



Administering Avaya G450 Branch Gateway

Release 10.2.x
Issue 3
December 2024

Notices

© 2026 Avaya LLC. All Rights Reserved.

You may, at your own risk, assemble a MyDocs collection solely for your own internal business purposes, which constitutes a modification to the original published version of the publications. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of publications. You agree to defend, 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, your modifications, additions or deletions to the publications.

A single topic or a collection of topics may come from multiple Avaya publications. All of the content in your collection is subject to the legal notices and disclaimers in the publications from which you assembled the collection. For information on licenses and license types, trademarks, and regulatory statements, see the original publications from which you copied the topics in your collection.

Except where expressly stated by Avaya otherwise, no use should be made of materials provided by Avaya on this site. All content on this site and the publications provided by Avaya including the selection, arrangement and design of the content is owned by Avaya and/or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. Avaya owns all right, title and interest to any modifications, additions or deletions to the content in the Avaya publications.

Notice

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

Warranty

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

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, please contact your Avaya Sales Representative.

Documentation disclaimer

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

Link disclaimer

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

Copyright

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

written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Virtualization

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

How to Get Help

For additional support telephone numbers, go to the Avaya Support website: <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 62368-1 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. 62368-1 / UL 62368-1 latest edition.

This product may contain Class 1 laser devices.

- Class 1 Laser Product
- Luokan 1 Laserlaitte
- Klass 1 Laser Apparat

Electromagnetic Compatibility (EMC)

Avaya LLC 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 LLC. 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 LLC, 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
	04DU9.1K N	6.0F	RJ48C, RJ48M
	04DU9.1S N	6.0F	RJ48C, RJ48M
120A4 channel service unit	04DU9.DN	6.0Y	RJ48C

If this equipment causes harm to the telephone network, the telephone company will notify you in advance that temporary discontinuance of service may be required. But if advance notice is not practical, the telephone company will notify the customer as soon as possible. Also, you will be advised of your right to file a complaint with the FCC if you believe it is necessary.

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

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

A plug and jack used to connect this equipment to the premises wiring and telephone network must comply with the applicable FCC Part 5 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 LLC in the United States of America hereby certifies that the equipment described in this document and bearing a TIA TSB-168 label identification number complies with the FCC's Rules and Regulations 47 CFR Part 68, and the Administrative Council on Terminal Attachments (ACTA) adopted technical criteria.

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

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

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 matériel est conforme aux spécifications techniques applicables d'Industrie Canada.

European Union Declarations of Conformity



This device when installed complies with the essential requirements and other relevant provisions of the EMC Directive 2014/30/EU, and Safety LV Directive 2014/35/EU.

A copy of the Declaration may be obtained from <https://support.avaya.com> or Avaya LLC, 350 Mt. Kemble Avenue, Morristown, NJ USA 07960 USA.

European Union Battery Directive



Avaya LLC supports European Union Battery Directive 2006/66/EC. Certain Avaya LLC 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, Hosted Service(s), and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, its licensors, its suppliers, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the Documentation, Hosted Service(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya LLC.

All non-Avaya trademarks are the property of their respective owners.

Downloading Documentation

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

Contact Avaya Support

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

Contents

Chapter 1: Introduction	21
Purpose	21
Change history	21
Chapter 2: Branch gateway network configurations	22
Basic configuration	22
Port redundancy configuration	22
Port and switch redundancy configuration	23
Rapid spanning tree protocol configuration	23
RSTP and switch redundancy configuration	24
Chapter 3: Configuration overview	25
Defining the Console interface	25
Defining the USB-modem interface	26
Other interfaces	26
Define other interfaces	26
Configuration using CLI	27
Configuration changes and backup	27
Saving configuration changes and backing them up	28
Firmware version control	28
Using an older version of firmware	28
Chapter 4: Branch Gateway access	29
CLI access	29
Logging to CLI	29
CLI contexts	29
Using CLI help	30
CLI access using the local network	31
Accessing CLI locally using a computer	31
CLI access using modems	31
Accessing CLI using a USB modem	32
USB port settings	32
Branch Gateway serial modems	33
CM access	33
Security overview	34
Login permissions	34
User account management	34
Login authentication	38
SSH protocol support	40
SCP protocol support	46
RADIUS authentication	46
Special security features	47

Commands used to configure Telnet access.....	47
Gateway secret management.....	48
DoS attacks.....	49
Managed security services.....	51
Enhanced Access Security Gateway (EASG).....	56
Managing EASG.....	56
Viewing EASG product certificates.....	59
Managing EASG site certificates.....	59
Viewing EASG status.....	61
Viewing product id.....	61
Service logins with Enhanced Access Security Gateway (EASG) authentication.....	62
Chapter 5: Basic device configuration.....	63
Defining an interface.....	63
Primary Management Interface (PMI) configuration.....	64
Setting the PMI of the Branch Gateway.....	64
Active and configured PMI.....	65
PMI configuration CLI commands.....	65
Example of defining a default gateway.....	66
Branch Gateway Controller configuration.....	66
Locating the Branch Gateway serial number.....	67
Survivability and migration options.....	67
MGC list configuration.....	68
About setting reset times.....	71
Example for setting reset times.....	72
Accessing the registered MGC.....	72
H.248 Registration Source Port.....	73
ICC or Survivable Remote Server monitoring.....	73
Summary of MGC list configuration commands.....	73
DNS resolver.....	74
DNS resolver features.....	74
Typical DNS resolver application – VPN failover.....	75
Configuring DNS resolver.....	75
Using DNS resolver to resolve a hostname.....	78
DNS resolver maintenance.....	78
DNS resolver configuration commands.....	78
Device status viewing.....	79
The show mm command.....	79
The show module and show mg list config commands.....	80
Device status commands.....	80
OOB.....	81
oob-interface configuration.....	81
no oob-interface.....	81
show oob-interface.....	81

set non-oob-interfaces access.....	81
Software and firmware management.....	82
File transfer.....	82
Software and firmware upgrades.....	82
Software and firmware uploads from the gateway.....	86
Chapter 6: Standard Local Survivability (SLS).....	98
Media module compatibility with SLS.....	98
SLS features.....	99
Avaya telephones supported in SLS.....	99
Call processing functionality in SLS mode.....	101
Call processing functionality not supported by SLS.....	102
Provisioning data.....	102
Standard Local Survivability data sources and communication paths.....	103
SLS entry.....	103
Unregistered state.....	104
Setup state process.....	104
Registered state process.....	104
Teardown state.....	104
SLS interaction with specific Branch Gateway features.....	105
Direct Inward Dialing in SLS mode.....	105
Multiple call appearances in SLS mode.....	106
Hold in SLS mode.....	106
DCP and IP phones.....	106
Using the Flash button.....	107
Using the switchhook button.....	107
Call Transfer in SLS mode.....	108
Using contact closure in SLS mode.....	109
Administering IP Softphone in SLS mode.....	110
SLS logging activities.....	111
Example of CDR log entries and format.....	111
Example of CDR log with contact closure.....	112
SLS configuration.....	113
SLS configuration rules.....	113
Configuring CM for SLS.....	113
Inherited Class of Restriction (COR) permissions.....	115
Station screen field descriptions for the Branch Gateway.....	115
SLS ARS Entry page field descriptions.....	123
Enabling SLS.....	125
Disabling SLS.....	125
Activating changes in SLS.....	126
Prerequisites for using the CLI to manually configure SLS administration on the Branch Gateway.....	126
DS1 circuit pack field descriptions.....	134

Collecting signaling groups data.....	138
Signaling Group field descriptions.....	138
Collecting administered ISDN-BRI trunks data.....	139
ISDN-BRI Trunk field descriptions.....	139
Collecting Feature Access Codes data.....	141
Feature Access Code field descriptions.....	142
Collecting system parameters data.....	143
Codecs supported in SLS.....	143
General system parameters field descriptions.....	143
Collecting ARS dial patterns data.....	144
ARS Dial Patterns field descriptions.....	144
Collecting Incoming Call Handling data.....	145
Incoming call handling data field descriptions.....	145
Configuration of the SLS data through the CLI.....	146
Creating the SLS administration data set on the Branch Gateway.....	147
Administering station parameters.....	149
Class values in SLS station context.....	151
Module-port values in SLS station configuration mode.....	151
Administering DS1 parameters.....	152
ISDN Layer 3 country codes.....	154
ISDN Layer 3 country protocols for ISDN Primary Rate service.....	155
Administering BRI parameters.....	156
Trunk group assignment.....	158
Administering trunk-group parameters.....	158
Maximum number of members in a trunk group.....	163
SLS group type assignments.....	163
Module-port values in SLS trunk-group context for analog trunks.....	164
Trunk port values in SLS trunk-group context for digital trunks.....	164
Administering signaling-group parameters.....	165
Administering dial-pattern parameters.....	166
Administering incoming-routing parameters.....	167
Summary of SLS configuration commands.....	168
Chapter 7: Switch Ethernet port configuration.....	178
Ethernet ports on the Gateway switch.....	178
Ethernet ports on the Branch Gateway router.....	178
Cables used for connecting devices to the fixed router.....	178
Roadmap for configuring switch Ethernet ports.....	179
Summary of switch Ethernet port configuration CLI commands.....	179
Configuring the WAN Ethernet port.....	181
Roadmap for configuring additional features on the WAN Ethernet port.....	181
WAN Ethernet port traffic shaping.....	181
About backup interfaces.....	182
Summary of WAN Ethernet port configuration CLI commands.....	182

DHCP client configuration.....	183
DHCP client applications.....	183
Configuring the DHCP client.....	184
Examples of DHCP lease release and renew.....	185
Commands used for DHCP client maintenance.....	186
Examples of configuring DHCP client logging messages.....	186
Summary of DHCP client configuration CLI commands.....	186
LLDP configuration.....	187
Supported TLVs.....	188
Configuring LLDP.....	188
Summary of LLDP configuration CLI commands.....	189
Chapter 8: System logging.....	191
Types of logging sinks.....	191
Syslog server configuration.....	192
Defining Syslog servers.....	192
Disabling Syslog servers.....	193
Deleting Syslog servers.....	194
Displaying the status of the Syslog server.....	194
Syslog sink default settings.....	194
Syslog message format.....	195
Commands used to copy a syslog file.....	195
Configuring a log file.....	195
Disabling logging system messages to a log file.....	196
Deleting current log file and opening an empty log file.....	196
Log file message format.....	197
set logging file retention.....	197
show logging file retention.....	198
Configuring a session log.....	198
Example discontinuation of the display of system messages.....	199
Example display of session logging configuration.....	199
Session logging message format.....	199
Logging filter configuration.....	200
Commands used to set the logging filters.....	200
Severity levels.....	200
Default sink severity levels.....	201
Application filtering.....	201
Syslog server example.....	202
Log file example.....	203
Session log example.....	203
Accessing diagnostic logs.....	203
Summary of logging configuration CLI commands.....	204
Chapter 9: VoIP QoS.....	206
RTP and RTCP configuration.....	206

Header compression configuration.....	206
Header compression configuration options.....	207
Header compression support by interface.....	207
Configuring IPHC.....	207
Summary of IP Header compression CLI commands.....	209
Configuring VJ header compression.....	210
Commands used to display and clear header compression statistics.....	211
Commands used to configure QoS parameters.....	212
Commands used to configure RTCP QoS parameters.....	212
Commands used to configure RSVP parameters.....	212
Summary of QoS, RSVP, and RTCP configuration CLI commands.....	212
Weighted Fair VoIP Queuing.....	213
Summary of WFVQ configuration CLI commands.....	213
Priority queuing.....	214
Summary of priority queueing configuration CLI commands.....	214
Chapter 10: Modems interfaces	216
USB-modem interface configuration.....	216
Example of IP address to USB port assignment.....	216
The ppp authentication command parameters.....	216
Summary of CLI commands for configuring the USB port for modem use.....	217
Console port and modem configuration.....	218
Summary of CLI commands for configuring the Console port for modem use.....	218
Chapter 11: WAN interfaces	220
Serial interface overview.....	220
Layer 1 T1 port with two channel groups.....	220
E1/T1 port channel group.....	221
USP port using PPP protocol.....	221
USP port using frame relay protocol.....	222
Frame Relay multipoint topology support.....	222
Configuring the initial WAN.....	222
The Avaya MM340 E1/T1 WAN media module.....	223
Configuring Avaya MM340 E1/T1 WAN media module.....	223
E1/T1 default settings.....	225
Commands used to reset and display controller counters.....	226
Commands used to activate loopback mode on an E1/T1 line.....	226
Summary of E1/T1 ports configuration commands.....	226
Avaya MM342 USP WAN media module.....	227
Configuring Avaya MM342 USP WAN media module.....	227
USP default settings.....	229
Summary of USP port configuration commands.....	229
PPP configuration.....	230
PPPoE overview.....	231
Frame relay.....	235

Configuring frame relay.....	235
Commands used to reset and display frame relay interface counters.....	237
Summary of frame relay commands.....	237
WAN configuration and testing connectivity.....	238
Commands used for WAN configuration and testing connectivity.....	238
Summary of WAN configuration verification commands.....	239
Backup interfaces.....	239
Modem dial backup.....	241
Modem dial backup logging messages.....	253
Dialer Messages.....	253
Console messages.....	254
USB Modem Messages.....	255
PPP Messages.....	256
Summary of modem dial backup commands.....	257
ICMP keepalive.....	258
Dynamic CAC.....	261
Object tracking.....	263
Frame relay encapsulation features.....	276
Priority DLCI.....	278
Chapter 12: Emergency Transfer Relay.....	283
ETR state configuration.....	283
Activating ETR manually.....	283
Deactivating ETR manually.....	284
Restoring ETR to automatic activation.....	284
Summary of ETR commands.....	284
Chapter 13: SNMP.....	285
Agent and manager communication.....	285
SNMP versions.....	286
SNMPv1.....	286
SNMPv2c.....	287
SNMPv3.....	287
Users.....	287
Groups.....	288
Views.....	289
SNMP trap configuration.....	290
snmp-server host command parameters.....	290
Notification types.....	291
Summary of SNMP trap configuration commands.....	291
Summary of SNMP access configuration commands.....	292
Dynamic trap manager.....	293
Dynamic trap manager parameters.....	293
Summary of dynamic trap manager configuration commands.....	294
SNMP configuration examples.....	294

Chapter 14: Media encryption using AES-256	296
Screen for administering Media encryption using AES-256	296
Administering Media encryption using AES-256	296
Detailed description	297
Chapter 15: Encrypted SRTCP	298
Detailed description	298
Encrypted SRTCP	298
Screen for administering Encrypted SRTCP	298
Administering Encrypted SRTCP	299
Interactions for Encrypted SRTCP	299
Chapter 16: Contact closure	300
Configuring contact closure hardware	300
Software contact closure	301
Contact closure modes	301
Configuring contact closure software	301
Showing contact closure status	302
Summary of contact closure commands	302
Chapter 17: Announcement files	303
Uploading announcement files to a remote SCP server	303
Downloading announcement files from a remote SCP server	304
Uploading announcement files to a remote FTP server	304
Downloading announcement files from an FTP server	304
Uploading an announcement file to a USB mass storage device	305
Downloading an announcement file from a USB mass storage device	305
Uploading announcement files to a remote HTTP or HTTPS server	305
Downloading announcement files from an HTTP or HTTPS server	306
Uploading announcement files to a remote SCP server via Avaya SBC tunnel	306
Downloading announcement files from a remote SCP server via Avaya SBC tunnel	307
Erasing an announcement file from the directory	307
Renaming an announcement file in the directory	307
Displaying the announcement files stored in the directory	308
Displaying the status of a download process	308
Displaying the status of an upload process	308
Summary of announcement files commands	309
Dynamic time slots allocation	310
Summary of dynamic time slots allocation commands	310
Chapter 18: Advanced switching	311
VLAN configuration	311
VLAN Tagging	311
Multi VLAN binding	312
Gateway VLAN table	312
Ingress VLAN Security	313
ICC-VLAN	313

Configuring ICC-VLAN.....	313
VLAN configuration examples.....	313
server-blade-vlan.....	315
server-blade-oob-vlan.....	316
no server-blade-oob-vlan.....	316
show server-blade-vlan.....	316
show server-blade-oob-vlan.....	317
Summary of VLAN commands.....	317
Port redundancy.....	318
Secondary port activation.....	319
Switchback.....	319
Port redundancy configuration commands.....	319
Port redundancy configuration examples.....	320
Summary of port redundancy commands.....	320
Port mirroring.....	321
Port mirroring configuration examples.....	321
Summary of port mirroring commands.....	321
Spanning tree.....	321
Spanning tree protocol.....	322
Spanning tree per port.....	322
Rapid Spanning Tree Protocol (RSTP).....	322
Spanning tree configuration examples.....	324
Summary of spanning tree commands.....	325
Port classification.....	326
Port classification configuration examples.....	326
Summary of port classification commands.....	326
Chapter 19: Monitoring applications.....	328
RMON.....	328
RMON configuration examples.....	328
Summary of RMON commands.....	329
RTP statistics.....	330
Configuring the RTP statistics application.....	331
RTP statistics output.....	338
RTP statistics examples.....	351
Summary of RTP statistics commands.....	360
Packet sniffing.....	361
What can be captured.....	361
Roadmap for configuring packet sniffing.....	362
Configuring capture lists.....	363
Analyzing captured packets.....	372
About simulating packets.....	375
Summary of packet sniffing commands.....	376
Interface status reports.....	378

Reporting of interface status.....	378
Summary of interface status commands.....	378
Echo cancellation.....	379
Summary of echo cancellation commands.....	379
Integrated analog testing – Test and Heal.....	380
Hardware support for integrated analog testing.....	380
Types of tests.....	381
Types of test lines.....	381
Setting up a test profile.....	382
Displaying and clearing profiles.....	383
Launching and cancelling a test.....	383
Displaying test results.....	384
Healing trunks.....	384
Displaying corrections.....	384
Summary of integrated analog testing commands.....	384
Service Level Agreement Monitor Agent.....	386
Chapter 20: Router.....	387
Enabling and disabling the router.....	387
Interface configuration.....	388
Router interface concepts.....	388
Configuring an IP interface.....	389
Interface configuration examples.....	389
Summary of basic interface configuration commands.....	390
Unnumbered IP interfaces.....	391
Unnumbered IP on an interface configuration.....	392
Configuring IP on an interface configuration.....	392
Unnumbered IP examples.....	392
Summary of unnumbered IP interface configuration commands.....	393
Routing sources.....	393
Routing table configuration.....	394
Next hops.....	395
Static route types.....	395
Configuring multiple next hops.....	395
Deleting a route and its next hops.....	396
Via-interface static route.....	396
Permanent static route.....	396
Discard routes.....	397
Summary of routing table commands.....	397
GRE tunneling.....	398
Packet routing to a GRE tunnel.....	399
Prevention of nested tunneling in GRE tunnels.....	399
Optional GRE tunnel features.....	401
Setting up a GRE tunnel.....	403

GRE tunnel application example.....	404
Summary of GRE tunneling commands.....	405
DHCP and BOOTP relay.....	407
DHCP.....	407
BOOTP.....	407
DHCP/BOOTP relay.....	407
Summary of DHCP and BOOTP relay commands.....	408
DHCP server.....	409
Typical DHCP server application.....	410
Configuring the DHCP server.....	410
Deleting an IP address binding.....	413
DHCP pool configuration examples.....	413
Commands for displaying DHCP server information.....	414
Summary of DHCP Server commands.....	415
Broadcast relay.....	417
Directed broadcast forwarding.....	417
NetBIOS rebroadcast.....	417
Summary of broadcast relay commands.....	417
ARP table.....	418
Overview of ARP.....	418
Static and dynamic table entries.....	418
Adding static ARP table entries.....	419
Removing static and dynamic entries.....	419
Changing an entry in the ARP table.....	420
Summary of ARP table commands.....	420
Proxy ARP.....	420
Summary of Proxy ARP commands.....	420
ICMP errors.....	421
Summary of ICMP errors commands.....	421
Routing information protocol (RIP).....	421
RIPv1.....	422
RIPv2.....	422
RIPv1 vs. RIPv2.....	422
Prevention of routing loops in RIP.....	422
Commands used to prevent routing loops in RIP.....	422
RIP distribution access lists.....	423
Configuring a distribution access list example.....	423
RIP limitations.....	424
Summary of RIP commands.....	424
Open shortest path first (OSPF).....	426
OSPF dynamic Cost.....	426
OSPF limitations.....	427
Summary of OSPF commands.....	427

Route redistribution.....	429
Export default metric.....	430
Summary of route redistribution commands.....	430
VRRP.....	431
VRRP configuration example.....	431
Summary of VRRP commands.....	432
Fragmentation.....	433
Summary of fragmentation commands.....	434
Chapter 21: IPSec VPN.....	435
Overview of IPSec VPN configuration.....	435
IPSec VPN configuration model.....	435
Overview of IPSec VPN components.....	436
IPSec VPN components.....	436
Summary of configuration commands.....	437
Site-to-site IPSec VPN.....	439
IPSec VPN maintenance.....	454
Typical installations for IPSec VPN.....	456
Typical failover applications.....	478
Introduction to the failover mechanism.....	478
VPN keepalives.....	479
Backup peer mechanism.....	479
Failover using GRE.....	479
Redundancy and load sharing modes.....	480
Hub and spoke with hub redundancy/load sharing using GRE.....	480
Configuring VPN hub redundancy and load sharing topologies using GRE.....	481
VPN hub redundancy and load sharing topologies.....	481
VPN hub redundancy and load sharing topologies example.....	482
Failover using DNS.....	485
VPN DNS topology.....	485
Configuring the VPN DNS topology.....	485
VPN DNS topology example.....	487
Failover using a peer-group.....	490
Failover VPN topology using a peer-group.....	491
Configuring the failover VPN topology using a peer-group.....	491
Failover VPN topology using a peer-group example.....	493
Checklist for configuring site-to-site IPSec VPN.....	496
Summary of VPN commands.....	499
Chapter 22: Policy lists.....	504
Types of policy lists.....	504
Access control lists.....	504
QoS lists.....	505
QoS list parts.....	505
Allowed values on QoS fields.....	506

Use of policy-based routing.....	506
Policy list management.....	506
Policy list configuration.....	507
Creating or editing a policy list.....	507
Creating a list based on an existing list.....	507
Defining list identification attributes.....	508
Policy list attributes.....	508
Default actions.....	508
Deleting a policy list.....	509
Policy list attachments.....	509
Packets entering the interface.....	509
Packets exiting the interface.....	509
Policy lists to packets.....	509
Policy list attachment configuration.....	510
Attaching policy lists and access control lists.....	510
Attaching policy lists and QoS lists.....	510
Removing a list.....	511
Device-wide policy lists.....	511
Defining global rules.....	512
Policy rule configuration.....	512
Editing and creating rules.....	513
Policy lists rule criteria.....	513
Composite operations.....	517
Pre-configured composite operations for access control lists.....	517
Pre-configured composite operations for QoS lists.....	518
Configuring composite operations.....	519
Adding composite operation to an IP rule.....	519
Composite operation example.....	519
DSCP table.....	520
Changing an entry in the DSCP table.....	520
Policy list displays and tests.....	521
Policy list commands in context.....	521
Simulating packets.....	522
Simulated packet properties.....	523
Summary of access control list commands.....	523
Summary of QoS list commands.....	525
Chapter 23: Policy-based routing.....	529
Policy-based routing.....	529
Chapter 24: Synchronization.....	531
Defining a clock source.....	531
Setting the synchronization source.....	532
Disassociating a clock source.....	532
Enabling and disabling automatic failover and fallback.....	533

Synchronization status.....	533
Displaying synchronization status.....	533
Summary of synchronization commands.....	534
Chapter 25: TLS / Certificate Management.....	535
TLS.....	535
TLS certificate stores.....	535
Certificate validation.....	537
Mutual authentication.....	537
Chapter 26: Federal Information Processing Standards (FIPS).....	538
Federal Information Processing Standards.....	538
FIPS Security Level of the Cryptographic Module.....	538
Determining FIPS Certified Firmware is installed.....	539
FIPS Approved Mode of Operation.....	539
Prerequisites for entering FIPS Approved Mode.....	540
Determining FIPS Approved Mode is enabled.....	540
Determining Configuration is FIPS Compliant.....	540
Backup and restore of Gateway configuration.....	541
Before Enabling or Disabling FIPS Approved Mode.....	541
Enabling FIPS Approved Mode.....	542
Maintaining FIPS Approved Mode.....	542
Disabling FIPS Approved Mode.....	542
Administration procedures.....	542
FIPS-related CLI commands.....	543
Non-compliant CLI Commands in FIPS Approved Mode.....	543
Warnings for unencrypted communication in FIPS Approved Mode.....	544
Enabling FIPS Approved Mode.....	544
Disabling FIPS Approved Mode.....	549
FIPS Error States and LED Status Indicators.....	553
Power-up Testing.....	553
Error States.....	554
Zeroization Status during Error State 1.....	554
Chapter 27: Resources.....	556
Branch Gateway documentation.....	556
Finding documents on the Avaya Support website.....	556
Accessing the port matrix document.....	557
Avaya Documentation Center navigation.....	557
Training.....	559
Viewing Avaya Mentor videos.....	559
Support.....	560
Appendix A: Traps and MIBs.....	561
Branch Gateway traps.....	561
Appendix B: ASG authentication.....	574
ASG authentication CLI commands.....	574

Replacing the ASG authentication file.....	574
Appendix C: Surv-MIB files	577
Avaya-SURV-MIB files.....	577

Chapter 1: Introduction

Purpose

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

Change history

Issue	Date	Summary of changes
3	December 2024	For Release 10.2.1, added the following sections: • Public Key Authentication process on page 41 • Enabling or Disabling SSH Public Key Authentication on page 42 • Generating SSH Key Pair on Linux on page 43 • Generating SSH Key Pair on Windows on page 43 • Downloading Public Key to Branch Gateway on page 44 • Using SSH client to Connect Public Key Authentication for Linux on page 45 • Using SSH client to Connect Public Key Authentication for Windows on page 45
2	February 2024	Updated the following sections: Configuring ISAKMP policies on page 440 Configuring transform-sets on page 441
1	December 2023	10.2 Document release.

Chapter 2: Branch gateway network configurations

Basic configuration

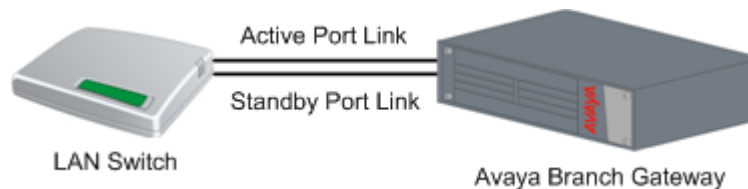
You can deploy the Branch Gateway basic configuration in a LAN. The basic configuration does not support redundancy. You can connect Branch Gateway to an external LAN switch using one of the two Ethernet LAN ports located on the front panel of the gateway.



Port redundancy configuration

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

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



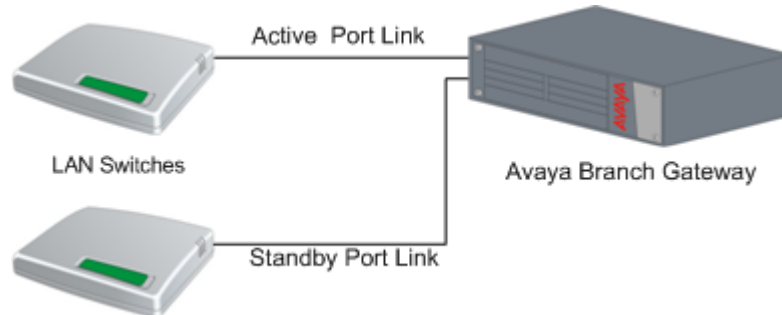
Related links

[Port redundancy](#) on page 318

Port and switch redundancy configuration

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

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



Related links

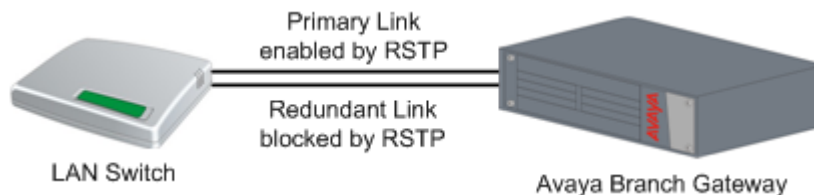
[Port redundancy](#) on page 318

Rapid spanning tree protocol configuration

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

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

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



Related links

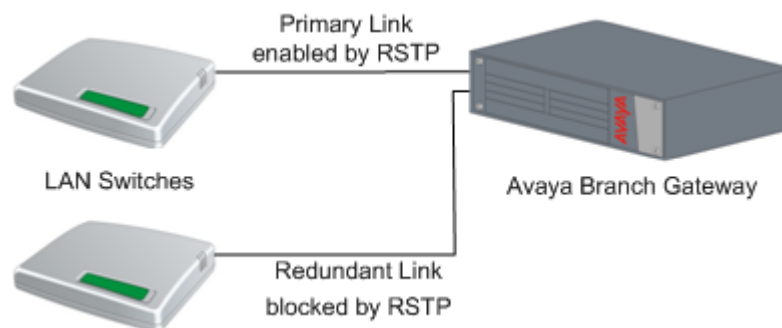
[Spanning tree](#) on page 321

RSTP and switch redundancy configuration

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

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

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



Related links

[Spanning tree](#) on page 321

Chapter 3: Configuration overview

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

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

Configure Branch Gateway based on different access methods. For more information on the initial branch gateway configurations, see the *Deploying and Upgrading Avaya G430 or G450 Branch Gateway Guide*.

Defining the Console interface

About this task

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

Procedure

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

Note:

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

Example

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

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

Defining the USB-modem interface

About this task

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

Procedure

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

Example

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

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

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

Other interfaces

Your system specifications might require that you define other interfaces.

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

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

Related links

[Defining an interface](#) on page 63

Define other interfaces

You can perform most Branch Gateway configuration tasks using the Branch Gateway CLI. To define other interfaces, you must first define a PMI and then register the Branch Gateway with an MGC.

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

Related links

[Primary Management Interface \(PMI\) configuration](#) on page 64

[Branch Gateway Controller configuration](#) on page 66

Configuration using CLI

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

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

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

Related links

[CLI access](#) on page 29

Configuration changes and backup

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

- Running configuration
- Startup configuration

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

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

 Note:

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

Saving configuration changes and backing them up

Procedure

1. To save changes to the configuration of the Branch Gateway, enter `copy running-config startup-config` or `copy edge running-config startup-config`

A copy of the running configuration becomes the new startup configuration.

2. Back up either the running configuration or the startup configuration to a FTP, TFTP, SCP, or an HTTPS server on your network, or to a USB flash drive.

Firmware version control

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

- Bank A
- Bank B

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

To switch to an older version of the firmware, enter `set boot bank bank-x`.

Related links

[Software and firmware upgrades](#) on page 82

Using an older version of firmware

About this task

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

Procedure

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

Chapter 4: Branch Gateway access

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

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

CLI access

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

You can use the following methods to access CLI:

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

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

Logging to CLI

Procedure

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

Related links

[Login permissions](#) on page 34

CLI contexts

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

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

Entering the Loopback interface

Procedure

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

* Note:

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

Using CLI help

About this task

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

Procedure

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

Specifically:

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

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

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

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

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

Example

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

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

CLI access using the local network

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

Accessing CLI locally using a computer

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

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

Accessing Branch Gateway through the Services port

About this task

You can access CLI locally using a computer.

Procedure

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

Note down any change to IP addresses, DNS servers, or WINS entries you change when configuring your laptop.

4. Set the IP address of SSH to 192.11.13.6.

Note:

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

CLI access using modems

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

Accessing CLI using a USB modem

Procedure

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

Related links

[USB-modem interface configuration](#) on page 216

[Login permissions](#) on page 34

[Summary of CLI commands for configuring the USB port for modem use](#) on page 217

USB port settings

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

Branch Gateway serial modems

The Branch Gateway supports the following serial modems:

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

Accessing the CLI using a serial modem

Procedure

1. Connect a modem to the Console port on the front panel of the Branch Gateway.
Use an RJ-45 serial cable to connect the modem.
2. Make sure the Console port is properly configured for modem use.
3. From the remote computer, create a dialup network connection to the Branch Gateway.
Use the TCP/IP and PPP protocols to create the connection. Configure the connection according to the configuration of the COM port of the remote computer. By default, the Branch Gateway uses PAP authentication. If your network has a RADIUS server, you can use RADIUS authentication for the PPP connection.
4. Open any standard telnet program on the remote computer.
5. Open a telnet session to the IP address of the Console port on the Branch Gateway.
6. Configure the serial connection on the remote computer to match the configuration of the Console port on the Branch Gateway.

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

CM access

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

You can access CM with any of the following tools:

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

Related links

[Branch Gateway Controller configuration](#) on page 66

Security overview

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

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

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

Login permissions

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

User account management

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

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

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

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

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

Related links

[CLI access](#) on page 29

[CLI access using modems](#) on page 31

Privilege level

When you access CLI, you must enter a username. An administrator assigns a privilege level to each username. 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, Read-write, Admin.

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

Creating a username, password, and privilege level

About this task

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

* Note:

The administrator can force a new user to change the password on their first login by using the following command: **login authentication change-password-on-first-login**.

Procedure

At the command prompt, type the following:

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

Example

```
g450ab2-025(super)# username john access-type read-write
Enter new password: *****.
Confirm password: *****.
User account added.
g450ab2-025(super)#
```

Changing user privileges

About this task

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

Procedure

1. At the command prompt, type:

```
no username <the username>
```

2. At the command prompt, type **username** <the username> **access-type** <access type>

Example:

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

Commands to regulate password length and content

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

- **login authentication min-password-length**
- **login authentication min-password-digit-chars**
- **login authentication min-password-lower-chars**
- **login authentication min-password-upper-chars**

- `login authentication min-password-special-chars`
- `login authentication max-password-class-repeated-chars`
- `login authentication max-password-repeated-chars`

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

Commands used to manage password lockout and disabling

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

- `login authentication lockout`
- `login authentication inactivity-period`

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

Password expiry management

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

Changing a password

About this task

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

Procedure

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

Result

The new password you enter must match the password policies.

Commands used to display user account information

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

- `show username`

- `show login authentication`

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

User accounts CLI commands

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

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

Table continues...

Command	Description
login authentication max-password-class-repeated-chars	Set the maximum number of consecutive characters of the same class (uppercase, lowercase, digits, symbols) in a password (default not checked).
password	Change the password of a user account.
show login authentication	View the login authentication settings and information. This includes information about the configured lockout period, inactivity period, expiration period, password length, and characters that must be included in the password.
show username	Display information about the local user accounts.
username	Add or remove a local user account.

Login authentication

Examples for displaying Login authentication information

Procedure

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

For example:

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

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

 Note:

ASG authentication file is no longer supported from Release 7.1.2. This command is only used to verify if an ASG authentication file is available before downgrading to a previous release.

For example:

```
(super)# show auth-file info
Authentication File (AF) information:
```

```
AF-ID :7000012345
Date/time : 15:02:27 23-AUG-2015
Major release : 6.x
```

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

For example:

```
(super)# show username
User          Access  Account  Active
account       level   type
-----
root          admin   local    yes
snmpv3        admin   local    yes
craft         admin   Services yes
inads         tech    Services yes
init          dev     Services yes
rasaccess     read-only Services no
sroot         dev     Services yes
```

4. View EASG status using **EASGstatus**

For example:

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

5. View the services users status using **EASGManage listUsers**

For example:

```
G430-ab-006(super)#EASGManage listUsers
User name      Enabled  Locked
-----
craft          yes      no
inads          yes      no
init           yes      no
rasaccess      no       no
sroot          yes      no
```

Examples of configuring Login authentication

You can perform the following login configurations:

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

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

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

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

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

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

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

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

SSH protocol support

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

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

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

Note:

SSH supports IPv4 and IPv6.

Password authentication process

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

Enabling SSH on Branch Gateway

Procedure

1. Enter `ip ssh` to enable SSH authentication.

SSH is enabled by default.

2. (Optional) Use the `crypto key generate rsa key-size 2048` or `crypto key generate ecdsa key-size 256(or 384, 512)` to configure the server auth-key

Disabling SSH on Branch Gateway

Procedure

1. Use the `disconnect ssh` command to disconnect an existing SSH session.
2. Use the `no ip ssh` command to disable the SSH server that disconnects all active SSH sessions.
3. Use the `show ip ssh` command to display information on SSH configuration in addition to information about any active SSH sessions.

Public Key Authentication process

- The Branch Gateway also supports the SSH Public Key Authentication process which allows a user to login using a public/private pair of keys with more cryptographic strength than passwords. The public key is downloaded and associated with a Branch Gateway user account. The private key, also called the identity, is used to authenticate access to the Branch Gateway user account. Therefore, with this method, it is very important to protect access to this private key with an embedded password and/or access for only approved users.
- With Public Key Authentication on Branch Gateway, it is important to remember that the key pairs are associated with a Branch Gateway local users created by default (For example, root) or with the `username` command. This should not be confused with the user names on the client system (For example, Linux or Windows) where the keys were created or where the SSH client resides.
- The Branch Gateway supports public key files (i.e. `authorized_keys` files) in the OpenSSH format. This key format has the fields in the table below delimited by whitespace. All SSH `authorized_keys` options used for advanced features (For example, set environment variable, execute command, and more) are ignored.

Key Field	Description	Examples
#	Any line starting with the “#” character is a comment that is ignored.	# BGW1 root authorized_key file

Table continues...

Key Field	Description	Examples
Key Type	A known string describing the type of key.	ssh-rsa ecdsa-sha2-nistp256 ecdsa-sha2-nistp384 ecdsa-sha2-nistp521
Key Text String	The public key in BASE64 format.	AAAAE2VjZHNh AzRQM=
Key Comments	User defined comments about the key.	BGW1-root-key
Example <pre># BGW1 root authorized_key file ecdsa-sha2-nistp256 AAAAE2VjZHNh AzRQM= BGW1-root-key</pre>		

- The file system space reserved for all the public keys is limited to 128KB. This prevents any possible conflict with other Branch Gateway features sharing this space such as announcements.

Using the Public Key Authentication

Following are the methods to use the public key authentication:

1. [Enabling or Disabling SSH Public Key Authentication](#) on page 42
2. [Generating SSH Key Pair on Windows](#) on page 43 or [Generating SSH Key Pair on Linux](#) on page 43
3. [Downloading Public Key to Branch Gateway](#) on page 44.
4. [Using SSH client to Connect Public Key Authentication for Linux](#) on page 45 or [Using SSH client to Connect Public Key Authentication for Windows](#) on page 45

Enabling or Disabling SSH Public Key Authentication

About this task

This topic gives instruction on how to enable or disable SSH public key authentication along with example.

Procedure

1. Enter **show ssh-server-configuration** to see current state of Public Key Authentication
2. Enter **ssh-server-configuration** to enter context menu for SSH server configuration.
3. Enter **set pubkey-authentication on** to enable Public Key Authentication (or **off** to disable).
4. Enter **exit** to leave sub-menu for SSH server configuration.
5. Enter **copy running-config startup-config** to save configuration changes.
6. Enter **reset** to load new configuration; or, if logged in from console, restart the SSH server with the **no ip ssh** command followed by the **ip ssh** command.

Next steps

[Generating SSH Key Pair on Linux](#) on page 43 or [Generating SSH Key Pair on Windows](#) on page 43

Generating SSH Key Pair on Linux

About this task

This topic gives instructions on how to generate SSH key pair on Linux along with an example.

Before you begin

- You must enable SSH public key authentication.

Procedure

1. Use **ssh-keygen** command to generate key pair.

The filename (-f) and comment (-C) options should be used to specify useful information about the key files.

```
ssh-keygen -t rsa-sha2-512 -b 2048 -f bgw1-root-key -C bgw1-root-  
rsa-sha2-512-2048
```

2. Do one of the following:

- a. To generate a private key using password, enter the password which is associated with the private key and again enter the password for confirmation.
- b. To generate a private key without using password, press **Enter** button twice.

Result

The process generates the key pair.

bgw1-root-key is for Private key.

bgw1-root-key.pub is for Public key.

Next steps

[Downloading Public Key to Branch Gateway](#) on page 44

Generating SSH Key Pair on Windows

About this task

This topic gives instructions on how to generate SSH key pair on Windows along with an example.

Before you begin

- You must enable SSH public key authentication.

Procedure

1. Run PuTTY Key Generator (PuTTYgen).
2. For **Type of key to generate**, select either RSA or ECDSA.
3. For RSA, enter **Number of bits in generated key**

4. For ECDSA, enter **Curve to use for generating this key**
5. Select **Generate** and move cursor in random pattern within PuTTYgen window until key is generated.
6. (Optional) Change comment for the key.
7. (Optional) Enter a password for the private key; or leave the fields blank for a passwordless private key.
8. Select **Save public key** and provide a name for the public key (For example, bg1-root-key.putty).
9. Select **Save private key** and provide a name for the private key (For example, bg1-root-key.ppk).
10. Select **Conversions/Export OpenSSH key** and save a new public key file (For example, bg1-root-key.putty2).
11. Copy this new key to a Linux server and use ssh-keygen to generate an OpenSSH format used by the Branch Gateway.

```
ssh-keygen -y -f bg1-root-key.putty.2 > bg1-root-key.pub
```
12. An Alternative to step [10](#) on page 44 and [11](#) on page 44, copy the Putty public key and manually create an OpenSSH key with a text editor.

This file has the format as mentioned in the [table](#) on page 41.

Next steps

[Downloading Public Key to Branch Gateway](#) on page 44

Downloading Public Key to Branch Gateway

About this task

This topic gives instructions on how to download public key to Branch Gateway.

Before you begin

- You must enable SSH public key authentication.
- You must generate SSH key pair on Linux or Windows.

Procedure

Enter **copy scp authorized-keys to download keys** for a certain user (or use HTTPS or USB).

```
copy scp authorized-keys root keys/bgw1-root-key.pub 192.168.1.10
ssh-server-configuration
ssh-server-configuration):# show authorized-keys root verbose
exit
```

Next steps

[Using SSH client to Connect Public Key Authentication for Linux](#) on page 45 or [Using SSH client to Connect Public Key Authentication for Windows](#) on page 45

Using SSH client to Connect Public Key Authentication for Linux

Before you begin

- You must enable SSH public key authentication.
- You must generate SSH key pair on Linux or Windows.
- You must download public key to Branch Gateway.

Procedure

Use SSH client to connect using Public Key Authentication (Linux).

```
> ssh -i keys/bgw1-root-key root@192.168.1.20
```

Using SSH client to Connect Public Key Authentication for Windows

About this task

This topic gives instructions on how to use SSH client to Connect Public Key Authentication for Windows.

Before you begin

- You must enable SSH public key authentication.
- You must generate SSH key pair on Linux or Windows.
- You must download public key to Branch Gateway.

Procedure

1. Create a Putty session by specifying the IP address, Port, and SSH type.
 - **Host Name (or IP address):** 192.168.1.20
 - **Port:** 22
 - **Connection type:** SSH
2. Select Connection/Data. Enter the Branch Gateway username associated with the key.

Auto-login username: root
3. Select Connection/SSH/Auth/Credentials tab. Select Putty private key file (or use Pagent to load the private key).

Private key file for authentication: C:\bgw1-root-key.ppk
4. Select Session and Save the profile. Select Open to open the SSH session and enter password for the private key if necessary.

Saved Sessions: bgw1-root-pka

Summary of SSH configuration commands

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

SCP protocol support

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

The process of establishing an SCP session is the same process as described in [SSH protocol support](#) on page 40, except that the roles of Branch Gateway and the client computer are reversed.

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

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*.

Using RADIUS authentication

Procedure

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

RADIUS authentication configuration commands

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

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

Special security features

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

Commands used to configure Telnet access

The Telnet protocol is disabled by default. You can enable and disable the Branch Gateway's ability to establish incoming and outgoing Telnet connections using the following commands. These commands are secured commands and are not displayed together with the running configuration (using the `show running-config` command). To see the status of these commands, use the `show protocol` command.

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

Telnet access configuration commands

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

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

Gateway secret management

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

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

Note:

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

Configuring the Master Configuration Key

Procedure

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

Result

The new MCK is now in effect.

DoS attacks

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

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

SYN attack

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

The SYN attack is characterized by the following pattern:

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

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

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

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

SYN cookies

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

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

- Not maintaining any state for half-open inbound TCP sessions, thus preventing the SYN attack from depleting memory resources.

SYN cookies can maintain no state for half-open connections by responding to SYN requests with a SYN-ACK that contains a specially crafted initial sequence number (ISN), called a cookie. The value of the cookie is not a pseudo-random number generated by the system, but the result of a hash function. The hash result is generated from the source IP, source port, destination IP, destination port, and some secret values. The cookie can be verified when receiving a valid third ACK that establishes the connection. The verification ensures

that the connection is a legitimate connection and that the source IP address was not spoofed.

- Employing the SYN cookies method at a lower point in the network stack than 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.

SYN attack notification

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

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

Commands used to maintain SYN cookies

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

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

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

SYN cookies configuration commands

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

Command	Description
<code>clear tcp syn-cookies counters</code>	Clear the SYN cookies counters

Table continues...

Command	Description
<code>show tcp syn-cookies</code>	Show SYN cookies statistics for inbound TCP connections
<code>tcp syn-cookies</code>	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 and VPN devices can be at risk for DoS attacks. The Branch Gateway identifies predefined or custom-defined traffic patterns as suspected attacks and generates SNMP notifications, referred to as Managed Security Services (MSS) notifications.

