovery password 50
PBR lists 583, 585, 588, 589, 592, 597
attaching to interface 585
attaching to Loopback interface 583, 585
CLI commands 597
deleting 592
editing rules 589
modifying 592
name 585
rule criteria 588
rules 585, 588
PC device for CLI access 30
Permanent routes 430
Permit / Deny 137
PIM 32, 133
accessing 32
description 32
SLS configuration 133
ping 254
Ping 253
pmi 65, 66
PMI 64–66
CLI commands 66
configuration 64
entering the interface context 65
explanation 64
resetting the interface 65
setting location information 65
setting system contact information 65
setting the system name 65
showing the PMI 65
PMI, active and configured 66
pmi6 66
Poison-reverse 462
Policy 256, 553–573, 575–577
access control lists 554
attaching policy list to interface at IACL 561
attaching policy lists to an interface 560
attaching QoS list to interface at ingress QoS list 561, 562
changing DSCP table entries 573
configuring composite operations 572
copy list 557, 558
create access control lost 557

create QoS list 557
creating policy lists 557
creating rules 565
default actions 559
defining global rules 563
defining list identification attributes 558
defining policy lists 557
deleting a policy list 559
deleting a QoS list 559
destination port range 567
device wide policy lists 563
displaying access control lists 563
displaying composite operation lists 563
displaying ip rules 565
displaying policy lists in DSCP table context 575
displaying policy lists in general context 575
displaying policy lists in QoS list context 575
displaying policy lists in QoS list rule context 575
DSCP as rule criteria 569
DSCP default value 573
DSCP methods 573
DSCP table 573
edit access control list 557
editing policy lists 557
editing rules 565
example composite operation 573
fragments 569
ICMP code 568
ICMP type 568
managing policy lists 556
mapping DSCP to a CoS 573
modem dial backup and 256
network security with access control lists 554
overview 553
policy lists and loopback interfaces 563
policy-based routing, Policy-based routing 556
policy-based routing, see Policy-based routing 556
precongifured composite operations 570
precongifured for QoS lists 571
QoS fields 555
QoS list 557
QoS list parts 555
QoS lists 555
rule criteria 564
sequence of device-wide policy list application 563
sequence of policy list application 560
simulated packet properties 576, 577
simulating packets 576
source port range 567
specifying a destination ip address 566
specifying an ip protocol 566
specifying operations 570
TCP, establish bit 569
testing policy lists 575
using ip wildcards 564
Policy-based routing 291, 433, 583–585, 588, 591
applications 584
applying object tracking to next-hops 585
attaching list to interface 585
based on DSCP 584
cancelling object tracking on next-hops 591
changing the object tracker on a next-hop 591
defining next hop lists 585
distinguishing between voice and data 584
object tracking and 291
overview 583
packets not considered router packets 583
PBR lists, PBR lists 583
PBR lists, see PBR lists 583
routing to GRE tunnel 433
rules 588
saving the configuration 585
used to define backup routes 585
VoIP 584
policy-based routing application 595
Port 130
Station 130
Port classification 341, 342
CLI commands 342
Ports 341
Port classification, see Ports 341
Port mirroring 334, 335
CLI commands 335
description 334
Port redundancy 17, 18, 331–334
CLI commands 334
configuration 332
description 331
disabling 332
displaying information 333
enabling 332
LAN deployment 17, 18
secondary port activation 332
setting redundancy-intervals 333
switchback 332
port redundancy schemes 333
Ports 202, 297, 331, 334, 337, 341, 421
alternate 337
analog line 297
backup 337
classification 341
Fast Ethernet, Fast Ethernet port 202