MSS reporting mechanism

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

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

Note:

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

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

Related links

[Syslog server configuration](#) on page 192

[Viewing QoS traps, QoS fault traps, and QoS clear traps](#) on page 345

Configuring MSS

About this task

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

Procedure

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 CM, see Avaya Aura[®] Communication Manager documentation.

DoS attack classifications

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

DoS Attack	Description
LAND_ATTACK	Land attack packets with the source IP the same as an IP address
TCP_URGENT_ATTACK	TCP packets with the URGENT option set
ICMP_RATE_LIMIT	ICMP (echo) requests exceeding a pre-defined rate
SMURF_ATTACK	ICMP echo packets with limited broadcast destination address
FRAGGLE_ATTACK	UDP packets with limited broadcast destination address
SYN-FLOOD	The number of unacknowledged TCP SYN-ACK exceeds a predefined rate
UNREACHABLE_PORT_ATTACK	TCP/UDP IP packets sent to unreachable ports
MALFRAGMENTED_IP	Malfragmented IP packets on TO-ME interfaces
MALFORMED_IP	Malformed IP packets. The Branch Gateway reports malformed IP packets when: • The IP version in the IP header is a value other than 4 • The IP header length is smaller than 20 • The total length is smaller than the header length
MALFORMED_ARP	ARP messages with bad opcode
SPOOFED_IP	For all routable packets, the Branch Gateway report reception of IP spoofed packets
UNKNOWN_L4_IP_PROTOCOL	Packets with unknown (unsupported or administratively closed) protocol in IP packet with TO-ME interface as a destination
UNAUTHENTICATED_ACCESS	Failure to authenticate services

Custom DoS classifications

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

Related links

[Policy lists](#) on page 504

Examples for defining a DoS class using ACLs

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

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

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

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

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

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

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

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

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

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

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

- Use the following example to exit the ACL rule:

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

- Use the following example to exit the ACL:

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

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

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

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

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

Related links

[Policy lists rule criteria](#) on page 513

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
-----
1       icmp      Src Any
      Any      Dst 255.255.255.255  Host         Any Type     Deny-Notify
      Any      Any Code        No
Dos classification: smurf
Deflt   Any      Src Any
      Any      Dst Any
      Any      Any
Gxxx-001(super-ACL 301)# exit
Gxxx-001(super)# interface vlan 203
//activate Access Control list 301 for incoming packets on interface vlan 203:
Gxxx-001(super-if:VLAN 203)# ip access-group 301 in
Done!
```

MSS configuration CLI commands

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

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

Table continues...

Command	Description
<code>show snmp</code>	Display SNMP configuration information
<code>snmp-server dynamic-trap-manager</code>	Modify the SNMP settings of the dynamic trap manager
<code>snmp-server group</code>	Define a new SNMPv3 group, or configure settings for the group
<code>snmp-server host</code>	Identify an SNMP management server, and specify the kind of messages it receives
<code>snmp-server user</code>	Configure settings for an SNMPv3 user

Enhanced Access Security Gateway (EASG)

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

Managing EASG

Enabling EASG authentication

About this task

You can enable the EASG authentication for all Avaya logins.

Before you begin

Login to the application CLI interface.

Procedure

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

```
EASGManage enableEASG
```

The system displays the following message:

```
By enabling Avaya Logins you are granting Avaya access to your
system. This is necessary to maximize the performance and value
of Avaya support entitlements, allowing Avaya to resolve product
issues in a timely manner.
```

```
In addition to enabling the Avaya Logins, this product should
be registered with Avaya and technically onboarded for remote
connectivity and alarming. Please see the Avaya support site
(support.avaya.com/registration) for additional information for
registering products and establishing remote access and alarming.
Do you want to continue (Y/N)?
```


2. When the system prompts, type `Y`.

The system displays the following message:

```
EASG is Enabled.
Done!
```

Disabling EASG authentication

About this task

You can disable the EASG authentication for all Avaya logins.

Before you begin

Login to the application CLI interface.

Procedure

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

```
EASGManage disableEASG
```

The system displays the following message:

```
By disabling Avaya Logins you are preventing Avaya access to your
system.
This is not recommended, as it impacts Avaya's ability to provide
support
for the product. Unless the customer is well versed in managing
the
product themselves, Avaya Logins should not be disabled.
Do you want to continue (Y/N)?
```

2. When the system prompts, type `Y`.

The system displays the following message:

```
EASG is disabled.
Done!
```

Enabling EASG authentication for specified user

About this task

You can enable the EASG authentication for a specified user.

Before you begin

Login to the application CLI interface.

Procedure

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

```
EASGManage enable {user}
```

The system displays the following message:

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

2. When the system prompts, type `Y`.

The system displays the following message:

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

Disabling EASG authentication for specified user

About this task

You can disable the EASG authentication for a specified user.

Before you begin

Login to the application CLI interface.

Procedure

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

```
EASGManage disable {user}
```

The system displays the following message:

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

2. When the system prompts, type `Y`.

The system displays the following message:

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

Viewing available EASG users list

About this task

You can view the available EASG users list.

Before you begin

Login to the application CLI interface.

Procedure

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

```
EASGManage listUsers
```

The system displays the available EASG users list.

Viewing EASG product certificates

Viewing EASG product certificate information

About this task

You can view the EASG product certificate information.

Before you begin

Login to the application CLI interface.

Procedure

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

EASGProductCert

The system displays the following message:

```
Subject:          CN=G450 Media Gateway 7.1.2, OU=EASG, O=Avaya Inc.
Serial Number:    10023
Start Date:       Jul 27 23:04:02 2017 GMT (-60 days)
Expiration Date:  Jul 27 04:00:00 2032 GMT (5418 days)
Trust Chain:
  1. O=Avaya, OU=IT, CN=AvayaITrootCA2
  2. DC=com, DC=avaya, DC=global, CN=AvayaITserverCA2
  3. O=Avaya Inc, OU=EASG, CN=EASG Intermediate CA
  4. CN=Product EASG Intermediate CA, OU=EASG, O=Avaya Inc.
  5. CN=G450 Media Gateway 7.1.2, OU=EASG, O=Avaya Inc.
```

Managing EASG site certificates

Copying and installing EASG site certificate using scp

About this task

You can copy and install EASG site certificate using scp.

Before you begin

Login to the application CLI interface.

Procedure

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

EASGSiteCertManage copy scp {filename} {ip-address}

The system copies and installs EASG site certificate.

Copying and installing EASG site certificate using usb device

About this task

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

Before you begin

Login to the application CLI interface.

Procedure

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

```
EASGSiteCertManage copy usb usb-device filename
```

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

Deleting installed EASG site certificate

About this task

You can delete the installed EASG site certificate.

Before you begin

Login to the application CLI interface.

Procedure

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

```
EASGSiteCertManage delete {installed_pkcs7_name | all}
```

The system deletes the installed site certificate

Viewing valid EASG site certificates list

About this task

You can view the valid EASG site certificates list.

Before you begin

Login to the application CLI interface.

Procedure

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

```
EASGSiteCertManage list
```

The system displays the following message:

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

Viewing valid installed EASG site certificate information

About this task

You can view the valid installed EASG site certificate information.

Before you begin

Login to the application CLI interface.

Procedure

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

```
EASGSiteCertManage show {installed_pkcs7_name}
```

The system displays the following message:

```

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

```

Viewing EASG status

Viewing EASG status

About this task

You can view the EASG status is enabled or disabled.

Before you begin

Login to the application CLI interface.

Procedure

To view the EASG status, run the command:

```
EASGStatus
```

The system displays the following message:

```
EASG is Enabled.
```

Viewing product id

About this task

You can view the product id.

Before you begin

Login to the application CLI interface.

Procedure

To view the product id, run the command:

```
product-id
```

The system displays the following message:

```
39ad6805e054169a3da624581fd40976
Done!
Done!
```

Service logins with Enhanced Access Security Gateway (EASG) authentication

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

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

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

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

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

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

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

Chapter 5: Basic device configuration

Basic device configuration enables you:

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

Defining an interface

About this task

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

Procedure

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

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

For example:

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

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

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

Primary Management Interface (PMI) configuration

The 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.
- Uploading and downloading files and software images using SCP, HTTPS, FTP and TFTP protocols.

The first IP address you configure on the Branch Gateway automatically becomes the PMI.

You can later designate any of the Branch Gateway's interfaces to serve as the Branch Gateway's PMI. The PMI can be of IPv4 or IPv6 address type. If you are not sure which interface to use as the PMI, check with your system administrator.

Setting the PMI of the Branch Gateway

About this task

Use this procedure to set the PMI of the Branch Gateway.

Procedure

1. Type the **interface** command to enter the interface context 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 is not defined, define it at this step.

2. Type one of the following:
 - **pmi** for an IPv4 PMI.
 - **pmi6** for an IPv6 PMI.
3. To return to the general context, type 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 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 the general context.

If you use this command before you reset the Branch Gateway, the following occurs:

- **Active PMI**, **Active PMI6**, and **Configured PMI** display.
- Active and the Configured PMI must be the same IP address.

Active and configured PMI

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

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

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

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

PMI configuration CLI commands

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

Root level command	Command	Description
interface (fastethernet serial tunnel vlan loopback dialer)	-	Enter configuration mode for the FastEthernet, Serial, 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

Table continues...

Root level command	Command	Description
<code>set system location</code>	-	Set the location information for this Branch Gateway system
<code>set system name</code>	-	Set the name of the Branch Gateway system
<code>show pmi</code>	-	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 shows how to configure the IP address 132.55.4.45 as the default gateway:

```
ip default-gateway 132.55.4.45
```

Example

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

```
ip default-gateway serial 3/1:1
```

Example

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

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

Branch Gateway Controller configuration

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

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

Release 7.1 and later support the following commands:

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

Media Gateway supports the following new enhancements from Release 10.1:

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

Locating the Branch Gateway serial number

About this task

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

Procedure

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

Survivability and migration options

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

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

Note:

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

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

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

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

 Note:

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

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

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

Related links

[Standard Local Survivability \(SLS\)](#) on page 98

[Modem dial backup](#) on page 241

MGC list configuration

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

- `set mgc list`: Create a list of valid MGCs.

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

Branch Gateway MGC settings

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

You can also use FQDN for the MGC list.

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

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

Note:

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

Related links

[Standard Local Survivability \(SLS\)](#) on page 98

Example of setting Branch Gateway MGC

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

```
Gxxx-001(super)# set mgc list 135.6.8.99+2001:db8::370:7334,135.34.54.2,2001:db8::1428:57ab
Done!
```

Results from the set mgc list command

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

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

Showing the current MGC list

About this task

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

Procedure

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

Example

To view media gateway controller configured for Enterprise Mode:

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

PRIMARY MGC HOST, Primary Search Time : 1 min(s)
IPv4 Address      IPv6 Address
-----
-- Not Available -- 100:0:0:0:0:0:803

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

sls disabled

Done!
```

To view media gateway controller configured for Edge Mode:

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

PRIMARY MGC HOST, Primary Search Time : 1 min(s)
-----
sbc@productidDC1.customerid.avayacloud.com

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

Changing the MGC list

Procedure

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

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

About setting reset times

If the connection between Branch Gateway and the registered MGC is lost, Branch Gateway attempts to recover the connection. Use the **set reset-times primary-search** command and the **set reset-times total-search** command to set the timeout for the Branch Gateway's search for the primary MGC and the other MGCs on its MGC list, respectively. Use the **set reset-times transition-point** command to configure the point at which the primary MGCs in the list end and the LSPs or ESSs 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 must 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. After 40 minutes branch gateway drops all the calls, resets the media modules, and searches for all the MGCs on a round-robin basis from the list.

Accessing the registered MGC

Procedure

Access the MGC according to the following:

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

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

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

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

Use the **session mgc** on an S8300D running VSP.

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

For example:

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

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

For example:

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


H.248 Registration Source Port

With the following CLI commands, you can define or view the source port range that the gateway uses to register to Communication Manager:

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

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

In Edge mode, if the registration source port range is configured to use a small range of ports, the gateway might fail to register with Communication Manager after a gateway reboot. For example, use the command `set registration source-port-range 1024 1025` for specifying the port range.

Use as wide a range as possible when using the `set registration source-port-range` command or use the `set registration default source-port-range` command to define the source port range.

ICC or Survivable Remote Server monitoring

The gateway uses an internal heartbeat to monitor the S8300 servers status condition when an S8300 server is inserted in the Branch Gateway.

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

Summary of MGC list configuration commands

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

Command	Description
<code>clear mgc list</code>	Remove one or more MGCs from the MGC list
<code>set icc-monitoring</code>	Enable or disable heartbeat monitoring of an MGC in ICC or Survivable Remote Server mode
<code>set mgc list</code>	Create a list of valid Media Gateway Controller(s)
<code>set reset-times</code>	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

Table continues...

Command	Description
<code>show icc-monitoring</code>	Display the status of the ICC/Survivable Remote Server monitoring process
<code>show mgc</code>	Display the state and setup parameters of the currently active MGC
<code>show mgc list</code>	Display the IP addresses of the MGCs on the MGC list
<code>show recovery</code>	Show the Branch Gateway connection recovery setup

DNS resolver

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

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

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

Related links

[IPSec VPN](#) on page 435

DNS resolver features

Branch Gateway supports the following DNS resolver features:

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

Note:

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

- FastEthernet with PPPoE
- Dialer interface
- Serial interface

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

Related links

[Configuring the DHCP client](#) on page 184

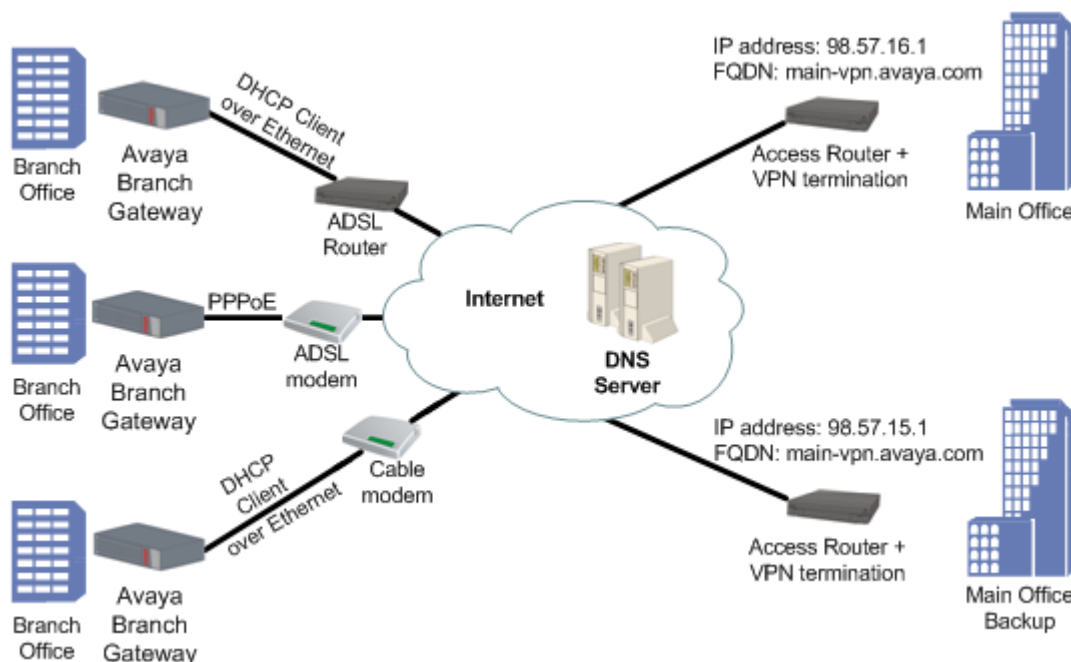
Typical DNS resolver application – VPN failover

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

The VPN branch office(s) connect to two main offices (the VPN remote peers) that are configured *with the same FQDN name*, but have different IP addresses. When a branch office makes a DNS query to resolve the VPN remote peer name to an IP address, it receives a list with the IP addresses of both main offices, selects the first one, and builds a VPN tunnel with it. If the first main office fails, the branch office sends another DNS query, and receives the IP address of the second main office in reply. It will then start a VPN tunnel with the second main office.

* Note:

VPN is supported in IPv4 only.



Related links

[Failover using DNS](#) on page 485

Configuring DNS resolver

Procedure

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

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

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

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

3. Add a DNS server to the DNS servers list using the **name-server** command.

- Assign an index number that ranks the DNS server by priority.
- Specify the IP address of the DNS server.

4. Repeat Step 3 to configure additional DNS servers in the list.

You can configure up to six DNS servers.

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

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

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

- Assign an index number that ranks the domain name by priority.
- Specify the domain name.

6. Repeat Step 5 to configure additional domain names.

You can configure up to six domain names.

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

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

The default value is 2.

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

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

The default value is 3 seconds.

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

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.
- For PPP, enable automatic discovery of DNS servers by entering **ppp ipcp dns request**.

Example

```
ip domain name-server-list
description
name-server 1
.
.
name-server 6

ip domain list 1
.
.
ip domain list 6

ip domain retry

ip domain timeout

show ip domain

ip domain lookup
```

DNS resolver configuration example

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

```
Gxxx-001(config)# ip domain name-server-list 1
Gxxx-001(config-name-server-list:1)# description "All DNS servers"
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.

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.

Related links

[System logging](#) on page 191

DNS resolver configuration commands

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

Root level command	Second level command	Description
<code>clear ip domain statistics</code>	-	Clear the DNS resolver's statistics counters
<code>interface {dialer serial console FastEthernet USB-modem}</code>	-	Enter the interface configuration mode for a Dialer, Serial, Console, FastEthernet, or USB-modem interface
-	<code>ppp ipcp dns request</code>	Enable or disable requesting DNS information from the remote peer during the PPP/IPCP session

Table continues...

Root level command	Second level command	Description
<code>ip domain list</code>	-	Specify static domain names (suffixes) to complete non-FQDN names (hostnames that do not end with a dot)
<code>ip domain lookup</code>	-	Enable or disable the DNS resolver
<code>ip domain name-server-list</code>	-	Enter the context of the DNS servers list, or set up the list
-	<code>description</code>	Set a name for the DNS servers list
-	<code>name-server</code>	Add a DNS server to the list of up DNS servers
<code>ip domain retry</code>	-	Set the number of retries for a DNS query
<code>ip domain timeout</code>	-	Set the timeout for a DNS query
<code>nslookup</code>	-	Resolve a hostname to an IP address
<code>show ip domain</code>	-	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.
<code>show ip domain statistics</code>	-	Display the DNS resolver's statistics counters
<code>show protocol</code>	-	Display the status of a specific management protocol, or all protocols

Device status viewing

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

The show mm command

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

- Slot number
- Uptime
- Type of media module

- Description
- Serial number and other hardware identification numbers
- Firmware version
- Number of ports
- Fault messages

The show module and show mg list config commands

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

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

Device status commands

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

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

OOB

oob-interface configuration

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

 Note:

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

no oob-interface

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

 Note:

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

show oob-interface

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

set non-oob-interfaces access

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

 Note:

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

Software and firmware management

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

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

File transfer

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

- Install software and firmware upgrades on Branch Gateway
- Install firmware upgrades on media modules
- Backup and restore configuration settings

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

Note:

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

Software and firmware upgrades

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

- Firmware for Branch Gateway
- Firmware for media modules

Note:

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

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

Firmware bank management

The Branch Gateway has two firmware banks:

- Bank A
- Bank B

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

Displaying firmware versions in the banks

Procedure

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

Bank management changes

By default, when you turn on or reset the Branch Gateway, the Branch Gateway loads firmware from Bank B. To change the default bank from which firmware is loaded during startup, use the `set boot bank` command. For example, to configure the Branch Gateway to load firmware from Bank A on startup, enter `set boot bank bank-A`. Now, when you reset the Branch Gateway, it will load firmware from Bank A.

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

Loading firmware from the non-default bank

About this task

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

Procedure

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

Result

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

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

To upgrade software or firmware, you must obtain an upgrade file from Avaya. Place the file on your SCP, FTP, TFTP, or HTTPS server. Then, use one of the following commands to upload the file to Branch Gateway. For each of these commands, include the full path of the file and the IP

address of the SCP, FTP, TFTP, or HTTPS host as parameters. When you enter the command, the CLI prompts you for a username and password.

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

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

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

```
copy tftp module \version\mm710v3.fdl 192.1.1.10 2
```

Example

The following example downloads a firmware version with the path and file name C:\g450_sw_41_24_0.bin from an FTP server with the IP address 149.49.134.153 to Bank A of Branch Gateway.

```
copy ftp SW_imageA C:\g450_sw_41_24_0.bin 149.49.134.153
```

Example

The following example downloads a firmware version with the path and file name C:\g450v4_sw_41_24_0.bin from an FTP server with the IP address 149.49.134.153 to Bank A of Branch Gateway.

```
copy ftp SW_imageA C:\g450v4_sw_41_24_0.bin 149.49.134.153
```

Example

The following example downloads a firmware version with the path and file name C:\g450v4_sw_41_24_0.bin from an SCP server with the IP address 149.49.134.153 to Bank A of Branch Gateway.

```
copy scp SW_imageA g450/g450v4_41_24_0.bin 172.16.1.22
```

* Note:

The G450 hardware vintage 4 uses a different software image. The filename starts with g450v4_sw. G450 hardware vintage 1 to 3 use a software image starting with g450_sw.

Example

The following example downloads the software image file, g450_sw_41_44_0.bin (for G450 or G430 hardware vintage 1.x, 2.x, 3.x) from the HTTPS server with URL my.webserver.com with the username dan:

```
g450-025(super)# copy http SW_imageA https://dan@my.webserver.com/images/
g450_sw_41_44_0.bin
Enter WebServer Password:Resolving hostname to IP address
Press any key to stop the operation
```

Upgrading software and firmware using a USB mass storage device

About this task

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

Procedure

1. Obtain an upgrade file from Avaya and place it on your PC.
2. Insert the USB mass storage device into the PC's USB port, and copy the software or firmware file(s) to the USB mass storage device.
3. Remove the USB storage device from the PC, and insert it in Branch Gateway USB port.
4. Copy the software or firmware files to Branch Gateway using one of the following commands:
 - `copy usb SW_imageA`
 - `copy usb SW_imageB`
 - `copy usb module`
 - `copy usb phone-imageA` (or `imageB`, or `imageC`, or `imageD`)
 - `copy usb phone-scriptA` (or `phone-scriptB`)
 - `copy usb announcement-file`
 - `copy usb auth-file`
 - `copy usb startup-config`
 - `copy usb easg`
 - `EASGSiteCertManage copy usb`
5. Use the `show download software status` command to display the status of the firmware download process.

Upgrading firmware using the USB mass storage device “restore” command

About this task

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

Procedure

1. Backup the Branch Gateway by entering `backup config usb usbdevice0 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.
2. Obtain the firmware upgrade file(s) from Avaya and place them on your PC.
3. Insert the USB mass storage device into the PC's USB port, and copy the firmware file(s) to the USB mass storage device as follows:
 - a. Copy Branch Gateway firmware files to the root directory.
 - b. Copy the Device Manager firmware file to the root directory.
 - c. Copy media modules' firmware files to the MM sub directory.

- d. Copy IP phone firmware files to the IPPHONE sub directory.
4. Remove the USB mass storage device from the PC, and insert it in the Branch Gateway USB port.
5. Enter **restore usb usbdevice0 backup-name**, where *backup-name* is the root directory path and name on the USB mass storage device.
6. Enter **show restore status** to check the status of the restore operation.

The report lists the upgraded files.

Related links

[Sample backup directory after backup](#) on page 90

Software and firmware uploads from the gateway

Files copied to a USB mass storage device

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

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

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

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

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

- announcement-file. Announcements files
- capture-file. The packet sniffing buffer
- cdr-file. A Call Detail Recording (CDR) file for the calls in SLS mode
- dhcp-binding. The DHCP binding file

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

- announcement-file. Announcements files

- capture-file. The packet sniffing buffer
- cdr-file. A Call Detail Recording (CDR) file for the calls in SLS mode
- dhcp-binding. The DHCP binding file

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

- announcement-file. Announcements files
- capture-file. The packet sniffing buffer
- cdr-file. A Call Detail Recording (CDR) file for the calls in SLS mode
- dhcp-binding. The DHCP binding file

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

- announcement-file. The Announcements file
- capture-file. The packet sniffing buffer
- startup-config. The configuration file
- dhcp-binding. The DHCP binding file
- syslog file

Software and firmware management commands

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

Command	Description
copy ftp module	Upgrade the firmware on a media module from an FTP server by entering this command followed by the module number of the module you want to upgrade.
copy ftp SW_imageA	Upgrade Branch Gateway firmware into Bank A from an FTP server.
copy ftp SW_imageB	Upgrade Branch Gateway firmware into Bank B from an FTP server.
copy tftp module	Upgrade the firmware on a media module from a TFTP server.
copy tftp SW_imageA	Upgrade Branch Gateway firmware into Bank A from a TFTP server.
copy tftp SW_imageB	Upgrade Branch Gateway firmware into Bank B from a TFTP server.
copy https module	Upgrade the firmware on a media module from a HTTP or HTTPS server.
copy https SW_imageA	Upgrade Branch Gateway firmware into Bank A from an HTTP or HTTPS server.
copy https SW_imageB	Upgrade Branch Gateway firmware into Bank B from an HTTP or HTTPS server.
copyedge scp module	Upgrade the firmware on a media module from an SCP server via Avaya SBC tunnel.

Table continues...

Command	Description
<code>copyedge scp SW_imageA</code>	Upgrade Branch Gateway firmware into Bank A from an SCP server via Avaya SBC tunnel.
<code>copyedge scp SW_imageB</code>	Upgrade Branch Gateway firmware into Bank B from an SCP server via Avaya SBC tunnel.
<code>copy usb announcement-file</code>	Upgrade announcements files from the USB mass storage device.
<code>copy https announcement-file</code>	Upgrade announcements files from an HTTP or HTTPS server.
<code>copyedge scp announcement-file</code>	Upgrade announcements files from an SCP server via Avaya SBC tunnel.
<code>copy usb auth-file</code>	Upgrade the authorization file from the USB mass storage device.
<code>copy usb module</code>	Upgrade the firmware on a media module from the USB mass storage device.
<code>copy usb phone-image</code>	Upgrade phone images from the USB mass storage device.
<code>copy usb phone-script</code>	Upgrade phone scripts from the USB mass storage device.
<code>copy usb startup-config</code>	Upgrade the startup configuration file from the USB mass storage device.
<code>copy scp SW_imageA</code>	Downloads a software image from an SCP server into Bank A. The command prompts for the username and password.
<code>copy scp SW_imageB</code>	Downloads a software image from an SCP server into Bank B. The command prompts for the username and password.
<code>copy scp easg</code>	Copy and install an EASG Site Certificate using scp.
<code>copy usb SW_image</code>	Upgrade Branch Gateway firmware into Bank A or into Bank B, from the USB mass storage device.
<code>copy usb easg</code>	Copy and install an EASG Site Certificate using a USB device.
<code>dir</code>	List all files in the USB mass storage device connected to Branch Gateway.
<code>set boot bank</code>	Set the default bank from which firmware is loaded during startup.
<code>show boot bank</code>	Display the bank from which Branch Gateway is currently set to load its firmware upon startup or reset.
<code>show download software status</code>	Display the status of the firmware download process.
<code>show image version</code>	Display the firmware version of the image on both memory banks of the device.

 Note:

Branch Gateway has four G450 hardware versions. Use the **show system** command to check the hardware version. If the Model is G450v4, it uses a different software image: `g450v4_sw_x_y_z.bin`.

Backup and restores using a USB mass storage device

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

* Note:

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

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

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

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

+ Tip:

Use a USB mass storage device with LED indication.

Related links

[Upgrading software and firmware using a USB mass storage device](#) on page 84

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 helpful in restoring the Branch Gateway's configuration if it becomes faulty, or in restoring the entire Branch Gateway.

Use at least 256 MB, a 128 MB USB mass-storage device can only hold one backup directory 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 **copy running-config startup-config** to commit the current configuration to NVRAM.

3. Enter **backup config usb usbdevice0 backup-name**, where **backup-name** is the backup directory path and file name, you are creating on the USB mass-storage device.

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

4. Before unplugging the USB mass-storage device, use the **safe-removal usb** command to safely remove the USB mass-storage device.
5. You can use the **show backup status** command to display information regarding the status of a backup of the Branch Gateway configuration to a USB mass-storage device.

Sample backup directory after backup

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

Root directory	Sub-directory	Files / Sub-directory	Comments
backup-23-Aug-2015	-	-	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	-
-	trust	esag h248reg sla syslog web CRL	TLS certificates for each feature except for CRL which is certificate revocation list

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

Procedure

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

Replicating Branch Gateway using a USB mass-storage device

About this task

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

Important:

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

Procedure

1. Make sure you have a backup of the faulty Branch Gateway on a USB mass-storage device.
2. Transfer the media modules, including the S8300 if installed, from the faulty Branch Gateway into the corresponding slots of the new Branch Gateway.
3. Connect the new Branch Gateway to a power source.
4. In the new Branch Gateway, enter `show image version` to find out which of the two image banks holds the older Branch Gateway firmware version, and what version it is.
5. If the new Branch Gateway firmware version is 26.x.y or above, add Branch Gateway firmware to the USB mass-storage device, as follows:
 - a. From Avaya support Website, download to your PC the same version of Branch Gateway firmware as was running in the faulty Branch Gateway.
 - b. Insert the USB mass-storage device into the PC's USB port.
 - c. Copy Branch Gateway firmware file to the root backup directory in the USB mass-storage device.
6. Add the firmware files of the media modules to the USB mass-storage device, as follows:
 - a. From PLDS, download to your PC the firmware files of the media modules installed in the gateway.

For each media module, download all firmware corresponding to the various hardware vintage/suffix versions available for that module. If you are not sure which media

modules you have, you can download the firmware files of all media modules. The restore operation uses only the files needed.

- b. Insert the USB mass-storage device into the PC's USB port.
- c. Copy the firmware files from the PC to the MM sub directory in the USB mass-storage device.

Do not change the firmware file names.

7. You can optionally add the firmware files of the IP phones to the USB mass-storage device, as follows:

- a. From PLDS, download to your PC the firmware files (booter and application) of up to two supported IP phones, as well as the 46xxupgrade.txt or 46xxupgrade.scr file.
- b. Insert the USB mass-storage device into the PC's USB port.
- c. Copy the IP phone files from the PC to the USB mass-storage device.

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

 Note:

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

8. View the backup directory on the USB mass-storage device.
9. 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, and so on.

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

The report lists the files restored.

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

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

Result

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

Next steps

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

Related links

[Backing up administration and configuration files using a USB mass-storage device](#) on page 89

Sample backup directory after replication

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

Root directory	Sub-directory	Files	Comments
backup-23-Aug-2015	-	-	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
-	-	g450_sw_41_24_0.bin	Branch Gateway hardware versions 1.x, 2.x, and 3.x
-	-	g450v4_sw_41_24_0.bin	Branch Gateway hardware version 4.x
-	IPPHONE	-	IP phone scripts and images directory
-	-	46xxupgrade.scr	-
-	-	46xxsettings.txt	-
-	-	4601dape1_82.bin	-
-	-	4601dbte1_82.bin	-
-	MM	-	Media modules firmware directory. The media module firmware is copied from PLDS
-	-	mm722v2.fdl	-
-	-	mm714v67.fdl	-
-	-	mm711h20v67.fdl	-
-	-	mmanalogv67.fdl	-
-	GWANNC	-	Branch Gateway announcements and music-on-hold file directory
-	-	DanAnnouncement.wav	-
-	-	DanaAnnouncement.wav	-

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

Procedure

1. Backup 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.

2. From PLDS, 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, to enable a successful restore.

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

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



Note:

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

Related links

[Sample backup directory after backup](#) on page 90

USB backup, restore, and replication commands

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

Command	Description
backup config usb	Back up the Branch Gateway configuration to a USB mass-storage
copy usb sw_imageA	Download a software image from an external USB mass storage device into Bank A

Table continues...

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

Configuration file backup and restore

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

Note:

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

You can:

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

Related links

[Configuration changes and backup](#) on page 27

[Gateway secret management](#) on page 48

[Backup and restores using a USB mass storage device](#) on page 89

Configuration file backup and restore commands

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

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

List of files on the Branch Gateway

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

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

Chapter 6: Standard Local Survivability (SLS)

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

SLS is supported on IPv4 only.

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

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

Media module compatibility with SLS

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

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

Table continues...

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

SLS features

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

Avaya telephones supported in SLS

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

Table continues...

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

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

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

Module name	CLI interface name
1603	4610
1608	4610
1616	4620
9608	4620 ₃
9608G	4620 ₃
9610, FW V2.0 +	4606 ¹
9611G	4620 ₃
9620, FW V2.0 +	4610 ¹
9621G	4620 ₃
9630, FW V2.0 +	4620 ¹
9640, FW V2.0 +	4620 ¹
9641G	4620 ₃
9641GS	4620 ₃
9650, FW V2.0 +	4620 ¹

¹ For R4.0, the firmware must be build 26_39 or newer. For R5.0, the firmware must be build 27_27 or newer.

Call processing functionality in SLS mode

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

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

 Important:

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

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

Related links

[SLS logging activities](#) on page 111

Call processing functionality not supported by SLS

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

Provisioning data

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

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

 Note:

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

Standard Local Survivability data sources and communication paths

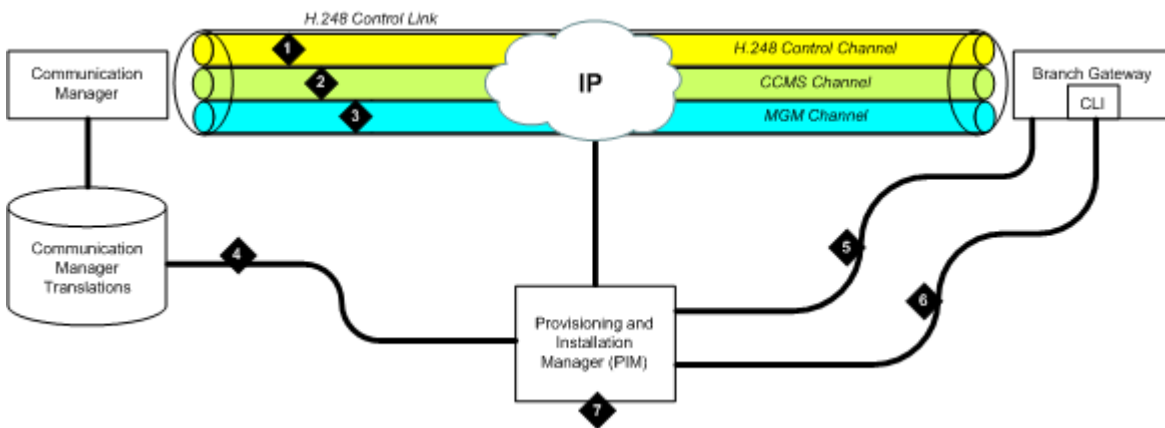


Table 2: Figure notes:

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

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

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

Related links

[Configuring CM for SLS](#) on page 113

SLS entry

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

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

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

Unregistered state

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

Setup state process

In this transitional state, SLS performs the following activities:

1. Checks for proper provisioning data. If there is insufficient provisioning, the registration request is denied, and SLS returns to the Unregistered state.
2. Initializes SLS components, such as Gatekeeper data (for example, IP endpoint's E.164 addresses and passwords), dial plan, and ARS routing.
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.

Teardown state process

1. Tears down endpoint objects.

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

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

SLS interaction with specific Branch Gateway features

SLS interacts differently with the various Branch Gateway features.

Direct Inward Dialing in SLS mode

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

Note:

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

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

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

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

Warning:

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

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

Multiple call appearances in SLS mode

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

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

Note:

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

Example

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

Hold in SLS mode

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

The Hold feature in SLS does not support:

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

DCP and IP phones

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

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

Analog telephones

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

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

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

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

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

Using the Flash button

Procedure

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

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

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

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.

Call Transfer in SLS mode

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

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

Transferring a call on DCP and IP phones

Procedure

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

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

2. Dial the third party's number on your phone.

3. You can either:

- Wait for the third party to answer and announce the call, then either press the **Transfer** button again or hang up.
- Transfer the call before the third party answers by pressing the **Transfer** button again.

Result

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

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

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 109.
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 110.
 - If the Branch Gateway number does not match the local Branch Gateway number, SLS plays an intercept tone and terminates the session.
4. Dial the contact closure code, for example **1** for contact pair #1, and **2** for contact pair #2.
- You hear stutter tone and then silence, confirming these valid codes. If you dial an invalid contact closure number, you hear an intercept tone.
- Contact closure feature activations appear in the CDR log.

 Note:

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

Related links

[Example of CDR log entries and format](#) on page 111

Contact closure / SLS feature interactions

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

Related links

[Contact closure](#) on page 300

Administering IP Softphone in SLS mode

About this task

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

Procedure

1. Access the CM administrative SAT interface.

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

 Note:

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

Related links

[Accessing the registered MGC](#) on page 72

SLS logging activities

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

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

 Note:

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

- Contact closure

Example of CDR log entries and format

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

An interpretation of the first entry is:

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

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

Example of CDR log with contact closure

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

An interpretation of this entry is:

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

SLS configuration

SLS configuration rules

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

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

Related links

[Prerequisites for using the CLI to manually configure SLS administration on the Branch Gateway](#) on page 126

[Enabling SLS](#) on page 125

[Activating changes in SLS](#) on page 126

Configuring CM for SLS

About this task

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

Procedure

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

For example:

```
change node-names ip                                     Page 1 of 2
      Name                IP Address
gateway1
198.152.1.200
(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. Type the IP address of the Branch Gateway in the **IP Address** field.
4. Submit the screen.
5. At the SAT, enter **change system-parameters mg-recovery-rule 1** to display the System Parameters Media Gateway Automatic Recovery Rule screen.
6. Type a description of the rule in the **Rule Name** field.

7. 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.

8. Submit the screen.
9. At the SAT, enter **display media-gateway 1** to display the Media Gateway screen.
10. Verify the following fields:

- **Name** field (20 characters maximum) must match the administered name of the gateway.
- **Max Survivable IP Ext** field only appears when the **Type** field is Gxxx .

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

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

 Important:

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

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

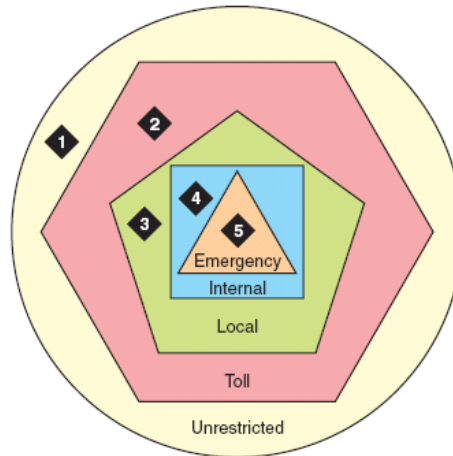
13. Submit the screen.

Related links

[Accessing the registered MGC](#) on page 72

[Configuration of the SLS data through the CLI](#) on page 146

Inherited Class of Restriction (COR) permissions



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

Table 3: Figure notes:

1. **Unrestricted:** Users can dial any valid routable number, except an ARS pattern specifically administered as **deny:** . ETR functionality and calls through the CO are permitted in this class.
2. **Local:** Users can only dial these call types:
 - **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

Security Code

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

- Extended User Administration of Redirected Calls
- Personal Station Access

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

The required security code length is administered system wide.

Type

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

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

 Note:

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

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

Table continues...

Telephone type	Model	Administered as
	7101A, 7102A	7101A
	7103A Programmable and Original	7103A
	7104A	7104A
	8110	8110
	DS1FD	DS1FD
	7302H, 7303H	7303S
	Voice Response Unit (VRU) with C&D tones	VRU
	VRU without C&D tones	2500
Single-line DS1/DSO	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
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+

Table continues...

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

Table continues...

Telephone type	Model	Administered as
IP Telephone	4601+  Note: When you add a new 4601 IP telephone, you must use the 4601+ station type. This station type has the Automatic Callback feature enabled.	4601+
	4602+  Note: When you add a new 4602 IP telephone, you must use the 4602+ station type. This station type has the Automatic Callback feature enabled.	4602+
	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

Table continues...

Telephone type	Model	Administered as
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: You must administer any telephone with SIP firmware used for SIP networking as a 4620SIP, 96xxSIP, or 16CC SIP telephone.  Note: Communication Manager Release 6.2 and later do not support 1616SIP CC and 4620SIP CC telephones.	4620SIP
	9601SIP	9608SIP
	9620, 9630, 9630G 9640, 9640G with SIP firmware	96xx or 96xxSIP telephone
	9608 with SIP firmware	9608SIP
	9611 with SIP firmware	9611SIP
	9621 with SIP firmware	9621SIP
	9641 with SIP firmware	9641SIP
	9608 with SIP firmware (for call center)	9608SIPCC
	9611 with SIP firmware (for call center)	9611SIPCC
	9621 with SIP firmware (for call center)	9621SIPCC
	9641 with SIP firmware (for call center)	9641SIPCC
	AvyaSIP	J139, J159, J189
	AvyaSIPCC	J189CC
H.323 SoftPhone	application Road Warrior	H.323 or DCP type
	Native H.323	H.323
	Singleconnect	H.323 or DCP type
	Any NI-BRI (N1 and N2) telephone	NI-BRI
	7505D	7505D
	7506D	7506D
	7507D	7507D

Table continues...

Telephone type	Model	Administered as
	8503D	8503D
	8510T	8510T
	8520T	8520T
Personal computer	6300/7300	PC
(voice/data)	6538/9	Constellation
Test Line	ATMS	105TL
No hardware assigned at the time of administration.		• Use XDID when Communication Manager assigns a DID number to the station. • Use XDIDVIP when the administrator later assigns a DID number to the station. • Use virtual to map the station and other extensions to one physical telephone.
Key telephone system interface	—	K2500
AWOH	any digital set	—
	CTI station	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
x or X	Indicates that there is no hardware associated with the port assignment since the switch was set up, and the administrator expects that the extension has a non-IP set. Or, the extension had a non-IP set, and it dissociated. Use x for Administered WithOut Hardware (AWOH) and Computer Telephony (CTI) stations, as well as for SBS Extensions.
IP	Indicates that there is no hardware associated with the port assignment since the switch was set up, and the administrator expects that the extension would have an IP set. This is automatically entered for certain IP station set types, but you can enter for a DCP set with softphone permissions. This changes to the s00000 type when the set registers.

Table continues...

Valid Entry	Usage
xxxVmpp	Specifies the Branch Gateway. • xxx is the Branch Gateway number, which is in the range 001 to 999. • 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

Survivable GK Node Name

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

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

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

Survivable COR

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

Available for all analog and IP station types.

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

Survivable Trunk Dest

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

Available for all analog and IP station types.

Valid Entry	Usage
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 Avaya Aura® Communication Manager*.

* Note:

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

SLS ARS Entry page field descriptions

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

Dialed String

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

Min

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

Max

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

Del

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

Replacement String

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

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

Call Type (ARS only)

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

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

Table continues...

Valid entry	Usage	China Number 1, Call Type
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 CM server.

Permit / Deny

Indicates whether the call should be permitted or denied.

Enabling SLS

Procedure

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

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

Procedure

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

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

Activating changes in SLS

About this task

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

Procedure

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

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

3. Enter **set sls enable**

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

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

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

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

Note:

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

SLS data set preparation

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

! Important:

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

SLS capacities

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

Branch Gateway model	IP stations
G450 ²	240

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

Related links

[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.
6. Gather the necessary information for the following fields:
 - Extension
 - Port

² 340 stations maximum (all types)

- Type - Only 2500 is the accepted Type
- Survivable COR
- Survivable Trunk Dest
- Switchhook Flash
- Name

Related links

[Station screen field descriptions for the Branch Gateway](#) on page 115

Collecting DCP stations data

Procedure

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

The system displays the extension number assigned to the port.

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

(Optional) - used for the registration of an IP Softphone (RoadWarrior)

 - Type - as any of the following types:
 - 2402
 - 2410
 - 2420
 - 6402
 - 6402D
 - 6408
 - 6408+
 - 6408D

- 6408D+
- 6416D+
- 6424D+
- 8403B
- 8405B
- 8405B+
- 8405D
- 8405D+
- 8410B
- 8410D
- 8411B
- 8411D
- 8434D
- Survivable COR
- Survivable Trunk Dest
- Expansion Module
- Name

For more information about these fields, see Station screen field descriptions for the branch gateway.

Collecting IP stations data

Procedure

1. At the SAT, enter **list media-gateway** to display a list of administered gateways.
 2. Look for supported gateways in the **Type** field.
 3. Enter **display media-gateway**.
 4. Read the reported IP address for this gateway.
 5. Enter **list node-name** and compare the IP address of the Branch Gateway in the list with the IP address of the gateway that you are administering for SLS.
- When you find a match in the node-name screen, read the assigned node-name. This will be used to do a pattern match with a field on the IP Station screen in Step [6](#) on page 129.
6. Enter **list station type type**, where *type* is one of the supported IP stations.

The report lists all IP phones that could have the **Survivable GK Node-Name** administered to the target media gateway. The **Survivable GK Node-Name** uniquely associates an IP phone with a particular Branch Gateway.