Fast Ethernet, see Fast Ethernet port 202
FastEthernet 421
FastEthernet, see Fast Ethernet port 421
mirroring, see Port mirroring 334
opening traffic 337
redundancy, Port redundancy 331
redundancy, see Port redundancy 331
roles in RSTP 337
PPP 31, 249, 422
as default WAN protocol 249
connection 31
supported on Serial interfaces 422
ppp authentication, ASG authentication 40, 41
ppp authentication, USB port 246
ppp chap hostname 250, 251, 259, 266
ppp chap password 250, 251, 259
ppp chap refuse 250, 251
ppp chap-secret 246
ppp ipcp dns request 76, 79, 250, 251, 273, 533
ppp pap refuse 250, 251
ppp pap sent username 251
ppp pap sent-username 259
ppp pap-sent username 250
ppp timeout authentication 246
ppp timeout authentication, USB port 246
ppp timeout ncp 250, 251
ppp timeout retry 250, 251
PPP/IPCP address negotiation 250
PPPoE 249–251
authentication 250
CLI commands 251
description 249
shutting down client 250
pppoe-client persistent delay 250, 251
pppoe-client persistent max-attempts 250, 251
pppoe-client service-name 250, 251
pppoe-client wait-for-ipcp 250, 251
pre-classification 579
pre-shared-key 486, 547
Primary Management IP address (PMI) 22
Priority queueing 242
CLI commands 242
Priority Queuing 242
Priority VoIP queuing 240
priority-queue 241, 242
Privilege levels 35
creating 35
description 35
profile 412, 415
protect crypto-map 492, 547
Protocol Version 151
Provisioning 24
muiltiple gateways 24
Provisioning and Installation Manager 32
PIM 32
Provisioning and Installation Manager (PIM) 24
Provisioning and Installation Manager, see PIM 32
Proxy ARP 459
CLI commands 459
Purpose 13

Q

QoS 238–240, 242, 349, 353, 354, 364, 368
analyzing fault and clear trap output 368
CLI commands 239
configuration 238
displaying parameters 238
fair packet scheduling 240
fault and clear traps 354
metrics for RTP statistics application 349
policy, Policy 238
policy, see Policy 238
Priority Queuing 242
queue sizes for VoIP traffic 238
resolving conflicts 238
SNMP traps 353
traps in messages file 364
traps, viewing 364
VoIP Queuing 242
Weighted Fair VoIP Queuing 240
QoS allowed values 556
QoS list 579
CLI commands 579
queue-limit 242
Queues 240, 242
fair packet scheduling 240
Priority 242
Priority Queuing 242
VoIP 242
VoIP Queuing 242
Weighted Fair VoIP Queuing 240
Quick Start for Hardware Installation for the Avaya Branch Gateway G430 13
Quick Start for Hardware Installation for the Avaya G350 Branch Gateway 13

R

RADIUS authentication 33, 48
RAS 256, 258, 259, 266
dialer strings for modem dial backup 266

modem dial backup and 256
modem dial backup configuration options 258
modem dial backup prerequisites 259
serving multiple branch offices 258
Recovery password 50
redistribute 464, 468, 470, 471
related resources 15
Avaya Mentor videos 15
release dhcp 207, 208
Remote Access Server 256
RAS 256
Remote Access Server, see RAS 256
remote calls from analog to IP telephones 373
remote calls from IP telephone to IP telephone 375
Remote services logins 39
remove nfas-interface 187
remove port 187
rename announcement-file 322, 324
renew dhcp 207, 208
Replacement String 135
AAR and ARS Digit Conversion Table 135
reset 65
restore 93, 97
restore usb 87, 93, 97
restoring ETR to automatic activation 298
Restoring the Branch Gateway 93
using the Branch Gateway USB port 93
RIP 428, 460–464, 466, 470, 471
advertising static routes 428
CLI commands 464
compared to OSPF 466
default metric 471
description 460
distribution access lists 462
limitations 463
poison-reverse 462
preventing loops 462
RIPv1 461
RIPv2 461
split-horizon 462
using with OSPF 470
versions supported 460
RIPv1 and RIPv2 differences 461
RMON 343, 345
agent 343
CLI commands 345
overview 343
rmon alarm 345
RMON configuration examples 344
rmon event 345
rmon history 345
Route redistribution 460, 470, 471
CLI commands 471
configuration 470
description 470
metric translation 470
metrics 471
Router .. 47, 49, 51, 199, 419–421, 425, 443, 454, 460, 466, 467, 472, 475
backup 472
computing path 466
configuration commands 47, 49, 51
configuring BOOTP 443
configuring broadcast relay 454
configuring DHCP 443
configuring unnumbered ip addresses 425
connecting to fixed router port 199
determining shortest path 467
disabling 419, 420
displaying interfaces 425
enabling 419, 420
features 419
fragmentation 475
fragmentation, see Fragmentation 475
interfaces 421
load balancing 472
OSPF Autonomous System Boundary 467
overview 419
redundancy 472
RIP 460
RIP, see RIP 460
setting the borrowed ip interface 425
unnumbered ip interfaces in table 425
virtual 472
router ospf 266, 273, 468, 471
Router port, connecting to 199
router rip 464, 471
router vrrp 474
Routes 433
setting route preference 433
Routing 556
policy based, Policy 556
policy based, see Policy 556
Routing Information Protocol 460
see RIP 460
routing sources 427
Routing table 428, 431
CLI commands 431
deleting static routes 428
description 428
RSA authentication 45
RSTP 18, 19, 337, 338