7. Once a match is made between the station screen's **Survivable GK Node-Name** and the target gateway's **Node-Name** , gather the values for the given IP station per:
 - Extension
 - Security Code
(IP only) - used for the registration of the IP endpoint
 - Type — as any of the following types:
 - 4601
 - 4602
 - 4602SW
 - 4606
 - 4610SW
 - 4612
 - 4620
 - 4620SW
 - 4621
 - 4622
 - 4624
 - 4625
 - Survivable COR
 - Survivable Trunk Dest
 - Expansion Module
 - Name

Related links

[Station screen field descriptions for the Branch Gateway](#) on page 115

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 163 as a reference to identify how the particular media module has been configured for serving as a trunk port, and then use the various **list** commands on CM to look for physical port matches in the various trunk SAT forms in order to discover what translation information is needed.

4. Identify the analog trunk ports.
5. Identify the BRI trunk ports.
6. Identify the digital DS1 trunk ports.
7. Identify the Branch Gateway modules and check for provisioned trunk ports.
8. At the SAT, enter **display port portid**, where *portid* is the trunks port on the target gateway.

The system reports the Trunk Group Number/Member Number for this particular port.

9. Once you know the Trunk Group Number, gather trunk-group information for the following fields:
 - Group Type
 - Outgoing Dial Type
 - Trunk Group Number
 - TAC
 - Port
 - Digit Treatment
 - Digits
 - Trunk Type
 - Group Name
 - Codeset to Send Display
 - Codeset to Sent National IEs
 - Outgoing Channel ID Encoding
 - Digit Handling (in/out)
 - Network (Japan) Needs Connect Before Disconnect
 - Send Name
 - Send Calling Number
 - Incoming Calling Number - Format
 - Incoming Destination
 - Trunk Hunt
 - Sig Grp

Related links

[Module-port values in SLS trunk-group context for analog trunks](#) on page 164

[Trunk port values in SLS trunk-group context for digital trunks](#) on page 164

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 - 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

Table continues...

Name	Description
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
Sig Grp	Specifies the Signaling Group Number that is the manager of this ISDN trunk member

Collecting DS1 trunks data

Procedure

1. At the SAT, enter **display ds1 location** to display the DS1 administration for a particular circuit pack **location**.
2. Gather the following DS1 information for each DS1 facility:
 - Name
 - Bit-Rate
 - Signaling Mode
 - Channel Numbering
 - Connect
 - Interface
 - Side
 - Country Protocol
 - Protocol Version

- DCP/Analog Bearer Capability
- Interface Companding
- ITN-C7 Long Timers

3. Repeat the **display ds1 location** command and press **Enter** for each circuit pack that you want to include in the SLS data set.

DS1 circuit pack field descriptions

Name

Assigns a significant, descriptive name to the DS1 link. Use the vendor's circuit ID for the link in this field because that information helps troubleshoot problems with the link. This field can also be used to indicate the function or the destination of this DS1 facility. Accepts up to 15 characters.

 Note:

Avaya BRI deskphones support only ASCII characters because non-ASCII characters, such as Eurofont and Kanafont, show up incorrectly.

Bit Rate

 Note:

TN464C and later release circuit packs have an option switch that must be set to match this **Bit Rate** value.

Valid Entry	Usage
1.544	The maximum transmission rate for DS1 circuit packs that support T-1 service.
2.048	The maximum transmission rate for DS1 circuit packs that support E-1 service.

Signaling Mode

Selects the signaling method used for the DS1 link. This mode must match the method used by the network services provider.

Valid Entry	Usage
CAS	Channel Associated Signaling. Out-of band signaling with E1 service. This setting yields 30 64-kbps B-channels for voice or data transmission. Channel 0 is used for framing while channel 16 carries signaling. Used for Enterprise Mobility User (EMU)/ EC500 administration.
robbed-bit	In-band signaling with T1 service. This setting yields 24 56-kbps B-channels for voice transmission.
isdn-pri	Either T1 or E1 ISDN service. This setting supports both Facility Associated Signaling and Non-Facility Associated Signaling.

Table continues...

Valid Entry	Usage
isdn-ext	Either T1 or E1 ISDN service. This setting supports only Non-Facility Associated Signaling.  Note: NFAS is primarily a feature for ISDN-T1 connections offered by service providers in North America and Hong Kong. However, it can also be used on private-network connections, and in that context it is possible to set up NFAS using ISDN-E1 interfaces.
common-chan	Out-of-band signaling with T1 service. This setting yields 23 64-kbps B-channels for voice or data transmission. Channel 24 is used for signaling.

Channel Numbering

The ETSI and ISO QSIG specifications require that B-channels on an E1 be encoded as 1 to 30 in the Channel ID IE. Prior to the existence of this field, Communication Manager only used this scheme for Country Protocols 2a (Australia) and 13a (Germany 1TR6). Available only with ISDN-PRI signaling on a private network. The interface must be peer master or peer slave.

2.048 bit rate options:

- timeslot
- sequential

If Communication Manager is connected via QSIG trunks to a switch or server supporting the ETSI QSIG or ISO QSIG specifications, this field must be sequential.

Connect

To control communications at layers 2 and 3 of the ISDN-PRI protocol, this field to specifies what is on the far end of this DS1 link.

Available only for ISDN-PRI signaling.

Valid Entry	Usage
pbx	The DS1 link is connected to another switch in a private network.
line-side	Communication Manager is acting as the network side of an ISDN-PRI interface. Used to connect to Roll About Video equipment.
network	The DS1 link connects Communication Manager to a local telephone company central office or any other public network switch.
host	The DS1 link connects Communication Manager to a computer.

Interface

Controls how the server negotiates glare with the far-end switch. The servers at either end of the DS1 link must have complementary settings in this field. Otherwise, the D-channel cannot function. For example, if the Avaya S8XXX server at one end of the link is administered as network, the other end must be administered as user. Available only when this DS1 link is providing an ISDN-PRI connection in a private network.

Private network applications in the U.S.

Valid Entry	Usage
network	The server overrides the other end when glare occurs, and when connecting the server to a host computer.
user	The server releases the contested circuit and looks for another when glare occurs, and when connecting the server to a public network.

Private network applications outside the U.S.

Valid Entry	Usage
peer-master	The switch overrides the other end when glare occurs.
peer-slave	The switch releases the contested circuit and looks for another when glare occurs.

Side

Use this field to control how Communication Manager must resolve glare at layer 3 over an ISDN-PRI link in QSIG private networks. The system displays this field only if the **Interface** type is peer-master or peer-slave.

Caution:

You must correctly pair with the administration of the far-end server. If the far-end server is administered as the **b** side, you must set the **Side** field to **a**, regardless of whether the layer 2 is peer-master or peer-slave, and vice versa.

Valid entry	Usage
a	The Interface is peer-master. Communication Manager overrides the far-end when glare occurs.
b	The Interface is peer-slave. Communication Manager releases the contested circuit and looks for another when glare occurs.

Country Protocol

The country protocol used by the far-end server. For connections to a public network, your network service provider can tell you which country protocol they are using.

Available only with ISDN-PRI and CAS signaling.

Valid Entry	Usage
1 to 25	The country protocol used by the local telephone company central office at which this link terminates.
etsi	The network service provider uses the European Telecommunications Standards Institute (ETSI) protocol and the 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** type is pbx, and the **Interface** type is user or network.

Valid Entry	Usage
a, b, c, d	Selects the protocol that matches the network service provider's protocol in countries whose public networks allow multiple layer-3 signaling protocols for ISDN-PRI service. Contact the network service provider to verify that the protocols match.



Warning:

The AT&T Switched Network Protocol prohibits restricted displays of connected numbers. Display problems occur if you administer the 1a country-protocol/ protocol-version combination on the DS1 screen and administer the ISDN-PRI Trunk Group to restrict sending the connected number.

DCP/ANALOG Bearer Capability

Sets the information transfer capability in a bearer capability IE of a setup message to speech or 3.1kHz. Available only with the ISDN-PRI **Signaling Mode**.

Valid Entry	Usage
3.1kHz	Provides 3.1 kHz audio encoding in the information transfer capability.
speech	Provides speech encoding in the information transfer capability.

Interface

Controls how the server negotiates glare with the far-end switch. The servers at either end of the DS1 link must have complementary settings in this field. Otherwise, the D-channel cannot function. For example, if the Avaya S8XXX server at one end of the link is administered as network, the other end must be administered as user. Available only when this DS1 link is providing an ISDN-PRI connection in a private network.

Private network applications in the U.S.

Valid Entry	Usage
network	The server overrides the other end when glare occurs, and when connecting the server to a host computer.
user	The server releases the contested circuit and looks for another when glare occurs, and when connecting the server to a public network.

Private network applications outside the U.S.

Valid Entry	Usage
peer-master	The switch overrides the other end when glare occurs.
peer-slave	The switch releases the contested circuit and looks for another when glare occurs.

ITN-C7 Long Timers

Controls the T302 and T303 timers.

Available only if the **Signaling Mode** is isdn-pri.

Valid Entry	Usage
y	Increases the length of the long timers.
n	Uses the default long timers.

Collecting signaling groups data

1. Collect the following information from the Communication Manager Signaling Group screen for ISDN-PRI administration only:
 - Trunk Group for Channel Selection
 - Associated Signaling
 - Primary D-channel
 - Trunk Board
 - Interface Id

Signaling Group field descriptions

Trunk Group for Channel Selection

Available only if **Group Type** is atm, h.323, or isdn-pri.

Valid Entry	Usage
1 to 2000	Trunk group number used for channel selection.

Associated Signaling

Available only if **Group Type** field is isdn-pri.

Valid Entry	Usage
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

Name

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

Note:

Avaya BRI deskphones support only ASCII characters because non-ASCII characters, such as Eurofont and Kanafont, show up incorrectly.

ISDN-BRI Trunk/Interface

Determines glare handling.

ISDN-BRI Trunk/Side

QSIG glare handling, when **Interface** is peerSlave.

ISDN-BRI Trunk/Country Protocol

Specifies the Layer 3 signaling protocol used by the country-specific service provider.

ISDN-BRI Trunk/DCP/Analog Bearer Capability

Sets the Information Transfer capability in the Bearer Capability IE of the SETUP message.

Companding Mode

Specifies the companding mode used by the far end switch.

TEI

LAPD address assignment for the **TEI** field.

Directory Number

The directory numbers assigned to the interface and allocated to two separate endpoints. This field must be administered in pairs. Accepts up to 10 characters.

SPID

The Service Profile Identifier (SPID) expected by the far end. Accepts up to 12 characters. Communication Manager prevents changing this field unless the port is busied out or unadministered. The only protocol supported for SPID initialization is Country Code 1. Trunks are not put in service if SPID installation is unsuccessful. Leading zeroes are significant and must not be ignored.

Endpt Init

Indicates whether the far end supports endpoint initialization. Communication Manager blocks you from changing this field unless the port is busied out or unadministered.

Valid Entry	Usage
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

- At the SAT, enter **display system-parameters customer-options** to display the Customer Options screen.
- 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 141.
 - 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**
- Look up the location of the gateway, as follows:
 - At the SAT, enter **list media-gateway** to get the gateway's number.
 - At the SAT, enter **display media gateway number**, where *number* is the gateway number you obtained in Step a on page 141.

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 141.

Feature Access Code field descriptions

Contact Closure Open Code

FAC used to open a contact closure relay. Contact closures control electrical devices remotely. Users use an FAC to activate electrical devices such as electrical door locks. If **Contact Closure Close Code** is administered, then **Contact Closure Open Code** must also be administered.

This value must conform to the FACs or dial access codes defined by the dial plan.

Contact Closure Close Code

FAC used to close a contact closure relay. Contact closures control electrical devices remotely. Users use an FAC to activate electrical devices such as electrical door locks. If **Contact Closure Open Code** is administered, then **Contact Closure Close Code** must also be administered.

This value must conform to the FACs or dial access codes defined by the dial plan.

Contact Closure Pulse Code

FAC used to pulse a contact closure relay.

This value must conform to the FACs or dial access codes defined by the dial plan.

Auto Route Selection (ARS) Access Code 1

FAC used to access ARS. The system can automatically choose the least-expensive way to send a toll call. You can have one ARS access code for local and one for long distance, and route accordingly.

This value must conform to the FACs or dial access codes defined by the dial plan.

Auto Route Selection (ARS) Access Code 2

Additional FAC used to access ARS.

This value must conform to the FACs or dial access codes defined by the dial plan.

ARS FAC

This is used instead of the Features screen ARS FAC entry if the Loc No. that correlates to the gateway has an entry in this screen that overrides the general ARS FAC(s).

CAS Remote Hold/Answer Hold-Unhold Access Code

FAC used by a Centralized Attendant Service (CAS) attendant to place calls on hold and answer calls held at a remote server running Communication Manager. This FAC can also be used by an analog station. Flashing the switch-hook for the proper interval (between 200 and 1000 ms)

while talking on an existing call causes the existing call to be placed on soft hold, using which the analog user can dial the Answer Hold-Unhold FAC to Hard hold the call.

This value must conform to the FACs or dial access codes defined by the dial plan.

Collecting system parameters data

Procedure

1. At the SAT, enter **list media-gateway** to display a list of administered gateways.
2. Look for supported gateways in the **Type** field.
3. Once you have determined the media gateway of interest, note its IP-Network-Region.
4. At the SAT, enter **display ip-network-region *n***, where *n* is the gateway's administered IP-Network-Region.

Read the **Codec-set** field value from the IP Network Region screen.

5. At the SAT, enter **display ip-codec-set *n***, where *n* is the **Codec-set** field value from the IP Network Region screen.

The report lists the supported codes in the **Audio Codec** field.

6. At the SAT, enter **display system-parameters features** to display the Feature Related System Parameters screen.
7. Scroll to page 10 and read the value of the **Date Format on Terminals** field.
8. At the SAT, enter **display media-gateway *n***, where *n* is the administered number of the Media Gateway of interest, to display the Media Gateway screen.
9. Read the **Max Survivable IP Ext** field value.

Codecs supported in SLS

There can be up to seven distinct codec-sets in use in the system. However, only one codec set is active for the network region in which the gateway is located.

SLS only supports two codecs:

- G.711 A-law
- G.711 U-law

General system parameters field descriptions

For information about the fields on the IP codec set screen, see Avaya Aura® Communication Manager Screen Reference.

Date Format on Terminals

Applies to 64xx and 24xx DCP terminals, and to 46xx IP terminals.

Max Survivable IP Ext

This field describes the maximum IP phone registrations allowed.

Collecting ARS dial patterns data

About this task

To gather the route patterns and ARS analysis in CM, you must first know which trunk groups are assigned to the gateway of interest. After verifying this information, perform the following steps:

Procedure

1. At the SAT, enter `list route-pattern trunk-group n`, where *n* is an administered trunk group, to display the administered route patterns.
2. For the first preference for this route-pattern entry, read the values of the following fields:
 - No Deleted Digits
 - Inserted Digits
3. At the SAT, enter `list ars analysis` to search the ARS Analysis table for row entries whose **Route Pattern** field matches the route-pattern values that were obtained in Step 1 on page 144. Once you discover a match with **Route Pattern**, use the entries from this row in the ARS Analysis table to complete the following three entries for the SLS Dial-Pattern table:
 - Min
 - Max
 - Dialed String

ARS Dial Patterns field descriptions

No Deleted Digits

Specifies the number of dialed digits to be deleted from the beginning of the dialed string. The default is 0.

General system parameters/Inserted Digits

Specifies the digit string to be inserted at the beginning of the dialed string. The default is blank.

Min

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

Max

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

Dialed String

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

Collecting Incoming Call Handling data

About this task

To gather the Incoming Call Handling Treatment and ARS Digit Conversion information in CM, you must first know which trunk groups are assigned to the gateway of interest. After verifying this information, perform the following steps:

Procedure

1. At the SAT, enter `display inc-call-handling-trmt trunk-group n`, where *n* is an administered trunk group.
2. For each entry, read the values of the following fields:
 - Called Number
 - Called Len
 - Del
 - Insert

Incoming call handling data field descriptions

Called Number

Valid Entry	Usage
1 to 16	Specifies the leading digits received for an incoming call.
blank	Matches any number associated with the specified service or feature.

Called Len

Valid Entry	Usage
0 to 21	The number of digits received for an incoming call. Zero is used when the Public Switched Telephone Network (PSTN) provider does not provide any "Number Digits" within the received 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 <dial-string>` to enter the second-level sub-context for administering dial pattern strings
- incoming-routing context that is invoked by entering `incoming-routing <tgnum> <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.

* Note:

Review [Summary of SLS configuration commands](#) on page 168 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 <name>** command.

 Note:

Branch Gateway administered name must match the name in the CM administration.

3. At Branch Gateway command prompt, enter **sls** to begin entering SLS data.
The command line prompt changes to (super-sls)# to indicate that you are in SLS data entry mode. Entering **exit** ends the SLS data entry mode session, and the command line prompt returns to its original state.
4. If you want to change the maximum allowable IP registrations from the default, enter **set max-ip-registrations n**, where *n* is from 1 to 240.
5. Use the **set date-format** command to set a date format for the SLS data set.
6. Use the **set ip-codec-set** command to select the country-specific G.711 codec set within the SLS data set: g.711mu or g.711a.
7. Administer the slot configuration information by entering **set slot-config <slot-number> <board-type>**, where <slot-number> is the slot where the Media Module is located and <board-type> is the Media Module type.
8. Administer the station information.
9. Administer DS1 trunks as required.
10. Administer BRI links as required.
11. Administer the trunk groups.
Note that you can add members to the trunk group only after you administer the signaling group information.
12. Administer the signaling groups.
13. Administer ARS dial patterns for outgoing calls.
14. Administer digit treatment for incoming routed calls.
15. Optionally administer the attendant feature for the purpose of call routing by entering **set attendant <access-code> <extension>**, where <access-code> specifies the dial access code for the attendant feature, and <extension> specifies the station which serves as the branch office attendant position.

Incoming trunk calls that have dialed strings that cannot be completely routed, will now be routed by SLS to this attendant position. In addition, stations in the branch office may directly dial the attendant using the `<access-code>`.

16. Administer the Feature Access Codes (FACs) by entering `set fac <feature> <fac>`, where `<feature>` is one of the following:

- `ars1`
- `ars2`
- `hold`
- `contact-open`
- `contact-close`
- `contact-pulse`

`<fac>` is a 1 to 4 digit string that includes the digits 0 through 9, excluding * and # for analog rotary phones. The `<fac>` string must be unique and must not conflict with station extension numbers and Trunk Access Codes (TACs).

Examples

- `set fac ars2 *9`
- `set fac contact-close 8`

 Note:

The “*” and “#” characters are not available on rotary-dial, analog phones.

17. At the Branch Gateway command prompt, enter `exit` to leave the sls context.

The Branch Gateway command prompt reverts to that of the original login.

18. After all of the SLS features are administered, at the Branch Gateway command prompt enter `set sls enable` to enable SLS on the Branch Gateway.

 Note:

If you enabled SLS and then entered additional administration, you must first disable SLS by entering `set sls disable`, and then re-enable it by entering `set sls enable`. This will cause the SLS application to resynchronize its administrative database with the Branch Gateway's CLI command database.

19. At the Branch Gateway command prompt, enter `copy running-config startup-config` to save the changes.

Related links

[Administering DS1 parameters](#) on page 152

[Administering BRI parameters](#) on page 156

[Administering trunk-group parameters](#) on page 158

[Administering signaling-group parameters](#) on page 165

[Administering dial-pattern parameters](#) on page 166

[Administering incoming-routing parameters](#) on page 167

[Media module compatibility with SLS](#) on page 98

Administering station parameters

Procedure

1. At the Branch Gateway command prompt, enter **station <extension> <class>** to enter a second-level sub-context to administer each phone that you want covered by SLS.

In this command, <extension> is a 1 to 16 digit numeric string that may begin with 0, and class <class> is analog, dcp, or ip.

For example, **station 1234567 ip** administers an IP phone with the extension “1234567”.

The command line prompt changes to **sls-station <extension>** to indicate that you are in the station context for SLS administration. Entering **exit** ends the station configuration mode, and the command line prompt returns to its original state. If you want to remove the station from the SLS administration, enter **clear station <extension>** at the command line interface. Enter **exit** to leave the second-level station context to return to the (super-sls)# context.

2. Depending on the class (analog, dcp, or ip, set in Step 1 on page 149), enter set type <model>, where <model> is a value from [Class values in SLS station context](#) on page 151.

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 149), 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 151.

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 149), you cannot run this command.

You cannot select these modules or ports if they are already assigned as DID trunks.

Examples:

- If an MM711 is inserted into slot V3 and an analog station is to be administered for port #5, then **set port v305** sets the previously-administered analog station “1234567” to the fifth physical analog station port on the Branch Gateway’s media module.
- If an MM712 is inserted into slot V2 and a DCP station is to be administered for port #1, then **set port v201** sets the previously-administered dcp station “1234567” to the first physical DCP station port on the Branch Gateway’s media module.

4. Enter `set cor <cor type>` to set the class of restriction (COR) for this extension, where `<cor type>` is one of the following:

- emergency
- internal (default)
- local
- toll
- unrestricted

There exists a hierarchical relationship among the calling-restriction categories. As you move from the most restricted COR (emergency) to the least restricted (unrestricted), each level increases the range of dialing abilities. For example, toll includes the dialing privileges of local, internal, and emergency.

For example, `set cor unrestricted` gives a station unrestricted dialing.

5. If this station is administered to be included into a pool of stations that are allowed to receive incoming analog loop-start trunk calls, enter `set trunk-destination yes`.
6. If this is an IP phone (set in Step 1 on page 149), 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 CM.

 Note:

Passwords are not required for analog or DCP phones unless an IP Softphone is using the administrative identity of a DCP phone, in which case the password is required.

7. To enable DCP or IP phones (set in Step 1 on page 149) to have an expansion module, enter `set expansion-module yes`.
8. For analog phones (set in Step 1 on page 149) 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 CM. Type the name string inside double quotes.
10. Enter `show` to check the station administration of the station being programmed.

The report lists the station parameters. For example:

Extension	Type	Port	Cor	Trunk-Des	Exp-Mod	Flash	Password
49139	ip4620	IPAddr	local	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.

Related links

[Inherited Class of Restriction \(COR\) permissions](#) on page 115

Class values in SLS station context

analog	dcp	H.323
analog2500 ³	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
	MM714	4 possible ports (ports 1-4)	-

Table continues...

³ Since there is just one entry, the model is optional; analog2500 is the default value.

Gateway	Media module	Analog station ports*	DCP
	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 CM (`add trunk-group n`). Type the name string inside double quotes.

3. Enter `set bit-rate <rate>` to set the maximum transmission rate in Mbps for the DS1 facility.

The rate can be either 1544 (T1) or 2048 (E1).

4. Enter `set signaling-mode <mode-type>` to set the signaling mode for the DS1 facility, where `<mode-type>` is one of the following values:

- `cas`. Out-of-band signaling for E1 service, yielding thirty 64 kbps B-channels for voice transmission
- `robbed bit`. In-band signaling for T1 service, yielding twenty-four 56 kbps B-channels for voice transmission
- `isdnpri`. T1 or E1 ISDN Primary Rate service (supports both FAS and NFAS)
- `isdnext`. NFAS T1 or E1 ISDN service for:
 - T1 facility, in which all 24 channels are for bearer transport
 - E1 facility, in which all 31 channels are for bearer transport

5. Enter **set channel-numbering** *<method>* to select the channel-numbering method for B-channels on an E1 interface, where *<method>* is one of the following values:
 - seq. Sequential codes of B-channels 1-30 in the ISDN Channel Identification IE
 - tslot. Timeslot method
6. Enter **set connect** *<far-end>* to specify the equipment at the far-end of the DS1 link, where *<far-end>* is one of the following values:
 - host. Data application (computer or server)
 - lineside. Terminal equipment (video multiplexer)
 - network. Central office
 - pbx. Private communication system (another pbx)
7. If the far-end equipment is specified as **pbx** (set in Step 6), enter **set interface** *<glare-mode>* to specify the glare-handling convention, where *<glare-mode>* can be one of the following values:

For non-QSIG calls:	For QSIG calls:
• 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).
9. Enter **set side** *<side>* to specify the glare mode: either a or b.
10. If the DS1 link is employed with ISDN, enter **set country-protocol** *<country-code>* to specify the ISDN Layer 3 country protocol type, where *<country-code>* is one of the values in [ISDN Layer 3 country codes](#) on page 154:
11. For countries whose public networks allow for multiple ISDN Layer 3 country protocols for ISDN Primary Rate service, enter **set protocol-version** *<option>* to specify the mode.

Verify that the protocol version matches the country specified in **set country-protocol** (set in Step 9).
12. If the DS1 link is employed with ISDN, enter **set bearer-capability** *<bearer>* to set the **Information Transfer Rate** field of the Bearer Capability IE, where *<bearer>* is one of the following values:
 - 3khz. 3.1 kHz audio encoding
 - speech. Speech encoding

13. Enter **set interface-companding** <type> to set the interface to agree with the companding method used by the far-end of the DS1 circuit for SLS mode, where <type> is one of the following values:
 - alaw. A-law companding
 - ulaw. U-law companding
14. Enter **set long-timer** yes | no to increase the duration of the T303 (call establishment) timer, where:
 - yes. The T303 timer is extended from 4 seconds to 13 seconds
 - no. The T303 timer remains at 4 seconds
15. Enter **show** to check the DS1 administration.

The report lists the DS1 parameters. For example:

```
Name = 'Willow Steet 2'
DS1  Rate Signaling Channel Connect Interface Side Protocol Ver Bearer Cmpd Ltm
-----
v3 1544   isdnpri      seq network      user    a country1  a speech ulaw  no
```

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

Related links

[ISDN Layer 3 country protocols for ISDN Primary Rate service](#) on page 155

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
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

Table continues...

Country Code	Country
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)	a
	National ISDN-1	b
	Nortel mode (also known as DMS)	c
	Telecordia (NI-2)	d
Country 2 (Australia)	Australia National PRI	a
	ETSI	b
	invalid	c
	invalid	d
Country 10 (United Kingdom)	DASS	a
	ETSI	b
	invalid	c
	invalid	d
Country 12 (France)	French National PRI	a
	ETSI	b
	invalid	c
	invalid	d

Table continues...

Country code	Description	Possible Values
Country 13 (Germany)	German National PRI	a
	ETSI	b
	invalid	c
	invalid	d
ETSI	Full message set, including RESTART	a
	No RESTART message	b
	invalid	c
	invalid	d

Administering BRI parameters

Procedure

1. Enter **bri <slot-address>**, where *<slot-address>* is any permitted port.

The command line prompt changes to **sls-bri <slot-address>**. If you want to remove the BRI link from the SLS administration, enter **exit** to leave the second-level bri context and return to the (super-sls)# context, and then enter **clear bri <slot-address>**.

2. Enter **set name <name>** to identify the user name for the DS1 trunk.

Use the 1-27 character name, as specified on CM (**add trunk-group n**). Type the name string inside double quotes.

3. Enter **set interface <glare-mode>** to specify the glare-handling convention.

<glare-mode> can be one of the following values:

For non-QSIG calls:	For QSIG calls:
• 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

4. If the BRI link is employed with ISDN, and the glare-handling convention is specified as **peerMaster** or **peerSlave** for the ISDN link (set in Step 3),
5. Enter **set side <side>** to specify the glare mode: either a or b.
6. If the BRI link is employed with ISDN, enter **set country-protocol <country-code>** to specify the ISDN Layer 3 country protocol type, where *<country-code>* is any of the values listed in [ISDN Layer 3 country codes](#) on page 154.

7. 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
8. Enter **set interface-companding <type>** to set the far-end companding method, where **<type>** is one of the following values:
 - alaw. A-law companding
 - ulaw. U-law companding
9. If the BRI link is employed with ISDN, enter **set tei-assignment <tei>** to select the method by which the Layer 2 (LAPD) protocol obtains its Terminal Endpoint Identification (TEI) address.
tei is one of the following values:
 - auto. TEI is assigned by the network provider
 - zero. TEI is fixed administratively
10. Enter **set directory-number-a <number>** to assign a directory number to the B1 channel of the BRI link.
<number> is the provisioned number received from the network provider. The **number** value must be identical to the number the network provider has assigned to the circuit.
11. Enter **set directory-number-b <number>** to assign a directory number to the B2 channel of the BRI link.
<number> is the provisioned number received from the network provider. The **number** value must be identical to the number the network provider has assigned to the circuit.
12. Enter **set spid-a number** to assign an SPID to the B1 channel of the BRI link.
13. Enter **set spid-b number** to assign an SPID to the B2 channel of the BRI link.

 Note:

All BRI links must have SPIDs properly configured for the link to function. SPIDs are received from the network service provider.

14. If the BRI link is employed with ISDN, enter **set-endpoint-init {yes | no}** to determine whether or not the far-end supports endpoint initialization.
15. If the BRI link is employed with ISDN, enter **set layer1-stable {yes | no}** to determine whether or not to keep the physical layer active (stable) between calls.
 Some European countries require that the physical layer is deactivated when there is no active call.
16. Enter **show** to check the BRI administration.

The report lists the BRI parameters. For example:

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

17. Enter **exit** to leave the bri context in SLS.

Trunk group assignment

You can create a trunk group that does not have any assigned members. Once a valid port is assigned as a trunk group member, this trunk group then becomes active and may be employed by SLS call processing for incoming/outgoing trunk operation. The slot-configuration table is used, together with the port capacity for the given module, to determine the validity of a port assignment at administration time.

As a result, there may not be more active trunk groups than there are physical trunk members within a given Branch Gateway. In addition, a combo-port may only be used for one active assignment. For example, the analog station/DID trunk ports may be either allocated to serve as an analog station or as an analog DID trunk, but not both.

The maximum limits for a given trunk type are defined by the slot-configuration assignment for the Branch Gateway. The maximum number of ports allowed per interface module is defined in [SLS group type assignments](#) on page 163.

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.

 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 CM (**add trunk-group n**). Type the name string inside double quotes.

10. For ISDN trunks, enter **set codeset-display <codeset>** to identify which Q.931 codesets are allowed to send display information to the user phone: codeset0, codeset6, or codeset7.
11. For ISDN trunks, enter **set codeset-national <codeset>** to identify which Q.931 codesets are allowed to send National Information Elements (IEs, or display information) to the user phone: codeset6 or codeset7.
12. For ISDN trunks, enter **set channel-preference <type>** to define how the **Channel Identification IE** field is encoded, where **<type>** can be one of the following:
- exclusive. The central office must have the ability to grant a call on this channel or reject the call attempt
 - preferred. The central office might offer the call request on another available channel
13. For ISDN trunks, enter **set digit-handling method** to define the order of reception/transmission to be considered with the flow of inbound/outbound:
- enbloc-enbloc
 - enbloc-overlap
 - overlap-enbloc
 - overlap-overlap

Enbloc requires sending the entire collected digit string in one block. Overlap sends the digits one at a time as they are collected.

14. For ISDN trunks, enter **set japan-disconnect <yes | no>** to specify whether to perform a disconnect sequence (CONNECT message followed by a DISCONNECT message).
15. For ISDN trunks, enter **set send-name <method>** to define whether or not the calling, connected, called, or busy party's administered name is sent to the network on outgoing or incoming calls.

<method> can be one of the following:

- no. The name is not sent to the network for incoming or outgoing calls
- yes. The name is sent to the network for incoming or outgoing calls
- restricted. The name is sent to the network as "Presentation restricted"

 Note:

For this release, specify **<method>** as **no**, since sending a Calling Party Name is a future feature.

16. For ISDN trunks, enter **set send-number** *<method>* to define whether or not the calling, connected, called, or busy party's administered number is sent to the network on outgoing or incoming calls.

<method> can be one of the following:

- no. The number is not sent to the network for incoming or outgoing calls
- yes. The number is sent to the network for incoming or outgoing calls
- restricted. The number is sent to the network as "Presentation restricted"

 Note:

For this release, specify *<method>* as **no**, since sending a Calling Party Number is a future feature.

17. For ISDN trunks, enter **set numbering-format** *<type>* to specify the numbering plan for this trunk in Standard Local Survivability (SLS).

The numbering plan encodes the **Numbering Plan Indicator** and **Type of Number** fields in the Calling/Connected Party Number IE in the ISDN protocol.

<type> can be one of the following:

- unknown. Both the Numbering Plan Indicator and Type of Number are unknown
- public. The Numbering Plan Indicator meets the E.164 standard and the Type of Number is national

 Note:

The SLS application is intended to operate into PSTN trunk interfaces. For this reason, the only two choices for network numbering plans identification are public (E.464) and unknown (no particular plan). For this release, specify **type** as unknown since SLS does not currently support an administrative table to calculate the Calling Party Number that is consistent with the numbering plan of the PSTN service provider.

18. For non-ISDN digital trunks, analog loop-start and analog ground-start trunks, enter **set incoming-destination extension** to identify an extension to directly receive an incoming trunk call, for example, an attendant or a voice response/recording system.
19. For non-ISDN digital trunks, enter **set incoming-dialtone** *<yes | no>* to specify whether to provide a dial tone in response to far-end trunk group seizures.
20. For a DS1 circuit, enter **set trunk-hunt** *<type>* to specify the trunk-hunting search within a facility in an ISDN trunk group or through a non-ISDN digital trunk group, where *<type>* is one of the following:
- ascend. A linear search from the lowest to the highest numbered available channels
 - circular. A circular search beginning with the point at which the search previously ended. When the search has reached the top of the channel list, it resumes at the bottom of the list in wrap-around fashion
 - descend. A linear search from the highest to the lowest numbered available channels

21. Enter **show** to check the trunk-group administration.

The following example shows all four trunk members assigned to one trunk-group:

```

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    tlinband   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

Table continues...

Group type	Media module	Number of ports/ channels	Description of trunks that may be assigned
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 isdnnext
e1-isdn	MM710	30	D-channel is associated with this facility (FAS)
e1-isdn	MM710	31	D-channel is not associated with this facility (NFAS), and the DS1's signaling-mode is set to isdnnext
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.
 - 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** *<dial-pattern>*, where *<dial-pattern>* is a dial pattern to be used on outgoing calls.
The command line prompt changes to `super-sls/dial-pattern <dial-pattern>`. 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** *<dial-pattern>*.
2. Enter **set type** *<dial-type>*, where *<dial-type>* specifies the type of outbound call and the dialing privileges available for outbound calls.
Each level of call includes the previous level's dialing privileges. For example, **loc1** has the calling privileges of **iop**, **intl**, etc.
3. Enter **set max-length** *<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 tgroup** *<tgroup>* to designate a trunk-group for which this dialed string is assigned.
6. Enter **set deny no** to permit stations to originate outgoing trunk calls.
7. At the command-line enter **set insert-digits** *<digits>* to define the digits to insert into a dialed string, if required.
8. Enter **set delete-digits** *<digits>* to define the number of digits to be deleted from a dialed string, if required.

Note:

You can either insert or delete digits, but not both.

9. Enter **show** to check the outbound dial-pattern string administration.

The report lists the dial-pattern parameters. For example:

Dialed-String/Deny	Min/Max Length	Type	Trunk Group	Delete/Insert Digits
5381000/n	9/9	loc1	2	1/303
5385000/n	9/9	loc1	3	1/720

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

Related links

[Inherited Class of Restriction \(COR\) permissions](#) on page 115

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.

Procedure

1. Enter **incoming-routing <tgnum><mode>**, where **<tgnum>** is an existing ISDN trunk group number and **mode** is the protocol used for receiving incoming digits.

<mode> can be either **enbloc** or **overlap**.

The command line prompt changes to **sls-incoming-routing <tgnum>**. If you want to remove the incoming routing treatment from the SLS administration, enter **exit** to leave the second-level incoming-routing context and return to the (super-sls)# context, and then enter **clear internal-routing <tgnum> <mode>**.

2. If the **mode** is set to **enbloc** (in Step 1), you must:
 - Enter **set delete-digits <digits>** to define the number of digits to be deleted from a dialed string.
 - Enter **set insert-digits <digits>** to define the number of digits to be inserted at the beginning of a dialed string.
 - Enter **set match-pattern <pattern>** to define the beginning digit pattern of an incoming alphanumeric dial string to be matched against.

- Enter **set length** *<length>* to define the length of the dialed string.
3. If the **mode** is set to **overlap** (in Step 1), you may configure only one of the following options:
 - Enter **set delete-digits** *<digits>* to define the number of digits to be deleted from a dialed string.
 - Enter **set insert-digits** *<digits>* to define the number of digits to be inserted at the beginning of a dialed string.

 Note:

This action takes place after the deletion task has been completed for the enbloc-receiving mode.

4. Enter **exit** to leave the incoming-routing context in SLS.
5. Enter **show** to check the incoming-routing administration.

The report lists the incoming-routing parameters for all dial patterns that have been administered. For example:

Match_pattern	Length	Del	Insert-digits	Mode	tgnum
234	7	3	5381000	enbloc	98
235	7	3	5381001	enbloc	99

Summary of SLS configuration commands

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

Root Level Commands	First Level Context Commands	Second Level Context Commands	Description
set sls	-	-	Enable or disable SLS
show sls	-	-	Display SLS status: enabled or disabled
sls	-	-	Enter the sls context
-	bri	-	Administer an ISDN Basic Rate Interface (BRI) port for SLS
-	-	set bearer-capability	Set the Information Transfer Rate field of the Bearer Capability IE in SLS
-	-	set country-protocol	Specify the ISDN Layer 3 country protocol type in SLS
-	-	set directory-number-a	Assign a directory number to the B1 channel of the BRI interface in SLS

Table continues...

Root Level Commands	First Level Context Commands	Second Level Context Commands	Description
-	-	set directory-number-b	Assign a directory number to the B2 channel of the BRI interface in SLS
-	-	set endpoint-init	Determine whether or not the far-end supports endpoint initialization in SLS
-	-	set interface	Specify the glare-handling convention for a BRI link in SLS
-	-	set interface-companding	Set the interface to agree with the companding method used by the far-end of the DS1 circuit for SLS mode
-	-	set layer1-stable	Determine whether or not to keep the physical layer active (stable) between calls in SLS
-	-	set name	Identify the user name for an ISDN facility in SLS
-	-	set side	Specify the glare-handling conditions when the set interface command is administered as peerMaster or peerSlave for the ISDN link in SLS
-	-	set spid-a	Assign a Service Profile Identifier (SPID) to the B1 channel of the BRI link in SLS
-	-	set spid-b	Assign a Service Profile Identifier (SPID) to the B2 channel of the BRI link in SLS
-	-	set tei-assignment	Select the method by which the Layer 2 (LAPD) protocol obtains its Terminal Endpoint Identification (TEI) address in SLS
-	-	show	List all BRI SLS parameters for this BRI port
-	clear attendant	-	Delete the administered attendant provisioning in SLS
-	clear bri	-	Delete the administration for a given BRI channel in SLS

Table continues...

Root Level Commands	First Level Context Commands	Second Level Context Commands	Description
-	<code>clear dial-pattern</code>	-	Delete a single dialed string pattern entry in the SLS data set
-	<code>clear ds1</code>	-	Delete the administration for a specific DS1 channel in SLS
-	<code>clear fac</code>	-	Delete an administered Feature Access Code for SLS
-	<code>clear incoming-routing</code>	-	Delete an entry for a particular incoming routed string that is associated with a given trunk group in SLS
-	<code>clear sig-group</code>	-	Delete the administration for a given ISDN signaling group in SLS
-	<code>clear slot-config</code>	-	Delete the slot and the board administration in the Branch Gateway for SLS
-	<code>clear survivable-config</code>	-	Set the SLS parameters to their default values
-	<code>clear station</code>	-	Delete a particular extension number in the SLS data set
-	<code>clear trunk-group</code>	-	Delete a trunk group entry from the SLS data set
-	<code>dial-pattern</code>	-	Administer ARS dial patterns for SLS
-	-	<code>set delete-digits</code>	Specify the number of digits to be deleted from the beginning of the dialed string for an outbound call in SLS
-	-	<code>set deny</code>	Permit or deny access to an outbound trunk in SLS
-	-	<code>set insert-digits</code>	Specify the number of digits to be inserted at the beginning of the dialed string for an outbound call in SLS
-	-	<code>set max-length</code>	Establish the maximum length of the dialed string in SLS
-	-	<code>set min-length</code>	Establish the minimum length of the dialed string in SLS
-	-	<code>set tgnum</code>	Designate the trunk-group number in SLS

Table continues...

Root Level Commands	First Level Context Commands	Second Level Context Commands	Description
-	-	set type	Administer the type of outbound call in SLS
-	-	show	List all dial-pattern SLS parameters
-	ds1	-	Administer DS1 trunks for SLS
-	-	set bearer-capability	Set the Information Transfer Rate field of the Bearer Capability IE in SLS
-	-	set bit-rate	Set the maximum transmission rate for the DS1 facility in SLS
-	-	set channel-numbering	Select the channel-numbering method for B-channels on an E1 interface in SLS
-	-	set connect	Specify the equipment at the far-end of the DS1 link in SLS
-	-	set country-protocol	Specify the ISDN Layer 3 country protocol type in SLS
-	-	set interface	Specify the glare-handling convention for a DS1 link in SLS
-	-	set interface-companding	Set the interface to agree with the companding method used by the far-end of the DS1 circuit for SLS mode
-	-	set long-timer	Increase the duration of the T303 (call establishment) timer in SLS
-	-	set name	Identify the user name for a DS1 facility in SLS
-	-	set protocol-version	Specify country protocol for countries whose public networks allow for multiple ISDN Layer 3 country protocols for ISDN Primary Rate service in SLS
-	-	set side	Specify the glare-handling conditions when the set interface command has been administered as peerMaster or peerSlave for the ISDN link in SLS

Table continues...

Root Level Commands	First Level Context Commands	Second Level Context Commands	Description
-	-	set signaling-mode	Set the signaling mode for the DS1 facility in SLS
-	-	show	List all SLS parameters for this DS1 interface
-	incoming-routing	-	Administer digit-treatment for incoming routed calls in SLS
-	-	set delete-digits	Specify number of digits to be deleted from the beginning of the dialed string for an inbound trunk call in SLS
-	-	set insert-digits	Specify number of digits to be inserted at the beginning of the dialed string for an inbound trunk call in SLS
-	-	set length	Specify the length of the dialed string in SLS
-	-	set match-pattern	Specify the beginning digit pattern of the incoming alphanumeric dial string to be matched against in SLS
-	-	show	List all incoming-routing SLS parameters
-	set attendant	-	Specify the dial access code for the attendant feature, and specify the station which serves as the branch office attendant position
-	set date-format	-	Set a date format for the SLS data set
-	set fac	-	Administer the Feature Access Code for SLS
-	set ip-codec-set	-	Configure an IP codec set within the SLS data set
-	set max-ip-registrations	-	Configure the maximum number of IP registrations allowed in the SLS data set
-	set slot-config	-	Define the slot and the board type in the Branch Gateway for SLS
-	show attendant	-	Display the administered attendant provisioning

Table continues...

Root Level Commands	First Level Context Commands	Second Level Context Commands	Description
-	show bri	-	List the administered BRI parameters for SLS
-	show date-format	-	Display the current date format for the SLS data set
-	show dial-pattern	-	List all dial-pattern strings in the SLS data set
-	show ds1	-	List the administered DS1 parameters for SLS
-	show fac	-	List the administered Feature Access Codes for SLS
-	show incoming-routing	-	Show all of the administered dial patterns in SLS for trunk groups
-	show ip-codec-set	-	List the codec set entries for SLS
-	show max-ip-registrations	-	Display the maximum IP registration administration in the SLS data set
-	show sig-group	-	List all administered signaling groups in SLS
-	show slot-config	-	Define the slot and the board administration in the Branch Gateway for SLS
-	show station	-	Display extension-specific SLS data parameters
-	show trunk-group	-	Display trunk group administration in SLS
-	sig-group	-	Administer signaling groups for SLS
-	-	add nfas-interface	Identify a list of DS1 modules that are controlled by the primary D-channel in SLS
-	-	remove nfas-interface	Remove a member from a NFAS-managed DS1 group in SLS
-	-	set associated-signaling	Specify whether the D-channel is physically present in the DS1 interface in SLS
-	-	set primary-dchannel	Identify the D-channel number in SLS

Table continues...

Root Level Commands	First Level Context Commands	Second Level Context Commands	Description
-	-	set trunk-group- chan-select	Specify the trunk-group number that can accept incoming calls in cases where the Information 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

Table continues...

Root Level Commands	First Level Context Commands	Second Level Context Commands	Description
-	-	<code>clear tac</code>	Remove a trunk access code (TAC) assignment from a trunk group in SLS
-	-	<code>remove port</code>	Remove the port assignment from a trunk group in SLS
-	-	<code>set busy-disconnect</code>	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
-	-	<code>set cbc</code>	Specify whether the ISDN trunk group will operate by declaring the service type explicitly on a call-by-call basis
-	-	<code>set cbc-parameter</code>	Specify the type of service or feature being declared in the Network Services Facility information element
-	-	<code>set cbc-service-feature</code>	Define what class of service is being specified, as part of the scocs service declared in the Network Services Facility information element
-	-	<code>set channel-preference</code>	Define how the Channel Identification IE field is encoded in SLS
-	-	<code>set codeset-display</code>	Specify which Q.931 codesets are allowed to send display information to the user phone in SLS
-	-	<code>set codeset-national</code>	Specify which Q.931 codesets are allowed to send National Information Elements to the user phone in SLS
-	-	<code>set dial</code>	Define the method for sending outbound digits in SLS
-	-	<code>set digit-handling</code>	Define how the inbound/outbound calls handle the transmission/reception of the dialed pattern in SLS

Table continues...

Root Level Commands	First Level Context Commands	Second Level Context Commands	Description
-	-	set digits	Define the inserted dial string that is added to the beginning of the received DID incoming dial string for analog DID trunks or for DS1 TIE trunks using 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
-	-	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

Table continues...

Root Level Commands	First Level Context Commands	Second Level Context Commands	Description
-	-	set trunk-hunt	Specify the trunk-hunting search within a facility in an ISDN trunk group or through a non-ISDN digital trunk group in SLS
-	-	show	List all trunk-group SLS parameters for this trunk-group

Chapter 7: Switch Ethernet port configuration

Ethernet ports on the Gateway switch

The switch on the Gateway has 10/100/1000 Mbps fixed switch ports on the front panel (ports 10/5 and 10/6).

Ethernet ports on the Branch Gateway router

The router on the Branch Gateway has 10/100 Mbps fixed router ports on the front panel (ports 10/2 and 10/4).

Cables used for connecting devices to the fixed router

Use a standard network cable when you connect one of the following devices to the fixed router port:

- WAN endpoint device
- Switch
- Router

Use a crossover network cable when you connect a computer or other endpoint device to the fixed router port. For all other Ethernet ports on the Branch Gateway, you can use either a standard network cable or a crossover network cable to connect any device.

Roadmap for configuring switch Ethernet ports

For basic configuration of a switch Ethernet port, use the commands listed below. You can also configure the following features on a switch Ethernet port:

- Advanced switching features, including VLANs.
- VoIP queuing. To configure VoIP queuing on a switch port, configure a VLAN for the port. Then configure VoIP queuing on the VLAN.
- Access control policy lists and QoS policy lists. To configure policy lists on a switch port, configure a VLAN for the port. Then configure policy on the VLAN.
- SNMP Link Up and Link Down traps.

Related links

[Advanced switching](#) on page 311

[Commands used to configure QoS parameters](#) on page 212

[Policy lists](#) on page 504

[SNMP trap configuration](#) on page 290

Summary of switch Ethernet port configuration CLI commands

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

Command	Description
<code>set port auto-negotiation-flowcontrol-advertisement</code>	Set the flow control advertisement for the specified Gigabit Ethernet ports when performing auto-negotiation
<code>set port duplex</code>	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.
<code>set port enable disable</code>	Enable or disable a port or a range of ports
<code>set port flowcontrol</code>	Set the send/receive mode for flow control frames (IEEE 802.3x or proprietary) for a full-duplex port
<code>set port level</code>	Set the default packet priority level for untagged packets
<code>set port name</code>	Configure a name for a port

Table continues...

Command	Description
<code>set port negotiation</code>	Enable or disable auto-negotiation on the port
<code>set port speed</code>	Set the speed of a port or range of ports
<code>show port auto-negotiation-flowcontrol-advertisement</code>	Display the flow control advertisement for a Gigabit port used to perform auto-negotiation
<code>show port edge state</code>	Display the edge state of a port
<code>show port flowcontrol</code>	Display port flow control information
<code>set port duplex</code>	Configure the duplex type (full or half-duplex) of an Ethernet or Fast Ethernet port or range of ports
<code>set port edge admin state</code>	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).
<code>set port enable disable</code>	Enable or disable a port or a range of ports
<code>set port flowcontrol</code>	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 <code>show port flowcontrol</code> command to display port flow control information.
<code>set port level</code>	Set the default packet priority level for untagged packets Packets traveling through a port set at normal priority must be served only after packets traveling through a port set at high priority are served.
<code>set port name</code>	Configure a name for a port
<code>set port negotiation</code>	Enable or disable auto-negotiation on the port When negotiation is enabled, the speed and duplex of a Fast Ethernet port is determined by auto-negotiation. If negotiation is disabled, the user can set the speed and duplex of a Fast Ethernet port.
<code>set port point-to-point admin status</code>	Set the connection type of the port to one of the following arguments: • force-true. The port is treated as if it were connected point-to-point • force-false. The port is treated as if it were connected to shared media • auto. The Branch Gateway tries to automatically detect the connection type of the port

Table continues...

Command	Description
<code>set port speed</code>	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.
<code>show port edge state</code>	Display the edge state of a port
<code>show port flowcontrol</code>	Display port flow control information

Configuring the WAN Ethernet port

Procedure

1. Use the `interface fastethernet 10/2` or `interface fastethernet 10/4` command to enter the context of the port interface.
2. Perform basic configuration of the interface.
3. Use the Ethernet WAN port configuration commands in the context of the port interface.

Related links

[Interface configuration](#) on page 388

Roadmap for configuring additional features on the WAN Ethernet port

- Primary Management Interface (PMI).
- Advanced router features.
- VoIP queuing.
- Access control policy lists and QoS policy lists.
- SNMP Link Up and Link Down traps.

Related links

[Primary Management Interface \(PMI\) configuration](#) on page 64

[Router](#) on page 387

[Commands used to configure QoS parameters](#) on page 212

[Policy lists](#) on page 504

[SNMP trap configuration](#) on page 290

WAN Ethernet port traffic shaping

You can use traffic shaping to determine the data transfer rate on the WAN Ethernet port. To set traffic shaping, use the `traffic-shape rate` command in the interface context. To disable traffic shaping, use the `no` form of the `traffic-shape rate` command. Traffic shaping works in tandem with the configured bandwidth. If you change the traffic shape rate, this automatically

changes the bandwidth. Similarly, if you change the bandwidth, this automatically changes the traffic shape rate.

 Note:

The traffic shape rate is determined in bits. The bandwidth is determined in kilobytes.

Related links

[Commands used to configure QoS parameters](#) on page 212

About backup interfaces

You can configure backup relations between a pair of any Layer 2 Serial interfaces, including the FastEthernet interface.

Related links

[Backup interfaces](#) on page 239

Summary of WAN Ethernet port configuration CLI commands

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

Root level command	Command	Description
interface fastethernet		Enter interface fastethernet configuration mode
	autoneg	Set the port speed and duplex to auto-negotiation mode
	no autoneg	Disable the auto-negotiation mode
	duplex	Set the duplex setting (full or half) for the interface
	keepalive-track	Bind an object tracker to the interface to check whether it is up When activated, the object tracker sends health check packets at defined intervals to the other side of the interface. If the configured number of consecutive keepalive requests are not answered, the interface track state changes to down. The object tracker continues monitoring the interface, and when its track state changes to up, the interface state changes to up.
	shutdown	Set the administrative status of the current interface to down or up
	no shutdown	Restore the administrative status of the interface to up.
	speed	Set the speed for the interface
	traffic-shape rate	Configure traffic shaping for outbound traffic on the current interface

DHCP client configuration

You can configure Branch Gateway to function as a DHCP (Dynamic Host Configuration Protocol) client.

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

In addition to receiving an IP address, Branch Gateway DHCP client can optionally request to receive a domain name, a list of default routers, and a list of available DNS servers.

 Note:

Branch Gateway can function as both a DHCP server and a DHCP client simultaneously. That is, you can connect a cable modem for an Internet connection to the WAN Fast Ethernet in order to use Branch Gateway as a DHCP client. At the same time, you can activate the DHCP server on Branch Gateway for use by clients, such as, IP phones and PCs connected to the LAN ports. The DHCP server on Branch Gateway does *not* serve Internet devices connected over the WAN Fast Ethernet ports.

You can also enable the DHCP client on the VLAN interface.

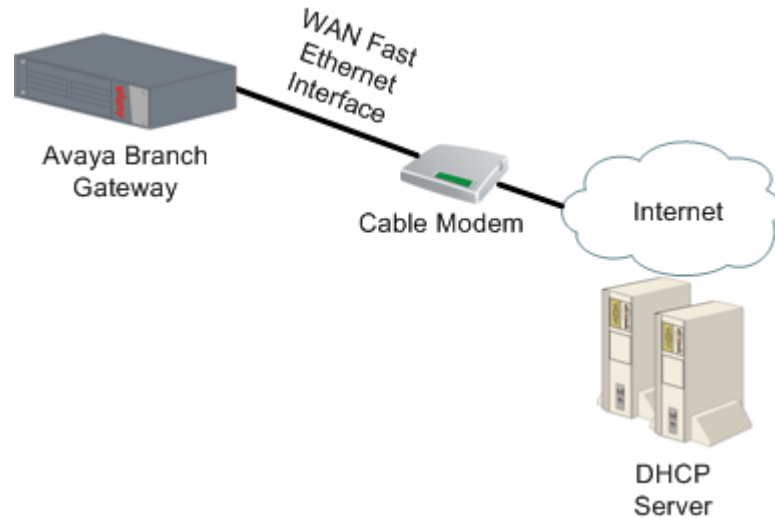
The DHCP client only supports IPv4.

Related links

[DHCP server](#) on page 409

DHCP client applications

The typical application of DHCP client in Branch Gateway involves requesting and receiving an IP address from the service provider's DHCP server, to enable a broadband Internet connection via cable modem.



Configuring the DHCP client

Procedure

1. Enter the context of the FastEthernet interface.

For example:

```
Gxxx-001# interface fastethernet 10/2
Gxxx-001(config-if:FastEthernet 10/2) #
```

2. Optionally, configure DHCP client parameters.

If you do not configure these parameters, their default values are used:

- Use the **ip dhcp client client-id** command to set the client identifier for the DHCP client. By default, the client identifier is usually the MAC address of the Branch Gateway FastEthernet interface.
- Use the **ip dhcp client hostname** command to set the hostname for the DHCP client. By default, the DHCP client uses the Branch Gateway's hostname.
- Use the **ip dhcp client lease** command to set the lease requested by the DHCP client. The lease is the length of time that the IP address provided by the DHCP server remains in effect. By default, the client does not request a specific lease from the DHCP server and uses the lease set by the DHCP server.
- Use the **ip dhcp client request** command to determine which DHCP options the DHCP client requests from the DHCP server. By default, the DHCP client requests all DHCP options.

For example:

```
Gxxx-001(config-if:FastEthernet 10/2) # ip dhcp client client-id hex
01:00:04:0D:29:DC:68
Done!
Gxxx-001(config-if:FastEthernet 10/2) # ip dhcp client hostname "Gxxx-A"
Done!
Gxxx-001(config-if:FastEthernet 10/2) # ip dhcp client lease 1 4 15
```



```
Done!
Gxxx-001(config-if:FastEthernet 10/2)# no ip dhcp client request domain-name
Done!
```

3. Optionally, use the **ip dhcp client route track** command to apply an object tracker to monitor the DHCP client's default route.

The object tracker continuously checks the validity of the default route, that is, whether data can be transmitted over the default route. Whenever the object tracker determines that the default route has become invalid, the route is dropped from the routing table and traffic is routed to alternate routes. If the default route becomes valid again, it is added back to the routing table.

Note that if several default routers are learned from a specific interface, the object tracker tracks only the first one.

For example:

```
Gxxx-001(config-if:FastEthernet 10/2)#ip dhcp client route track 3
Done!
```

4. Enable the DHCP client by entering **ip address dhcp**.

A message appears, displaying the IP address and mask assigned by the DHCP server. For example:

```
Gxxx-001(config-if:FastEthernet 10/2)# ip address dhcp
Done!
Interface FastEthernet 10/2 assigned DHCP address 193.172.104.161, mask
255.255.255.0
```

 Note:

Whenever you change the value of a DHCP client parameter (such as, client-id, or client hostname), enter **ip address dhcp** again to re-initiate DHCP address negotiation using the new values.

5. Use the **show ip dhcp-client** command to view the DHCP client parameters.

Related links

[Object tracking provisioning](#) on page 267

[Typical application – tracking the DHCP client default route](#) on page 274

[Summary of DHCP Server commands](#) on page 415

Examples of DHCP lease release and renew

- The **release dhcp** command example:

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

- The **renew dhcp** command example:

```
(super)# renew dhcp FastEthernet 10/2
Done!
```

A message appears displaying the IP address and mask assigned by the DHCP server. For example:

```
Interface FastEthernet 10/2 assigned DHCP address 193.172.104.161, mask 255.255.255.0
```

For a description of these commands, see *Avaya G450 Branch Gateway CLI Reference*.

Commands used for DHCP client maintenance

- `show ip dhcp-client`
- `show ip dhcp-client statistics`
- `clear ip dhcp-client statistics`

For a description of these commands, see *Avaya Branch Gateway G450 CLI Reference*

Examples of configuring DHCP client logging messages

- `set logging session enable` command example.

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

- `set logging session condition dhcpc` example:

```
Gxxx-001# set logging session condition dhcpc Info
Done!
CLI-Notification: write: set logging session condition dhcpc Info
```

 Note:

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

For a description of these commands, see *Avaya G450 Branch Gateway CLI Reference*.

Related links

[System logging](#) on page 191

Summary of DHCP client configuration CLI commands

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

Root level command	Command	Description
<code>clear ip dhcp-client statistics</code>	-	Clear the DHCP client statistics counters
<code>interface fastethernet</code>	-	Enter interface fastethernet configuration mode
-	<code>clear ip dhcp-client statistics</code>	Clear the DHCP client statistics counters

Table continues...

Root level command	Command	Description
-	<code>ip address dhcp</code>	Enable or disable IP address negotiation via DHCP (applies to WAN FastEthernet interfaces only)
-	<code>ip dhcp client client-id</code>	Set the client identifier for the DHCP client
-	<code>ip dhcp client hostname</code>	Set the client hostname for the DHCP client
-	<code>ip dhcp client lease</code>	Set the lease requested by the DHCP client
-	<code>ip dhcp client request</code>	Specify which DHCP options the DHCP client requests from the DHCP server
-	<code>ip dhcp client route track</code>	Apply object tracking in order to monitor the DHCP client's default route
-	<code>show ip dhcp-client</code>	Display the configuration of the DHCP client
-	<code>show ip dhcp-client statistics</code>	Display the DHCP client statistics counters
<code>release dhcp</code>	-	Releases a DHCP lease for an interface. This effectively releases the client IP address, and no IP address is allocated to the specified interface.
<code>renew dhcp</code>	-	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.
<code>show ip dhcp-client</code>	-	Display the configuration of the DHCP client
<code>show ip dhcp-client statistics</code>	-	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 enables 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 through 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 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 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 through chassis ID and port ID values. Multiple LLDP devices can reside on a single port, using a hub for example, and all the devices are reported through MIB. You can enable (Rx-only, TX-only, and Rx or Tx) or disable LLDP mode of operation on a per-port basis.

Supported TLVs

Mandatory TLVs

- End-of-LDPDU
- Chassis ID
- Port ID
- Time to Live

Optional TLVs

- Port description
- System description
- System name
- System capabilities
- Management address

Optional 802.1 TLVs

- VLAN name
- Port VLAN

Configuring LLDP

Procedure

1. Enable the LLDP agent globally using the **set 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.

Supported ports for LLDP

You can configure only ports 10/5 and 10/6 to support LLDP.

Summary of LLDP configuration CLI commands

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

Command	Description
<code>set lldp re-init-delay</code>	Set the delay from when a port is set to LLDP “disable” until re-initialization is attempted
<code>set lldp system-control</code>	Enable or disable the LLDP application globally per device or stack
<code>set lldp tx-delay</code>	Set the TxDelay , which is the minimal delay in seconds between successive LLDP frame transmissions, on each port
<code>set lldp tx-hold-multiplier</code>	Set the TxHoldMultiplier , which is a multiplier on the TxInterval that determines the actual TTL value sent in an LLDP frame
<code>set lldp tx-interval</code>	Set the TxInterval , the interval at which the device transmits LLDP frames
<code>set port lldp</code>	Change the administrative LLDP status of a port
<code>set port lldp tlv</code>	Enable or disable the transmission of the optional TLVs on a per port basis
<code>show lldp</code>	Display the LLDP information received on each port
<code>show lldp config</code>	Display the global LLDP configuration
<code>show port lldp config</code>	Display port-level LLDP configuration
<code>show port lldp vlan-name config</code>	Show the VLANs that are being transmitted on a specific port

Chapter 8: System logging

System logging is a method of collecting system messages generated by system events. The Branch Gateway includes a logging package that collects system messages in several output types. Each of these types is called a sink. When the system generates a logging message, the message can be sent to each sink that you have enabled.

System messages do not always indicate problems. Some messages are informational, while others may help to diagnose problems with communications lines, internal hardware, and system software.

By default, all sinks are disabled. When enabled, log file and Syslog sink settings can be saved by using the command: **copy running-config startup-config** to save the running configuration to the startup configuration. However, the Session sink and its settings are deleted when the session is terminated.

You can define filters for each sink to limit the types of messages that the sink receives.

The logging facility logs configuration commands entered through the CLI or SNMP, and system traps and informative messages concerning the functioning of various processes. However, a user with user privileges who enables the log can only see the entered commands. For example, a user with read-only privileges cannot see entered commands having a read-write user level. In addition, the log does not display confidential information, such as, passwords and VPN pre-shared keys.

Related links

[Logging filter configuration](#) on page 200

Types of logging sinks

Sink	Description
Syslog	Logging messages are sent to up to three configured servers, using Syslog protocol as defined in RFC 3164. Messages sent to the Syslog server are sent as UDP, TCP, and TLS messages.
Log file	Logging data is saved in the flash memory. These compressed, cyclic files serve as the system logging database.

Table continues...

Sink	Description
Session	Logging messages are sent to the terminal screen as follows: • For a local connection, messages appear online on the local terminal. • For a remote Telnet/SSH connection, messages appear online on the remote terminal. This sink is deleted whenever a session ends.

Syslog server configuration

A Syslog server is a remote server that receives logging messages using the Syslog protocol. This enables storage of large log files that you can use to generate reports.

Defining Syslog servers

About this task

You can define up to three Syslog servers with either IPv4 or IPv6 addresses..

Procedure

1. Define the Syslog server by entering **set logging server** followed by the IP address of the server and optionally the transport (UDP, TCP or TLS) and server port.

For example (UDP Syslog server):

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

or (TLS Syslog server and certificate for TLS connection):

```
Gxxx-001(super)# set logging server 2001:db8::2179::1 tls
Gxxx-001(super)# copy scp root-ca syslog syslogcert.crt 172.16.1.22
```

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 to enable the server.

For example:

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

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
 - alert. Log alert
 - audi. Log audit
 - clkd. Clock daemon
 - clkd2. Clock daemon
 - daemon. Background system process
 - ftpd. FTP daemon
 - kern. kernel
 - local0 – local7. For local use
 - lpr. Printing
 - mail. Electronic mail
 - news. Usenet news
 - ntp. NTP subsystem
 - sec. Security
 - syslog. System logging
 - uucp. Unix-to-Unix copy program
 - user. User process
4. Optionally, limit access to the Syslog server output by typing the **set logging server access-level** command, followed by an access level (read-only, read-write, or admin) and the IP address of the Syslog server.

If you do not define an access level, the default read-write level is used.

For example:

```
Gxxx-001(super)# set logging server access-level read-only 147.2.3.66
Done!
```

Only messages with the appropriate access level are sent to the Syslog output.

5. Optionally, define filters to limit the types of messages received.

Related links

[Logging filter configuration](#) on page 200

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 10.129.179.178
*****
Message logging configuration of SYSLOG sink ***
Sink Is Enabled
Sink default severity: Warning
Server name: 10.129.179.178
Transport Type: TLS
TLS state: connected
Port: 6514
Server facility: local7
Server access level: read-write
```

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 a product identification number.

Commands used to copy a syslog file

You can copy the syslog file from Branch Gateway to another location using FTP, SCP, TFTP, or HTTPS or locally to a USB mass storage device.

Use any of the following commands to copy a syslog file:

- `copy syslog-file ftp.`
- `copy syslog-file scp`
- `copy syslog-file tftp`
- `copy syslog-file usb`
- `copy syslog-file https`
- `copyedge syslog-file scp`

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

Related links

[Summary of logging configuration CLI commands](#) on page 204

Configuring a log file

About this task

A log file is a file of data concerning a system event, saved in the flash memory. The log files serve as the system logging database, keeping an internal record of system events.

Procedure

1. Enter **set logging file enable**.

```
Gxxx-001(super)# set logging file enable
Done!
```

2. Optionally, define filters to limit the types of messages received.

Related links

[Logging filter configuration](#) on page 200

Disabling logging system messages to a log file

Procedure

Enter **set logging file disable**.

```
Gxxx-001(super)# set logging file disable
Done!
```

Deleting current log file and opening an empty log file

Procedure

Enter **clear logging file**

```
Gxxx-001(super)# clear logging file
Done!
```

Example display of log file messages

The **show logging file content** command displays the messages in the log file. Note that the user enabling the log sees only entered commands with a user-level no higher than the user's privileges. A user with read-only privileges does not see entered commands that have a read-write user level.

Example

```
(super)# show logging file content
<190>Aug 23 16:28:32 149.49.77.11 -NoTag: -NoUTC 2015 055 1
mediagateway.g430 | 0 coldStart[BOOT-Informational: System boot up
from cold reset, ID=e34d38263d29a5246ce93aa5b666f884
<187>Aug 23 16:28:32 149.49.77.11 -NoTag: -NoUTC 2015 525 1
mediagateway.g430 | 0 MSY-TRPMAJNA[VOICE-Error: No Call Controller
Found, ID=e34d38263d29a5246ce93aa5b666f884
<190>Aug 23 14:30:25 149.49.77.11 -NoTag: -NoUTC 2015 965 1
mediagateway.g430 | 0 BOOT MESSAGE[BOOT-Informational: Booting from
bank B with firmware version 29.22.50, ID=N/A
<190>Aug 23 14:30:25 149.49.77.11 -NoTag: -NoUTC 2015 965 1
mediagateway.g430 | 0 coldStart[BOOT-Informational: System boot up
from cold reset, ID=e34d38263d29a5246ce93aa5b666f884
<187>Aug 23 14:30:25 149.49.77.11 -NoTag: -NoUTC 2015 425 1
mediagateway.g430 | 0 MSY-TRPMAJNA[VOICE-Error: No Call Controller
Found, ID=e34d38263d29a5246ce93aa5b666f884
```

Example display of conditions defined for the file output sink

The following example shows the output from the **show logging file condition** command.

Example

```
(super)# show logging file condition
*****
*** Message logging configuration of FILE      sink ***
Sink Is Enabled
Sink default severity: Informational
```

Log file message format

Log file messages appear in first-in, last-out order. They have the following format:

```
08/23/2015,10:55:09:CLI-Notification: root:    set port disable 10/6
08/23/2015,10:49:03:SWITCHFABRIC-Notification: Port Connection Lost on Module 10
port 5
```

Each message provides the following information:

- Severity
- The date and time (if available)
- The logging application
- The process ID (if available)
- The UTC offset (if available)
- The year
- Milliseconds
- Log format
- The severity level
- The Branch Gateway type
- The message text

set logging file retention

Defines the period of time in days that log content will be retained.

Syntax

```
set logging file retention {retention_days}
```

retention_days must be either:

- A value between 1 and 9999, inclusive
- Unlimited

Example:

```
# set logging file retention unlimited
Log retention time is unlimited.
Done!
```

```
# show logging file retention
Log retention time is unlimited.
Done!
```

```
# set logging file retention 30
Log retention time is 30 days.
Done!
```

```
# show logging file retention
Log retention time is 30 days.
Done!
```

```
# set logging file retention 10000
Error: Parameter 1 (<retention_days>) value (10000) > maximum value(9999)
set logging file retention -- Set log retention time in days
Syntax : set logging file retention <retention_days>
```

show logging file retention

Shows the period of time in days that has been set using the **set logging file retention** command

Syntax

show logging file retention

Example:

```
# set logging file retention 30
Log retention time is 30 days.
Done!
```

```
# show logging file retention
Log retention time is 30 days.
Done!
```

Configuring a session log

About this task

A session log is the display of system messages on the terminal screen. It is automatically deleted when a session ends.

Procedure

1. Enter **set logging session enable**.

```
Gxxx-001(super)# set logging session enable
Done!
```

*** Note:**

If the device is connected to several terminals, a separate session log is established for each terminal.

2. Optionally, define filters to limit the types of messages received.

Example discontinuation of the display of system messages

The following output is an example of the `set logging session disable` command used to discontinue the display of system messages to the terminal screen.

Example

```
(super)# set logging session disable
Done!
```

Example display of session logging configuration

The following output is an example of the `show logging session condition.` command that displays whether session logging is enabled or disabled, and lists all filters defined for session logging.

Example

```
(super)# show logging session condition
*****
*** Message logging configuration of SESSION sink ***
Sink Is Enabled
Sink default severity: Warning
Session source ip: 172.16.1.231
```

Session logging message format

Session logging messages are arranged chronologically and have the format shown in the following example:

```
08/23/2015,10:49:03:SWITCHFABRIC-Notification: Port Connection Lost on Module 10
port 5 was cleared
08/23/2015,10:55:09:CLI-Notification: root:  set port disable 10/6
```

Each message provides the following information:

- The date and time (if available)
- The logging application
- The severity level
- The message text

*** Note:**

The user enabling the log only sees entered commands with a user-level no higher than the user's own privileges. For example, a user with read-write privileges cannot see entered commands with an admin user level.

Logging filter configuration

You can use filters to reduce the number of collected and transmitted messages. The filtering options are based on message classification by severity for each application. For a specified sink, you can define the threshold severity level for message output for each application. Messages pertaining to the specified applications, that have a severity level stronger than or equal to the defined threshold, are sent to the specified sink. Messages with a severity level weaker than the defined threshold are not sent.

Commands used to set the logging filters

For each sink, you can set logging filters by specifying a severity level per application, as follows:

- **set logging server condition application severity ip address** creates a filter for messages sent to a specified Syslog server.
- **set logging file condition application severity** creates a filter for messages sent to a log file.
- **set logging session condition application severity** creates a filter for messages sent to a session log on a terminal screen where:
 - **application** is the application for which to view messages (use all to specify all applications).
 - **severity** is the minimum severity to log for the specified application (use none to disable logging messages for the specified application).
 - **ip address** is the IP address of the Syslog server.

For example:

```
Gxxx-001(super)# set logging server condition dialer critical 147.2.3.66
Done!
Gxxx-001(super)# set logging file condition dhcp 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

Table continues...

Severity level	Code	Description
critical	2	Critical condition
error	3	Error condition
warning	4	Warning condition
notification	5	Normal but significant condition
informational	6	Informational message only
debugging	7	Message that only appears during debugging

Default sink severity levels

Syslog: Warning

Log file: Informational

Session from terminal: Informational

Session from telnet/ssh: Warning

Application filtering

You can define filters for any application listed in the following table.

Application	Description
arp	Address Resolution Protocol mechanism
boot	System startup failures
cdr	Call Detail Recording. Registers the active calls in SLS mode.
cli	CLI
config	Configuration changes
console	Serial modem messages
dhcp-relay	DHCP requests relaying
dhcpc	DHCP client package
dhcps	DHCP server package
dialer	Dialer interface messages
dnsc	DNS client package
fan	Cooling system
filesystem	File system problem (flash)
ids	IDS events, specifically a SYN attack heuristic employed by the SYN cookies feature
iphc	IP header compression
ipsec	VPN IPSEC package
isakmp	VPN IKE package

Table continues...

Application	Description
ospf	Open Shortest Path First protocol
policy	Policy package
ppp	PPP protocol
pppoe	PPP over Ethernet
proxy-arp	Proxy ARP
qos	QoS messages
router	Core routing system failures
rtp-stat	RTP MIB statistics
saa	RTR-probes messages
security	Secure logging (authentication failure)
snmp	SNMP agent
stp	Spanning tree package
supply	Power supply system
switchfabric	Switch fabric failures
system	Operating system failures
tftp	Internal TFTP server
threshold	RMON alarms
tracker	Object tracker messages
usb	USB devices messages
usb-modem	USB modem messages
vj-comp	Van Jacobson header compression messages
vlan	VLAN package
voice	Voice failures
wan	WAN plugged-in expansion

Syslog server example

The following example defines a Syslog server with the following properties:

- IP address 147.2.3.66
- Logging of messages enabled
- Output to the Kernel facility
- Only messages that can be viewed by read-write level users are received
- Filter restricts receipt of messages from all applications to those less severe than error

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

```
Gxxx-001(super)# set logging server access-level read-write 147.2.3.66
Done!
Gxxx-001(super)# set logging server condition all error 147.2.3.66
Done!
```

Log file example

The following example enables the logging of system messages to a log file in the flash memory and creates a filter to restrict the receipt of messages from the **boot** application to those with severity level of informational or more severe, and messages from the **cascade** application to those with severity level of alert or more severe.

```
Gxxx-001(super)# set logging file enable
Done!
Gxxx-001(super)# set logging file condition boot informational
Done!
Gxxx-001(super)# set logging file condition cascade alert
Done!
```

Session log example

The following example enables a session log for a user wishing to debug the ISAKMP application, while only receiving messages of severity level error or stronger for all other applications. Therefore, the user sets the default severity level for all applications to error, and then sets the severity of the ISAKMP application to informational. Finally, the user displays the filter settings.

```
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
```

Accessing diagnostic logs

About this task

Use this procedure to capture log files.

Procedure

1. Log on to the gateway as root.
2. Enable screen capture logging in your terminal emulation program.
3. Run the **show all logs** command.

4. Send a copy of the screen capture log file to Avaya through an email or as an attachment.

For more information about accessing diagnostic logs, see *CLI Reference Avaya Branch Gateway G450*, 03-602056.

For example:

```
iW}ZH~YL{ }Z (^E^M)=}EsZ^E}Z
ZH~YL{ }Zj^M}ZZZZZZDZJ@_3
Zl{~=ZNLMR}EZZZZZZDZw3_
Zl~'=';^E}ZK}EsZ~NZDZ"@:w:_3
Z!lZjLMR}EZZZZZZDZ0:w
ZiW}Zl^>}YZn^=^ZzsDZ

))))))))))))))))))))))))))))))))))))))))))))))))))))))))))))

Z###Z.dizM}DZwD0TD0_Z###Z

?glgiZA~/2z{ }Z}Md=OZ

))))))))))))))))))))))))))))))))))))))))))))))))))))))))))))
ZZg??onZZZZHHpnn WWDMMDss:WsZZZZgKgjiZhtjnAgZZZZZZg??j+ZZZZZZZt.qwZZZZZZZt.q0
      Z              Z              Z              Z
Z
ZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZli?
ZZZZZZZZZZZZ

))))))))))))))))))))))))))))))))))))))))))))))))))))))))))))
Z?glgiZonZZHHpnn WWDMMDss:WsZZZZZZZZZZZZZZZZZZZZZZZZZZZZZZli?
      Z
Z