designating ports as edge ports 338
displaying port point-to-point status 338
displaying the port edge state 338
fast network convergence 338
features 337
LAN deployment 18, 19
manually configure uplink and backbone ports .. 338
role of ports 337
setting port-to-port admin status 338
RSVP 239
RTCP 231
RTP 231, 346, 348
configuring 231
overview 346
statistics application functionality 346
viewing configuration thresholds 348
RTP header compression 232
Header compression 232
RTP header compression, see Header compression 232
RTP session data 346
RTP statistics 379
CLI commands 379
RTP statistics application 347–357, 364, 370
configuration and output examples 370
configuring 347
configuring additional trap destinations 354
configuring fault and clear traps 354
configuring QoS traps 353
configuring thresholds 350
display session information 357
displaying RTP session statistics 357
displaying VoIP engine RTP statistics 356
enabling 351
enabling traps 354
modifying the statistics window 354
QoS metric thresholds 348
QoS metrics 349
resetting 351
sample network 370
setting QoS event thresholds 350
setting QoS indicator thresholds 350
setting the trap rate limiter 355
statistics summary report output 356
viewing configuration 352
viewing QoS traps in messages file 364
rtp-echo-port 403, 407
rtp-stat clear 351, 379
rtp-stat event-threshold 350, 379
rtp-stat fault 354, 355, 379
rtp-stat min-stat-win 354, 379
rtp-stat qos-trap 354, 379
rtp-stat qos-trap-rate-limit 355, 379
rtp-stat service 379
rtp-stat thresholds 350, 379
rtp-stat-service 351
rtp-test-port 403, 407
rtr 281, 293
RTR 281
Object tracking 281
rtr-schedule 281, 293
RTR, see Object tracking 281
running-config startup-config 24, 25

S

safe-removal usb 97
scheduler 403, 407
SCP 47, 319
transferring announcement files using 319
Secure Shell protocol 45
SSH 45
Security 33, 50, 55, 327
DoS attack detection 55
overview 33
special features 50
VLANs 327
Security Associations (SAs) 477
Security Code 124
self-identity 486, 547
Serial interfaces 278, 422
dynamic bandwidth reporting 278
server-name 452
Services interface 21
Services port 30
connecting console and PC devices 30
session 72, 73
Session log 223
Logging 223
Session log, see Logging 223
session mgc 395
set associated-signaling 183, 187
set attendant 163, 187
set balance 414, 415
set bearer-capability (bri) 173, 187
set bearer-capability (ds1) 172, 187
set bit-rate 169, 187
set boot bank 84, 89
set busy-disconnect 187
set cbc 187
set cbc-parameter 187
set cbc-service-feature 187
set channel-numbering 187
set channel-preferences 176, 187

set codeset-display 176, 187
set codeset-national 187
set connect 169, 187
set contact-closure admin 316, 318
set contact-closure pulse-duration 316, 318
set cor 165, 187
set country-protocol (bri) 173, 187
set country-protocol (ds1) 169, 171, 187
set crosstalk-destination 412, 415
set crosstalk-port 412, 415
set crosstalk-responder 412, 415
set date-format 163, 187
set delete-digits (dial-pattern) 184, 187
set delete-digits (incoming-routing) 185, 187
set deny 184, 187
set destination 412, 415
set dial 175, 187
set digit-handling 176, 187
set digit-treatment 176, 187
set digits 176, 187
set directory-number-a 173, 187
set directory-number-b 173, 187
set dscp 490, 547
set echo-cancellation analog 409
set echo-cancellation config analog 409
set echo-cancellation config voip 409
set echo-cancellation voip 409
set endpoint-init 173, 187
set etr 297
set etr 7 auto 298
set expansion-module 165, 187
set fac 187
set icc-monitoring 73
set incoming-destination 176, 187
set incoming-dialtone 176, 187
set insert-digits (dial-pattern) 184, 187
set insert-digits (incoming-routing) 185, 187
set interface (bri) 173, 187
set interface (ds1) 169, 187
set interface-companding (bri) 173, 187
set interface-companding (ds1) 169, 187
set ip-codec-set 163, 187
set japan-disconnect 176, 187
set layer 1-stable 173, 187
set length 185, 187
set lldp re-init-delay 211, 212
set lldp system-control 211, 212
set lldp tx-delay 211, 212
set lldp tx-hold-multiplier 211, 212
set lldp tx-interval 211, 212
set logging file 225, 229
set logging file condition 225
set logging file disable 221
set logging file enable 220
set logging server 216, 229
set logging server access level 229
set logging server access-level 216
set logging server condition 225, 229
set logging server disable 216
set logging server enable 216
set logging server facility 216, 229
set logging session 229, 268
set logging session condition 225
set logging session condition dhcpc 208
set logging session disable 223
set logging session enable 208
set logging session, dialer interface 273
set logging session, DNS resolver 79
set logging session, session log 223
set logging session, VPN 500
set long-timer 169, 187
set match-pattern 185, 187
set max-ip-registrations 163, 187
set max-length 184, 187
set mediaserver 72, 73
set mgc list 69, 73
set min-length 184, 187
set mss-notification rate 56
set name (bri) 173, 187
set name (ds1) 169, 187
set name (station) 165, 187
set name (trunk-group) 176, 187
set numbering-format 176, 187
set password 165, 187
set peer 489, 490, 547
set peer group 490
set peer-group 547
set pfs 485, 547
set pim-lockout 163, 187
set port 165, 187, 412, 415
set port auto-negotiation-flowcontrol-advertisement 200
set port classification 342
set port duplex 200
set port edge admin state 200, 338, 340
set port flowcontrol 200
set port level 200
set port lldp 211, 212
set port lldp tlv 211, 212
set port mirror 335
set port name 200
set port negotiation 200
set port point-to-point admin status 200, 338, 340

set port redundancy 332, 334
set port redundancy enable|disable 332, 334
set port redundancy-intervals 332–334
set port spantree 340
set port spantree cost 340
set port spantree force-protocol-migration 340
set port spantree priority 340
set port speed 200
set port static-vlan 330
set port trap 309
set port vlan 330
set port vlan-binding-mode 330
set primary-dchannel 183, 187
set protocol-version 171, 187
set qos bearer 238, 239
set qos control 238, 239
set qos rsvp 239
set qos rtcp 239
set qos signal 238, 239
set radius authentication 49
set radius authentication retry-number 49
set radius authentication retry-time 49
set radius authentication secret 49
set radius authentication server 49
set radius authentication udp-port 49
set receive-gain 414, 415
set reset-times 71, 73
set responder 412, 415
set responder-type 412, 415
set security-association lifetime 547
set security-association lifetime kilobytes 485
set security-association lifetime seconds 485
set send-name 176, 187
set send-number 176, 187
set side (bri) 173, 187
set side (ds1) 169, 187
set signaling-mode 169, 187
set slot-config 163, 187
set sls 137, 163, 187
set snmp community 310
set snmp retries 310
set snmp timeout 310
set snmp trap 309
set spantree default-path-cost 340
set spantree enable/disable 340
set spantree forward-delay 340
set spantree hello-time 340
set spantree max-age 340
set spantree priority 340
set spantree tx-hold-count 340
set spantree version 340
set spid-a 173, 187
set spid-b 173, 187
set supervision 176, 187
set swhook-flash 165, 187
set sync interface 601, 604
set sync source 601, 602, 604
set sync switching 603, 604
set system contact 65, 66
set system location 65, 66
set system name 65, 66
set tac 176, 187
set tei-assignment 173, 187
set terminal recovery password 50
set tgnum 184, 187
set transform-set 490, 547
set transmit-gain 414, 415
set trunk 330
set trunk-destination 165, 187
set trunk-group-chan-select 183, 187
set trunk-hunt 176, 187
set type 412, 415
set type (dial-pattern) 184, 187
set type (station) 165, 187
set utilization cpu 82
set vlan 326, 330
setting buffer-size 391
Setting synchronization 601
    Synchronization 601
Setting synchronization, see Synchronization 601
show (bri) 173, 187
show (dial-pattern) 184, 187
show (ds1) 169, 187
show (incoming-routing) 185, 187
show (profile) 413, 415
show (sig-group) 183, 187
show (station) 165, 187
show (trunk-group) 176, 187
show announcement-file 324
show announcements-files 322
show attendant 187
show auth-file info 40, 43
show backup status 97
show boot bank 84, 89
show bri 187
show cam vlan 330
show capture-dummy-headers 396
show cna testplug 403, 407
show composite-operation, access control list 563, 577
show composite-operation, policy list 575
show composite-operation, QoS list 579
show contact-closure 317, 318