))))))))))))))))))))))))))))))))))))))))))))))))))))))))))))
G450-gloin-031 (super) #
```

Summary of logging configuration CLI commands

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

Command	Description
<code>copy syslog-file ftp</code>	Copy the syslog file to a remote server using FTP
<code>copy syslog-file scp</code>	Copy the syslog file to a remote server using SCP
<code>copy syslog-file tftp</code>	Copy the syslog file to a remote server using TFTP
<code>copy syslog-file usb</code>	Upload the syslog file from the Branch Gateway to the USB mass storage device
<code>copy syslog-file https</code>	Copy the syslog file to a remote server using HTTPS
<code>copyedge syslog-file scp</code>	Copy the syslog file to a remote server using SCP via Avaya SBC tunnel

Table continues...

Command	Description
<code>clear logging file</code>	Delete the message log file being stored in non-volatile memory (NVRAM), including the history log, and open a new, empty log file
<code>clear logging server</code>	Delete the specified Syslog message server from the Syslog server table
<code>set logging file</code>	Manage the logging of system messages to non-volatile memory (NVRAM)
<code>set logging server</code>	Define a new Syslog output server for remote logging of system messages
<code>set logging server access-level</code>	Set the access level associated with a Syslog server sink
<code>set logging server condition</code>	Set a filter for messages sent to the specified Syslog server. Messages can be filtered by source system, severity, or both.
<code>set logging server enable disable</code>	Enable or disable a specific Syslog server
<code>set logging server facility</code>	Define an output facility for the specified Syslog server
<code>set logging session</code>	Manage message logging for the current console session
<code>show logging file condition</code>	Display all conditions that have been defined for the file output sink
<code>show logging file content</code>	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.
<code>show logging server condition</code>	Display the filter conditions defined for the Syslog output sink
<code>show logging session condition</code>	Display the filter conditions defined for message logging to the current console session

Chapter 9: VoIP QoS

Branch Gateway provides voice services over IP data networks using VoIP. VoIP is a group of protocols for transmitting and receiving various types of voice data over an IP network. VoIP includes protocols for transmitting and receiving the following types of information:

- Digitally encoded voice data
- Call signalling information
- Call routing information
- QoS information

VoIP uses the RTP and RTCP protocols to transmit and receive digitally encoded voice data.

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

RTP and RTCP configuration

VoIP uses the RTP and RTCP protocols to transmit and receive digitally encoded voice data. RTP and RTCP are the basis of common VoIP traffic. RTP and RTCP run over UDP and incur a 12-byte header on top of other (IP, UDP) headers. Running on PPP or frame relay, these protocols can be compressed.

Header compression configuration

Header compression reduces the size of packet headers, thus reducing the amount of bandwidth needed for data. The header compression method is because of the header fields remain constant or change in predictable ways throughout the session. Thus, instead of constantly retransmitting the header, each side keeps a context table of the sessions (the normal headers), and while sending and receiving packets it replaces the full-length headers with one or two bytes CID (context-id) plus unpredictable deltas from the last packet.

The Branch Gateway offers both RTP header compression, for reducing the amount of bandwidth needed for voice traffic, and TCP and UDP header compression, for reducing the amount of bandwidth needed for non-voice traffic.

For header compression purposes, any UDP packet with an even destination port within a user-configurable range of ports, is considered an RTP packet.

The Branch Gateway enables decompression whenever compression is enabled. However, when enabling header compression on a Frame Relay interface, you must first verify that the remote host is also employing header compression. Header compression on a Frame Relay interface does not check what the remote host is employing. Thus, it may compress headers even when the remote host is not configured to decompress headers.

You can configure how often a full header is transmitted, either as a function of time or of transmitted compressed packets.

Header compression configuration options

The Branch Gateway offers two options for configuring header compression:

- IP Header compression (IPHC) method, as defined by RFC 2507. IPHC-type compression applies to RTP, TCP, and UDP headers.
- Van Jacobson (VJ) method, as defined in RFC 1144. VJ compression applies to TCP headers only.

Note:

VJ compression and IPHC cannot co-exist on an interface, and IPHC always overrides VJ compression. Thus, if you define both VJ compression and IPHC, only IPHC is enabled on the interface regardless of the order of definition.

Header compression support by interface

Interface type		Supported compression methods
Serial	-	-
-	PPP	IPHC and VJ
-	Sub-Frame-Relay with IETF encapsulation	IPHC only
-	Sub-Frame-Relay with non-IETF encapsulation	RTP header compression using the IPHC method, and TCP header compression using the VJ method
Dialer		IPHC and VJ

Note:

Non-IETF encapsulation is compatible with other vendors.

Configuring IPHC

About this task

IPHC 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:**

After 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 IP Header compression CLI commands

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

Root level command	First level command	Description
<code>clear ip rtp header-compression</code>	-	Clear IP RTP header compression statistics for all enabled interfaces or for a specific interface. To clear RTP compression statistics for all enabled interfaces, do not enter an interface type and number. Clearing the statistics does not cause renegotiation of parameters.
<code>clear ip tcp header-compression</code>	-	Clear TCP header compression statistics for all enabled interfaces or for a specific interface. To clear TCP compression statistics for all enabled interfaces, do not enter an interface type and number. Clearing the statistics does not cause renegotiation of parameters.
<code>interface (dialer serial)</code>	-	Enter the Dialer or Serial interface context
-	<code>ip rtp compression-connections</code>	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
-	<code>ip rtp header-compression</code>	Enable both RTP and TCP header compression on the current interface
-	<code>ip rtp max-period</code>	Set the maximum number of compressed headers that can be sent between full headers
-	<code>ip rtp max-time</code>	Set the maximum number of seconds between full headers
-	<code>ip rtp non-tcp-mode</code>	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 .
-	<code>ip rtp port-range</code>	Set the range of UDP ports considered as RTP on the current interface
-	<code>ip tcp compression-connections</code>	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.

Table continues...

Root level command	First level command	Description
<code>show ip rtp header-compression</code>	-	Display header compression statistics for a specific interface. If no interface is specified, statistics for all interfaces are displayed.
<code>show ip rtp header-compression brief</code>	-	Display a subset of header compression statistics in the form of a table
<code>show ip tcp header-compression</code>	-	Display TCP header compression statistics for a specific interface
<code>show ip tcp header-compression brief</code>	-	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.
- 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:**

After header compression is enabled, any change to a header compression parameter is effective.

3. To disable VJ TCP header compression on an interface, use the **no ip tcp header-compression** command in the interface context.

Summary of Van Jacobson header compression CLI commands

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

Root level command	First level command	Description
clear ip tcp header-compression	-	Clear TCP header compression statistics for all enabled interfaces or for a specific interface
interface (dialer serial)	-	Enter the Dialer or Serial interface context
-	ip tcp compression-connections	Set the total number of TCP header compression connections supported on the current interface
-	ip tcp header-compression	Enable TCP header compression on the current interface
show ip tcp header-compression	-	Display TCP header compression statistics for a specific interface. If no interface is specified, statistics for all interfaces are displayed. Use this command regardless of which compression method is employed.
show ip tcp header-compression brief	-	Display a subset of TCP header compression statistics in the form of a table

Commands used to display and clear header compression statistics

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

- **show ip rtp header-compression**
- **show ip tcp header-compression**
- **clear ip rtp header-compression**
- **clear ip tcp header-compression**

Commands used to configure QoS parameters

Branch Gateway uses MGCP (H.248) protocol for call signalling and call routing information. Use the following commands to configure QoS for signalling and VoIP traffic.

- `set qos control`
- `set qos signal`
- `show qos-rtcp`
- `set qos bearer`

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

Commands used to configure RTCP QoS parameters

Use the following commands to set the RTCP QoS parameters.

- `set qos rtcp`
- `show qos-rtcp`

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

Commands used to configure RSVP parameters

VoIP can use the RSVP protocol to reserve network resources for voice data while communicating with other Gateways and other VoIP entities, such as, IP phones and Softphones.

- `set qos rsvp`
- `show qos-rtcp`

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

Summary of QoS, RSVP, and RTCP configuration CLI commands

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

Command	Description
<code>set qos bearer</code>	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).
<code>set qos control</code>	Define the source for QoS control parameters: local or remote
<code>set qos rsvp</code>	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).

Table continues...

Command	Description
set qos rtcp	Set values for RTCP parameters. The RTCP parameters that can be set include enabling or disabling RTCP reporting capability, setting the IP address of the monitor, setting the reporting period (the default is five seconds), and defining the listening port number. This command supports IPv4 and IPv6.
set qos signal	Set QoS signaling parameters (DSCP or 802.1Q) for the Media Gateway Processor.
show qos-rtcp	Display QoS, RSVP, and RTCP parameters for IPv4 and IPv6.

Weighted Fair VoIP Queuing

Weighted Fair VoIP Queuing (WFVQ) combines Weighted Fair Queuing (WFQ) for data streams and priority VoIP queuing to provide the real-time response time that is required for VoIP.

WFQ applies 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 SSH. 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. Also, this is the only queueing mode available on a per-PVC basis for serial interfaces when frame relay traffic shaping is enabled.

Summary of WFVQ configuration CLI commands

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

Root level command	Command	Description
interface (serial fastethernet dialer)	-	Enter the Serial, FastEthernet, or Dialer interface configuration context
-	fair-queue-limit	Specify the maximum number of packets that can be queued in the weighted fair queue. The upper and lower limits of this command depend on the amount of bandwidth configured for the interface. Use this command only for troubleshooting.
-	fair-voip-queue	Enable Weighted Fair VoIP Queuing (WFVQ) on the current interface. WFVQ is the recommended queuing mode for interfaces. The no form of the fair-voip-queue command does not exist. If you enter the command no fair-voip-queue , it will actually enable WFVQ if WFVQ is not already enabled.

Table continues...

Root level command	Command	Description
-	priority-queue	Enable or disable priority queueing mode in a Serial or FastEthernet interface.
-	show queue	Display information about the real-time status of output queues for the current interface
-	voip-queue	Enable or disable custom queueing for VoIP traffic. If you disable custom queueing, WFVQ is re-enabled.
show queueing	-	Display the WFVG configuration

Priority queueing

Priority queueing enables you to queue packets according to the priority of each packet. There are four levels of priority. The total number of packets in all queues cannot exceed 5000.

You can enable priority queueing on the following interfaces:

- Serial (DS1 PPP L2-L3, DS1 PPP L2, USP PPP L2, USP PPP L2-L3)
- FastEthernet (L2, L2-L3) - when Traffic Shaping is configured
- Serial (DS1 FR L2, USP FR L2) - when Frame Relay Traffic Shaping is not configured
- Dialer (L2, L2-L3)

Priority queueing is disabled by default, since the default and recommended queueing method is WFVQ.

The high priority queue can be further split into two parts for voice traffic: control packets and bearer packets. This is called VoIP queueing. When VoIP queueing is enabled, the bearer queue size is calculated to meet the estimated queueing delay, which is 20 ms by default. You can re-estimate the queueing delay, which results in a change in the bearer queue size.

Summary of priority queueing configuration CLI commands

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

Root level command	Command	Description
interface (serial fastethernet dialer)	-	Enter the Serial, FastEthernet, or Dialer interface configuration context

Table continues...

Root level command	Command	Description
-	priority-queue	Enable or disable priority queuing mode in a Serial or FastEthernet interface. By default, priority queuing is off, and WFVQ is enabled on all serial interfaces and all FastEthernet interfaces for which traffic-shaping is enabled.
-	no priority-queue	Disable priority queuing and re-enable WFVQ.
-	queue-limit	Set the size of any of the four priority queues, in packets, for a given interface or interface type. The default sizes depend on the bandwidth of the interface.
-	no queue-limit	Restore the packet size to its default value, using the interface bandwidth
-	voip-queue	Enable or disable custom queueing for VoIP traffic.
-	no voip-queue	Disable VoIP queueing and re-enable WFVQ
-	voip-queue-delay	Set the maximum query delay for which to estimate the high priority queue size necessary to meet the queuing delay.
show queueing	-	Display the priority queue configuration

Chapter 10: Modems interfaces

You can connect either a USB or a serial modem to Branch Gateway. A USB modem must be connected to the USB port on Branch Gateway chassis. A serial modem must be connected to the Console port (CONSOLE) on Branch Gateway chassis.

The USB port and the Console port require configuration for modem use.

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

* Note:

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

USB-modem interface configuration

By default, the USB interface is enabled. Its default parameter values are:

- **Interface status:** = up
- **PPP timeout absolute:** = 10
- **ppp authentication:** = ras
- **ip address:** = 10.3.248.253 255.255.255.252

Example of IP address to USB port assignment

The following example describes how the **ip address** command assigns the IP address 192.168.22.33 to the USB port: (if:USB)# ip address 192.168.22.33 255.255.255.0

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

The ppp authentication command parameters

The **ppp authentication** command is used with any of the following parameters:

- **pap.** Password Authentication Protocol. An unencrypted password is sent for authentication.
- **chap.** Challenge Handshake Authentication Protocol. An encrypted password is sent for authentication. To configure this password, use the **ppp chap-secret** command.

*** Note:**

If the Branch Gateway firmware is replaced by an earlier firmware version, the **ppp chap-secret** is erased, and must be re-configured.

*** Note:**

ppp authentication is not supported in the FIPS mode.

- ras. Remote Access Service mode is being used for authentication. This is the default.
- none. No password is sent

*** Note:**

The **ppp authentication** command changes the PPP authentication parameters of the Console port as well as the USB port, even if you use the command in USB-modem interface context.

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

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

Root level command	Command	Description
interface usb-modem	-	Enter USB-modem interface configuration context
-	async modem-init-string	Change the default modem initialization string
-	async reset-modem	Reset the connected modem. You can use this command from within an active PPP session over the USB modem
-	ip address	Assign an IP address and mask to an interface. This is the IP address to which a remote user can connect using SSH/Telnet.
-	ip peer address	Change the IP address offered to a requesting calling host during PPP/IPCP connection establishment. By default, the interface offers its own IP address plus one.
-	ppp authentication	Configure the authentication method used when starting a client session on the PPP server.
-	ppp chap-secret	Configure the shared secret used in PPP sessions with CHAP authentication
-	ppp timeout authentication	Set the maximum time to wait for an authentication response
-	show ppp authentication	Display PPP authentication status

Table continues...

Root level command	Command	Description
-	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.

Console port and modem configuration

The Console port is labeled CONSOLE. The Console port is an RJ-45 socket that functions as a serial port. You can connect a console device or serial modem to the Console port to access the CLI.

You can set the Console port so that it automatically detects whether a console device or a modem is connected to it. Enter **async mode interactive** to set the Console port to use modem mode every time an Avaya proprietary modem cable is plugged into the Console port. If you do not want the Console port to automatically detect when a modem is connected to it, enter **async mode terminal** to disable interactive mode.

 Note:

By default, async mode is set to **terminal**.

Related links

[CLI access](#) on page 29

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

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

Root level command	Command	Description
interface console	-	Enter Console interface configuration context. Use the no form of this command to set the console parameters to their default values.

Table continues...

Root level command	Command	Description
-	async mode interactive	Enter modem mode every time the proprietary modem cable is plugged into the Console port
-	async mode terminal	Disable interactive mode on the Console
-	async modem-init-string	Change the default modem initialization string
-	async reset-modem	Reset the connected modem
-	ip address	Assign an IP address and mask to an interface. This is the IP address to which a remote user can connect using Telnet.
-	ip peer address	Change the IP address offered to a requesting calling host during PPP/IPCP connection establishment. By default, the interface offers its own IP address plus one.
-	ppp authentication	Configure the authentication method used when starting a client session on the PPP server
-	ppp chap-secret	Configure the shared secret used in PPP sessions with CHAP authentication
-	ppp timeout authentication	Set the maximum time to wait for an authentication response
-	show ppp authentication	Display PPP authentication status
-	shutdown	Disconnect an active PPP session and shut down the modem
-	speed	Set the PPP baud rate to be used by asynchronous PPP ports.
-	timeout absolute	Set the number of minutes until the system automatically disconnects an idle PPP incoming session. By default, there is no timeout.

Chapter 11: WAN interfaces

You can use an MM340 E1/T1 media module or an MM342 USP media module as an endpoint for a WAN line on Branch Gateway. You can use a Fast Ethernet port on Branch Gateway chassis as the endpoint for a WAN line by configuring the FastEthernet interface for PPP over Ethernet (PPPoE). Branch Gateway serves as a router, as well as the endpoint, for the WAN line.

*** Note:**

The WAN interface modules are no longer available and the G450 version 4 does not support the MM340 and MM342 WAN interfaces.

Related links

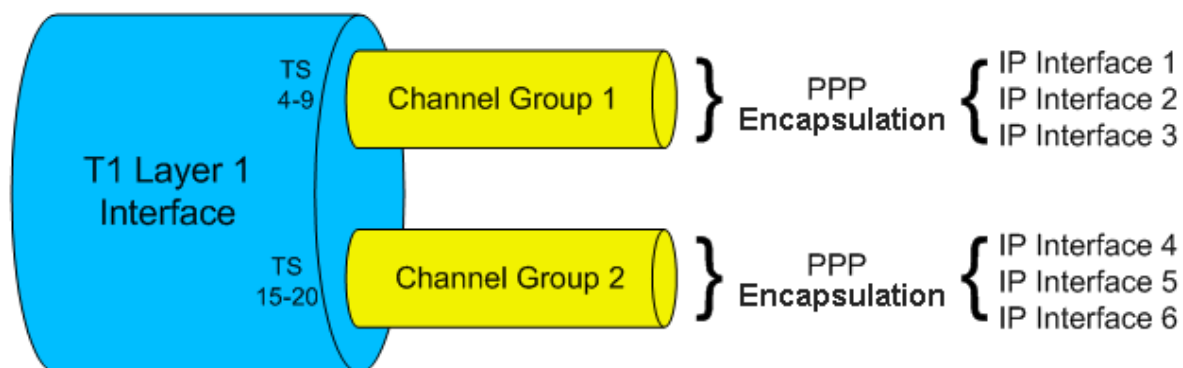
[Router](#) on page 387

Serial interface overview

A Serial interface is a virtual interface that is created over a portion of an E1/T1 or USP port on a WAN media module. Serial interfaces support PPP and frame relay encapsulation protocols.

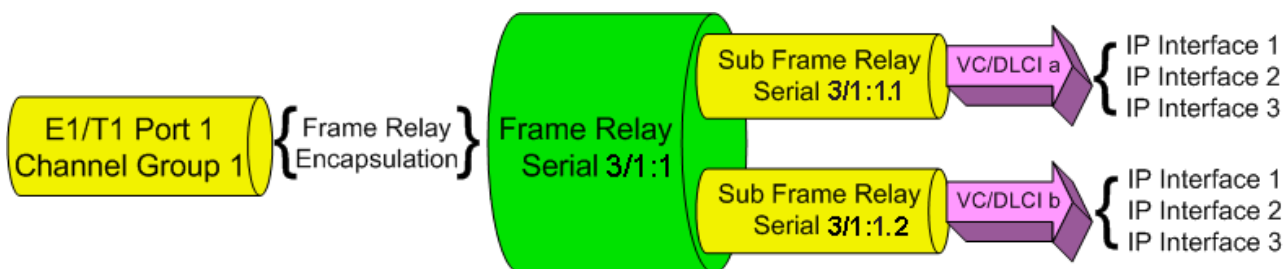
Layer 1 T1 port with two channel groups

The following figure illustrates a Layer 1 T1 port with two channel groups defined. All data from each channel group is encapsulated using PPP protocol, and is distributed over the multiple IP interfaces defined for each channel group.



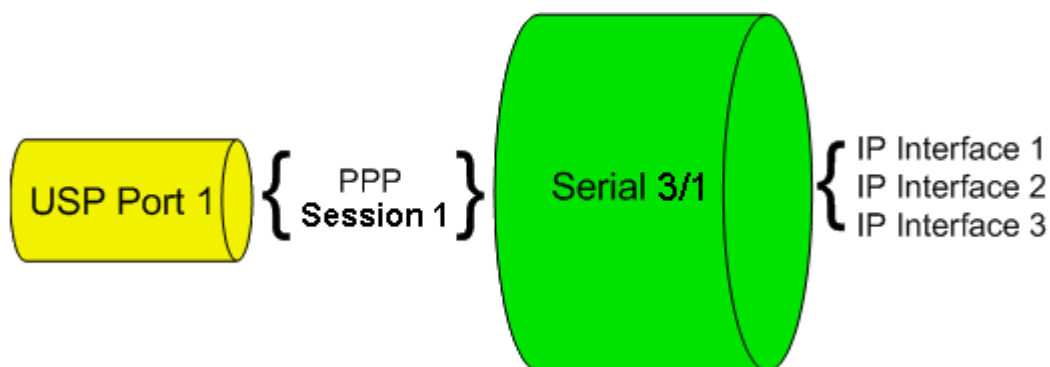
E1/T1 port channel group

The following figure illustrates an E1/T1 port channel group. All data from the channel group is encapsulated using frame relay protocol. The data is sent via a frame relay Serial interface and sub-interfaces over the multiple IP interfaces defined using Data Link Connection Identifier (DLCI).



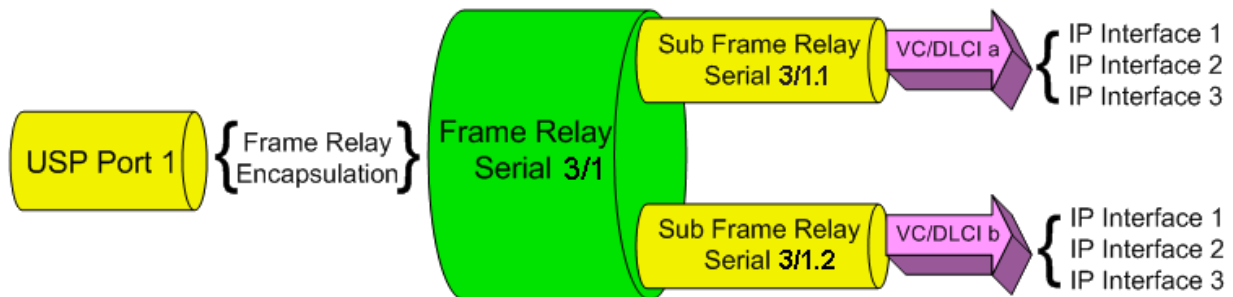
USP port using PPP protocol

The following figure illustrates a USP port. All data from the USP port is encapsulated using the PPP protocol, and is sent via a Serial interface over the multiple IP interfaces defined for the Serial interface.



USP port using frame relay protocol

The following figure illustrates a USP port. All data from the USP port is encapsulated using the frame relay protocol, and is sent through a frame relay Serial interface and sub-interfaces over the single IP interfaces defined using DLCI.



Frame Relay multipoint topology support

Branch Gateway supports point-to-point frame relay connections. To enable you to use the Gateway as an endpoint in a Point to Multi-Point (PTMP) topology, Branch Gateway supports inverse ARP replies. Branch Gateway responds to inverse ARP queries received on frame relay sub-interfaces with the proper inverse ARP replies.

When you connect Branch Gateway as an endpoint in a PTMP configuration, you need to increase the OSPF timers manually. Use the `ip ospf network point-to-multipoint` command in Serial interface context to increase the OSPF timers with the following values:

- Increase the OSPF Hello Interval to 30 seconds
- Increase the OSPF Dead Interval to 120 seconds

Related links

[Open shortest path first \(OSPF\)](#) on page 426

Configuring the initial WAN

Procedure

1. Add one of the following WAN media modules:

- Avaya MM340 E1/T1 media module
- Avaya MM342 USP media module

*** Note:**

You can also use the Fast Ethernet port on the Branch Gateway chassis as the endpoint for a WAN line by configuring this interface for PPPoE.

2. Connect the WAN line to the media module.

For more information see

For more information, see *Installing and Upgrading the Avaya Branch Gateway G450*.

3. Configure the WAN interface on the WAN media modules MM340 and MM342.
4. By default, a Branch Gateway WAN interface uses Point-to-Point Protocol (PPP).
5. If you want frame relay encapsulation on the WAN, configure frame relay.
6. Test the WAN configuration.

See WAN configuration and testing connectivity section.

7. Enter **copy running-config startup-config** to save the configuration.

Related links

[Configuring PPPoE](#) on page 232

The Avaya MM340 E1/T1 WAN media module

Configuring Avaya MM340 E1/T1 WAN media module

About this task

Use this procedure to configure Avaya MM340 E1/T1 WAN media module.

Procedure

1. Optionally, use the **show controllers** command to display the current settings.
2. Enter **show ds-mode** to check whether the Branch Gateway is configured for E1 or T1 operation.
3. Use the **ds-mode** command to set the mode of the Branch Gateway to E1 or T1.
Changing the line type requires resetting the module. The default value is T1.
4. Use the **controller {e1 | t1} module_number/port_number** command to enter Controller context for the port to be configured.
The prompt changes to:(super-if:Serial s/p)#, where s is the slot number of the media module, and p is the port number.
5. Use the following commands to change the clock source, frame type, linecode, or cable length parameters from the default settings:
 - For T1 mode:
 - **clock source line|internal** (default is line)
 - **framing sf|esf** (default is sf)

- **linecode** **ami|b8zs** (default is ami)
- **cablelength** **long|short** (default is long, gain26, 0db)

*** Note:**

Use the **cablelength** command to configure the cable's transmit and receive levels. If the cable is longer than 655 feet, use the command **cablelength long gain26|gain36 -15db|-22.5db|-7.5db|0db** (default is gain26, 0db). If the cable is 655 feet or less, use the command **cablelength short 133ft|266ft|399ft|533ft|655ft** (default is 133ft). When using the **cablelength short** form of the command, the transmit attenuation is configured using the loop length.

- **fdl** **ansi|att|both** (default is both)

*** Note:**

The **fdl** command defines the type of Facility Data Link loopback that the remote line is requested to enter. This command can only be used when ESF framing is defined.

- For E1 mode:

- **clock source** **line|internal** (default is line)
- **framing** **crc4|no-crc4|unframed** (default is crc4)
- **linecode** **ami|hdb3** (default is hdb3)

6. Use the **channel-group** command to specify the channel group and time slots to be mapped, as well as the DS0 speed.

Example:

- For T1 mode: **channel-group 1 timeslots 1,3-5,7 speed 64** configures time slots numbered 1, 3-5, and 7 to be mapped in channel-group number 1, and sets the DS0 speed to 64 kbps. The default DS0 speed for T1 mode is 56
- For E1 mode: **channel-group 1 timeslots 1,3-5,7 speed 64** configures time slots numbered 1, 3-5, and 7 to be mapped in channel-group number 1, and sets the DS0 speed to 64 kbps. The default DS0 speed for E1 mode is 64.

7. Enter **exit** to return to general context.

The prompt returns to:

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

8. Use the **interface serial** command to enter the Serial interface context.

Specify the slot number of the media module, the port number, the channel group number, and optionally, the IP interface number.

If you do not specify an IP interface number for the first Serial interface that you define on a channel group, the Branch Gateway automatically assigns IP interface number 0. For

each additional Serial interface that you define on the channel group, use a different IP interface number.

For example:

- **interface serial 3/1:1.** Enter a serial interface on the media module in slot number 3, on port number 1, with channel group number 1.
- **interface serial 4/1:2.3.** Enter a serial interface on the media module in slot number 4, on port number 1, with channel group number 2, and with IP interface number 3.

*** Note:**

If you use the **framing unframed** command in Step 5 for an E1 port, a channel group is automatically created on the entire E1 bandwidth. The channel group has the number 0. In Step 8, enter **interface serial s/p:0**, where s is the slot number and p is the port number.

*** Note:**

After the Serial interface is created, its default encapsulation is PPP.

9. Configure the interface encapsulation.

By default, the Serial interface uses PPP encapsulation.

10. Use the **ip address** command to configure the IP address and subnet mask of the interface.
11. Enter **exit** to return to general context.

The prompt returns to:

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

12. If needed, repeat Step 8 through Step 10 to configure additional IP interfaces on the same channel group.
13. If needed, repeat Step 6 through Step 10 to configure additional channel groups on the same E1 or T1 port.
14. Test the WAN configuration.
See WAN configuration and testing connectivity.
15. Enter **copy running-config startup-config** to save the configuration.

E1/T1 default settings

Function	Default setting
DS mode	T1
E1 framing	CRC4

Table continues...

Function	Default setting
T1 framing	SF
E1 linecode	HDB3
T1 linecode	AMI
Clock source	Line
T1 cable length	Long, Gain 26,0 db
Speed	E1: 64kbps T1: 56kbps

Commands used to reset and display controller counters

Use the following commands to reset counters on a controller interface:

- `clear controller counters`
- `remote`

Use the following commands to display counters on a controller interface:

- `show controllers`
- `show controllers remote`

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

Commands used to activate loopback mode on an E1/T1 line

Use the following loopback commands to activate or deactivate loopback mode for an E1 or T1 line.

- `loopback diag`
- `loopback local`
- `loopback remote`

Summary of E1/T1 ports configuration commands

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

Root level command	Command	Description
<code>clear controller counters</code>	-	Reset the controller counters
<code>controller</code>	-	Enter configuration mode for a specific controller

Table continues...

Root level command	Command	Description
-	cablelength long (T1)	Set transmit and receive levels for a cable longer than 655 feet
-	cablelength short (T1)	Set transmit levels for a cable of length 655 feet or shorter
-	channel-group	Create a channel group logical interface for a PPP or Frame Relay session
-	clock source	Set the clock source for an E1 or T1 controller
-	fdl	Define the type of Facility Data Link loopback that the remote line is requested to enter
-	framing	Set the frame type for an E1 or T1 data line
-	linecode	Set the type of line-code transmission for the E1 or T1 line
-	loopback	Put a T1 or E1 line into loopback mode or disable loopback mode
-	loopback remote	Request a remote station to activate or deactivate a line or payload loopback signal on the controller interface. This command is applicable only to a T1 line.
ds-mode	-	Set the mode of the controller: e1 or t1
interface serial	-	Enter Serial interface or sub interface configuration context
-	ip address	Configure the IP address and subnet mask of the interface
show controllers	-	Display status information about a controller interface
show controllers remote	-	Display controller statistics from a peer station
show ds-mode	-	Display the current mode of the controller

Avaya MM342 USP WAN media module

Configuring Avaya MM342 USP WAN media module

Procedure

1. Use the **interface serial** command to enter the context of the interface.

Specify the slot number of the media module, the port number, and optionally the IP interface number.

If you do not specify an IP interface number for the first Serial interface that you define on a port, the Branch Gateway automatically assigns IP interface number 0. For each additional Serial interface that you define on the port, use a different IP interface number.

For example:

- **interface serial 3/1.** Enter a serial interface on the media module in slot number 3, on port number 1.
- **interface serial 4/1.2.** Enter a serial interface on the media module in slot number 4, on port number 1, with IP interface number 2.

```
Gxxx-001(super)# interface serial 3/1
```

The prompt changes to:

```
Gxxx-001(super-if:serial 3/1)#
```

2. Use the following commands to change the idle characters, transmitter delay, encoding type, bandwidth parameters, line monitoring, and from their default settings:

- **idle character flags | marks.** Set the bit pattern used to indicate an idle line. Use the **no** form of this command to restore the default value (flags).
- **transmitter-delay number.** Set the minimum number of flags to be sent between successive packets. Use the **no** form of the command to restore the transmitter-delay value to the default (0).

 Note:

The **transmitter-delay** command is usually used when the DCE equipment that is connected directly to the Gateway, or the router on the WAN have a receive buffer that is not large enough to hold the traffic sent by the Gateway. In this case, configure **transmitter-delay** on the DCE equipment or the remote router in order to preserve the high performance that you had when **transmitter-delay** was configured to 0 on the Gateway.

- **nrzi-encoding.** Enable the non-return-to-zero inverted (NRZI) line coding format on the specified interface. Use the **no** form of the command to disable NRZI encoding.
- **bandwidth kbps.** Set the bandwidth parameter manually for the interface. Use the **no** form of this command to restore the bandwidth parameter to its default value (2,048). The manually specified bandwidth value overrides the dynamically calculated bandwidth during route cost calculations.

 Note:

If you are using the USP port as a clock source, configure the port's bandwidth to match the DCE clock rate.

- **ignore dcd.** Specify how the system monitors the line to determine if it is up or down. Specify **ignore dcd** to ignore DCD signals, and instead use DSR/CTS signals to determine the line's status. Use the **no** form of the command to specify that DCD signals are used to determine line status.

- **invert txclock**. Invert the transmit clock signal from the data communications equipment (DCE). Use the **no** form of the command to restore the signal to not inverted.
3. Configure the interface encapsulation.
 4. Enter **exit** to return to general context.

The prompt returns to:

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

5. Repeat Step 1 to configure additional Serial interfaces on the USP port.
6. Test the WAN configuration.
7. Enter **copy running-config startup-config** to save the configuration.

Related links

[Configuring frame relay](#) on page 235

[Commands used for WAN configuration and testing connectivity](#) on page 238

USP default settings

Function	Default setting
Encoding	NRZ
Bandwidth	2,048 kbps
Line-up indicator signal	DCD

Summary of USP port configuration commands

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

Root level command	Command	Description
interface serial	-	Enter Serial interface or sub interface configuration context
-	bandwidth	Set the bandwidth parameter manually for this interface
-	idle-character	Set the bit pattern used to indicate an idle line
-	ignore dcd	Specify how the system monitors the line to determine if it is up or down
-	invert txclock	Invert the transmit clock signal from the data communications equipment (DCE)
-	ip address	Configure the IP address and subnet mask of the interface
-	nrzi-encoding	Enable or disable the non-return-to-zero inverted (NRZI) line coding format on the interface

Table continues...

Root level command	Command	Description
-	transmitter-delay	Set the minimum number of flags to be sent between successive packets

PPP configuration

Configuring PPP

About this task

PPP is the default encapsulation on a WAN port. If the encapsulation has been changed to frame relay and you want to restore PPP encapsulation, or to change the PPP parameters:

Procedure

1. Ensure that you are in the context of a serial interface that is defined on the port.
If you are not in the context of a serial interface, use the **interface serial** command. To view all Serial interfaces that are defined, use the **show interfaces serial** command.
2. If the interface is not already configured to use PPP encapsulation, enter **encapsulation ppp** to change the encapsulation to PPP.
3. **(Optional)** Change the queuing mode of the interface.
4. Use the following commands to change the interface parameters:
 - **ip address**. Configure the IP address and subnet mask of the interface.
 - **ppp timeout ncp**. Set the maximum time to wait for the network layer to negotiate. If this time is exceeded, the Gateway restarts the PPP session.
 - **ppp timeout retry**. Set the maximum time to wait for a response during PPP negotiation.
 - **keepalive**. Enable keepalive or change the interval to which keepalive is set. When activated, keepalive performs the initial negotiation and sends health checks at defined intervals to the other side of the interface. To deactivate keepalive, use the **no** form of the command or set the health check interval to 0.
5. Enter **exit** to return to general context.
The prompt returns to:

```
Gxxx-001(super)#
```
6. Test the WAN configuration.
7. Enter **copy running-config startup-config** to save the configuration.

Related links

[Weighted Fair VoIP Queuing](#) on page 213

[Commands used for WAN configuration and testing connectivity](#) on page 238

Summary of PPP configuration commands

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

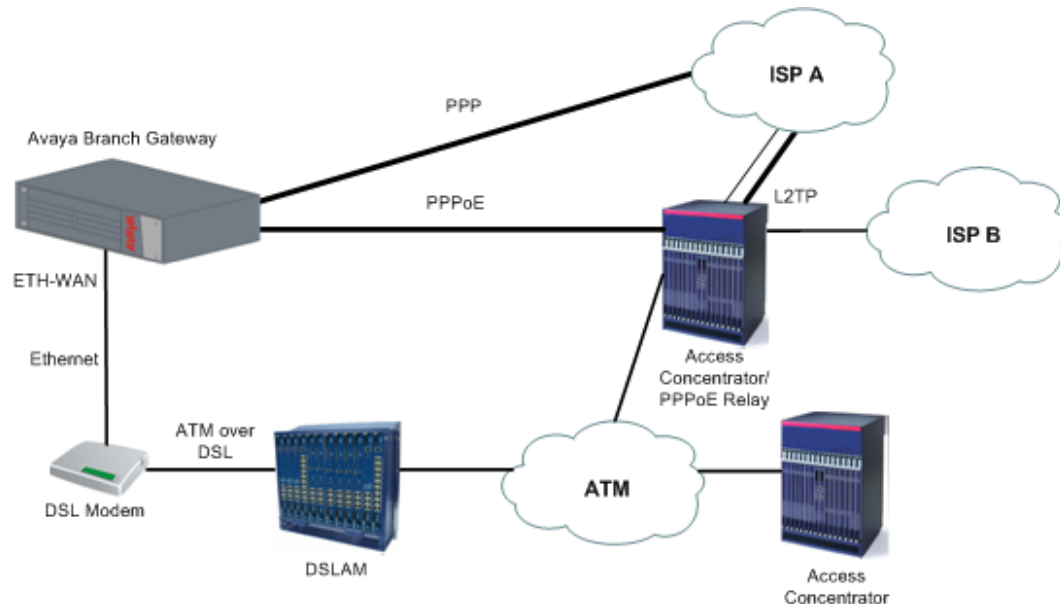
Root level command	Command	Description
<code>interface serial</code>	-	Enter Serial interface or sub interface configuration context
-	<code>encapsulation</code>	Set the encapsulation mode for a Serial interface: PPP or frame relay
-	<code>ip address</code>	Configure the IP address and subnet mask of the interface
-	<code>keepalive</code>	Enable PPP keepalive, in order to maintain a persistent connection
-	<code>ppp timeout ncp</code>	Set the maximum time, in seconds, that PPP allows for negotiation of a network layer protocol
-	<code>ppp timeout retry</code>	Set the maximum time to wait for a response during PPP negotiation
<code>show interfaces</code>	-	Display interface configuration and statistics for a particular interface or all interfaces

PPPoE overview

You can configure ETH WAN Fast Ethernet ports as a WAN port using PPPoE (PPP over Ethernet). PPPoE offers dialup style authentication and accounting and allows subscribers to dynamically select their ISP.

PPPoE is a client-server protocol used for carrying PPP-encapsulated data over Ethernet frames. A PPPoE client can establish a tunnel that carries PPP frames between a dialing host (the Branch Gateway) and an access concentrator. This enables the use of PPP authentication protocols (CHAP and PAP). Unlike other tunneling protocols such as L2TP and PPTP, PPPoE works directly over Ethernet rather than IP.

A typical broadband access network is based on ADSL modems configured as transparent Ethernet bridges. ADSL modems use ATM protocol, and the transparent bridging is done to a well known ATM VC. On the other side of the telephone line is a device called a DSLAM. The DSLAM terminates the ADSL physical layer, collects the ATM cells from the various ADSL subscribers, and places them on the SP ATM infrastructure. The Ethernet frames from the customer's host device can reach one or more access concentrators, which are the remote access servers.



Configuring PPPoE Procedure

1. Enter the FastEthernet interface context with the `interface fastethernet 10/2` command.
2. Enter `encapsulation pppoe` to change the encapsulation to PPPoE.

You must change the encapsulation to PPPoE before configuring an IP address on the interface.

* Note:

You cannot use PPPoE if:

- An IP address must not be configured on the interface
- Dynamic CAC is not enabled on the interface.
- The interface is not part of a primary-backup interface pair.

3. Use the `ip address` command to configure an IP address and subnet mask for the interface.

In most cases, PPPoE tunnels require a 32-bit subnet mask.

Alternatively, you can enter `ip address negotiated` to obtain an IP address via PPP/IPCP negotiation.

* Note:

You cannot configure PPP/IPCP address negotiation if DHCP address negotiation is already configured on the interface.

4. Configure an authentication method and parameters:

- For PAP authenticating, enter **ppp pap-sent username** followed by a user name and password. For example:

```
Gxxx-001(super-if:FastEthernet 10/2)# ppp pap-sent username avaya32 password
*****
Done!
```

- For CHAP authentication, enter **ppp chap hostname** followed by a hostname, and **ppp chap password** followed by a password. For example:

```
Gxxx-001(super-if:FastEthernet 10/2)# ppp chap hostname avaya32
Done!
Gxxx-001(super-if:FastEthernet 10/2)# ppp chap password *****
Done!
```

5. If the Branch Gateway is connected to the Internet via the FastEthernet interface configured for PPPoE, and you define a VPN tunnel which specifies remote hosts by name, it is recommended to use the **ppp ipcp dns request** command.

The command requests the list of available DNS servers from the remote peer during the PPP/IPCP session. The DNS servers are used by the DNS resolver to resolve hostnames to IP addresses.

6. Enter **exit** to return to general context.

The prompt returns to:

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

7. Test the configuration.

See WAN configuration and testing connectivity.

8. Enter **copy running-config startup-config** to save the configuration.9. Optionally, shut down the port and the PPPoE client, if configured, with the **shutdown** command in the interface context.**Related links**

[Dynamic CAC](#) on page 261

[Backup interfaces](#) on page 239

[DHCP client configuration](#) on page 183

Summary of PPPoE commands

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

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

Table continues...

Root level command	Command	Description
-	<code>ip address</code>	Configure an IP address and subnet mask for the interface
-	<code>ip address negotiated</code>	Obtain an IP address via PPP/IPCP negotiation
-	<code>keepalive</code>	Enable PPP keepalive, in order to maintain a persistent connection
-	<code>keepalive-track</code>	Bind interface status to an object tracker to check whether the interface is up
-	<code>mtu</code>	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
-	<code>ppp chap hostname</code>	Override the device hostname for PPP CHAP authentication
-	<code>ppp chap password</code>	Set the CHAP password for authentication with a remote peer
-	<code>ppp chap refuse</code>	Prevent the device from authenticating with CHAP after the device is requested by the remote peer
-	<code>ppp ipcp dns request</code>	Enable or disable requesting the list of available DNS servers from the remote peer during the PPP/IPCP session
-	<code>ppp pap refuse</code>	Prevent the device from authenticating with PAP after the device is requested by the remote peer
-	<code>ppp pap-sent username</code>	Set the Password Authentication Protocol (PAP) password for authentication with the remote peer
-	<code>ppp timeout ncp</code>	Set the maximum time, in seconds, that PPP allows for negotiation of a network layer protocol
-	<code>ppp timeout retry</code>	Set the maximum time to wait for a response during PPP negotiation
-	<code>pppoe-client persistent delay</code>	Set the interval between pppoe-client dial attempts
-	<code>pppoe-client persistent max-attempts</code>	Limit the number of consecutive connection establishment retries
-	<code>pppoe-client service-name</code>	Set the PPPoE Client service-name

Table continues...

Root level command	Command	Description
-	pppoe-client wait-for-ipcp	Set the amount of time (in seconds) between establishment of the PPPoE tunnel and establishment of the IPCP tunnel. If this time is exceeded, the PPPoE client terminates the PPPoE tunnel.
-	shutdown	Shut down the port, and the PPPoE client, if configured

Frame relay

Configuring frame relay

Procedure

1. Ensure that the port is configured on the media module.
2. Ensure that you are in the context of a serial interface that is defined on the port.

If you are not in the context of a serial interface, use the **interface serial** command. To view all Serial interfaces that are defined, use the **show interfaces serial** command.

3. Use the **encapsulation frame-relay** command to change the encapsulation to frame relay.

You can optionally specify the encapsulation type: IETF (RFC1490/RFC2427) or non-IETF. The default encapsulation type is IETF.

 Note:

Non-IETF encapsulation is compatible with other vendors.

4. If needed, use the **frame-relay lmi** commands to change the Local Management Interface (LMI) parameters from their default values, or enter **frame-relay traffic-shaping** to activate traffic shaping on the frame relay interface.
5. Optionally, change the queuing mode of the interface.
6. Enter **exit** to return to general context.

The prompt returns to:

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

7. Enter **interface serial if.fr-sub-if point-to-point** to create a frame relay sub-interface and enter the context of the interface.

For example:

- **interface serial 3/1:2.1 point-to-point**. Create frame relay sub-interface number 1 on the E1/T1 media module in slot number 3, on port number 1, with channel group number 2
- **interface serial 4/1:2.3.2 point-to-point**. Create frame relay sub-interface number 3 on the E1/T1 media module in slot number 4, on port number 1, with channel group number 2, and with IP interface number 2
- **interface serial 3/1.2 point-to-point**. Create frame relay sub-interface number 2 on the USP media module in slot number 3, on port number 1
- **interface serial 4/1.2.1 point-to-point**. Create frame relay sub-interface number 2 on the USP media module in slot number 4, on port number 1, with IP interface number 1

 Note:

Currently only point-to-point frame relay sub-interfaces are supported.

8. Enter **frame-relay interface-dlci DLCI-number** to configure a Data Link Connection Identifier (DLCI) for the frame relay sub-interface.

You can optionally specify the encapsulation type: IETF (RFC1490/RFC2427) or non-IETF. The default encapsulation type is IETF.

 Note:

Non-IETF encapsulation is compatible with other vendors.

9. If required, use the **frame-relay priority-dlci-group** command to configure a Priority DLCI group.

The arguments for this command are the DLCIs you want to assign to high, medium, normal, and low priority traffic, respectively. For example, the command **frame-relay priority-dlci-group 17 18 19** assigns DLCI 17 to high priority traffic, DLCI 18 to medium priority traffic, and DLCI 19 to normal and low priority traffic.

10. Use the **ip address** command to configure an IP address and subnet mask for the frame relay sub-interface.
11. Enter **exit** to return to general context.

The prompt returns to:

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

12. If needed, repeat Step [7](#) on page 235 through Step [11](#) on page 236 to configure additional frame relay sub-interfaces on the same Serial interface.
13. If needed, repeat Step [2](#) on page 235 through Step [12](#) on page 236 to configure frame relay encapsulation for other Serial interfaces on the same WAN port.
14. Test the WAN configuration.

15. Enter `copy running-config startup-config` to save the configuration.

Related links

[Configuring Avaya MM342 USP WAN media module](#) on page 227

[Configuring Avaya MM340 E1/T1 WAN media module](#) on page 223

[Frame relay traffic shaping and FRF.12 fragmentation](#) on page 276

[Weighted Fair VoIP Queuing](#) on page 213

Commands used to reset and display frame relay interface counters

- `clear frame-relay counters`
- `show interfaces`

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

Summary of frame relay commands

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

Root level command	Command	Description
<code>clear frame-relay counters</code>	-	Clear the frame relay counters
<code>interface serial</code>	-	Enter Serial interface or sub interface configuration mode
-	<code>encapsulation</code>	Set the encapsulation mode for a Serial interface
-	<code>frame-relay class-dlci</code>	Associate a Virtual Channel with a named QoS or Traffic shaping template (map-class)
-	<code>frame-relay interface-dlci</code>	Associate a frame relay Virtual Channel with the current interface
-	<code>frame-relay lmi-n391dte</code>	Set the number of status enquiry intervals that pass before issuing a full status enquiry message
-	<code>frame-relay lmi-n392dte</code>	Set the maximum number of unanswered status enquiries the equipment accepts before declaring the interface down
-	<code>frame-relay lmi-n393dte</code>	Set the number of status polling intervals over which the error threshold is counted (the monitored event count)
-	<code>frame-relay lmi-type</code>	Manually define the type of the Local Management Interface (LMI) to use

Table continues...

Root level command	Command	Description
-	frame-relay priority-dlci-group	Assign Virtual Channels to priority classifications, for supporting traffic separation
-	frame-relay traffic-shaping	Turn on or off traffic shaping and frame relay fragmentation
-	ip address	Configure an IP address and mask for the interface
show interfaces	-	Display interface configuration and statistics for a particular interface or all interfaces

WAN configuration and testing connectivity

Commands used for WAN configuration and testing connectivity

After configuring the new interface, you can perform the following tests to verify that the new interface is operating correctly.

- For E1/T1 interfaces, use the **show controllers** command to view the status of the interface's controller. Verify that the controller is up, and that all error counters do not increase.

For all serial interfaces (E1/T1 and USB-modem), use the **show interfaces serial** command to verify that the interface and line protocol are both up. For example:

```
Serial x/y:z is up, line protocol is up
```

- For the USB-modem interface and the Fast Ethernet interface, use the **show interfaces** command to verify that all line signals are up. For example:

```
DCD = up DSR = up DTR = up RTS = up CTS = up
```

- Use the **show frame-relay pvc** command to view detailed PVC information, or **show frame-relay pvc brief** for a brief summary of PVC configuration.
- Use the following commands for more information about frame relay configuration:
 - **show frame-relay fragment**. Display frame relay fragmentation statistics and configuration on all PVCs associated with the interface.
 - **show frame-relay lmi**. Display LMI statistics for the interface.
 - **show frame-relay map**. Display a summary table of frame relay sub-interfaces and DLCIs associated with the sub-interfaces.
 - **show frame-relay traffic**. Display frame relay protocol statistics, including ARP requests and replies sent and received over the interface.
 - **show map-class frame-relay**. Display the map-class Frame Relay table.
- Use the **show traffic-shape** command to view traffic shaping and frame relay traffic shaping configuration parameters for all interfaces.

- Use the **show ip interface** command to display information about IP interfaces. To display information about a specific interface, include the name of the interface as an argument. To display information about the interface of a specific IP address, include the IP address as an argument.
- Enter **show running-config** to display the configuration running on the device.
- Enter **show startup-config** to display the configuration loaded at startup.
- Use the **ping** command to send ICMP echo request packets from the Branch Gateway to the interface Serial peer IP address and verify that it responds.

Summary of WAN configuration verification commands

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

Command	Description
ping	Check host reachability and network connectivity
show controllers	Display status information about a controller interface
show frame-relay fragment	Display frame relay fragmentation statistics and configuration on all PVCs, all PVCs associated with an interface, or a specific PVC
show frame-relay lmi	Display LMI statistics for a particular interface or for all interfaces. The output displayed differs depending on the type of interface.
show frame-relay map	Display a summary table of Frame Relay sub-interfaces and DLCIs associated with the sub-interfaces
show frame-relay pvc	Display detailed PVC information
show frame-relay pvc brief	Display brief PVC information
show frame-relay traffic	Display frame relay protocol statistics, including ARP requests and replies sent and received over Frame Relay interfaces
show interfaces	Display interface configuration and statistics for a particular interface or all interfaces
show ip interface	Display information about an IP interface
show map-class frame-relay	Display the map-class Frame Relay table
show traffic-shape	Display traffic shaping and frame relay traffic shaping configuration information

Backup interfaces

You can configure backup relations between a pair of any Layer 2 Serial interfaces. A backup interface is activated when the primary interface fails. The backup interface is deactivated when the primary interface is restored. A PPP session, frame relay interface, frame relay sub-interface, Dialer interface, FastEthernet interface, or Loopback interface can serve as a backup interface to any other Serial interface on the same module including interfaces on different serial ports.

 Note:

A frame relay interface in a primary or backup role overrides the role of its sub-interfaces.

If the FastEthernet interface serving as a backup interface is configured as a DHCP client, it sends no DHCP packets. Therefore, its IP address is not renewed until it becomes the primary interface. If the FastEthernet interface serving as a primary interface is configured as a DHCP client, the expiry of the leases on its IP address or no reception of an IP address does not activate the backup interface.

Backup delay configuration

Configurable activation and deactivation delays provide a damping effect on the backup interface pair. This eliminates primary-to-backup switching in case of fluctuating underlying Layer 2 interfaces. You can configure the following backup delays with the **backup delay** command:

- **failure delay.** The time in seconds between the primary interface going down and the backup interface activation. The default is 0 seconds. The maximum is 3600 seconds.
- **secondary disable delay.** The time in seconds between the primary interface restoration and the backup interface deactivation. The default is 0 seconds. The maximum is 3600 seconds. Both interfaces are active during this time to enable a smooth transition for the routing protocols. To keep the backup interface active indefinitely, use **never** as the secondary disable delay.

Example

You can use the following command to switch over immediately to the backup interface in case of failure, and pause 60 seconds before reverting to the primary interface:

```
Gxxx-001(super)# interface fastethernet 10/2
Gxxx-001(super-if:FastEthernet 10/2)# backup delay 0 60
Done!
Gxxx-001(super-if:FastEthernet 10/2)#
```

Interface backup relations rules

- Each interface can have only one backup interface.
- A backup interface can serve as a backup for only one other interface.
- Only one member of a primary and backup pair is active at any given time. An interface is automatically deactivated when configured as backup.
- The backup implementation does not protect against the failure of both interfaces. Therefore, if a backup interface fails while active, no switch to the primary interface is attempted.

When using frame relay encapsulation, the frame relay interface is considered down when its primary DLCI is down. The switchover back to the main interface occurs when the primary Data Link Connection Identifier (DLCI) is restored.

 Note:

The backup interface is not activated when the primary interface is administratively disabled.

Summary of backup interfaces commands

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

Root level command	Command	Description
interface (fastethernet loopback serial tunnel)	-	Enter FastEthernet, Loopback, Serial, or Tunnel interface configuration context
-	backup delay	Set the time to wait before switching over to the backup interface, in case of failure. You can also use this command to set a delay before reverting back to the primary interface.
-	backup interface	Set a backup interface for the current interface followed by the interface type and number. You must use this command from the context of the interface for which you are setting a backup interface.

Modem dial backup

The modem dial backup feature allows Branch Gateway to utilize a modem to provide redundant connectivity between Branch Gateway and IP phones in a small branch office and their primary Media Gateway Controller (MGC) at the headquarters or a regional branch office.

Even if Branch Gateway has Standard Local Survivability (SLS), or Enhanced Local Survivability (ELS) using a local S8300 in Survivable Remote Server mode, it is always preferable to continue working with the primary MGC, since features are lost when the system is fragmented.

Analog modems have limited bandwidth and high latency, and are therefore unfit for carrying VoIP traffic. However, using Dynamic Call Admission Control (CAC), Branch Gateway can be configured to report zero bandwidth for bearer traffic to the MGC when the primary WAN link fails. A matching configuration on the MGC allows it to block new calls, if their bearer is about to go over the modem dial backup interface, and to alert the user with a busy tone. In this case, the user is still able to place external calls manually if local PSTN trunks are available. Furthermore, CM 3.0 Inter-Gateway Alternate Routing (IGAR) may be configured to become active in such a case and to use the PSTN for transporting the voice bearer transparently between the sites, transparently to the user. For information about IGAR, see *Administrator Guide for Avaya Aura® Communication Manager*.

Modem dial backup is a generic data dial backup feature that can carry not only signalling but every type of IP traffic. However, the low bandwidth of an analog modem would be likely to cause congestion. The administrator must therefore ensure that VoIP signaling has priority over the Dialer interface. This can be performed using access control lists (ACL), QoS lists, and Weighted Fair Queuing (WFQ) priority schemes. The administrator should apply these tools in both Branch Gateway and the Remote Access Server (RAS).

You can configure modem dial backup to dial to an enterprise-owned RAS or to the Internet via an Internet Service Provider (ISP). Most ISPs mandate the use of the internal IPSec VPN gateway process to encrypt the traffic as it goes over the Internet.

*** Note:**

IPSec VPN adds overhead to each packet, further reducing available bandwidth.

Under ideal conditions, the bandwidth of the analog modem can reach 56 kbps for downlink (53 kbps in the US) and 33.6 kbps for uplink. However, sub-optimal PSTN quality may degrade the downlink bandwidth to 33.6 kbps, or even 28 kbps. This may not be enough to carry a single ISDN-PRI 64 kbps D-Channel for signalling over H.248 to and from the MGC, even without considering the need to support IP phones and/or analog or DCP trunks.

VoIP signaling consumes bandwidth when setting up and tearing down calls. However, calculations, testing, and field experience show that an analog modem can easily support a small branch office when the expected Busy Hour Call Completion (BHCC) is limited.

*** Note:**

The low bandwidth and high Round-Trip-Time (RTT) of analog modems (~100 ms) may lead to acceptable changes in Post-Dial-Delay (PDD) and offhook-to-dialtone delays.

Modem dial backup uses Branch Gateway backup interface functionality to activate the Dialer interface for modem dial backup when the primary interface fails and to deactivate the Dialer interface when the primary interface is up again. Currently, modem dial backup does not support such features as Dial On Demand Routing (DDR), callbacks, or RAS. Modem dial backup cannot receive backup calls.

*** Note:**

You can only backup one interface with modem dialer backup.

Using Branch Gateway backup interface functionality, you can designate the Dialer interface as the backup for the main WAN link. However, this method is not always available, since an 'up' WAN link status does not ensure connectivity, and the main WAN link may not even be directly connected to Branch Gateway.

The workaround is to use Branch Gateway object tracking feature to verify connectivity to the primary MGC using Respond Time Reports (RTRs) and object trackers. Configure object tracking to change the state of the Loopback interface accordingly, and configure the Dialer interface as a backup to the Loopback interface.

Modem dial backup uses a modem connected directly to Branch Gateway USB or Console port. The modem can also be used to access Branch Gateway CLI from a remote location. The modem cannot do both at the same time.

Finally, IP routing must be configured so that traffic to and from the site uses the Dialer interface when the primary interface is down. The Dialer interface can work both with static and dynamic routing (OSPF and RIP). Note that the latter mandates the use of unnumbered IP interfaces.

*** Note:**

Modem dial backup has complex interactions with other configuration modules within Branch Gateway and on your network. Before configuring modem dial-backup, Avaya recommends reading *Application Note - VoIP Network Resiliency*. This document discusses the issues of network design for maximum resiliency, capacity planning for optimum performance, configuration options for network devices, strategies for implementing routing across the network, and security concerns. Based on your existing network design, several redundancy scenarios featuring modem dial backup are available.

Modem dial backup does not support backup dial-ins or callbacks. Some backup configurations require the remote host to receive a request for connection, acknowledge, end the connection, and dial back the requester. This configuration is not supported.

Related links

[Dynamic CAC](#) on page 261

[Policy lists](#) on page 504

[Weighted Fair VoIP Queuing](#) on page 213

[Backup interfaces](#) on page 239

[Object tracking](#) on page 263

[CLI access using modems](#) on page 31

[Unnumbered IP interfaces](#) on page 391

[Modem dial backup interactions with other features](#) on page 247

Typical installations

The Branch Gateways were designed for small branch offices of a larger enterprise. Consequently, the same RAS may serve many branch offices, and, therefore, many Branch Gateways. A reasonable assumption is that not all branch offices would need modem dial backup at the same time. Therefore, the ratio of modem channels at the RAS to Branch Gateways at branch offices can be less than 1:1. There are several practical ways to configure the RAS server for use with modem dial backup Dialer interfaces:

- The RAS can assign an IP address to the calling Branch Gateway. This requires the RAS to identify the call gateway using the PAP/CHAP username, and install an appropriate static route to the branch office subnets accordingly. The username, password, and static route can be configured in an external RADIUS/TACACS+ server.
- The RAS server can use OSPF to learn the branch office subnets. This is much simpler to configure as all branch offices can share the same username and password. The Branch Gateway is configured to advertise the branch office subnets with OSPF. This feature requires the use of unnumbered IP addresses at the Branch Gateway and the RAS. Since the Dialer and the primary interfaces are not expected to be up at the same time, the RAS server can use passive-OSPF-interface and the Branch Gateway can use static via routes.
- The Branch Gateway can call an ISP RAS (which is likely to assign it a dynamic IP address) and open an IPSec VPN tunnel to an enterprise-owned VPN gateway.

While using OSPF and calling an ISP RAS are expected to be the most common scenarios, they involve complex interaction with IP routing and the remote RAS server. For more detailed configuration examples, see *Application Note - VoIP Network Resiliency*.

Prerequisites for configuring modem dial backup

- At least one dialer string, which determines the phone number(s) of the remote modem(s) dialed by the Dialer interface
- A configured interface to be backed up
- Read/write or admin access level
- A modem: Multitech MultiModem ZBA (MT5634ZBA), or MultimodemUSB (MT5634ZBA-USB), or USRobotics USB modem (5637)

* Note:

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

Use the maximum UART speed for the serial modem (115400 BAUD).

Configuring modem dial backup

Procedure

1. From the general context, use the **show interfaces console** or **show interfaces USB-modem** command to verify that the modem is connected. You may be required to enable the modem.
2. Enter **interface dialer**, followed by the identifier, to create the Dialer interface.

For example:

```
Gxxx-001(super)# interface dialer 1
Gxxx-001(if:dialer 1)#
```

The Dialer interface is created and can now be defined as a backup interface for an existing WAN interface.

3. Enter up to five dialer strings, using the **dialer string** command.

For example:

```
Gxxx-001(if:dialer 1)# dialer string 1 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 persistent 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-ipc** 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-ipc 100
Done!
```

7. Configure an authentication method and parameters, if required:

- For PAP authenticating, enter **ppp pap sent-username** followed by a username and password. For example:

```
Gxxx-001(if:dialer 1)# ppp pap sent-username avaya32 password *****
Done!
```

- For CHAP authentication, enter **ppp chap hostname** followed by a hostname, and **ppp chap password** followed by a password. For example:

```
Gxxx-001(if:dialer 1)# ppp chap hostname avaya32
Done!
Gxxx-001(if:dialer 1)# ppp chap password 123456
Done!
```

8. From the general context, use **show interfaces dialer 1** to verify that the Dialer interface has connected to the remote peer.

For example:

```
Gxxx-001(super)# show interfaces dialer 1
Dialer 1 is down, line protocol is down
Internet address is 4.5.6.7, mask is 255.255.255.0
MTU 1500 bytes, Bandwidth 28 kbit
IPSec PMTU: copy df-bit, Min PMTU is 300
Reliability 1/255 txLoad 255/255 rxLoad 255/255
Encapsulation PPP
Link status trap disabled
Keepalive track not set
Keepalive set (10 sec)
LCP Starting
IPCP Starting
Last dialed string:
Dial strings:
  1: 5555555
  2: 1234567
Dialing order is sequential
Persistent initial delay 5 sec
Wait 45 sec for IPCP
Weighted Fair VoIP queueing mode
Last input never, Last output never
Last clearing of 'show interface' counters never
5 minute input rate 0 bits/sec, 0 packets/sec
```

This command shows the interface status, including a summary of its definitions and settings. The status also tells you whether the interface is up and the dialup succeeded. In the example status, the interface is down and inactive.

9. Enter the context of the interface which the Dialer is to back up, and use the **backup interface** command to configure the Dialer interface as the backup interface.

For example:

```
Gxxx-001(if:serial 3/1:1)# backup interface dialer 1
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.
- The Branch Gateway's Console port is an RJ-45 asynchronous port that can be used to support the modem for dial backup. Thus, the Dialer can use the same serial modem that is used for remote access to the device. Asynchronous dialing and modem recognition options must be set on the Console port to support creation of the Dialer interface.
- A Branch Gateway USB port can be used to support a USB modem for dial backup. Thus, the Dialer can use the same USB modem that is used for remote access to the device. Asynchronous dialing and modem recognition options must be set on the USB port to support creation of the Dialer interface.
- The Dialer interface supports PAP and CHAP authentication for PPP connections. In addition, the Dialer interface can be configured to be a member of a VPN, allowing encryption of the modem traffic. Van Jacobsen compression is available for encrypted traffic over the Dialer interface, allowing optimal use of bandwidth.
- It is recommended to filter traffic through the Dialer interface to permit only those packets necessary for continued interaction with the CM server. Filtering can be accomplished using access control lists, which specify traffic permissible through a selected interface.
- Dynamic CAC can be used in conjunction with IGAR to provide a stable backup path for continued IP phone function in the event of a dial backup scenario. Dynamic CAC notifies the CM server that no bandwidth is available for bearer traffic, keeping the dial circuit from becoming fully congested. IGAR provides a path for gateway-to-gateway traffic destined for

a remote CM server by forcing voice calls to and from the branch office to use the PSTN for bearer traffic. For more information on configuring IGAR, see *Administrator Guide for Avaya Aura® Communication Manager* .