show controller 254
show correction 415
show crypto ipsec sa 496, 547
show crypto ipsec transform-set 499, 547
show crypto isakmp peer 499, 547
show crypto isakmp peer-group 499, 547
show crypto isakmp policy 499, 547
show crypto isakmp sa 499, 547
show crypto ispsec sa 499
show crypto map 499, 547
show date-format 187
show dial-pattern 187
show download announcement-file status 322–324
show download software status 86, 89
show download status 99
show ds1 187
show dscp-table 575, 579
show dynamic-cac 279
show echo-cancellation 409
show extension 187
show fac 187
show faults 82
show fragment 476
show frame-relay fragment 254
show frame-relay lmi 254
show frame-relay map 254
show frame-relay pvc 254
show frame-relay traffic 254
show icc-monitoring 73
show icc-vlan 328, 330
show image version 82, 89, 93, 97
show incoming-routing 187
show interface 246
show interfaces, dialer interface 259, 273
show interfaces, GRE tunnel 441
show interfaces, interface status 400
show interfaces, unnumbered IP interface 425
show interfaces, VLANs 330
show interfaces, WAN configuration 254
show ip access-control-list 575, 577
show ip active-lists 499, 547, 593
show ip arp 458
show ip capture-list 390
show ip crypto-list 499
show ip crypto-list list# 499
show ip crypto-lists 547
show ip dhcp-client 208
show ip dhcp-client statistics 207, 208
show ip dhcp-pool 452
show ip dhcp-server bindings 452
show ip dhcp-server statistics 452
show ip distribution access-lists 464
show ip domain 79
show ip domain statistics 79
show ip icmp 460
show ip interfaces 254
show ip next-hop-list all 593
show ip ospf 468
show ip ospf database 468
show ip ospf interface 468
show ip ospf neighbor 468
show ip ospf protocols 468
show ip pbr-list 593
show ip protocols 464
show ip qos-list 575, 579
show ip reverse-arp 458
show ip route 431
show ip route best-match 431
show ip route static 431
show ip route summary 431
show ip rtp header-compression 234
show ip rtp header-compression brief 234
show ip ssh 46, 47
show ip tcp header-compression 234, 237
show ip tcp header-compression brief 234, 237
show ip telnet 51
show ip track-table 431
show ip vrrp 474
show ip-codec-set 187
show ip-qos-list 579
show ip-rule, access control list 577
show ip-rule, policy based routing 589, 593
show ip-rule, policy list 575
show ip-rule, QoS list 579
show keepalive-icmp 276, 277
show last-pim-update 187
show list 558, 575, 577, 579, 593
show lldp 211, 212
show lldp config 212
show logging file condition 222, 229
show logging file content 221, 225, 229
show logging server condition 219, 229
show logging session condition 223, 229
show login authentication 37, 38, 43
show map-class frame-relay 254
show max-ip-registration 187
show mediaserver 73
show mg list_config 81, 82
show mgc 70, 73, 82
show mgc list 70, 73
show mm 81
show module 81, 82