- Static IP addressing for the Dialer interface may not be feasible. Dynamic IP addressing is available to enable you to connect to the remote network through an ISP. ISPs commonly provide IP addressing for connected ports on an as-needed basis. IP unnumbered links are available to supply addressing in situations where you wish to run routing over your network link without committing a subnet.
- Object tracking can be used with the Loopback interface to provide an alternative method for activating the Dialer interface when connectivity with the main office is lost. This is useful in configurations where the WAN interface is not connected directly to the Branch Gateway. Use object tracking to configure RTRs to verify connectivity with the main office. If the RTR fails, the object tracker can be configured to change the status of the Loopback interface to down. If the Dialer interface is configured as the backup for the Loopback interface, the Dialer interface will automatically dial when connectivity fails.

Note:

In a situation where the same modem is used for inbound Avaya Service calls and outbound dial backup calls, only one call can be active at any time.

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

Related links

[Backup interfaces](#) on page 239
[Console port and modem configuration](#) on page 218
[PPPoE overview](#) on page 231
[Header compression configuration](#) on page 206
[Policy lists](#) on page 504
[Dynamic CAC](#) on page 261
[Dynamic local peer IP](#) on page 460
[Unnumbered IP interfaces](#) on page 391
[Object tracking](#) on page 263

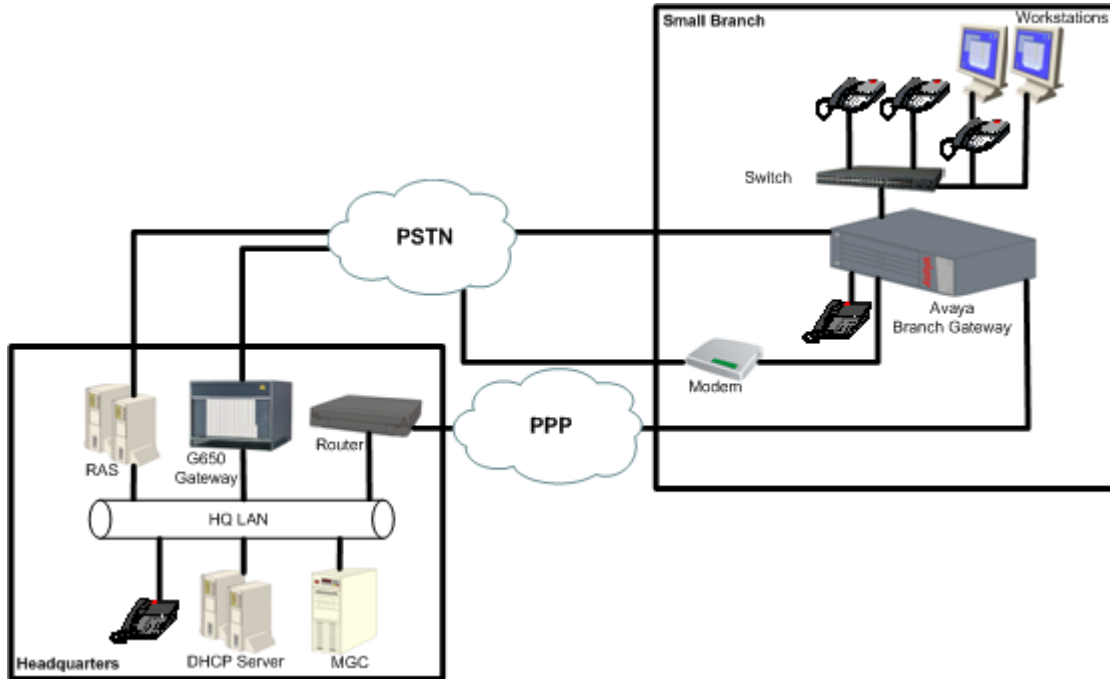
Configuration example

This example sets up a modem dial backup for the WAN link between a branch office and the headquarters data center. The branch office is connected to the corporate network using a Branch Gateway. IP phone users in the branch office connect to an MGC located in the headquarters data center, and an RAS is located in the headquarters data center, with multiple phone lines available for dial access. The primary WAN connection is a PPP link connected to the serial 3/1 port. The Dialer PPP session uses CHAP encryption. The corporate network is routed using OSPF. An analog trunk connects the branch office to the PSTN for non-corporate bearer traffic.

*** Note:**

When using a broadband modem (either xDSL or cable), it is recommended to run the VPN application.

The following figure shows the network topology.



Command sequence

```
!Step 1
Gxxx-001(super-if:Loopback 1)# exit
Gxxx-001(super)# interface loopback 1
Gxxx-001(super-if:Loopback 1)# ip address 149.49.4.5 255.255.255.252
Done!
Gxxx-001(super-if:Loopback 1)# exit
Gxxx-001(super)#
!Step 2
Gxxx-001(super)# ip access-control-list 305
Gxxx-001(super-ACL 305)# name "Block-RTP-to_Modem-bkp"
Done!
Gxxx-001(super-ACL 305)# ip-rule 20
Gxxx-001(super-ACL 305/ip rule 20)# composite-operation "Deny"
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 console
Done!
Gxxx-001(super-if:Dialer 1)# ip unnumbered 1 Loopback 1
Done!
Gxxx-001(super-if:Dialer 1)# ip access-group 305 out
Done!
Gxxx-001(super-if:Dialer 1)# exit
Gxxx-001(super)#
!Step 11
Gxxx-001(super)# interface console
Gxxx-001(super-if:Console)# async mode interactive
Done!
Gxxx-001(super-if:Console)# async modem-type MultiTech-ZBA
Done!
Gxxx-001(super-if:Console)# exit
Gxxx-001(super)#
Step 12
Gxxx-001(super)# interface serial 3/1:1
Gxxx-001(if:serial 3/1:1)# backup interface Dialer 1
Done!
Gxxx-001(if:serial 3/1:1)# exit
Gxxx-001(super)#
Step 13
Gxxx-001(super)# router ospf
Gxxx-001(super router:ospf)# network 149.49.4.4 0.0.0.3 area 0.0.0.5
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.

3. Create the Dialer interface using the **interface dialer** command.

The Dialer interface is created and is available as a backup link for a WAN interface. Only one Dialer interface can be created on the Branch Gateway.

4. Assign a PPP authentication method with the **ppp chap hostname** command.

The Dialer interface authenticates its PPP sessions to the remote RAS server using CHAP authentication and a username of area5. The username area5 must be configured on the RAS as a legitimate user.

5. Assign an initial delay for dialing with the **dialer persistent initial delay** command.

The initial delay prevents the Dialer from dialing out unnecessarily on reboot. The primary WAN interface often requires a few moments to register itself as up, and during that period, the initial delay prevents the device from activating the Dialer.

6. Assign a reset delay for the dialer string list using the **dialer persistent delay** command.

The reset delay determines the amount of time between cycles of call attempts, once all dialer strings have been attempted.

7. Enter up to five dialer strings using the **dialer string** command.

When the Dialer interface is activated, the Dialer first attempts to connect to the number associated with dialer string 1. If the connection attempt fails, the Dialer attempts to connect to the number associated with the next dialer string. These strings represent hunt group phone numbers configured on the RAS server in the headquarters data center.

8. Associate the Dialer interface with its physical port with the **dialer modem-interface** command.

The Dialer interface must be configured to use a physical interface on the device to which the modem is connected. Modem dial backup is supported on both the Console port and the USB port.

9. Configure the modem to participate in network routing with the **ip unnumbered** command.

An unnumbered interface uses the IP address of the interface configured in the command. In this example, the Loopback interface has been created for the Dialer interface to use its IP information. This IP information allows the unnumbered interface to forward and receive IP traffic without actually assigning a static IP address to the Dialer interface.

10. Assign an access control list to the Dialer interface using the **ip access-group** command.

All traffic passing through the Dialer interface must meet the conditions of the access control list associated with this access group or be rejected. In this example, the access-group references access control list 305, which is created to block all outgoing traffic across the Dialer interface other than the VoIP signalling traffic between the branch office gateway and the MGC in the headquarters data center.

11. Configure the Console port to support the modem with the **interface console** command.

The physical interface must be configured to use the attached modem. Each modem type has different initialization requirements. The only modems supporting modem dial backup are the MultiTech ZBA series modems.

12. Assign the Dialer interface to the interface you want to back up with the **backup interface dialer** command.

For example, interface Dialer 1 is selected as the backup interface to interface Serial 3/1:1, the primary WAN connection to the headquarters network. The Dialer activates in the event of a failure of the serial port and all permitted traffic transverses the Dialer interface.

13. Configure the Loopback interface to participate in the OSPF network using the **router ospf** command.

For example, a group of branch offices are assigned to OSPF area 5. This configuration allows filtering to take place at the border points and minimizes topology updates on the headquarters data center routers.

Related links

[Policy lists](#) on page 504

[Modems interfaces](#) on page 216

[Backup interfaces](#) on page 239

[Open shortest path first \(OSPF\)](#) on page 426

Modem dial backup maintenance

The Branch Gateway generates specific log messages for Dialer interface activity when configured to do so. Certain dialer-related log messages are generated to aid you in troubleshooting problems with modem dial backup. In addition, messages generated by the modem and the PPP session are available to help with troubleshooting modem dial backup issues.

Commands used to activate session logging

To activate session logging for modem dial backup functions, type the following commands. Logging messages will be sent to the terminal screen.

- **set logging session condition dialer information**
- **set logging session condition console information**
- **set logging session condition usb-modem information**
- **set logging session condition ppp information**

Note:

Not all logging messages indicate problems. Some are generated to provide information on normal working activity of the Dialer interface.

Syslog and log file logging are also available.

Related links

[System logging](#) on page 191

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 the primary WAN interface for which the Dialer interface has been configured as the backup interface. When the primary WAN interface has been determined to be down, a message is sent indicating the occurrence of the triggering event for the Dialer. When the primary WAN interface is returned to an operational state, a message is generated indicating that the conditions for triggering the Dialer are no longer being met, and that the Dialer can be brought down.	None required.

Table continues...

Log Message	Severity	Possible cause	Action
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 modem, the timer begins. When the timer expires, the Dialer 1 timer expired message is sent, and the Dialer begins attempting to connect to the remote modem again.	None required.
Dialer 1 Modem is not ready	Warning	This message is generated when the Dialer interface has been triggered and the operational state of the Dialer is up, but the Dialer is unable to communicate with the modem.	Troubleshooting steps: • Check modem cable connection to serial port. • Check modem cable connection to modem. • Check power to modem.

Console messages

Console Messages are messages generated by a serial modem attached to the Console port.

Log Message	Severity	Possible cause	Action
Modem cable detected. Port speed <speed> baud.	Informational	When a modem cable is determined to be connected to the serial port, a message is generated indicating the successful connection of the modem cable and advertising the capabilities of the serial port for potential modem connections.	None required.
Modem Detection Failed	Warning	This message is generated when a modem cable is connected to the serial port, but no modem is detected. This message is generated every 30 minutes until the modem is detected.	Troubleshooting steps: • Check modem cable connection to modem. • Ensure that modem is powered on. • Check modem lights for an alarm.
Modem Ready	Informational	When the 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.
Init 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.
Modem cable unplugged	Warning	This message is generated when a Dialer interface is defined, but no modem cable is detected as being connected to the serial port.	Troubleshooting steps: • Check modem cable connection to serial port and reseal cable if necessary.
Connection established	Informational	When the 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 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.
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.

Table continues...

Log Message	Severity	Possible cause	Action
PAP passed/failed	Debug	This message is sent when the authenticating station responds to the PAP authentication request.	None required.
CHAP passed/failed	Debug	This message is sent when the authenticating station responds to the CHAP authentication request.	None required.
IPCP Up/Down	Debug	PPP uses IPCP to define the IP characteristics of the session. IP packets cannot be exchanged until IPCP is in the Up state.	None required.
IPCP IP reject	Warning	This message is generated when IPCP attempts to define the IP characteristics for a PPP session, but does not have the IP address of the local interface to define the session. Without IP address information on both sides of the session, the PPP session cannot begin passing IP traffic.	Troubleshooting steps: • Check Dialer interface configuration to ensure an IP address is configured, either as a static address or through Dynamic IP addressing or through IP unnumbered.

Summary of modem dial backup commands

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

Root level command	Command	Description
interface dialer	-	Enter the Dialer interface configuration context
-	dialer modem-interface	Associate a Dialer with a modem interface
-	dialer order	Set which dial strings are used upon a new dial trigger event
-	dialer persistent	Force the Dialer to attempt to reconnect every second
-	dialer persistent delay	Set the redial interval
-	dialer persistent initial delay	Set the minimum delay from boot to persistent dialing
-	dialer persistent max-attempts	Set the number of consecutive dial attempts for the dial list
-	dialer persistent re-enable	Set the persistent re-enable timer after the maximum number of dial attempts has been reached
-	dialer string	Add a phone number to the dial list

Table continues...

Root level command	Command	Description
-	dialer wait-for- ipcp	Set the maximum time the Dialer waits between dialing a number to successfully establishing PPP/ IPCP
-	ip address	Assign an IP address and mask to an interface
-	ip address negotiated	Enable obtaining an IP address via PPP/IPCP negotiation
-	ip unnumbered	Configure an interface to borrow an IP address from another interface
-	ppp ipcp dns request	Enable requesting DNS information from the remote peer during the PPP/IPCP session
interface (fastethernet loopback serial tunnel)	-	Enter the Console, FastEthernet, Loopback, Serial, or Tunnel interface configuration context
-	backup interface dialer	Set the Dialer interface as the backup interface for the current interface
ip default- gateway	-	Define a default gateway (router)
router ospf	-	Enable OSPF protocol on the system and to enter the Router configuration context
set logging session	-	Manage message logging for the current console session
show interfaces	-	Display interface configuration and statistics for a particular interface or all interfaces

ICMP keepalive

The ICMP keepalive feature, formerly known as extended keepalive, is available for WAN FastEthernet interfaces. ICMP keepalive is a mechanism for determining if a certain IP address is reachable. The source interface sends test packets (ping) and waits for a response. If no response is received after a certain number of tries, the connection is declared to be down.

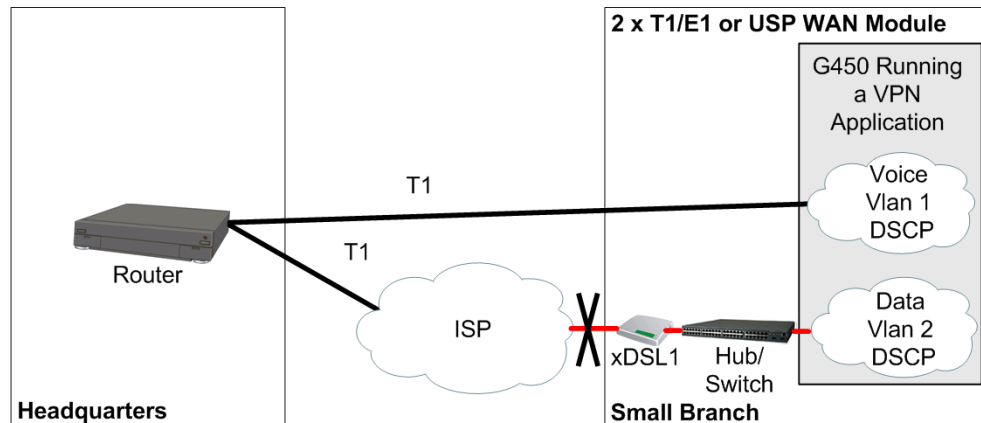
This feature provides a quick means to determine whether the interface is up or down. This is especially important for policy-based routing, in which it is important to determine as quickly as possible whether the next hop is available. See Policy-based routing section.

Note:

ICMP keepalive has been replaced by the object tracking feature that supports keepalive probes over WAN, FastEthernet, Loopback, PPPoE, Dialer PPP interfaces, and Frame relay sub-interfaces. ICMP keepalive is still supported for backward compatibility.

Normal keepalive is sufficient for testing the status of a direct connection between two points. However, in many situations, the system needs to know the status of an entire path in order to ensure that packets can safely traverse it.

ICMP keepalive is a mechanism that reports on the status of an IP address and its next hop. The destination interface is only declared to be alive if the next hop is also reachable. This feature is critical for mechanisms such as policy-based routing that must guarantee service on a particular path.



For example, your branch office may have a Branch Gateway that connects to Headquarters over a T1 line and via an xDSL connection to the Internet. The T1 line is used for voice traffic, while data packets are sent over the xDSL line. If the Fast Ethernet line protocol is up but the xDSL connected to it is down, then ICMP keepalive, which checks the next hop, correctly reports that the WAN path is down. Policy-based routing, which relies on the interface status to determine how packets are routed, can use ICMP keepalive to know the status of the interfaces on its next hop list.

*** Note:**

ICMP keepalive is not used with a GRE Tunnel interface. The GRE tunnel has its own keepalive mechanism.

You cannot configure both DHCP Client and ICMP keepalive on the WAN FastEthernet interface. You cannot configure both DHCP Client and ICMP keepalive on the same WAN FastEthernet interface.

Related links

[Object tracking](#) on page 263

[GRE tunneling](#) on page 398

[DHCP client configuration](#) on page 183

Command used for enabling the ICMP keepalive feature

Use the **keepalive-icmp** command in the context of the interface to enable the ICMP keepalive feature.

For more information about this command, see *Avaya Branch Gateway G450 CLI Reference*.

Commands used to define the ICMP keepalive parameters

Use the following commands to define the ICMP keepalive parameters.

- **keepalive-icmp timeout**
- **keepalive-icmp success-retries**
- **keepalive-icmp failure-retries**
- **keepalive-icmp interval**
- **keepalive-icmp source-address**
- **show keepalive-icmp**

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

Example of configuring ICMP keepalive

The following example configures ICMP keepalive on interface fastethernet 10/2 to send keepalive packets to IP address 135.64.2.12 using MAC address 11.22.33.44.55.66, at five second intervals. If a response is not received within one second, the keepalive packet is considered to have failed. After three consecutive failed packets, the interface is declared to be down. After two consecutive successful packets, the interface is declared to be up.

```
Gxxx-001# interface fastethernet 10/2
Gxxx-001(super-if:FastEthernet 10/2)# keepalive-icmp 135.64.2.12
11.22.33.44.55.66
Gxxx-001(super-if:FastEthernet 10/2)# keepalive-icmp interval 5
Gxxx-001(super-if:FastEthernet 10/2)# keepalive-icmp timeout 1
Gxxx-001(super-if:FastEthernet 10/2)# keepalive-icmp failure-retries 3
Gxxx-001(super-if:FastEthernet 10/2)# keepalive-icmp success-retries 2
Done!
```

Summary of ICMP keepalive configuration commands

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

Root level command	Command	Description
interface fastethernet	-	Enter the FastEthernet interface configuration context
-	keepalive-icmp	Enable the ICMP keepalive mechanism on an interface in the context of the interface. Use the no form of this command to deactivate the feature. Includes the following parameters: • destination ip address. The destination IP address for the keepalive packets. • next hop MAC address. The next hop MAC address for the keepalive packets. This parameter is only relevant for the WAN Fast Ethernet ports.

Table continues...

Root level command	Command	Description
-	<code>keepalive-icmp failure-retries</code>	Set the number of consecutive failed keepalive packets necessary to set the interface's keepalive status as down. The default value is 4.
-	<code>keepalive-icmp interval</code>	Set the interval (in seconds) between keepalive packets. The default value is 5.
-	<code>keepalive-icmp source-address</code>	Set the source IP address of the keepalive packets. The default value is the interface's primary IP address.
-	<code>keepalive-icmp success-retries</code>	Set the number of consecutive successful keepalive packets necessary to set the interface's keepalive status as up
-	<code>keepalive-icmp timeout</code>	Set the timeout (in seconds) for receiving the keepalive response. The default value is 1.
-	<code>show keepalive-icmp</code>	Display information about the extended keepalive settings

Dynamic CAC

Dynamic Call Admission Control (CAC) provides enhanced control over WAN bandwidth. When Dynamic CAC is enabled on an interface, the Branch Gateway informs the MGC of the actual bandwidth of the interface and instructs the MGC to block calls when the bandwidth is exhausted.

Dynamic CAC is especially useful in situations where a primary link is down and a backup link with less bandwidth than the primary link is active in its place. Without dynamic CAC, the MGC is unaware that the interface has switched over to the backup link. Thus, the MGC is unaware of the resulting changes in network topology and bandwidth available for the interface. Consequently, the MGC might allow calls through the interface that require more than the currently available bandwidth.

Note:

Dynamic CAC works in conjunction with the CM Call Admission Control: Bandwidth Limitation (CAC-BL) feature. A related feature is Inter-Gateway Alternate Routing (IGAR), which provides a mechanism to re-route bearer traffic from the WAN to the PSTN under certain configurable conditions. For more information on CAC-BL and IGAR, see *Administrator Guide for Avaya Aura® Communication Manager*.

You can enable dynamic CAC on the following interface types:

- FastEthernet
- Serial (PPP or frame relay)
- GRE Tunnel
- VLAN

*** Note:**

Since VLAN interfaces are always up, configuring dynamic CAC on a VLAN interface provides a means to have a default dynamic CAC bandwidth.

Dynamic CAC tasks

Task	Command
Enabling dynamic CAC and setting maximum bandwidth	dynamic-cac bbl
Displaying bandwidth information	show dynamic-cac

*** Note:**

Dynamic CAC also requires configuration of the CM. For details, see *Administrator Guide for Avaya Aura® Communication Manager*.

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

Summary of dynamic CAC configuration commands

For more information about these commands, see the *Avaya G450 CLI Reference*.

Root level command	Command	Description
interface (dialer serial loopback fastethernet tunnel vlan)	-	Enter the Dialer, Serial, Loopback, FastEthernet, Tunnel, or VLAN interface configuration context
-	dynamic-cac-bbl	Enable dynamic CAC on the interface and set the maximum bandwidth for the interface. The dynamic-cac bbl command includes the following parameters: • 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.

Table continues...

Root level command	Command	Description
<code>show dynamic-cac</code>	-	Display information about the most recent dynamic CAC event. The <code>show dynamic-cac</code> command displays the following information: • Current RBBL. The current actual bandwidth available on the interface. • Last event. The amount of time since the most recent update by the CAC process. • Last event BBL. The interface's bandwidth at the time of the most recent update by the CAC process.

Object tracking

With the Object tracking feature, you can track the state (up/down) of various objects in the system using keepalive probes, and notify registered applications when the state changes. In particular, object tracking is used to monitor Interface states and routes states, where routes can be static routes, the DHCP client default route, or PBR next hops.

The purpose of object tracking is to track the state (up/down) of various objects in the system using keepalive probes, and notify registered applications when the state changes. Configuring object tracking is a two-stage operation:

- The first stage is to define Respond Time Reports (RTRs), the basic building blocks of object tracking. RTRs actively monitor the reachability state of remote devices by generating probes at regular intervals. Each RTR, identified by a unique number, monitors one remote device, and learns the state of the device: up or down. The state of the RTR reflects the state of the device it is monitoring – either up or down.
- The second stage consists of defining Object Trackers using RTRs. The definition of object trackers is recursive. A simple object tracker monitors a single RTR, and its state directly reflects the state of the RTR. A more advanced object tracker is a track list, which is composed of multiple simple object trackers. The state of the track list is calculated based on the states of the objects in the list. Because a track list is itself an object tracker, the objects in a track list can be previously-defined track lists.

You can view a track list as monitoring the “health” of an entire group of remote devices. You can define how to calculate the overall health of the group based on the health (up/down) state of each individual device. For example, you can specify that the overall state is up only if all remote devices are up, or if at least one device is up. Alternatively, you can base the overall state on a threshold calculation.

Using object tracking, different applications can register with the tracking process, track the same remote devices, and each take different action when the state of the remote devices changes.

Configuring object tracking

Procedure

1. Configure RTRs to monitor remote devices and learn if their state is up or down.

Each RTR has a state:

- inactive. Not running
- up. The remote device is considered up
- down. The remote device is considered down

2. Configure object trackers to track the states of RTRs.

Each object tracker calculates its own state as either up or down based on the states of the elements it is tracking. Whenever the state of an object tracker changes, it notifies the applications registered with it.

An object tracker calculates its own state as follows:

- For an object tracker tracking a single RTR:
 - If the state of the RTR is up, the state of the object tracker is up.
 - If the state of the RTR is inactive or down, the state of the object tracker is down.

A track list applies a configurable formula (using a Boolean or a Threshold calculation) to the states of the objects comprising the list, and the result (up/down) is the state of the track list. For example, if the configured formula is the Boolean AND argument, then the state of the list is up if the state of all its objects is up, and down if the state of one or more of its objects is down.

Note:

You can register either a VPN tunnel or an interface with an object tracker. For more information see the definition of the **keepalive-track** command in the *Avaya Branch Gateway G450 CLI Reference*.

You cannot configure both DHCP Client and object tracking on the same WAN FastEthernet interface. You can however, configure tracking on the DHCP client default route.

Related links

[DHCP client configuration](#) on page 183

Configuring RTR

About this task

For each remote device whose state you wish to monitor:

Procedure

1. Enter **rtr**, followed by a number from 1 to 30, to create the RTR.

For example:

```
Gxxx-001(config)# rtr 5
Gxxx-001(config-rtr 5)#
```

2. Use the **type** command to specify the remote device by address, and specify the probing method to be employed by the RTR probe: ICMP Echo or TCP Connection.

If you specify a TCP Connection operation, also specify which port to probe in the remote device.

Examples:

```
Gxxx-001(config-rtr 5)# type echo protocol ipIcmpEcho 10.0.0.1
Gxxx-001(config-rtr icmp 5)#
```

```
Gxxx-001(config-rtr 5)# type tcpConnect dest-ipaddr 147.42.11.1 dest-port
80
Gxxx-001(config-rtr tcp 5)#
```

3. Optionally, use the **frequency** command to specify the frequency at which RTR probes are sent.

If you do not configure this parameter, the default value of five seconds is used.

For example:

```
Gxxx-001(config-rtr icmp 5)# frequency 2 seconds
Done!
```

4. Optionally, use the **dscp** command to set the DSCP value in the IP header of the probe packet, thus setting the packets' priority.

If you do not configure this parameter, the default value of 48 is used.

For example:

```
Gxxx-001(config-rtr icmp 5)# dscp 43
Done!
```

5. Optionally, use the **next-hop** command to specify the next-hop for the RTR probe, and bypass normal routing.

The **next-hop** command is disabled by default.

Use the **next-hop** command when the Branch Gateway is connected to a remote device via more than one interface, and you wish to monitor the state of one specific interface. When you specify the next-hop as the interface you wish to monitor, you ensure that the RTR will probe that interface.

When the RTR is used to monitor a static route, a PBR next hop, or the DHCP client default route, you must specify the same next-hop for the RTR. This ensures it will be sent over the next hop it should monitor.

If the interface is an Ethernet interface (FastEthernet not running PPPoE) or VLAN interface, specify also the interface's MAC address.

For example:

```
Gxxx-001(config-rtr icmp 5)# next-hop interface fastethernet 10/2
mac-address 00:01:02:03:04:05
Done!
```

6. Optionally, use the **source-address** command to specify a source IP address, instead of using the output interface's address.

By default, the **source-address** command is disabled, and RTR probes use the output interface's address.

Use the **source-address** command when you are probing a device located on the Internet, and specify as the source-address the Branch Gateway public IP address.

For example:

```
Gxxx-001(config-rtr icmp 5)# source-address 135.64.102.5
Done!
```

7. Optionally, configure the RTR parameters that determine when the state of the remote device is considered up or down.

If you do not configure these characteristics, their default values are used:

- Use the **wait-interval** command to specify how long to wait for a response from the device. When the wait-interval is exceeded, the probe is considered an unanswered probe. The default value is the current value of **frequency**.
- Use the **fail-retries** command to specify how many consecutive unanswered probes change the state of an RTR from up to down. The default value is 5.

 Note:

When an RTR starts running, its state is considered up.

- Use the **success-retries** command to specify how many consecutive answered probes change the state of an RTR from down to up. The default value is 5.

For example:

```
Gxxx-001(config-rtr icmp 5)# wait-interval 2 seconds
Done!
Gxxx-001(config-rtr icmp 5)# fail-retries 3
Done!
Gxxx-001(config-rtr icmp 5)# success-retries 1
Done!
```

8. Exit the RTR type context, and activate the RTR with the **rtr-schedule** command.

To deactivate the RTR, use the **no rtr-schedule** command.

For example:

```
Gxxx-001(config-rtr icmp 5)# exit
Gxxx-001(config)# rtr-schedule 5 start-time now life forever
```

Once an RTR's probing method and remote device address are configured, you cannot change them. If you exit the RTR type context and you want to modify the configuration of the RTR, you can enter the RTR context using the **rtr** command and specifying the RTR

ID. From the RTR context, you can run the various modification commands described in Steps 3 to 7.

Object tracking provisioning

About this task

To configure object tracking, you must first configure at least one simple object tracker, that is, an object tracker that tracks a single RTR. If you wish, you can then configure a track list which contains multiple simple object trackers and specifies how to calculate the overall state of the list. Note that a track list is itself an object tracker. Therefore, you can configure track lists containing object trackers which are either simple object trackers, or other track lists.

Configuring a simple object tracker

Procedure

1. Use the **track id rtr** command to specify the RTR to be tracked.

Enter a number from 1 to 50 as the unique ID for this object tracker.

For example:

```
Gxxx-001(config)# track 1 rtr 5
Gxxx-001(config-track rtr 1)#
```

2. Use the **description** command to enter a description for the object tracker.

For example:

```
Gxxx-001(config-track rtr 1)# description "track rtr-5"
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 *Avaya Branch Gateway G450 CLI Reference* .

Related links

[Summary of object tracking configuration commands](#) on page 275

Viewing RTR and object trackers logging

Procedure

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

For example:

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

2. Use the **set logging session condition saa** to view all RTR messages of level Info and above.

For example:

```
Gxxx-001# set logging session condition saa Info
Done!
CLI-Notification: write: set logging session condition saa Info
```

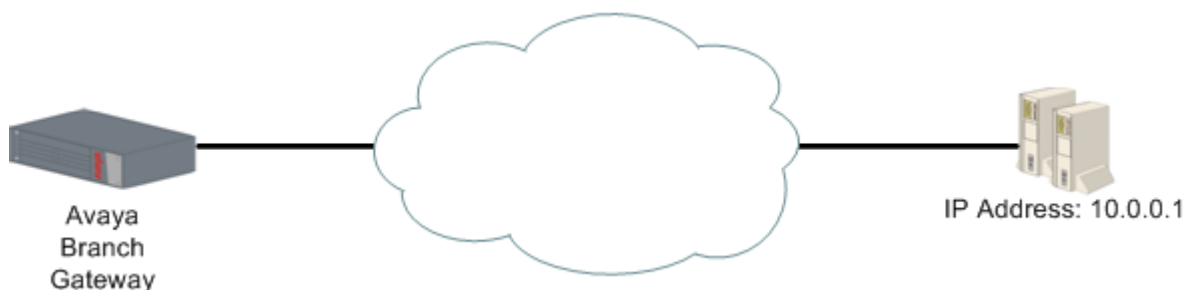
3. Use the **set logging session condition tracker** command to view all object tracker messages of level Info and above.

For example:

```
Gxxx-001# set logging session condition tracker Info
Done!
CLI-Notification: write: set logging session condition tracker Info
```

Example of tracking a single remote device

About this task



Procedure

1. The first step is to configure an RTR which tracks a remote device.

In this case, RTR 5 is configured to track the device at IP address 10.0.0.1. For example:

```
Gxxx-001(config)# rtr 5
Gxxx-001(config-rtr 5)# type echo protocol ipIcmpEcho 10.0.0.1
Gxxx-001(config-rtr icmp 5)# wait-interval 2 seconds
Done!
Gxxx-001(config-rtr icmp 5)# fail-retries 3
Done!
Gxxx-001(config-rtr icmp 5)# success-retries 1
Done!
Gxxx-001(config-rtr icmp 5)# exit
Gxxx-001(config)# rtr-schedule 5 start-time now life forever
```

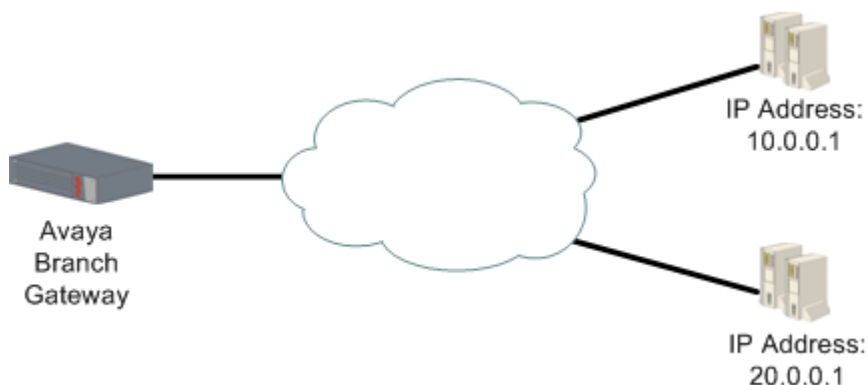
2. The second step is to configure an object tracker which tracks the state of RTR 5.

For example:

```
Gxxx-001(config)# track 1 rtr 5
Gxxx-001(config-track rtr 1)# description "track rtr-5"
Done!
Gxxx-001(config-track rtr 1)# exit
```

Example of tracking a group of devices

About this task



Procedure

1. The first step is to configure several RTRs.

In this case, RTR 5 tracks the device at IP address 10.0.0.1, and RTR 6 tracks the device at IP address 20.0.0.1. For example:

```
Gxxx-001(config)# rtr 5
Gxxx-001(config-rtr 5)# type echo protocol ipIcmpEcho 10.0.0.1
Gxxx-001(config-rtr icmp 5)# wait-interval 2 seconds
Done!
Gxxx-001(config-rtr icmp 5)# fail-retries 3
Done!
Gxxx-001(config-rtr icmp 5)# success-retries 1
Done!
Gxxx-001(config-rtr icmp 5)# exit
Gxxx-001(config)# rtr-schedule 5 start-time now life forever
Gxxx-001(config)# rtr 6
```

```
Gxxx-001(config-rtr 6)# type tcpConnect dest-address 20.0.0.1 dest-port 80
Gxxx-001(config-rtr tcp 6)# frequency 500 milliseconds
Done!
Gxxx-001(config-rtr tcp 6)# dscp 34
Done!
Gxxx-001(config-rtr tcp 6)# next-hop interface fastethernet 10/2 mac-address
00:01:02:03:04:05
Done!
Gxxx-001(config)# rtr-schedule 6 start-time now life forever
Gxxx-001(config-rtr tcp 6)# exit
```

2. The second step is to configure several object trackers.

In this case, object tracker 1 tracks the state of RTR 5, and object tracker 2 tracks the state of RTR 6. For example:

```
Gxxx-001(config)# track 1 rtr 5
Gxxx-001(config-track rtr 1)# description "track rtr-5"
Done!
Gxxx-001(config-track rtr 1)# exit
Gxxx-001(config)# track 2 rtr 6
Gxxx-001(config-track rtr 2)# description "track rtr-6"
Done!
Gxxx-001(config-track rtr 2)# exit
```

3. The third step is to configure a track list object tracker which tracks the states of object trackers 1 and 2, and calculates its own state using a boolean or threshold calculation.

In this case, a Boolean OR argument is used. This means that the track list is up if *either* object tracker 1 *or* object tracker 2 is up. For example:

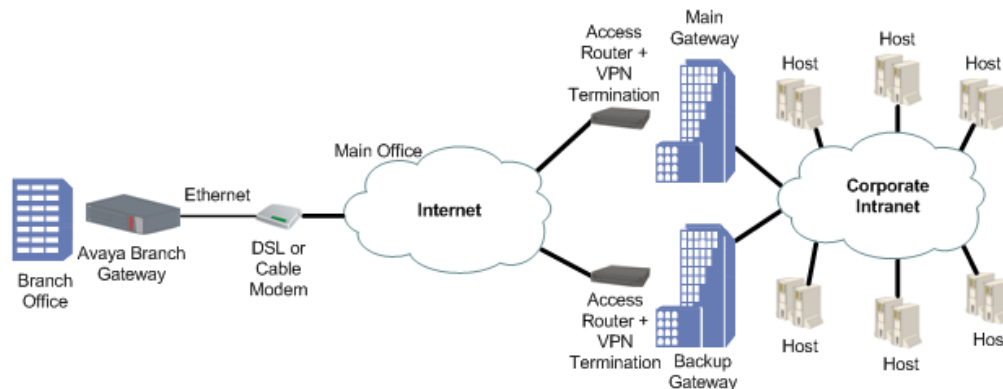
```
Gxxx-001(config)# track 10 list boolean or
Gxxx-001(config-track list 10)# description "track list rtr-5 and rtr-6"
Done!
Gxxx-001(config-track list 10)# object 1
Done!
Gxxx-001(config-track list 10)# object 2
Done!
Gxxx-001(config-track list 10)# exit
```

Typical object tracking applications

- Trigger the failover mechanism for VPN.
- Trigger the failover mechanism for interfaces.
- Track the state of a route: a static route, a PBR next hop, or the DHCP client default route.

Typical application – VPN failover using object tracking

In this application, Branch Gateway is connected to a remote site through an IPSec VPN tunnel. The remote site can be reached through two or more VPN gateways that can back each other up, such as a main gateway and a backup gateway. Object tracking can monitor the state of the current VPN connection, by monitoring one or more hosts that reside within the remote site's network. If the current connection is lost, Branch Gateway can failover to a backup gateway, and attempt to establish a VPN connection to it.



Related links

[Failover using a peer-group](#) on page 490

Typical application – backup for the WAN FastEthernet interface

This typical application illustrates the use of object tracking as a backup mechanism for PPPoE configured on the WAN FastEthernet interface. A track list monitors the state of the connection. If the WAN FastEthernet interface is down, another connection is used.

In this application, the Branch Gateway is connected to an xDSL modem through PPPoE encapsulation configured on interface WAN FastEthernet 10/2. The Branch Gateway is connected to the Internet through the xDSL modem.

* Note:

When using a broadband modem (either xDSL or cable), it is recommended to run the VPN application.

Configuring the backup mechanism

Procedure

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 Serial 3/1:1 as a backup interface for the WAN FastEthernet interface.

Thus, when the track list is down the Serial interface will be up until the track list is up 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 serial 3/1:1 interface
!
interface serial 3/1:1
    encapsulation ppp
    ip address 10.0.0.1          255.0.0.0
    exit
!
! Assign the serial 3/1:1 interface to be the backup interface for
! interface WAN FastEthernet 10/2.
!
interface fastethernet 10/2
    backup interface serial 3/1:1
    backup delay 0 60
    exit

```

Typical application – interface backup using policy-based routing

In the previous typical application, the **backup interface** command is used to specify a backup interface. This typical application illustrates an alternative to the **backup interface** command, using policy-based routing (PBR) which configures a routing scheme for specified traffic based on configured characteristics of the traffic. Thus, PBR can be used in combination with object tracking to configure a backup mechanism for interfaces.

For an example that uses policy-based routing as an alternative to the **backup interface** command, replace the last four lines of the previous typical application with the example below.

The example creates a next hop list that sends the specified traffic to the WAN FastEthernet interface that is running PPPoE encapsulation. If the WAN FastEthernet interface becomes unavailable, the next hop list routes the traffic to the Serial interface 3/1:1. PBR list 801 is created and assigned to interface VLAN 1, so that traffic defined in PBR list 801 passing through interface VLAN 1 is routed according to the next hop list.

*** Note:**

You can define a static route over the WAN FastEthernet interface running DHCP client. In such a case, the static route uses as the next hop the default router learned from the DHCP server. This is useful for GRE tunnels which are defined over the WAN Fast Ethernet running DHCP client. It is necessary to define static routes in order to prevent loops. Therefore, the IP route command allows configuration of static routes over WAN Fast Ethernet running DHCP client.

When the WAN Fast Ethernet is up, policy-based routing routes this traffic via the WAN FastEthernet interface. When the track list defined in the previous typical application is down, policy-based routing routes this traffic through the Serial interface 3/1:1. When the track list is up again, the traffic is again routed through the WAN FastEthernet interface.

```
! Create PBR list 801. This list routes traffic from IP address
! 149.49.42.1 to IP address 149.49.43.1 according to next hop list 10.
!
ip pbr-list 801
  name "list #801"
  ip-rule 10
    next-hop list 10
    source-ip host 149.49.42.1
    destination-ip host 149.49.43.1
  exit
exit

!
! Assign PBR list 801 to interface Vlan 1.
!
interface Vlan 1
  icc-vlan
  ip pbr-group 801
  ip address 149.49.42.254 255.255.255.0
  exit

!
! Configure next hop list 10 with interface fastethernet 10/2 as the
! first next hop, and interface Serial 3/1:1 as the second next hop.
!
ip next-hop-list 10
  next-hop-interface 1 FastEthernet 10/2
  next-hop-interface 2 Serial 3/1:1
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 *Avaya Branch Gateway G450 CLI Reference*.

Root level command	First level command	Second level command	Description
rtr	-	-	Enter Respond Time Reports (RTR) configuration mode. RTRs are the basic building blocks of object tracking.
-	type	-	Set the type of operation an RTR should employ in its probes, and specify the address of the remote device being probed
-	-	dscp	Set the DSCP value for the packets of the RTR probes
-	-	fail-retries	Set how many consecutive unanswered probes change the status of an RTR operation device from up to down
-	-	frequency	Set the frequency of the RTR probes
-	-	next-hop	Specify the next hop for the RTR probes, bypassing normal routing

Table continues...

Root level command	First level command	Second level command	Description
-	-	source-address	Set the source IP address for RTR operations
-	-	success-retries	Set how many consecutive answered probes change the status of an RTR operation device from down to up
-	-	wait-interval	Set how long to wait for a device to answer an RTR probe
rtr-schedule	-	-	Activate or stop an RTR operation
show rtr configuration	-	-	Display RTR configuration values
show rtr operational-state	-	-	Display the global operational status of the RTR feature
show track	-	-	Display tracking information
track	-	-	Configure an object tracker
-	description	-	Set a description for the object tracker
-	object	-	Add an object tracker to a track list
-	threshold count	-	Set the upper and lower thresholds for the threshold in the track list command

Frame relay encapsulation features

The Media Gateway supports the following frame relay encapsulation features:

- Frame relay traffic shaping and FRF.12 fragmentation
- Priority DLCI

Note:

The terms PVC (Permanent Virtual Circuit) and DLCI (Data Link Connection Identifier) describe the same entity and are interchangeable.