show next-hop 593
show pim-lockout 187
show pmi 65, 66
show point-to-point status 340
show port auto-negotiation-flowcontrol-advertisement 200
show port classification 342
show port edge state 338, 340
show port edge status 200
show port flowcontrol 200
show port lldp config 212
show port lldp vlan-name config 212
show port mirror 335
show port point-to-point status 338
show port redundancy 333, 334
show port trap 309
show port vlan-binding-mode 330
show ppp authentication 246
show profile 413, 415
show protocol 51
show protocols 79
show qos-rtcp 238, 239
show queue 241
show queueing 241, 242
show radius authentication 49
show recovery 72, 73
show restart-log 82
show restore status 87, 93
show result 414, 415
show result (profile) 414, 415
show rmon alarm 345
show rmon event 345
show rmon history 345
show rmon statistics 345
show rtp-stat config 379
show rtp-stat detailed 379
show rtp-stat sessions 379
show rtp-stat summary 356, 379
show rtp-stat thresholds 349, 379
show rtp-stat traceroute 369, 379
show rtr configuration 286, 293
show rtr operational-state 286, 293
show sig-group 187
show slot-config 187
show sls 187
show snmp 56, 309, 310, 354
show snmp engineID 310
show snmp group 310
show snmp retries 310
show snmp timeout 310
show snmp user 310
show snmp usertogroup 310
show snmp view 310
show spantree 340
show station 187
show sync timing 604
show system 68, 82, 90, 97
show tcp syn-cookies 54, 55
show temp 82
show timeout 82
show track 286, 293
show traffic-shape 254
show trunk 330
show trunk-group 187
show upload announcement-file status 323, 324
show upload auth-file status 40
show upload status 395
show username 37, 38, 43
show utilization 82
show vlan 327, 330
show voltages 82
shutdown 203
  WAN port 203
shutdown, CNA test plug 403, 407
shutdown, PPPoE 250, 251
shutdown, USB port 246
Side 150
sig-group 183, 187
signaling groups data 152
Signaling Mode 148
sink severity levels defaults 226
site-to-site IPSec VPN 545
SLA monitor 417
  overview 417
sls 163, 187
SLS .. 101–111, 113, 114, 116, 120, 133, 137–142, 147, 152, 153, 156, 158, 159, 161–163, 165, 169, 173, 176, 183–185, 187
  Avaya telephones supported in SLS 103
  call processing not supported by SLS 105
  call processing supported by SLS 104
  capabilities 101
  capacities 139
  capacities by Branch Gateway model 139
  CDR log 116
  CLI command hierarchy 187
  configuring 120
  configuring Avaya Aura™ Communication Manager for SLS 120
  configuring Communication Manager for SLS ... 120
  disabling 137, 138
  enabling 137, 138

entry in MGC list 107
features 102
interaction with, call transfer 113
interaction with, contact closure 114
interaction with, Direct Inward Dialing 110
interaction with, Hold feature 111
interaction with, multiple call appearances 110
interaction with, shared administrative identity with softphone 116
introduction 101
IP Softphone administration in SLS mode 116
logging 116
manual CLI configuration, administering BRI parameters 173
manual CLI configuration, administering dial-pattern parameters 184
manual CLI configuration, administering DS1 parameters 169
manual CLI configuration, administering incoming-routing parameters 185
manual CLI configuration, administering signaling-group parameters 183
manual CLI configuration, administering station parameters 165
manual CLI configuration, administering trunk-group parameters 176
manual CLI configuration, command sub-contexts 162
manual CLI configuration, commands hierarchy 187
manual CLI configuration, instructions 163
manual CLI configuration, introduction 138
manual CLI configuration, preparing SLS data set 139
manual CLI configuration, prerequisites 138
PIM configuration 133
preparing SLS data set .. 139, 141, 142, 152, 156, 158, 159, 161
preparing SLS data set, analog stations data 140
preparing SLS data set, DS1 trunks data 147
preparing SLS data set, ISDN-BRI trunks data .. 153
provisioning data 106
registered state process 108
states 107
states, registered 108
states, setup 108
states, teardown 109
states, unregistered 108
supported functionality 104
SLS changes 138
SLS codecs 159
SLS feature interactions 115
SLS station context class values 168
SNMP 55, 301–307, 311, 312, 353
agent and manager communication methods 302
changing user parameters 305
configuration examples 312
configuring traps 307
creating OID lists 306
creating user groups 306
creating users 305
default security name, read 303
default security name, write 303
DoS alerts 55
enabling traps and notifications 307
mapping user groups to views 305
MSS notifications 55
overview 301
potential agent residences 301
predefined user groups 305, 306
QoS 353
required information for creating views 307
setting dynamic trap manager parameters 311
user groups 305
user-based security model (USM) 304
USM security levels 304
version 1 303
version 2 303
version 3 304
versions 302
views 306
SNMP access configuration 310
CLI commands 310
SNMP trap configuration 309
CLI commands 309
snmp trap link-status 309
snmp-server community 310
snmp-server dynamic-trap-manager 56, 311, 312, 354
snmp-server enable notification 309
snmp-server enable notifications 307
snmp-server engineID 310
snmp-server group 56, 310
snmp-server host 56, 309, 354
snmp-server informs 309
snmp-server remote-user 310
snmp-server user 56, 305, 310
snmp-server view 310
Software 25
Firmware 25
Software, see Firmware 25
source-address 281, 293
source-ip 386
packet sniffing 386

source-ip, access control list 577
source-ip, crypto list rule 492, 547
source-ip, policy list 566
source-ip, QoS list 579
Spanning tree 336, 337, 339, 340
examples 339
CLI commands 340
configuration 336
disabling 337
protocol 336
speed 203
speed, USB port 246
SPI recovery 496
SPID 155
Split-horizon 462
SSH 45, 46
configuration 46
overview 45
Standard Local Survivability 101
SLS 101
Standard Local Survivability, see SLS 101
start-ip-addr 447, 452
static ARP table entries 457
Static routes 428–431, 470
advertising 428
applying object tracking 428, 429
configuring next hops 429
deleting 428, 430
description 428
discard route 431
dropping packets to 431
High Preference 429
inactive 428
load-balancing 428
Low Preference 429
permanent 430
redistributing to RIP and OSPF 470
types 429
station 187
subnet-mask 447, 449, 452
success-retries 281, 293
suggest-key 486, 547
support 15
contact 15
Survivability 69, 71
configuring the MGC list 69
setting reset times 71
Survivable COR 131
Survivable GK Node Name 131
Survivable Trunk Dest 132
Switch 199, 253, 421, 422
connecting to fixed router port 199
displaying configuration 253
interface 421, 422
Switch ports 200
configuring 200
Switch redundancy 18, 19
LAN deployment 18, 19
Switchback 332
Switchhook Flash 132
Switching 325, 421, 422
configuring 325
interface 421, 422
SYN attacks protection 52
SYN cookies 52
SYN attacks protection, see SYN cookies 52
SYN cookies 52–54
attack notification 54
configuring 54
introduction 52
overview 52
strategies employed 53
SYN flood attack protection 53
SYN cookies 53
SYN flood attack protection, see SYN cookies 53
Synchronization 601–604
CLI commands 604
defining a stratum clock source 601
disassociating specified primary or secondary clock source 602, 603
displaying synchronization timing 604
LED status 603
overview 601
setting interface 601
setting the sync source 601, 602
toggling sync source switching 603
Syslog server 216
see Logging 216
system parameters data 158

T

tcp destination-port 387, 567, 577, 579
tcp established 569, 577
TCP header compression 232
Header compression 232
TCP header compression, see Header compression 232
tcp source-port 387, 567, 577, 579
tcp syn-cookies 54, 55
TCP/IP connection 31
Telephones supported in SLS mode 103
telnet 51
Telnet 31, 50

accessing gateway via ... 31
enabling and disabling access ... 50
Telnet session ... 28
disconnecting ... 28
test-rate-limit ... 403, 407
TFTP ... 83
threshold count ... 284, 293
time constants, configuring ... 333
timeout absolute ... 246
timers basic ... 464
timers spf ... 468
TLVs ... 210
802.1 (optional) ... 210
mandatory ... 210
optional ... 210
supported ... 210
Tools ... 343, 346
for monitoring ... 343
VMON ... 346
traceroute ... 431
track ... 284, 293, 592
track list ... 284
track rtr ... 284
Traffic shaping ... 202, 253
displaying configuration ... 253
WAN Ethernet port ... 202
traffic-shape rate ... 202, 203
training ... 14
Transform-sets ... 479, 485
overview ... 479
VPN, defining ... 485
trap manager parameters ... 312
traps ... 607
TRK port ... 297
see Fixed analog trunk port ... 297
Trunk Group ... 137
trunk group data collection ... 143
Trunk Group for Channel Selection ... 153
trunk-group ... 187
tunnel checksum ... 441
tunnel destination ... 438, 441
tunnel dscp ... 441
tunnel key ... 441
tunnel path-mtu-discovery ... 441
tunnel source ... 438, 441
tunnel ttl ... 441
type ... 281, 293
Type ... 125
Station ... 125

U

UDP ... 232
header compression ... 232
udp destination-port ... 387, 567, 577, 579
udp source-port ... 387, 567, 577, 579
Unnumbered IP interface ... 256, 262, 424, 425
configuring ... 425
Dialer interface ... 256, 262
examples ... 425
feature overview ... 424
in routing table ... 425
upgrade using FTP/TFTP ... 85
USB mass storage device ... 86, 90
overview ... 90
upgrading firmware ... 86
USB mass-storage device ... 91, 93, 97
backing up the Branch Gateway ... 91
CLI commands ... 97
restoring the Branch Gateway ... 93
upgrading media modules ... 97
USB port ... 22, 31, 90, 245, 246
assigning IP address ... 22
CLI commands ... 246
configuring for modem use ... 31
connecting modem ... 31
default parameters ... 245
description ... 245
enabling ... 245
resetting ... 245
setting authentication method ... 246
User accounts ... 34, 38
CLI commands ... 38
managing ... 34
User authentication ... 33, 45
SSH ... 45
user privledge changes ... 36
username ... 38
Usernames ... 33–35
creating ... 35
managing ... 34
overview ... 33
USP WAN lines ... 249