Related links

[Priority DLCI](#) on page 278

[Header compression configuration](#) on page 206

Frame relay traffic shaping and FRF.12 fragmentation

Frame relay traffic shaping regulates the outgoing traffic rate on a per-DLCI basis. Each DLCI maintains a weighted fair VoIP queue scheduler to buffer the packets.

FRF.12 fragmentation allows for link fragmentation and interleaving (LFI), which reduces the serialization delay on narrow bandwidth PVCs. This is required for VoIP traffic.

You can configure the traffic shaping and fragmentation parameters within traffic shaping templates called map classes. A map class is comprised of the following parameters:

- **CIR.** Default = 56,000 bps
- **Committed Burst (BC) size.** Default = 7,000 bits
- **Excess Burst (BE) size.** Default = 0 bits
- **Fragmentation.** Fragment size, in bytes. Default = No Fragmentation.

You can configure up to 128 different map classes using different combinations of traffic shaping parameters. You then apply these map classes to a PVC.

 Note:

For a Priority DLCI group you must configure the Primary VC before associating a DLCI map class to the Priority DLCI group VCs. Removing the Primary VC after associating a DLCI map class to the Priority LCI group VCs, removes their map class configuration.

You can enable traffic shaping on a frame relay interface with the **frame-relay traffic-shaping** command. After you enable traffic shaping, a default map class is applied to all currently configured PVCs.

Tasks used to configure map classes

Task	Command
Create a map class, and enter the configuration context of the map class.	map-class frame-relay
Configure the CIR, in bits per second, for the outbound direction.	cir out
Configure the BC size, in bits, for the outbound direction.	bc out
Configure the BE size, in bits, for the outbound direction.	be out
Turn FRF.12 fragmentation on or off and to configure the fragment size.	fragment

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

Task for displaying configured map classes

Task	Command
Display a table of all configured map-classes.	show map-class frame-relay

Summary of frame relay traffic shaping commands

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

Root level command	Command	Description
interface serial	-	Enter the Serial interface or sub interface configuration context
-	frame-relay traffic-shaping	Turn on/off traffic shaping and frame relay fragmentation
map-class frame-relay	-	Create a map class, a QoS template which can later be assigned to DLCIs, and enter the configuration context of the map class
-	bc out	Configure the committed burst size in bits, for the outbound direction
-	be out	Configure the excess burst size in bits, for the outbound direction
-	cir out	Configure the Committed Information Rate in bits per second, for the outbound direction
-	fragment	Turn FRF.12 fragmentation on or off and configure the fragment size
show map-class frame-relay	-	Display the map class table

Priority DLCI

To implement new priority mechanisms, ISPs rely on new classes of service. Traffic types and users are divided into these classes and treated differently during peak periods. A premium, or first class user or traffic stream receives higher priority than a general user. This rating system ensures that the critical Internet user maintains peak performance. It also provides a means for ISPs to enhance the cost structure of network operations.

The Branch Gateway supports class-based traffic assignment (priority DLCI). Priority DLCI is a means for implementing QoS on frame relay circuits. The Branch Gateway separates traffic with different QoS levels to up to four different VCs on the same frame relay sub-interface. This feature enables you to assign unique Permanent VCs (PVC) for VoIP and non-VoIP traffic. You can set and adjust the priority using policy.

Configure Priority DLCI using the **frame-relay priority-dlci-group** command in the Serial sub-interface context. Specify the DLCIs in this command from the highest to lowest priority. If you specify less than four DLCIs, the last DLCI specified is automatically used for the missing priorities.

When using Priority DLCI, the primary DLCI is used to determine the state of the sub frame relay interface. When the primary DLCI is up, the sub frame relay interface is up. When the primary DLCI is down, the sub frame relay interface is down. Therefore, when using Priority DLCI, it is recommended to verify that the primary DLCI is set as the High Priority DLCI in the Priority DLCI group.

On the Branch Gateway, OSPF is mapped by default to the High Priority DLCI. For better network reliability, it is recommended to verify that the same configuration exists on the other side of the frame relay connection.

If one of the Priority DLCIs is down, its traffic is dropped.

Map the PVC control protocol on the routers at all ends of a multi-VC point-to-point link. Map this VC to the highest priority DLCI.

Related links

[Policy lists](#) on page 504

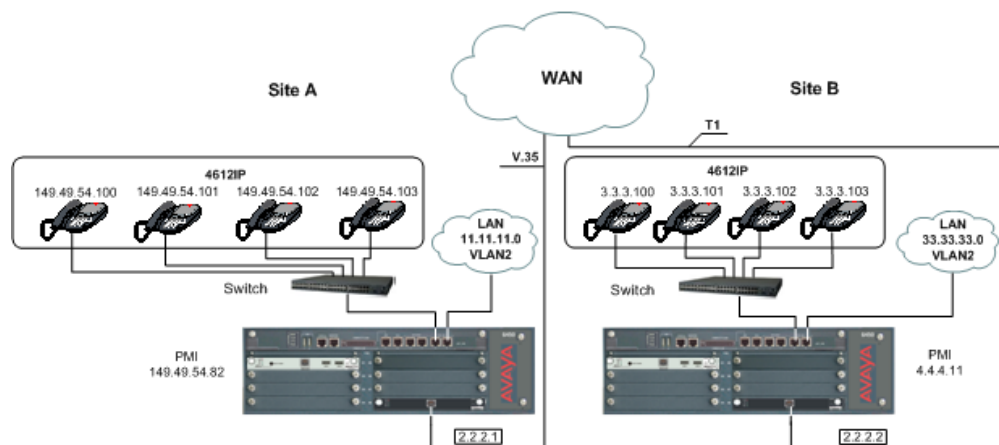
Summary of priority DLCI commands

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

Root level command	Command	Description
<code>interface serial</code>	-	Enter the Serial interface or sub interface configuration context
-	<code>frame-relay priority-dlci-group</code>	Assign Virtual Channels to priority classifications, for the purpose of traffic separation

PPP VoIP configuration

The following figure illustrates a common PPP VoIP configuration between two sites connected over a WAN:



Site A connection details

Site A contains four IP phones and a Branch Gateway with S8300 and one MM342 media module. The MM342 media module connects the Branch Gateway to the WAN through a USP 128 Kbps V.35 interface. The following are the connection details for Site A:

- The IP phones are configured with the following DSCP tagging:
 - Voice: DSCP 46
 - Voice control: DSCP 34

 Note:

The policy list in the next configuration is based on the assumption that the Branch Gateway, S8300, and the IP phones send VoIP control packets with a DSCP value of 34 and voice with a DSCP value of 46. If any of the components of the topology are sending control or voice packets with other DSCP values, you must make changes in the policy list.

- The default RTP UDP port range is 2048 to 3028
- The Network IPs (24 bit subnet masks):
 - IP phones: 149.49.54.0 (VLAN 1)
 - Data: 11.11.11.0 (VLAN 2)
 - Serial: 2.2.2.1
 - S8300: 149.49.54.81
 - Branch Gateway PMI: 149.49.54.82

Site B connection details

Site B contains four IP phones and a Branch Gateway with S8300 and one MM340 media module. The MM340 media module connects the Branch Gateway to the WAN through two-timeslot (128 Kbps) T1 interface. The following are the connection details for Site B:

- IP phones are configured with DSCP tagging:
 - Voice = DSCP 46
 - Voice control = DSCP 34
- The default RTP UDP port range is 2048 to 3028
- Network IPs (24 bit subnet masks):
 - IP phones = 3.3.3.0 (VLAN 1)
 - Data = 33.33.33.0 (VLAN 2)
 - Serial = 2.2.2.2
 - S8300 = 4.4.4.10
 - Branch Gateway PMI = 4.4.4.11

Configuration example for Site A

You can configure PPP VoIP on the Branch Gateway at Site A. Commands with footnotes are described at the end of the configuration procedure.

- Loopback and PMI interfaces configuration:

```
Gxxx-001# interface loopback 1
Gxxx-001(if:Loopback 1)# ip address 149.49.54.82 24
Done!
Gxxx-001(if:Loopback 1)# pmi
The Primary management interface has changed. Please copy the running configuration
to the start-up configuration file, and reset the device.
Gxxx-001(if:Loopback 1)# exit
```



```
Gxxx-001# copy running-config startup-config
Gxxx-001# reset
```

- **VLAN interface configuration:**

```
Gxxx-001# interface Vlan 1
Gxxx-001(if:Vlan 1)# ip address 149.49.54.24
Done!
Gxxx-001(if:Vlan 1)# exit
Gxxx-001# interface Vlan 2
Gxxx-001(if:Vlan 2)# ip address 11.11.11.1 24
Done!
Gxxx-001(if:Vlan 2)# exit
```

- **Serial interface configuration:**

```
Gxxx-001# interface serial 4/1
Gxxx-001(if:Serial 4/1)# ip address 2.2.2.1 24
Gxxx-001(if:Serial 4/1)# mtu 300
```

- **Note:**

Some LAN data applications do not support fragmented packets. In this case, do not change the MTU from its default of 1500.

```
Gxxx-001(if:Serial 4/1)# bandwidth 128
```

- **VoIP configuration:**

```
Gxxx-001(if:Serial 4/1)# ip rtp header-compression
Gxxx-001(if:Serial 4/1)# ip rtp compression-connections 20 (4)
Gxxx-001(if:Serial 4/1)# ip rtp port-range 2048 3028 (5)
Gxxx-001(if:Serial 4/1)# exit
```

- **Static routes configuration:**

```
Gxxx-001# ip default-gateway 4/1
```

* Description of footnoted commands (also applies to identical stages in configuring Site B):

- (1) At this stage you apply Priority 7 to Voice Control traffic.
- (2) At this stage you apply Priority 6 to RTP traffic.
- (3) At this stage you apply maximum trust between 802.1p priority and DSCP.
- (4) At this stage the number of connections (20) depends on the number of phones.
- (5) At this stage you are matching the RTP port range to that of the Gateway.
- (6) At this stage the default queue size is 6, and since RTP is enabled you can double the VoIP queue size.

Configuration example for Site B

You can configure PPP VoIP on the Branch Gateway at Site B.

- **Loopback and PMI interfaces configuration:**

```
Gxxx-001# interface loopback 1
Gxxx-001(if:Loopback1)# ip address 4.4.4.11 32
Done!
Gxxx-001(if:Loopback 1)# pmi
The Primary management interface has changed. Please copy the running configuration
to the start-up configuration file, and reset the device.
```

```
Gxxx-001(if:Loopback1)# exit
Gxxx-001# copy running-config startup-config
Gxxx-001# reset
```

- **VLAN interface configuration:**

```
Gxxx-001# interface Vlan 1
Gxxx-001(if:Vlan 1)# ip address 3.3.3.1 24
Gxxx-001(if:Vlan 1)# exit
Gxxx-001# interface Vlan 2
Gxxx-001(if:Vlan 1:2)# ip address 33.33.33.1 24
Gxxx-001(if:Vlan 1:2)# exit
```

- **Serial interface configuration:**

```
Gxxx-001# controller t1 4/1
Gxxx-001(controller:4/1)# channel-group 1 timeslots 1-2 speed 64
Gxxx-001(controller:4/1)# exit
Gxxx-001# interface serial 4/1:1
Gxxx-001(if:Serial 4/1:1)# ip address 2.2.2.2 24
Gxxx-001(if:Serial 4/1:1)# mtu 300
```



Note:

Some LAN data applications do not support fragmented packets. In this case, do not change the MTU from its default of 1500.

- **VoIP configuration:**

```
Gxxx-001(if:Serial 4/1:1)# ip rtp header-compression
Gxxx-001(if:Serial 4/1:1)# ip rtp compression-connections 20
Gxxx-001(if:Serial 4/1:1)# ip rtp port-range 2048 3028
Gxxx-001(if:Serial 4/1:1)# exit
```

- **Static routes configuration:**

```
Gxxx-001# ip route 1.1.1.0 24 serial 4/1:1
Gxxx-001# ip route 11.11.11.0 24 serial 4/1:1
```

Chapter 12: Emergency Transfer Relay

The Emergency Transfer Relay (ETR) feature provides basic telephone services in the event of system failure, such as a power outage or a failed connection to the MGC. An external 808A ETR relay panel can be used in conjunction with an analog media module (MM711, MM714, MM714B, or MM716). The ETR panel provides up to five incoming Central Office (CO) trunk loops to five selected G450 analog lines. Thus, one ETR panel supports up to five emergency lines. You can cascade a second ETR panel, providing support for up to 10 emergency analog phones. ETR is activated automatically upon system failure by closing the tip/ring contacts between the analog lines and the analog trunks. When ETR is activated, all calls are directed by the analog relays between the outside lines and the analog telephones. A current-loop detection circuit prevents ongoing calls from being disconnected when normal functioning resumes. If a call is in progress on an outside line when the problem ends, the call continues. The trunk port and analog line port passing through the ETR panel do not start to operate until the active call ends.

In addition, each MM714B media module installed in the Branch Gateway can provide identical ETR services in the event of system failure by connecting trunk port 5 to line port 4. You can install an MM714B media module in any slot. When ETR is active and the Branch Gateway has power, the ETR LED is lit.

ETR state configuration

By default, ETR is set to go into effect automatically in the event of power outage or a failed connection to the MGC. You can activate and deactivate ETR manually using the CLI.

Activating ETR manually

About this task

Use this command only for testing. The example below is used for the 808A ETR panel connected to the motherboard (slot-10).

Procedure

Enter `set etr 10 manual-on`

Deactivating ETR manually

Procedure

Enter `set etr 10 manual-off`.

Result

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

Restoring ETR to automatic activation

Procedure

Enter `set etr 10 auto`

If the system fails, the trunk and port in the MM714B, or the analog line connections and analog trunk connections passing through the ETR panel, are automatically latched.

 Note:

A call in progress is terminated when ETR is activated either automatically or manually.

Summary of ETR commands

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

Command	Description
<code>set etr</code>	Enable or disable ETR mode on Branch Gateway chassis or on an MM714B media module, or enable the gateway to control ETR mode automatically.
<code>show etr</code>	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) ETR status on Branch Gateway chassis shows only the Admin state.

Chapter 13: SNMP

SNMP uses software entities called managers and agents to manage network devices. The manager monitors and controls all other SNMP-managed devices or network nodes on the network. There must be at least one SNMP Manager in a managed network. The manager is installed on a workstation located on the network.

An agent resides in a managed device or network node. The agent receives instructions from the SNMP Manager, generates reports in response to requests from the SNMP Manager, and sends management information back to the SNMP Manager as events occur. The agent can reside on:

 Note:

SNMP is supported on IPv4 only.

- Routers
- Bridges
- Hubs
- Workstations
- Printers
- Other network devices

There are many SNMP management applications, but all these applications perform the same basic task. They allow SNMP managers to communicate with agents to configure, get statistics and information, and receive alerts from network devices. You can use any SNMP-compatible network management system to monitor and control a Branch Gateway.

Agent and manager communication

There are several ways that the SNMP manager and the agent communicate. The manager can:

Retrieve a value (get): The SNMP manager requests information from the agent, such as the number of users logged on to the agent device or the status of a critical process on that device. The agent gets the value of the requested Management Information Base (MIB) variable and sends the value back to the manager.

Retrieve the value immediately after the variable you name (get-next): The SNMP manager retrieves different instances of MIB variables. The SNMP manager takes the variable you name and then uses a sequential search to find the desired variable.

Retrieve a number of values (get-bulk): The SNMP manager retrieves the specified number of instances of the requested MIB variable. This minimizes the number of protocol exchanges required to retrieve a large amount of data.

 Note:

Get-bulk is not supported in SNMPv1. Keep the number of repetitions low so that the get-bulk replies are less than 1520 bytes.

Change a configuration on the agent (set): The SNMP manager requests the agent to change the value of the MIB variable. For example, you can run a script or an application on a remote device with a set action.

Receive an unsolicited message (notification): The SNMP manager receives an unsolicited message from an agent at any time if a significant, predetermined event takes place on that agent. When a notification condition occurs, the SNMP agent sends an SNMP notification to the device specified as the trap receiver or trap host. The SNMP Administrator configures the trap host, usually the SNMP management station, to perform the action needed when a trap is detected.

 Note:

For a list of traps and MIBS, see *Gateway Traps for the Avaya G450, and G700 Media Gateways*.

SNMP versions

There are currently three versions of SNMP:

- SNMPv1
- SNMPv2c
- SNMPv3

The Branch Gateway supports all three versions. The implementation of SNMPv3 on the Branch Gateway is backwards compatible. That is, an agent that supports SNMPv3 will also support SNMPv1 and SNMPv2c.

SNMPv1

SNMPv1 uses community strings to limit access rights. Each SNMP device is assigned to a read community and a write community. To communicate with a device, you must send an SNMP packet with the relevant community name.

By default, if you communicate with a device using only the read community, you are assigned the security name ReadCommN. This security name is mapped to the ReadCommG group by default. This allows you to view the agent's MIB tree, but you cannot change any of the values in the MIB tree.

If you communicate with a device using the write community, you are assigned the security name WriteCommN. This security name is mapped to the WriteCommG group by default. This allows you to view the agent's MIB tree and change any of the values in the MIB tree.

 Note:

If you delete the ReadCommN or WriteCommN users, the ReadCommG or WriteCommG groups, or the snmpv1WriteView or snmpv1View, you may not be able to access the device using SNMPv1 or SNMPv2c.

In addition, traps are sent to designated trap receivers. Packets with trap information also contain a trap community string.

SNMPv2c

SNMPv2c is very similar to SNMPv1. However, SNMPv2c adds support for the *get-bulk* action and supports a different trap format.

SNMPv3

SNMPv3 enables the following features over SNMPv1 or v2c:

- User authentication with a username and password
- Communication encryption between the Network Management Station (NMS) and the SNMP agent at the application level
- Access control definition for specific MIB items available on the SNMP agent
- Notification of specified network events directed toward specified users
- Definition of roles using access control, each with unique access permissions and authentication and encryption requirements

The basic components in SNMPv3 access control are users, groups, and views. In addition, SNMPv3 uses an SNMP engine ID to identify SNMP identity. An SNMP engine ID is assigned to each MAC address of each device in the network. Each SNMP engine ID should be unique in the network.

Users

SNMPv3 uses the User-based Security Model (USM) for security, and the View-based Access Control Model (VACM) for access control. USM uses the HMAC-MD5-96 and HMAC-SHA-96 protocols for user authentication, and the CBC-DES56 protocol for encryption or privacy.

An unlimited number of users can access SNMPv3 at the same time.

SNMP security levels

- **NoAuthNoPriv:** . This is the lowest level of SNMPv3 security. No MAC is provided with the message, and no encryption is performed. This method maintains the same security level as SNMPv1, but provides a method for limiting the access rights of the user.

- **AuthNoPriv:** . User authentication is performed based on MD5 or SHA algorithms. The message is sent with an HMAC that is calculated with the user key. The data part is sent unencrypted.
- **AuthPriv:** . User authentication is performed based on MD5 or SHA algorithms. The message is sent in encrypted MAC that is calculated with the user key, and the data part is sent with DES56 encryption using the user key.

snmp-server user command

Use the **snmp-server user** command to create a user or to change the parameters of an existing user. This command includes the following parameters:

- A user name for the user
- The name of the SNMP group with which to associate the user
- The SNMP version functionality that the user is authorized to use. Possible values are: v1 (SNMPv1), v2c (SNMPv2c), and v3 (SNMPv3).
- For an SNMPv3 user, which authentication protocol to use, if any. Possible values are: md5 (HMAC MD5), and sha (HMAC SHA-1). If you specify an authentication protocol, you must also configure an authentication password for the user. The authentication password is transformed using the authentication protocol and the SNMP engine ID to create an authentication key.
- For an SNMPv3 user, whether or not to use the DES/AES privacy protocol, and the user's privacy password if you enable DES/AES privacy.

Use the **no** form of the **snmp-server user** command to remove a user and its mapping to a specified group. If you do not specify a group, the **no** form of the **snmp-server user** command removes the user from all groups.

Groups

In SNMPv3, each user is mapped to a group. The group maps its users to defined views. These views define sets of access rights, including read, write, and trap or inform notifications the users can receive.

The group maps its users to views based on the security model and level with which the user is communicating with the Branch Gateway. Within a group, the following combinations of security model and level can be mapped to views:

- SNMPv1 security model and NoAuthNoPriv security level
- SNMPv2c security model and NoAuthNoPriv security level
- SNMPv3 security model and NoAuthNoPriv security level
- SNMPv3 security model and AuthNoPriv security level
- SNMPv3 security model and AuthPriv security level

If views are not defined for all security models and levels, a user can access the highest level view below the user's security level. For example, if the SNMPv1 and SNMPv2c views are undefined for a group, anyone logging in using SNMPv1 and SNMPv2c cannot access the device. If the

NoAuthNoPriv view is not defined for a group, SNMPv3 users with a NoAuthNoPriv security level can access the SNMPv2c view.

Pre-configured SNMP groups

The Branch Gateway includes the following pre-configured groups:

Group name	Security model	Security level	Read view name	Write view name	Notify view name
initial	v3 (USM)	NoAuthNoPriv	restricted	restricted	restricted
ReadCommG	v1	NoAuthNoPriv	snmpv1View	-	snmpv1View
ReadCommG	v2c	NoAuthNoPriv	snmpv1View	-	snmpv1View
WriteCommG	v1	NoAuthNoPriv	snmpv1 WriteView	snmpv1 WriteView	snmpv1 WriteView
WriteCommG	v2c	NoAuthNoPriv	snmpv1 WriteView	snmpv1 WriteView	snmpv1 WriteView
v3ReadOnlyG	v3 (USM)	AuthNoPriv	v3configView	-	v3configView
v3AdminViewG	v3 (USM)	AuthPriv	iso	iso	iso
v3ReadWriteG	v3 (USM)	AuthNoPriv	v3configView	v3configView	v3configView

snmp-server group command

Use the **snmp-server group** command to create an SNMPv3 group. Use the **no** form of the command to remove the specified group. You can define the following parameters with this command:

- The name of the group
- The SNMP security model
- The security level, for a group with the SNMPv3 security model
- The name of a read view to which the group maps users
- The name of a write view to which the group maps users
- The name of a notify view to which the group maps users

Views

There are three types of views:

Read Views: Allow read-only access to a specified list of Object IDs (OIDs) in the MIB tree

Write Views: Allow read-write access to a specified list of OIDs in the MIB tree

Notify Views: Allow SNMP notifications from a specified list of OIDs to be sent

Each view consists of a list of OIDs in the MIB tree. This list can be created using multiple **snmp-server view** commands to either add OIDs to the list or exclude OIDs from a list of all of the OIDs in the Branch Gateway's MIB tree. You can use wildcards to include or exclude an entire branch of OIDs in the MIB tree, using an asterisk instead of the specific node.

SNMPv3 view creation

To create an SNMPv3 view, the following information must be provided:

- **ViewName:** . A string of up to 32 characters representing the name of the view
- **ViewType:** . Indicates whether the specified OID is included or excluded from the view
- **OIDs:** . A list of the OIDs accessible using the view

SNMP trap configuration

When SNMP traps are enabled on the device, SNMP traps are sent to all IP addresses listed in the trap receivers table. You can add and remove addresses from the trap receivers table. In addition, you can limit the traps sent to specified receivers. You can also enable and disable link up/down traps on specified Branch Gateway interfaces. Use the following commands to configure the trap receivers table:

 Note:

You need an Admin privilege level to use the SNMP commands.

snmp-server host command parameters

You can define the following parameters with this command:

- The IP address of the recipient.
- Whether to send traps or informs to the recipient.
- The SNMP security model (v1, v2c, v3). For SNMPv1 and SNMPv2c, you must also specify the community name. For SNMPv3, you must specify the level of authentication and a username to use in notifications. Authentication levels are:
 - auth. Authentication without encryption
 - noauth. No authentication
 - priv. authentication with encryption
- The UDP port of the target host to use as the destination UDP port when sending a notification to this manager. Optional. The default is 162.

Notification filter groups, to modify the types of traps that are sent to the recipient. Optional. If not specified, all notification groups are sent.

Notification types

Various types of SNMP traps can be sent. You can modify the type of trap by setting the **notification-list** parameter of the **snmp-server host** command to one of the following types:

- **all**. All traps. This is the default.
- **generic**. Generic traps
- **hardware**. Hardware faults
- **rmon**. RMON rising/falling alarm
- **dhcp server**. DHCP server error, such as a DHCP IP conflict detection or notification of no IP address left for specific network
- **dhcp-clients**. DHCP client error, such as a DHCP client conflict detection
- **rtp-stat-faults**. RTP statistics: QoS fault/clear traps
- **rtp-stat-qos**. RTP statistics: end-of-call QoS traps
- **wan**. WAN router traps
- **media-gateway**. Branch Gateway traps (equivalent to G700 MGP traps)
- **security**. Security traps, such as unAuthAccess, macSecurity, unknownHostCopy, and accountLockout
- **config**. Configuration change notifications
- **eth-port-faults**. Ethernet port fault notifications
- **sw-redundancy**. Software redundancy notifications
- **temperature**. Temperature warning notifications
- **cam-change**. Changes in CAM notifications
- **13-events**. Duplicate IP, VLAN violations
- **policy**. Policy change notifications
- **link-faults**. ITC proprietary link down notifications
- **supply**. Main and backup power supply notifications

Summary of SNMP trap configuration commands

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

Root level command	Command	Description
interface (dialer fastethernet tunnel usb-modem)	-	Enter the context of the Dialer, Fast Ethernet, Tunnel, or USB-modem interface
-	snmp trap link-status	Enable or disable Link Up and Link Down traps on an interface
set port trap	-	Enable or disable SNMP Link Up and Link Down traps notifications and traps on a port
set snmp trap enable disable auth	-	Enable or disable authentication failure traps for all managers
set snmp trap enable disable frame-relay	-	Enable or disable frame relay traps for all managers
show port trap	-	Display information on SNMP generic Link Up and Link Down traps sent for a specific port or for all ports
show snmp	-	Display SNMP configuration information
snmp-server enable notifications	-	Enable or disable the sending of all traps and notifications from the Branch Gateway
snmp-server host	-	Identify an SNMP management server, and specify the kind of messages it receives. Use the no form of the command to remove the specified server, or to disable a particular set of notification types.
snmp-server informs	-	Configure the SNMPv3 timeout and retries for notifications

Summary of SNMP access configuration commands

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

Command	Description
ip snmp	Enable or disable the SNMP agent for the Branch Gateway
set snmp community	Create or modify an SNMPv1 community
set snmp retries	Set the number of times to attempt to communicate with a particular node
set snmp timeout	Specify the time to wait for a response before retrying the communication
show snmp	Display SNMP configuration information, including a list of SNMP notification receivers
show snmp engineID	Display the SNMPv3 engine ID for the Branch Gateway
show snmp group	Display a list of SNMPv3 groups

Table continues...

Command	Description
<code>show snmp retries</code>	Display the number of retry attempts to make when attempting to communicate with a node
<code>show snmp timeout</code>	Display the time to wait before resending a communication
<code>show snmp user</code>	Display configuration information for a specified SNMP user
<code>show snmp usertogroup</code>	Display a table of SNMPv3 users and the groups to which they are mapped
<code>show snmp view</code>	Display configuration information for all SNMP views
<code>snmp-server community</code>	Enable or disable SNMP access to the Branch Gateway
<code>snmp-server engineID</code>	Specify the SNMP Engine ID for the Branch Gateway
<code>snmp-server group</code>	Define a new SNMPv3 group, or configure settings for the group
<code>snmp-server remote-user</code>	Configure settings for a remote SNMPv3 user. If the user does not exist, it is created.
<code>snmp-server user</code>	Configure settings for an SNMPv3 user. If the user does not exist, it is created.
<code>snmp-server view</code>	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.

Dynamic trap manager parameters

When you use the `snmp-server dynamic-trap-manager` command, you can configure the following parameters:

- Whether to send traps or informs to the recipient
- The SNMP security model (v1 or v2c)
- The SNMP community name
- The UDP port of the target host to use as the destination UDP port when sending a notification to this manager. Optional.
- The types of traps to be sent. Optional. The default is to send all types of traps.

Related links

[Notification types](#) on page 291

Summary of dynamic trap manager configuration commands

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

Command	Description
clear dynamic-trap-manager	Remove administration of the dynamic trap manager
snmp-server dynamic-trap-manager	Specify the parameters of the dynamic trap manager feature

SNMP configuration examples

The following example enables link up/down traps on an Ethernet interface:

```
Gxxx-001(super)# interface fastethernet 10/3
Gxxx-001(super-if:FastEthernet 10/3)# snmp trap link-status
Done!
```

The following example displays SNMP information:

```
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
Enter authentication password : *****
Confirm authentication password : *****
Enter privacy password : *****
Confirm privacy password : *****
Done!
```

The following example creates a read-only user:

```
Gxxx-001# snmp-server user joseph ReadOnlyG v3 auth md5 priv des56 ktamatan
Enter authentication password : *****
Confirm authentication password : *****
Enter privacy password : *****
Confirm privacy password : *****
Done!
```

The following example creates a read-write user:

```
Gxxx-001# snmp-server user johnny ReadWriteG v3 auth md5 priv des56 ktamatan
Enter authentication password : *****
Confirm authentication password : *****
Enter privacy password : *****
Confirm privacy password : *****
Done!
```

The following example creates an admin user:

```
Gxxx-001# snmp-server user johnny v3AdminG v3 auth md5 priv des56 ktamatan
Enter authentication password : *****
Confirm authentication password : *****
Enter privacy password : *****
Confirm privacy password : *****
Done!
```

The following example sets the SNMPv1 read-only community:

```
Gxxx-001(super)# set snmp community read-only read
SNMP read-only community string set.
```

The following example sets the SNMPv1 read-write community:

```
Gxxx-001(super)# set snmp community read-write write
SNMP read-write community string set.
```

The following example enables link up/down trap on a LAN port on the G250:

```
G250-001(super)# set port trap 10/3 enable
Port 10/3 up/down trap enabled
```

The following example enables Link Up and Link Down traps on a LAN port on the Branch Gateway:

```
Gxxx-001(super)# set port trap 10/5 enable
Port 10/5 up/down trap enabled
```

The following example disables link up/down trap on a LAN port on the G250:

```
G250-001(super)# set port trap 10/4 disable
Port 10/4 up/down trap disabled
```

The following example disables Link Up and Link Down traps on a LAN port on the Branch Gateway:

```
Gxxx-001(super)# set port trap 10/5 disable
Port 10/5 up/down trap disabled
```

Chapter 14: Media encryption using AES-256

From Communication Manager Release 7.0, the AES encryption option now includes AES-256 cipher suite. AES-256 applies to voice media streams and video media streams for the IP network region that governs the IP codec set. The feature also introduces a mechanism to define the encrypted SRTCP policy for calls governed by the IP network region.

Screen for administering Media encryption using AES-256

Screen name	Purpose	Fields
ip-codec-set	To select a type of media encryption.	Media encryption

Administering Media encryption using AES-256

Before you begin

Ensure that the **Media Encryption Over IP?** field on the system-parameters customer-options screen is set to *y*.

Procedure

1. On the SAT screen, type `change ip-codec-set n`, where *n* is the number of the codec set that you want to change.
2. In the **Media encryption** field, type one of the following values:
 - To use encrypted and authenticated RTP with an 80-bit authentication tag, type `10-srtp-aescm256-hmac80`.
 - To use encrypted and authenticated RTP with a 32-bit authentication tag, type `11-srtp-aescm256-hmac32`.
3. Save and exit.

Detailed description

Advanced Encryption Standard (AES) is a widely used specification for data encryption. The AES standards describe a symmetric key algorithm. AES has a fixed block size of 128 bits and a key size of 128, 192, or 256 bits. Avaya Aura® Release 6.3 Feature Pack 4 supports AES-256 as part of TLS support over control channels. From Release 7.0, the AES-256 support extends to secure media streams.

To enable Media encryption feature, two more encryption choices are available for the **Media encryption** field on the ip-codec-set SAT screen. The choices are as follows:

- srtp-aescm256-hmac80
- srtp-aescm256-hmac32

Before Release 7.0, the **Media Encryption** field supported only three profiles. Release 7.0 onwards, the field supports five profiles.

You can add the following profiles to Media Encryption:

1. 10-srtp-aescm256-hmac80
2. 11-srtp-aescm256-hmac32
3. 1-srtp-aescm128-hmac80
4. 2-srtp-aescm128-hmac32
5. None

The AES-256 feature is supported on G450 Branch Gateway, G430 Branch Gateway, and Avaya Aura® Media Server (MS).

When you enable the AES-256 feature, Communication Manager determines the capability exchange with G450 Branch Gateway, G430 Branch Gateway, or Avaya Aura® Media Server (MS) and the 96x1 SIP phone. To establish call connections for media services encrypted with AES-256, an SDP media descriptor exchange occurs. During this exchange, Communication Manager functions as a back-to-back user agent. In this role, Communication Manager supports policy management over the SIP endpoints when the endpoints exercise capability negotiation.

Chapter 15: Encrypted SRTCP

Detailed description

With the Encrypted SRTCP feature, you can protect media control streams. To support this feature, the **Encrypted SRTCP** field is available on the ip-codec-set SAT screen. The following are the available policy modes:

- **Force Encrypted SRTCP:** To permit only encrypted SRTCP calls and to achieve high security standards. If you set the field to `enforce-enc-srtcp`, all the crypto profiles enforce encrypted SRTCP.
- **Best Effort:** To facilitate negotiation of the encrypted SRTCP parameter. If you set the field to `best-effort`, Communication Manager facilitates negotiation of Encrypted SRTCP capability between the endpoints. All endpoints must support negotiation to enforce the Best Effort policy mode.
- **Force Unencrypted SRTCP:** To support backward compatibility. If you set the field to `enforce-unenc-srtcp`, all the crypto profiles enforce unencrypted SRTCP.

Encrypted SRTCP

Use the Encrypted SRTCP feature to provide enhanced security for the media control streams associated with the RTP media stream.

 Note:

The RTP and RTCP streams are two consecutive UDP ports. The RTCP control stream conveys usage data. An example of usage data is the identification of the two parties on a given call.

Screen for administering Encrypted SRTCP

Screen name	Purpose	Fields
ip-codec-set	To select a policy option to activate the encrypted SRTCP.	Encrypted SRTCP

Administering Encrypted SRTCP

Before you begin

Ensure that the **Media Encryption Over IP?** field on the system-parameters customer-options screen is set to *y*.

Procedure

1. On the SAT screen, type `change ip-codec-set n`, where *n* is the number corresponding to the codec set that you want to change.
2. In the **Encrypted SRTCP** field, type `enforce-enc-srtcp`. You can select the **Best Effort** option if you want Communication Manager to negotiate encrypted SRTCP capability between endpoints.

 Note:

The default value for Encrypted SRTCP is `enforce-unenc-srtcp`. Endpoints earlier than Release 7.0 do not support encrypted SRTCP. Therefore, enforcing unencrypted SRTCP is preferable in networks that have Communication Manager Release 7.0 with earlier endpoints.

3. Save and exit.

Interactions for Encrypted SRTCP

This section provides information about how the Encrypted SRTCP feature interacts with other features in the system. Use this information to ensure that you receive the maximum benefits of the Encrypted SRTCP feature in any feature configuration.

Emergency calling

Using the encryption options, you cannot negotiate calls with the destination party because of protocol incompatibilities. The protocol incompatibility results in the inability to pass certain types of emergency calls. Therefore, you must configure the network to ensure best routing of calls.

Media Encryption using AES

If the RTP media encryption is set to none, the enforce-encrypted SRTCP rules do not apply to the RTP/RTCP streams.

Chapter 16: Contact closure

You can use contact closure to control up to two electrical devices remotely. With contact closure, you can dial feature access codes on a telephone to activate, deactivate, or pulse electrical devices such as electrical door locks. You can also activate and deactivate contact closure using CLI commands. You can only use feature access codes if you configure the Branch Gateway to use a server with CM software.

It is recommended that you use an Avaya Partner Contact Closure Adjunct™ for contact closure. For more information, see *Overview for the Avaya Branch Gateway G450*. 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 CM. For more information, see *Administrator Guide for Avaya Aura® Communication Manager*.

Related links

[Branch Gateway Controller configuration](#) on page 66

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 G450*.

Software contact closure

Contact closure modes

Mode	Description
mgc	The MGC controls contact closure. In mgc mode, the user dials feature access codes to activate and deactivate contact closure.
manual-trigger	Activates contact closure for the specified relay
manual-off	Deactivates contact closure for the specified relay

Configuring contact closure software

About this task

To configure the Branch Gateway to activate contact closure when the feature access code is dialed:

Procedure

1. Enter the **set contact-closure admin** command.

In the following example, the command sets contact closure to work in relay 1 of the Avaya Partner Contact Closure Adjunct™ 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 *Avaya Branch Gateway G450 CLI Reference*.

Command	Description
set contact-closure admin	Specify how the contact closure relay is controlled
set contact-closure pulse-duration	Set the length of time for the relay to return to normal after the call controller triggers the relay
show contact-closure	Display the status of one or all contact closure relays

Chapter 17: Announcement files

The Branch Gateway stores announcement files in an internal announcement directory. The Branch Gateway supports up to 256 announcement files, totalling up to 45 minutes of audio for announcements and music on hold. If a compact flash is installed with increased RAM, the Branch Gateway supports up to 1024 announcement files, for a total of 240 minutes. The motherboard contains additional RAM to support 1024 announcement files for G450v4. A total of 63 announcements can be played simultaneously, and one port may be used for recording. Recording, storing, and playing announcement files is controlled by CM.

Note:

For information about installing and using a compact flash and increased RAM, refer to *Job Aid: Installing the upgrade memory kit in the G450 / G430 Branch Gateway*.

Avaya Voice Announcement Manager (VAM) can be used to centrally manage announcement files for multiple voice systems, including Branch Gateways. VAM is designed to be installed on a customer-provided platform at a remote location. For information about VAM, see *Avaya Voice Announcement Manager Reference*.

The Branch Gateway supports:

- Secure transfer of announcement files to and from VAM using SCP
- Simple management operations for the announcement files stored in the announcement directory
- Dynamic allocation of announcement time slots for 64 announcement ports on an as-needed basis

Uploading announcement files to a remote SCP server

Procedure

Upload an announcement file to a remote SCP server, using the `copy announcement-file scp` command.

Specify the file name of the announcement file in the Branch Gateway announcement directory, followed by the IP address of the remote SCP server, and, optionally, a destination file name, including the full path.

For example:

```
Gxxx-001(super)# copy announcement-file scp local_announcement2.wav  
192.168.49.10 remote_announcement2.wav
```

Downloading announcement files from a remote SCP server

Procedure

Download an announcement file from a remote SCP server to the Branch Gateway announcement directory, using the **copy scp announcement-file** command.

Specify the file name of the announcement file on the remote SCP server, followed by the IP address of the remote SCP server, and, optionally, a destination file name, including the full path.

For example:

```
Gxxx-001(super)# copy scp announcement-file announcement_file1.wav  
192.168.49.10
```

Uploading announcement files to a remote FTP server

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 announcement file to a USB mass storage device

Procedure

Upload an announcement file to a USB mass storage device, using the **copy announcement-file usb** command.

Specify the file name of the announcement file in the Branch Gateway announcement directory, followed by the name of the USB device, and, optionally, a destination file name, including the full path.

Example

```
Gxxx-001(super)# copy announcement-file usb local_announcement2.wav  
usb-device0 remote_announcement2.wav
```

Downloading an announcement file from a USB mass storage device

Procedure

Download an announcement file from a USB mass storage device to the Branch Gateway announcement directory, using the **copy usb announcement-file** command.

Specify the name of the USB device, followed by the file name of the announcement file on the USB device, and, optionally, a destination file name, including the full path.

For example:

```
Gxxx-001(super)# copy usb announcement-file usb-device0 \temp\  
announcement_file1.wav local_announcement_file2.wav
```

Uploading announcement files to a remote HTTP or HTTPS server

Procedure

Upload an announcement file to a remote HTTP or HTTPS server, using the **copy announcement-file https** command.

Specify the file name of the announcement file in the Branch Gateway announcement directory, followed by the URL of the remote HTTP or HTTPS server, the transfer type, and optionally, the destination filename.

Example

```
Gxxx-001(super)# copy announcement-file https local_announcement2.wav  
http://user@www.example.com:8000/files/local_announcement2.wav
```

Downloading announcement files from an HTTP or HTTPS server

Procedure

Download an announcement file from an HTTP or HTTPS server to the Branch Gateway announcement directory, using the **copy https announcement-file** command.

Specify the URL of the announcement file on the HTTPS server followed by the optional transfer type, and, optionally, a destination file name, including the full path.

For example:

```
Gxxx-001(super)# copy http announcement-file http://www.example.com/files/ann123.wav
```

For example:

```
gxxx-001(super)# copy announcement-file http ann123.wav http://  
user@www.example.com:8000/files/ann123.wav
```

```
Enter WebServer password:
```

Uploading announcement files to a remote SCP server via Avaya SBC tunnel

Procedure

Uploads an announcement file from the Branch Gateway announcement directory to a remote SCP server using SCP via Avaya SBC tunnel, using the **copyedge announcement-file scp** command.

Specify the file name of the announcement file in the Branch Gateway announcement directory, followed by the file directory path and file server IP address of the remote SCP server.

For example:

```
Gxxx-001(super)# copyedge announcement-file scp local_announcement2.wav  
192.168.49.10
```

Downloading announcement files from a remote SCP server via Avaya SBC tunnel

Procedure

Downloads an announcement file from the Voice Announcements Manager or an SCP server via Avaya SBC tunnel to the Branch Gateway announcement directory, using the **copyedge scp announcement-file** command.

Specify the file name of the announcement file in the Branch Gateway announcement directory, followed by the file directory path and file server IP address of the remote SCP server.

For example:

```
Gxxx-001(super)# copyedge scp announcement-file c:\temp\announcement_file2.wav
192.168.49.10
```

Erasing an announcement file from the directory

Procedure

Erase an announcement file from the Branch Gateway announcement directory, using the **erase announcement-file** command.

Specify the name of the file.

For example:

```
Gxxx-001# erase announcement-file local_announcement1.wav
```

Renaming an announcement file in the directory

Procedure

Rename an announcement file in the Branch Gateway announcement directory, using the **rename announcement-file** command.

Specify the current name of the file followed by the new name.

For example:

```
Gxxx-001# rename announcement-file from_local_announcement1.wav
to_local_announcement1.wav
```

Displaying the announcement files stored in the directory

Procedure

Display the announcements files stored in the Branch Gateway announcement directory, using the **show announcements-files** command.

Optionally add the keyword **brief** to display less detail.