V

value ... 448, 449, 452
VAM ... 319
vendor-specific-option ... 449, 452
videos ... 15
Avaya Mentor ... 15

Virtual interface 421
Virtual Private Network 421, 477
see VPN 421
VPN 477
Virtual Private Network, see VPN 477
Virtual router 472
Virtual Router Redundancy Protocol 472
VRRP 472
Virtual Router Redundancy Protocol, see VRRP 472
Vlan 1 421
VLANs 278, 325–328, 330, 421, 422, 443
binding modes 326
clearing the VLAN table 327
CLI commands 330
configuration examples 328
description 422
DHCP/BOOTP requests 443
displaying the VLAN table 327
dynamic bandwidth reporting 278
ICC-VLAN 328
ingress security 327
multi VLAN binding 326
overview 325
setting the VLAN 326
setting vlan 2 example 328
switching interface 421, 422
table 327
tagging 326
VLMS 461
VMON, for troubleshooting QoS 346
VoIP 231, 238–240, 242, 256, 584
available transmission protocols 231
enabling queuing 238
fair packet scheduling 240
overview 231
priority over Dialer interface 256
queue delay 238
queue size 238
routing based on 584
RSVP protocol 239
VoIP queuing 242
Weighted Fair VoIP Queuing 240
VoIP Queuing 242
voip-queue 241, 242
voip-queue-delay 242
VPN 256, 289, 421, 432, 477, 479, 480, 482, 483, 485, 486, 489, 490, 492, 494–497, 499–501, 507, 509, 510, 520, 526, 527, 532, 538, 547
activating 497
assigning an access control list 495
basic parameters 483
clearing VPN data 500
CLI commands 547
commands summary 480
components and relationships 479
components overview 479
configuration, overview 482
configuration, procedure 482
continuous channel 509
coordinating with the VPN peer 483
crypto list, assigning to an interface 497
crypto list, configuring 492
crypto list, deactivating 494
crypto list, overview 479
crypto map, configuring 490
crypto map, overview 479
failover mechanisms 526
introduction 477
ISAKMP policies, configuring 483
ISAKMP policies, overview 479
logging 500
maintenance 499
modem dial backup and 256
NAT Traversal 496
object tracking for failover 289
peer-group, configuring 489
peer-group, overview 479
peer, configuring 486
peer, overview 479
show status 499
simple VPN topology 501
site-to-site configuration 482
transform-sets, configuring 485
transform-sets, overview 479
typical failover applications, failover using a peer-group 538
typical failover applications, failover using DNS 532
typical failover applications, failover using GRE 527
typical failover applications, failover using object-tracking 538
typical failover applications, overview 526
typical installations, configuring dynamic IP 507
typical installations, enabling continuous channel 509
typical installations, full or partial mesh 510
typical installations, full solution 520
typical installations, hub and spokes installation 501
VPN hub redundancy 528
VPN hub-and-spoke 521
VPN topology 502, 511
VRRP 472–474
CLI commands 474

configuration example 473
description 472

W

wait-interval 281, 293
WAN 249, 253, 254, 256, 274, 278, 421, 583
checking interface status 274
default protocol 249
Dialer interface as backup 256
dynamic bandwidth reporting 278
features 249
ICMP keepalive 274, 583
initial configuration 249
interfaces 421
overview 249
PPP 249
testing configuration 253
testing configuration, CLI commands 254
WAN endpoint device 199
connecting to fixed router port 199
WAN Ethernet port 202, 203
backup interfaces 203
configuring 202
traffic shaping 202
WAN Ethernet port feature configuration 202
WAN Ethernet ports 203
CLI commands 203
Warranty 15
Weighted Fair VoIP Queuing 240, 256
WFVQ 240, 241
CLI commands 241
Weighted Fair VoIP Queuing 240
WFVQ, see Weighted Fair VoIP Queuing 240