For example:

```
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 23 AUG 2015
8    4601dbtel_82.bin     Announcement2  8000          09:55:55 23 AUG 2015
9    4602dbtel_82.bin     Announcement3  16000         09:56:55 23 AUG 2015
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 *Avaya Branch Gateway G450 CLI Reference*.

Command	Description
<code>copy announcement-file ftp</code>	Upload an announcement file to a remote FTP server
<code>copy announcement-file scp</code>	Upload an announcement file to a remote SCP server
<code>copy announcement-file usb</code>	Upload an announcement file to a USB mass storage device
<code>copy announcement - file https</code>	Upload an announcement file from Branch Gateway announcement directory to a remote HTTP or HTTPS server
<code>copyedge announcement - file scp</code>	Upload an announcement file from Branch Gateway announcement directory to a remote SCP server
<code>copy ftp announcement-file</code>	Download an announcement file from an FTP server to Branch Gateway announcement directory
<code>copy scp announcement-file</code>	Download an announcement file from a remote SCP server to Branch Gateway announcement directory
<code>copy usb announcement-file</code>	Download an announcement file from a USB mass storage device to Branch Gateway announcement directory
<code>copy https announcement-file</code>	Download an announcement file from a remote HTTP or HTTPS server to Branch Gateway announcement directory
<code>copyedge scp announcement-file</code>	Download an announcement file from a remote SCP server through Avaya SBC tunnel to Branch Gateway announcement directory
<code>erase announcement-file</code>	Erase an announcement file from Branch Gateway announcement directory
<code>rename announcement-file</code>	Rename an announcement file in Branch Gateway announcement directory

Table continues...

Command	Description
<code>show announcements files</code>	Display the announcements files stored in Branch Gateway announcement directory
<code>show download announcement-file status</code>	Display the status of a download process of announcement files
<code>show upload announcement-file status</code>	Display the status of an upload process of announcement files

Dynamic time slots allocation

Branch Gateway dynamically allocates announcement time slots for announcement ports on an as-needed basis. This flexibility provides greater assurance of having time slots available for voice calls. However, Branch Gateway can also potentially run out of time slots for voice calls. To protect Branch Gateway from running out of time slots, use the `set fault-threshold timeslot` command, which determines at what level of time slots occupancy an SNMP trap is sent to the CM. If you see that Branch Gateway is often at 100% time slot capacity, you may need to add another Branch Gateway to your system.

Summary of dynamic time slots allocation commands

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

Command	Description
<code>set fault-thresholds timeslot</code>	Set time slot occupancy notification, by specifying the occupancy rate at which an SNMP trap is generated
<code>show fault-thresholds timeslot</code>	Display time slot occupancy

Chapter 18: Advanced switching

You can configure advanced switching on the switch ports of the Branch Gateway. The switch ports consist of the ETH LAN ports located on the front panel.

VLAN configuration

A VLAN is made up of a group of devices on one or more LANs that are configured so the devices operate as if they form an independent LAN. These devices can, in fact, be located on several different LAN segments. VLANs can be used to group together departments and other logical groups, thereby reducing network traffic flow and increasing security within the VLAN.

VLAN Tagging

VLAN Tagging is a method of controlling the distribution of information on the network. The ports on devices supporting VLAN Tagging are configured with the Port VLAN ID and Tagging Mode parameters.

The Port VLAN ID is the number of the VLAN to which the port is assigned.

Note:

You need to create a VLAN with the `set vlan` command before you can assign it to a port. You can also create a VLAN by using the `interface vlan` command, followed by the number of the VLAN (in other words., enter `interface vlan 2` to create VLAN 2).

Untagged frames and frames tagged with VLAN 0 entering the port are assigned the port's VLAN ID. Tagged frames are unaffected by the port's VLAN ID.

The Tagging Mode determines the behavior of the port that processes outgoing frames:

- If Tagging Mode is set to clear, the port transmits frames that belong to the port's VLAN table. These frames leave the device untagged.
- If Tagging Mode is set to IEEE-802.1Q, all frames keep their tags when they leave the device. Frames that enter the switch without a VLAN tag are tagged with the VLAN ID of the port through which they entered.

Multi VLAN binding

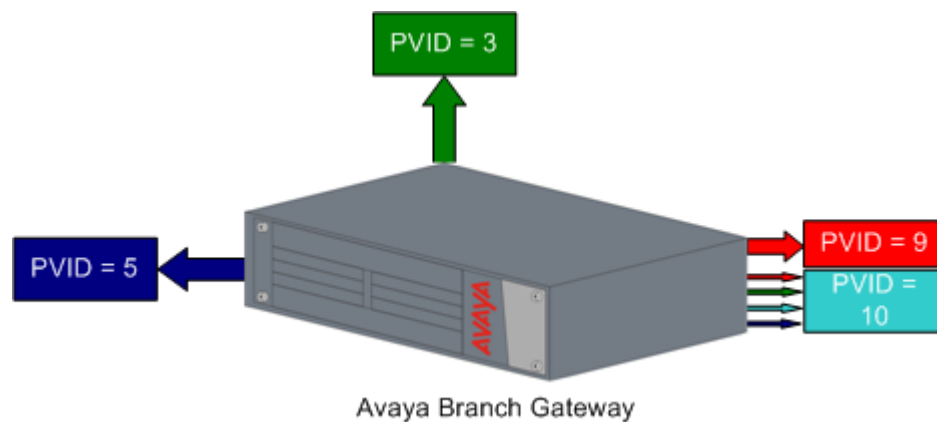
Multi VLAN binding, also known as Multiple VLANs per port, allows access to shared resources by stations that belong to different VLANs through the same port. This is useful in applications such as multi-tenant networks, where each user has a personal VLAN for privacy. The whole building has a shared high-speed connection to the ISP.

In order to accomplish this, Branch Gateway enables multiple VLANs per port. The available Port Multi-VLAN binding modes are:

Bound to Configured: The port supports all the VLANs configured in the switch

Statically Bound: The port supports VLANs manually configured on the port

The following figure shows these binding modes.



Bind to Configured

- The VLAN table of the port supports all the Static VLAN entries and all the ports' VLAN IDs (PVIDs) present in the switch
- VLANs 1, 3, 5, 9, 10 coming from the bus are allowed access through this port
- All the ports in Bound to Configured mode support the same list of VLANs

Static Binding

- The user manually specifies the list of VLAN IDs to be bound to the port, up to 64 VLANs
- Default mode for all ports
- Only VLAN 9, and any other VLANs statically configured on the port will be allowed to access this port

Gateway VLAN table

The Branch Gateway VLAN table lists all VLANs configured on the Branch Gateway. You can configure up to 64 VLANs. To display a list of VLANs, use the **show vlan** command.

When the VLAN table reaches its maximum capacity, you cannot configure any more VLANs. If this occurs, use the **clear vlan** command, followed by the name or number of the VLAN you

want to delete, to free space in the VLAN table. Any new VLANs configured by you are made known to all the modules in the system.

Ingress VLAN Security

Ingress VLAN Security enables easy implementation of security, and is always active. A port that is assigned to a VLAN allows packets tagged for that VLAN only to enter through that port. Unassigned packets receive the PVID of the port and are therefore allowed to enter.

ICC-VLAN

When the Branch Gateway includes an ICC, the ICC connects to the Branch Gateway through an internal switch. By default, the ICC is connected on Vlan 1. The VLAN to which the ICC connects is called the ICC-VLAN.

You can use the `icc-vlan` command to attach the ICC to a different VLAN. Enter the context of the VLAN interface to which you want to attach the ICC switch, and enter `icc-vlan`.

You can use the `show icc-vlan` command from the general context to show the current ICC-VLAN.

Configuring ICC-VLAN

About this task

You must enter the VLAN interface context to configure the ICC VLAN.

Procedure

1. Enter the VLAN interface context by using the `interface vlan` CLI command
2. Enter `icc-vlan`.

Example

The following example sets Vlan 2 as the ICC-VLAN:

```
Gxxx-001(super)# interface vlan 2
Gxxx-001(super-if:Vlan 2)# icc-vlan
Done!
Gxxx-001(super-if:Vlan 2)# exit
Gxxx-001(super)# show icc-vlan
VLAN 2
Gxxx-001(super)#
```

VLAN configuration examples

The following example deletes a statically bound VLAN from a port:

```
Gxxx-001(super)# clear port static-vlan 10/3 34
VLAN 34 is unbound from port 10/3
```

The following example deletes a VLAN and its interface:

```
Gxxx-001(super)# clear vlan 34
This command will assign all ports on VLAN 34 to their default in
```

```
the entire management domain - do you want to continue (Y/N)? y
All ports on VLAN-id assigned to default VLAN.
VLAN 34 was deleted successfully.
```

The following example sets the current VLAN as the ICC-VLAN:

```
Gxxx-001(super)# interface Vlan 66
Gxxx-001(super-if:Vlan 66)# icc-vlan
Done!
```

The following example enters configuration mode for a VLAN interface:

```
Gxxx-001(super)# interface Vlan 66
Gxxx-001(super-if:Vlan 66)#
```

The following example deletes a VLAN interface:

```
Gxxx-001(super)# no interface vlan 66
Done!
```

The following example statically binds a VLAN to a port:

```
Gxxx-001(super)# set port vlan-binding-mode 10/3 static
Set Port vlan binding method:10/3
```

The following example sets a port's VLAN ID:

```
Gxxx-001(super)# set port vlan 54 10/3
Port 10/3 added to VLAN 54
```

The following example sets a port's VLAN binding mode:

```
Gxxx-001(super)# set port vlan-binding-mode 10/3 bind-to-configured
Set Port vlan binding method:10/3
```

The following example configures the VLAN tagging mode of a port:

```
Gxxx-001(super)# set trunk 10/3 dot1q
Dot1Q VLAN tagging set on port 10/3.
```

The following example creates a VLAN:

```
Gxxx-001(super)# set vlan 2121 name Training
VLAN id 2121, vlan-name Training created.
```

The following example displays a list of the MAC addresses in the CAM of a VLAN:

```
Gxxx-001(super)# show cam vlan 54
Total Matching CAM Entries Displayed = 3
Dest MAC/Route Dest VLAN Destination Ports
-----
00:01:02:dd:2f:9f    54        6/13
00:02:2d:47:00:6f    54        10/3
00:02:4b:5b:28:40    54        6/13
```

The following example displays the ICC-VLAN:

```
Gxxx-001(super)# show icc-vlan
VLAN 1
```

The following example displays interface configuration and statistics for a VLAN:

```
Gxxx-001(super)# show interfaces Vlan 1
VLAN 1 is up, line protocol is up
Physical address is 00.04.0d.29.c6.bd.
MTU 1500 bytes. Bandwidth 100000 kbit.
Reliability 255/255 txLoad 1/255 rxLoad 1/255
```

```

Encapsulation ARPA, ICC-VLAN
Link status trap disabled
Full-duplex, 100Mb/s
ARP type: ARPA, ARP Timeout 04:00:00
Last input never, Last output never
Last clearing of 'show interface' counters never.
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
0 input drops, 0 output drops, 0 unknown protocols
0 packets input, 0 bytes
0 broadcasts received, 0 giants
0 input errors, 0 CRC
0 packets output, 0 bytes
0 output errors, 0 collisions

```

The following example displays port VLAN binding information:

```

Gxxx-001(super)# show port vlan-binding-mode 10
port 10/3 is bind to all configured VLANs

```

The following example displays VLAN tagging information:

```

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

```

server-blade-vlan

The command sets the main VLAN for the server in the selected slot.

Syntax

server-blade-vlan <slot | all>

Parameters

Paramater	Decsription	Posible Values	Default Value
<slot all>	The server blade slot number.	server blade slot (1, 5) or all for both slots	

User level

read-write

Context

Interface: VLAN (L2, L2-L3)

Example

```
# server-blade-vlan 5
```

server-blade-oob-vlan

The command sets the Out Of Band management VLAN for the server in the selected slot.

Syntax

```
server-blade-oob-vlan <slot | all>
```

Parameters

Paramater	Decsription	Possible Values	Default Value
<slot all>	The server blade slot number.	server blade slot (1, 5) or all for both slots	

User level

read-write

Context

Interface: VLAN (L2, L2-L3)

Example

```
# server-blade-oob-vlan 5
```

no server-blade-oob-vlan

The command clears the Out Of Band management VLAN for a server in the selected slot.

Syntax

```
no server-blade-oob-vlan <slot | all>
```

Parameters

Paramater	Decsription	Possible Values	Default Value
<slot all>	The server blade slot number.	server blade slot (1, 5) or all for both slots	

User level

read-write

Context

Interface: VLAN (L2, L2-L3)

Example

```
# no server-blade-oob-vlan 5
```

show server-blade-vlan

The command displays the vlan configuration for the S3800 in slot v1 and v5.

Syntax`show server-blade-vlan`**User level**

read-write

Context

general

Example

To display the server-blade-vlan.

`#show server-blade-vlan`**show server-blade-oob-vlan**

The command displays the status of vlan configured for the S3800 in slot v1 and v5 as out-of-band management interface.

Syntax`show server-blade-oob-vlan`**User level**

read-only

Context

general

Example

To display the server-blade-oob-vlan.

`#show server-blade-vlan`**Summary of VLAN commands**

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

Root level command	First level Command	Description
<code>clear port static-vlan</code>	-	Delete statically configured VLANs from the port
<code>clear vlan</code>	-	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
<code>interface vlan</code>	-	Create a VLAN interface, enter interface VLAN configuration mode, or delete a VLAN interface
-	icc-vlan	Set the current VLAN as the ICC-VLAN

Table continues...

Root level command	First level Command	Description
<code>set port static-vlan</code>	-	Assign a static VLAN to a port
<code>set port vlan</code>	-	Set the port VLAN ID (PVID)
<code>set port vlan-binding-mode</code>	-	Define the binding method used by ports
<code>set trunk</code>	-	Configure the VLAN tagging mode of a port
<code>set vlan</code>	-	Create or modify a VLAN
<code>show cam vlan</code>	-	Display all MAC entries in the CAM table for a specific VLAN
<code>show icc-vlan</code>	-	Display the current ICC VLAN
<code>show interfaces</code>	-	Display interface configuration and statistics for an interface or all interfaces
<code>show port vlan-binding-mode</code>	-	Display port VLAN binding mode information
<code>show trunk</code>	-	Display VLAN tagging information for all or less ports
<code>show vlan</code>	-	Display the VLANs configured in the Branch Gateway
<code>server-blade-oob-vlan</code>	-	Sets the Out Of Band management VLAN for the server in the selected slot.
<code>no-server-blade-oob-vlan</code>	-	Clears the Out Of Band management VLAN for a server in the selected slot.
<code>show server-blade-oob-vlan</code>	-	Displays the status of server-blade-vlan configured as the ICC out-of-band management interface.
<code>server-blade-vlan</code>	-	Sets the main VLAN for the server in the selected slot.
<code>show server-blade-vlan</code>	-	Display the server-blade-vlan.

Port redundancy

Redundancy involves the duplication of devices, services, or connections, so that in the event of a failure, the redundant duplicate can take over for the one that failed.

Since computer networks are critical for business operations, it is vital to ensure that the network continues to function even if a piece of equipment fails. Even the most reliable equipment might fail on occasion, but a redundant component can ensure that the network continues to operate despite such failure.

To achieve port redundancy, you can define a redundancy relationship between any two ports in a switch. One port is defined as the primary port and the other as the secondary port. If the primary port fails, the secondary port takes over.

*** Note:**

When port redundancy is activated on Branch Gateway, manually disabling the primary port will also disable the secondary port. To prevent the disabling of the secondary port, you must disable port redundancy before disabling the primary port.

Secondary port activation

The secondary port takes over within one second and is activated when the primary port link stops functioning. Subsequent switchovers take place after the minimum time between switchovers has elapsed. To set the minimum time between switchovers, use the **set port 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.

Port redundancy configuration commands

The following commands are used to configure port redundancy. For more information about these commands, see *Avaya Branch Gateway G450 CLI Reference*.

Enabling and disabling redundancy pairs

Procedure

To globally enable or disable the redundancy pairs you have defined, use the **set port redundancy enable/disable** command.

This command does not delete existing redundancy entries.

Defining or removing redundancy pairs

1. To define or remove redundancy pairs, see the **set port redundancy** command.
2. To ensure that there is no redundancy scheme already defined on any of the links, enter **show port redundancy**.

Configuring time constants

Procedure

To configure the two time constants that determine redundancy switchover parameters, use the **set port redundancy-intervals** command.

Displaying port redundancy schemes

Procedure

To display information about software port redundancy schemes defined for the switch, enter **show port redundancy**.

Port redundancy configuration examples

The following example creates a port redundancy pair:

```
G450-001(super)# set port redundancy 10/5 10/6 on 1
Monitor: Port 10/6 is redundant to port 10/5.
Port redundancy is active - entry is effective immediately
```

The following example deletes a port redundancy pair:

```
G450-001 (super)# set port redundancy 10/5 10/6 off
Entry Monitor removed: Port 10/6 is not redundant to port 10/5
```

The following example enables all configured port redundancies:

```
Gxxx-001(super)# set port redundancy enable
All redundancy schemes are now enabled
```

The following example disables all configured port redundancies:

```
Gxxx-001(super)# set port redundancy disable
All redundancy schemes are disabled but not removed
```

The following example configures the switchback interval for all configured port redundancies:

```
Gxxx-001(super)# set port redundancy-intervals 60 30
Done!
```

The following example displays port redundancy information:

```
G450-001 (super)# show port redundancy
Redundancy Name      Primary Port      Secondary Port      Status
-----
Monitor              10/5             10/6               primary
Minimum Time between Switchovers: 60
Switchback interval: 30
```

Summary of port redundancy commands

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

Command	Description
set port redundancy	Define or remove redundancy pairs
set port redundancy enable disable	Globally enable or disable port redundancy pairs defined on the Branch Gateway
set port redundancy-intervals	Configure the two time constants that determine redundancy switchover parameters
show port redundancy	Display information about software port redundancy pairs defined on the Branch Gateway

Port mirroring

Port mirroring copies all received and transmitted packets (including local traffic) from a source port to a predefined destination port, in addition to the normal destination port of the packets. Port mirroring, also known as “sniffing,” is useful in debugging network problems.

Port mirroring allows you to define a source port and a destination port, regardless of port type. For example, a 10 Mbps and a 100 Mbps port can form a valid source/destination pair. You cannot, however, define the port mirroring source and destination ports as the same source and destination ports.

You can define one source port and one destination port on each Branch Gateway for received (Rx), transmitted (Tx), or transmitted and received (both) traffic.

Port mirroring configuration examples

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

```
G450-001(super)# set port mirror source-port 10/5 mirror-port 10/6 sampling always
direction rx
Mirroring rx packets from port 10/5 to port 10/6 is enabled
```

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

```
G450-001(super)# show port mirror
port mirroring
Mirroring both Rx and Tx packets from port 10/5 to port 10/6 is enabled
```

The following example disables port mirroring:

```
Gxxx-001(super)# clear port mirror
```

Summary of port mirroring commands

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

Command	Description
<code>clear port mirror</code>	Delete a port mirroring pair
<code>set port mirror</code>	Define a port mirroring source-destination pair
<code>show port mirror</code>	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.

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

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
-----
10/5 not-connected 4 128
10/6 not-connected 4 128
```

Summary of spanning tree commands

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

Command	Description
set port edge admin state	Assign or de-assign RSTP edge-port admin state to a port for Rapid Spanning Tree Protocol (RSTP) treatment
set port point-to-point admin status	Specify a port's connection type
set port spantree	Enable or disable spanning tree for specific ports
set port spantree cost	Set the spanning tree cost of a port
set port spantree force-protocol-migration	Force the port to send a rapid spanning tree hello packet (Bridge Protocol Data Unit)
set port spantree priority	Set the spanning tree priority level of a port
set spantree default-path-cost	Set the version of the spanning tree default path cost used by the current bridge
set spantree enable disable	Enable or disable the spanning-tree algorithm for Branch Gateway
set spantree forward-delay	Specify the time used when transferring the state of a port to the forwarding state

Table continues...

Command	Description
<code>set spantree hello-time</code>	Specify the time interval between the generation of configuration BPDUs by the root
<code>set spantree max-age</code>	Specify the time to keep an information message before it is discarded
<code>set spantree priority</code>	Set the bridge priority for the spanning tree
<code>set spantree tx-hold-count</code>	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
<code>set spantree version</code>	Set the version of the spanning tree protocol used by the device
<code>show port edge state</code>	Display the edge state of a specified port
<code>show port point-to-point status</code>	Display the point-to-point status of a specific port or all ports
<code>show spantree</code>	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.

Note:

The 1 GB ports are classified as valuable by default.

Port classification configuration examples

The following example classifies a port as a valuable port:

```
Gxxx-001(super)# set port classification 10/5 valuable
Port 10/5 classification has been changed.
```

The following example displays the port classification of all ports:

```
G450-001(super)# show port classification
Port      Port Classification
-----
10/5      valuable
10/6      regular
```

Summary of port classification commands

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

Command	Description
<code>set port classification</code>	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)
<code>show port classification</code>	Display port classification for a specified port or all ports

Chapter 19: Monitoring applications

The Branch Gateway provides several software tools for monitoring and diagnosing your network. Use these tools to monitor the status of your network operations, and to analyze the flow of information.

RMON

Remote Monitoring (RMON), the internationally recognized network monitoring standard, is a network management protocol that allows network information to be gathered at a single workstation. You can use RMON probes to monitor and analyze a single segment only. When you deploy a switch on the network, there are additional components in the network that cannot be monitored using RMON. These components include the switch fabric, VLAN, and statistics for all ports.

RMON is the internationally recognized and approved standard for detailed analysis of shared Ethernet media. It ensures consistency in the monitoring and display of statistics between different vendors.

RMON's advanced remote networking capabilities provide the tools needed to monitor and analyze the behavior of segments on a network. In conjunction with an RMON agent, RMON gathers details and logical information about network status, performance, and users running applications on the network.

An RMON agent is a probe that collects information about segments, hosts, and traffic, and sends the information to a management station. You use specific software tools to view the information collected by the RMON agent on the management station.

You can configure RMON for switching on the Branch Gateway. The Branch Gateway uses RMON I, which analyzes the MAC layer (Layer 2 in the OSI seven-layer model). You can also configure a port to raise an SNMP trap whenever the port fails.

RMON configuration examples

The following example creates an RMON alarm entry:

```
Gxxx-001(super)# rmon alarm 1 1.3.6.1.2.1.16.1.1.1.5.16777216 20 delta
rising-threshold 10000 32 falling-threshold 1000 32 risingOrFalling root
alarm 1 was created successfully
```


The following example creates an RMON event entry:

```
Gxxx-001(super)# rmon event 32 log description "Change of device"
owner root
event 32 was created successfully
```

The following example creates an RMON history entry with an index of 80 on port 10/3, recording activity over 60 intervals (buckets) of 20 seconds each.

```
Gxxx-001(super)# rmon history 80 10/3 interval 20 buckets 60 owner root
history index 80 was created successfully
```

The following example displays information about an RMON alarm entry:

```
Gxxx-001(super)# show rmon alarm 1
alarm
alarm 1 is active, owned by root
Monitors ifEntry.1.16777216 every 20 seconds
Taking delta samples, last value was 0
Rising threshold is 10000, assigned to event # 32
Falling threshold is 1000, assigned to event # 32
On startup enable rising or_falling alarms
```

The following example displays information about an RMON event entry:

```
Gxxx-001(super)# show rmon event 32
event
Event 32 is active, owned by root
Description is Change of device
Event firing causes log,last fired 12:36:04
```

The following example displays information about an RMON history entry:

```
Gxxx-001(super)# show rmon history 80
history
Entry 80 is active, owned by root
Monitors the port 10/3 every 20 seconds
Requested # of time intervals, ie buckets, is 60
Granted # of time intervals, ie buckets, is 60
Sample # 2 began measuring at 0:21:16
Received 4081 octets, 41 packets,
0 broadcast and 10 multicast packets,
0 undersize and 0 oversize packets,
0 fragments and 0 jabbers,
0 CRC alignment errors and 0 collisions,
# of dropped packet events (due to a lack of resources): 0
Network utilization is estimated at 0
```

The following example displays RMON statistics for a port:

```
Gxxx-001(super)# show rmon statistics 10/3
Statistics for port 10/3 is active, owned by Monitor
Received 6952909 octets, 78136 packets,
26 broadcast and 257 multicast packets,
0 undersize and 0 oversize packets,
0 fragments and 0 jabbers,
0 CRC alignment errors and 0 collisions,
# of dropped packet events (due to a lack of resources): 0
# of packets received of length (in octets):
64:18965, 65-127:295657, 128-255:4033,
256-511:137, 512-1023:156, 1024-1518:0,
```

Summary of RMON commands

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

Command	Description
<code>clear rmon statistics</code>	Clear RMON statistics
<code>rmon alarm</code>	Create or delete an RMON alarm entry
<code>rmon event</code>	Create or delete an RMON event entry
<code>rmon history</code>	Create or delete an RMON history entry
<code>show rmon alarm</code>	Display information about a specific RMON alarm entry or all existing RMON alarm entries
<code>show rmon event</code>	Display a specific RMON event entry or all RMON event entries
<code>show rmon history</code>	Display a specific RMON history entry or all RMON history entries
<code>show rmon statistics</code>	Display RMON statistics for a specific interface or for all interfaces

RTP statistics

The RTP statistics application collects data and statistics for RTP sessions (streams) from Branch Gateway VoIP engine. You can view the data and configure SNMP traps to be generated when the QoS level falls below a configured level. RTP statistics support IPv4 and IPv6 addresses.

Insert content for the first section.

* Note:

An alternative tool available from Avaya for debugging QoS problems is VMON. VMON is an RTCP QoS reports collector. VMON support, available in all 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 Branch Gateway firmware, and does not require any dedicated hardware. For information about configuring VMON in CM, see *Administrator Guide for Avaya Aura® Communication Manager*.

Branch Gateway performs traceroutes whenever RTP statistics is enabled.

The RTP statistics application provides the following functionality:

1. Collects QoS data from Branch Gateway VoIP engines, including Real-Time Control Protocol (RTCP) data, traceroute reports, and information from the DSP regarding jitter buffer, internal delays, and so on.

* Note:

RTCP is a standard QoS report companion protocol to RTP. RTP endpoints periodically send RTCP report packets to their remote peer (or peers in multicast). RTCP reports include QoS data such as delay, jitter, and loss.

2. Collects call data from Branch Gateway, such as duration, start-time, and end-time.
3. Displays the RTP statistics in CLI and MIB formats.

4. Displays summary reports for the VoIP engines.
5. Assesses QoS status based on configurable thresholds on an extensive set of QoS metrics.
6. Generates QoS traps.

QoS traps are notifications sent via SNMP upon termination of an RTP stream that suffers from bad QoS. These notifications include extensive data about the session that enables offline troubleshooting of QoS problems. The trap rate is controlled by a configurable trap rate limiter.

 Note:

QoS trap generation is an especially convenient troubleshooting tool for large installations, since all devices that support the RTP statistics application can be configured to send traps to a single SNMP trap manager.

7. Generates QoS fault and clear traps.

QoS fault traps are notifications that are sent when more than a configurable number of active sessions have QoS indicators over the configured thresholds. A QoS clear trap is a notification that is sent after a QoS fault trap when the number of active RTP sessions with QoS indicators over the configured thresholds reduces to a specified number.

Configuring the RTP statistics application

About this task

To configure the RTP statistics application, work through a set of procedures.

Procedure

1. View RTP statistics thresholds.
2. Set up [RTP statistics thresholds](#) on page 333.
3. Set up the [RTP statistics application](#) on page 334.
4. View the [application configuration](#) on page 334.
5. Set up [QoS traps](#) on page 336.
6. Set up [QoS fault and clear traps](#) on page 337.
7. Set up the [trap rate limiter](#) on page 338.

Viewing RTP statistics thresholds

The RTP statistics application uses a system of thresholds to evaluate levels of QoS during RTP sessions. The thresholds are configured on several QoS metrics. Your configuration of the thresholds determines when the application evaluates a session as having bad QoS conditions.

This section describes the thresholds that you can configure, how you can view the thresholds that are currently configured, and the metrics on which you can configure them.

The RTP statistics application samples the VoIP engine every RTCP interval, which is configured in CM, where it is called “RTCP Report Period”. The RTCP interval is typically 5 to 8 seconds. For

information about configuring the RTCP interval (RTCP report period), see *Administrator Guide for Avaya Aura® Communication Manager*.

Thresholds types

About this task

A threshold on a metric: For example, you can configure a threshold on the metric 'packet loss'. The application samples the metric every RTP interval and increments a counter (event counter) if the sampled value is over the threshold. Hence, the 'event-counter' represents the number of times the metric was sampled over its threshold.

An event threshold: An event threshold is a threshold on an event counter. If QoS traps are configured, the application generates a QoS trap when, at the end of a session, one or more event counters are over their event thresholds. For example, if the event threshold for packet loss is 2, the application generates a QoS trap if packet loss is sampled over its threshold two or more times.

Thresholds on metric averages: The application calculates averages of some of the metrics. When an RTP session terminates, the application evaluates the average metrics and generates a QoS trap (if QoS traps are configured) if one of them is over its corresponding threshold.

* Note:

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

Viewing the configured thresholds

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

```
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

Table continues...

Metric	Description	Evaluation time
Codec RTT	An estimation of the overall Round Trip Time (RTT) on the voice-channel, including the network delay and internal delays. 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 <code>rtp-stat min-stat-win</code> .	Every RTCP interval
Average Loss	The average packet loss evaluation since the beginning of the RTP stream	At the end of the session
Remote Loss	The network loss according to the remote RTP receiver. The device learns of the remote packet loss from received RTCP messages.	Each time an RTCP packet is received
Average Remote Loss	The average remote network loss measurement since the beginning of the RTP stream	At the end of the session
RTT	The network RTT. This metric does not include internal delay. The device learns of the RTT from RTCP messages.	Each time an RTCP packet is received
Local Jitter	Variation in delay of packet delivery to the local peer	Every RTCP interval
Remote Jitter	Variation in delay of packet delivery to the remote peer. The device learns of the remote jitter from RTCP messages.	Each time an RTCP packet is received
SSRC Changes	The number of times the RTP SSRC field in received RTP packets has changed	Every RTCP interval

Configuring RTP statistics thresholds

About this task

Configure RTP statistics thresholds so that incrementation of QoS event counters coincides with real detectable bad QoS in your network. Optimal values are different for each network.

The Codec metrics, Codec loss and Codec RTT are useful for evaluating the actual user experience. The other metrics are useful for identifying network problems that contribute to QoS problems experienced by the user.

Procedure

1. Run the `rtp-stat thresholds` command to set thresholds on QoS indicators.

For example:

```
Gxxx-001(super)# rtp-stat thresholds echo-return-loss 5
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. Run the **rtp-stat event-threshold** command to set thresholds on QoS events.

For example:

```
Gxxx-001(super)# rtp-stat event-threshold echo-return-loss 2
Done!
```

With this example configuration, if echo-return-loss is sampled over its threshold more than twice during an RTP session, the application considers the session to have QoS faults.

Related links

[Viewing RTP statistics thresholds](#) on page 331

Setting up the RTP statistics application

About this task

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

You can view session data and automatic session traceroute results using the CLI.

Procedure

1. To enable the RTP statistics application, type **rtp-stat-service**.

Note:

Admin level access is required in order to use the **rtp-stat-service** command.

For example:

```
Gxxx-001# rtp-stat-service
The RTP statistics service is enabled (default: disabled)
```

2. To reset the RTP statistics application, type **rtp-stat clear**.

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

Viewing application configuration

About this task

View the application configuration to see if the application is enabled, which types of traps are enabled, and how the trap rate limiter and minimum statistics window are configured. The minimum statistics window is the minimum number of observed RTP sequence increments for which the application evaluates packet loss.

Procedure

Type **show rtp-stat config**.

```
Gxxx-001(super)# show rtp-stat config
RTP Statistic: Enabled
QoS Trap: Enabled
QoS Fault Trap: Enabled
    Fault: 2
    Clear: 0
QoS Trap Rate Limiter:
    Token Interval: 10.00 seconds
    Bucket Size: 5
Session Table:
    Size: 128
    Reserved: 64
Min Stat Win: 50
```

RTP statistics application outputs

The following table describes the output of the **show rtp-stat config** command.

Name	Description
RTP Statistic	Status of the RTP statistics application. Possible values: • Enabled. The application is enabled. • Disabled. The application is disabled.
QoS Trap	QoS trap status. Possible values: • Enabled. The RTP statistics application is configured to generate QoS traps. • Disabled. The RTP statistics application is not configured to generate QoS traps.
QoS Fault Trap	QoS fault trap status. Possible values: • Enabled. The RTP statistics application is configured to generate QoS fault and clear traps. • Disabled. The RTP statistics application is not configured to generate QoS fault and clear traps.
Fault	The QoS fault trap boundary. That is, the minimum number of active sessions with QoS faults that triggers a QoS fault trap.
Clear	The QoS clear trap boundary. That is, the reduced number of active sessions with QoS faults that triggers a QoS clear trap to be sent after a QoS fault trap was sent.
QoS Trap Rate Limiter:	
Token Interval	The displayed token interval is in seconds. The maximum long term trap rate, expressed as an interval in seconds. In the example shown, the maximum long term trap rate is one trap every 10 seconds.
Bucket Size	The maximum number of tokens stored in the token bucket of the trap rate limiter. This item limits the size of a QoS trap burst.
Session Table:	

Table continues...

Name	Description
Size	The maximum number of RTP session entries held in the session table in the gateway RAM
Reserved	The number of rows in the session table that are reserved for sessions with QoS problems. In the example shown, the table size is 128 and the reserved number is 64. If, from 1000 sessions only 300 had QoS problems, the session table will hold at least the last 64 sessions that had QoS problems. Note that if the last 128 sessions all had QoS problems, all rows in the session table will be filled with sessions that had QoS problems.
Min Stat Win	The minimum statistic window configured for the RTP statistics application. That is, the minimum number of observed RTP sequence increments for which the application evaluates packet loss.

Enabling QoS traps

About this task

You can configure the application to automatically generate QoS traps using SNMP at the termination of RTP sessions that have QoS problems. SNMP traps are automatically sent to the SNMP trap manager on the active Media Gateway Controller (MGC). You can also configure SNMP traps to be sent to an external trap manager. The application generates a QoS trap when, at the end of an RTP session, one or more event counters are over their event thresholds.

Caution:

If the thresholds for trap generation are set too low, a significant amount of trap traffic will be generated and negatively impact network performance.

Procedure

1. View the RTP statistic thresholds and modify their configurations as necessary.
2. If you need to modify the minimum statistic window, run the **rtp-stat min-stat-win** command.

```
Gxxx-001(super)# rtp-stat min-stat-win 50
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**.

```
Gxxx-001(super)# snmp-server host 136.9.71.47 traps v1 public
```


*** Note:**

When using the **snmp-server host** command, you can specify only to send certain types of traps to the specified trap manager. For example, **snmp-server host 1.1.1.1 traps v1 public rtp-stat-qos rtp-stats-faults** configures only QoS traps and QoS fault and clear traps to be sent to host 1.1.1.1.

To check your current SNMP configurations, enter **show snmp**. Traps are automatically sent to the active MGC by the dynamic trap manager feature. To configure the dynamic trap manager, use the command **snmp-server dynamic-trap-manager**.

4. Type **rtp-stat qos-trap** to enable the traps, if not already enabled.

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

QoS traps are now enabled.

Related links

[Configuring RTP statistics thresholds](#) on page 333

[Viewing RTP statistics thresholds](#) on page 331

[Dynamic trap manager](#) on page 293

QoS fault and clear traps

About this task

You can configure the RTP statistics application to send QoS fault and clear traps. A QoS fault trap is sent when a specified number of active RTP sessions have QoS indicators over the configured thresholds. A QoS clear trap is sent after a QoS fault trap when the number of active RTP sessions with QoS indicators over the configured thresholds reduces to a specified number. Since some RTP sessions can be very long, and QoS traps are sent only after the termination of the stream, QoS fault and clear traps are important for providing timely information about QoS problems.

*** Note:**

QoS fault traps appear in the Network Management Console Event Log Browser, indicating to the user that there are QoS problems in a specific network device. See the *Avaya Network Management Console User Guide*.

Configuring QoS fault and clear traps

Procedure

Use the **rtp-stat fault** command.

For example:

```
Gxxx-001(super)# rtp-stat fault 1 0
The fault trap boundary was set to 1 (default: 3)
The clear trap boundary was set to 0
```

With this example configuration, a QoS fault trap is sent if and when one active RTP session has QoS problems. A QoS clear trap is then sent if and when the number of active RTP sessions with QoS problems reaches 0.

The trap rate limiter

The application features a trap rate limiter. The trap rate limiter limits the rate at which QoS traps are sent. The rate limiter protects against overloading the trap manager with bursts of traps when a single event causes multiple RTP sessions to terminate simultaneously.

The trap rate limiter uses a token bucket scheme, in which traps are sent only if there are tokens in a virtual bucket. Tokens are added to the bucket every 'token interval,' which sets the maximum long term trap rate. Each time a trap is sent, the number of tokens in the bucket decrements. The 'bucket size' is the maximum number of tokens that the bucket can hold. The bucket size limits the trap burst size.

Configuring the trap rate limiter

Procedure

Use the `rtp-stat qos-trap-rate-limit` command.

For example:

```
Gxxx-001# rtp-stat qos-trap-rate-limit 2000 10
```

In this example configuration, the token-interval is 2000 and the bucket-size is 10. This means that a token is added to the bucket every 2000 hundredths of a second (20 seconds) and the bucket is limited to a maximum size of 10 tokens.

RTP statistics output

About this task

This section describes the reports, statistics, and traps you can view, how to view them, and how to understand the output.

Viewing RTP statistics summary reports

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

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

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

RTP statistics summary reports output

About this task

The following table describes the fields in the summary report.

Field	Description
Total QoS traps	The total number of QoS traps sent since the RTP statistics application was enabled or since the last use of the <code>rtp-stat clear</code> 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 <code>rtp-stat clear</code> command
QoS Fault/QoS Clear	General QoS state: QoS Fault means that the number of active RTP sessions with QoS faults is currently higher than the QoS fault boundary. QoS Clear means that the number of active RTP sessions with QoS faults is currently less than or equal to the QoS clear boundary. You can configure the QoS fault and clear boundaries using the <code>rtp-stat fault</code> command. See QoS fault and clear traps on page 337.
Engine ID	The ID of the VoIP engine. Since the Aura Media Gateway has one VoIP engine, one line appears in the table.
Description	Description of the VoIP engine
Uptime	The uptime of the RTP statistics application. This is the time since the RTP statistics application was enabled or since the last use of the <code>rtp-stat clear</code> 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   2015-08-23,10:51:36 10:59:07 G729      135.8.76.64
00032   * 2015-08-23,10:53:42 10:57:36 G729      135.8.76.107
00033   * 2015-08-23,10:58:21 10:59:06 G729      135.8.76.107
00034   2015-08-23,11:08:40 -        G729      135.8.76.64
00035   * 2015-08-23,11:09:07 -        G729      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:

```
G450-001(super)# show rtp-stat detailed 35
Session-ID: 351
Status: Terminated2
, QOS: Faulted3
, EngineId: 04
Start-Time: 2004-10-205
, 11:09:076
, End-Time: 2004-10-20,11:13:407
Duration: 00:04:338
CName: gwp@135.8.118.2529
Phone: 69:201110
Local-Address: 135.8.118.252:206111
SSRC 15461121212
Remote-Address: 135.8.76.107.206113
SSRC 2989801899 (0)14
Samples: 5415
(5 sec)16
Codec:
G72917
62B18
30mS19
Off20
, Silence-suppression(Tx/Rx) Disabled21
/Not-Supported22
,
Play-Time 272.610sec23
, Loss 0.0%24
#125
, Avg-Loss 0.1%26
, RTT 741mS27
#3828
,
Avg-RTT 570mS29
, JBuf-under/overruns 0.1%30
/0.0%31
, Jbuf-Delay 22mS32
,
Max-Jbuf-Delay 60mS33
Received-RTP:
Packets 923634
, Loss 0.0%35
#036
, Avg-Loss 0.0%37
, RTT 604mS38
#3839
, Avg-RTT
376mS40
, Jitter 0mS41
#042
, Avg-Jitter 0mS43
, TTL(last/min/max) 63/63/6344
,
Duplicates 045
, Seq-Fall 046
, DSCP 4647
, L2Pri 1248
, RTCP 5449
Transmitted-RTP:
VLAN 150
, DSCP 18451
, L2Pri 652
, RTCP 6253
Remote-Statistics:
```

```

Loss 0.0%54
#055
, Avg-Loss 0.0%56
, Jitter 0mS57
#058
, Avg-Jitter 0mS59
Echo-Cancellation:
Loss 45dB60
#161
, Len 32mS62
RSVP:
Status Disabled63
, Failures 064

```

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	2015-08-23
	6	The start time of the RTP session	Start-Time: 2015-08-23,11:09:07
End-Time	7	The end time of the RTP session	End-Time: 2015-08-23,11:13:40
Duration	8	The duration of the RTP session	Duration: 00:04:33
CName	9	format: gwt@<MGP-address>	CName: gwp@135.8.118.252

Table continues...

Field	Label	Description	From the CLI example
Phone	10	The local extension number and conference ID in format <i><conference ID>:<extension number></i>. Conference calls can involve more than one entry in the session table. Multiple sessions belonging to the same conference call can usually be identified by a common conference ID. Notes: • Phone data is received from CM only if VMON is configured. • If you are not running VMON, you can cause CM to send the phone data by configuring a dummy RTCP-server for the region, with a 'localhost' IP address (127.x.x.x).	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
	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

Table continues...

Field	Label	Description	From the CLI example
Play-Time	23	The overall time the codec played valid received frames	Play-Time 272.610sec
Codec Loss codec-loss%	24	The last value of codec loss sampled. Codec loss is the percentage of time the codec played fill frames due to lack of valid RTP frames. Possible causes include jitter and packet loss.	Loss 0.0% 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
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

Table continues...

Field	Label	Description	From the CLI example
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 be caused by switching to a backup WAN interface or route flaps.	Seq-Fall 0
DSCP	47	The last received DSCP value of the RTP packets	DSCP 46
L2Pri	48	The last received Layer 2 priority value of an RTP packet (usually IEEE802.1p)	L2Pri 12
RTCP	49	The total number of received RTCP packets	RTCP 54
Transmitted-RTP:			
VLAN	50	The VLAN-ID on which the RTP packets are transmitted	VLAN 1
DSCP	51	The DSCP of RTP packets	DSCP 184
L2Pri	52	The Layer 2 priority of transmitted RTP packets (usually 802.1p)	L2Pri 6
RTCP	53	The total number of transmitted RTCP packets	RTCP 62
Remote-Statistics: (Remote-Statistics items are calculated and evaluated upon reception of RTCP messages)			

Table continues...

Field	Label	Description	From the CLI example
Loss rem-loss%	54	The network loss experienced by the remote RTP receiver. The local RTP receiver learns about its remote peer statistics from RTCP packets.	Loss 0.0% 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
#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:

```
G450-001(super)# show rtp-stat detailed 35
Session-ID: 351
Status: Terminated2
, QOS: Faulted3
, EngineId: 04
Start-Time: 2004-10-205
, 11:09:076
, End-Time: 2004-10-20, 11:13:407
Duration: 00:04:338
CName: gwp@135.8.118.2529
Phone: 69:201110
Local-Address: 135.8.118.252:206111
SSRC 15461121212
Remote-Address: 135.8.76.107.206113
SSRC 2989801899 (0)14
Samples: 5415
(5 sec)16
Codec:
G72917
62B18
30ms19
Off20
, Silence-suppression(Tx/Rx) Disabled21
/Not-Supported22
,
Play-Time 272.610sec23
, Loss 0.0%24
#125
, Avg-Loss 0.1%26
, RTT 741ms27
#3828
,
Avg-RTT 570ms29
, JBuf-under/overruns 0.1%30
/0.0%31
, Jbuf-Delay 22ms32
,
Max-Jbuf-Delay 60ms33
Received-RTP:
Packets 923634
, Loss 0.0%35
#036
, Avg-Loss 0.0%37
, RTT 604ms38
#3839
, Avg-RTT
376ms40
, Jitter 0ms41
#042
, Avg-Jitter 0ms43
, TTL(last/min/max) 63/63/6344
,
```

```

Duplicates 045
, Seq-Fall 046
, DSCP 4647
, L2Pri 1248
, RTCP 5449
Transmitted-RTP:
VLAN 150
, DSCP 18451
, L2Pri 652
, RTCP 6253
Remote-Statistics:
Loss 0.0%54
#055
, Avg-Loss 0.0%56
, Jitter 0mS57
#058
, Avg-Jitter 0mS59
Echo-Cancellation:
Loss 45dB60
#161
, Len 32mS62
RSVP:
Status Disabled63
, Failures 064

```

QoS Trap output fields

The following table describes the fields in the QoS trap according to the numbered labels in the example.

Label	Description	From the trap example
1	The date on which the trap was received	Oct 20
2	The time at which the trap was received	11:13:40
3	The IP address of the local MGP	135.8.118.252
4	The Branch Gateway up time	sysUpTime.0 = Timeticks: (43147723) 4 days, 23:51:17.23
5	The trap name, which indicates that this is a QoS trap	snmpTrapOID.0 = OID: av RtpQoSTrap
6	The local gateway PMI	avRtpSessionLocAddrV4.0 = IpAddress: 135.8.118.252
7	The remote VoIP engine, gateway PMI, or IP phone address	avRtpSessionRemAddrV4.0 = IpAddress: 135.8.76.107
8	The duration of the RTP session	Duration: 00:04:33
9	Format: gwt@<MGP-address>	avRtpSessionCname.0 = STRING: gwp@135.8.118.252

Table continues...

Label	Description	From the trap example
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 CM if VMON is configured. • If you are not running VMON, you can cause CM to send the phone string data by configuring a dummy RTCP-server for the region, with a 'localhost' IP address (127.x.x.x).	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}
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	g729
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%

Table continues...

Label	Description	From the trap example
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}
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 201
 11:10:542
LZ-SIT-SR1 snmptrapd[9407]: 135.8.118.252
[135.8.118.252]: TrapsysUpTime.0 = Timeticks: (43131114) 4 days,
23:48:31.143
, snmpTrapOID.0 = OID: avRtpQoSFault4
, avRtpQoSFaultTh.0 =
INTEGER: 15
, avRtpQoSClearTh.0 = INTEGER: 06
Oct 201
 11:13:402
LZ-SIT-SR1 snmptrapd[9407]: 135.8.118.252
[135.8.118.252]: TrapsysUpTime.0 = Timeticks: (43147723) 4 days,
23:51:17.233
, snmpTrapOID.0 = OID: avRtpQoSClear4
, avRtpQoSFaultTh.0 =
```

```
INTEGER: 15
, avRtpQoS ClearTh.0 = INTEGER: 06
```

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
4	The trap name. Indicates that this is a QoS fault trap or a QoS clear trap.	snmpTrapOID.0 = OID: avRtpQoS Fault	snmpTrapOID.0 = OID: avRtpQoS Clear
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.	avRtpQoS FaultTh.0 = INTEGER: 1	avRtpQoS FaultTh.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.	avRtpQoS ClearTh.0 = INTEGER: 0	avRtpQoS ClearTh.0 = INTEGER: 0

Viewing automatic traceroute results

About this task

The VoIP engine automatically performs UDP traceroutes whenever the RTP statistics application is enabled.

A traceroute is performed per RTP session, 10 seconds after the session begins. A traceroute is not performed if there is another active session to the same destination for which a traceroute was already performed within the last five seconds.

Procedure

Use the **show rtp-stat traceroute** command.

You can filter the results according to subnet address by adding **destination-ip** and specifying the remote subnet address and subnet mask, or by specifying the rtp-statistics session index.

The traceroute results are displayed with the most recent first.

For example:

```
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: 2015-08-23,12:21:55
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: 2015-08-23,13:30:15
```

RTP traceroute results output

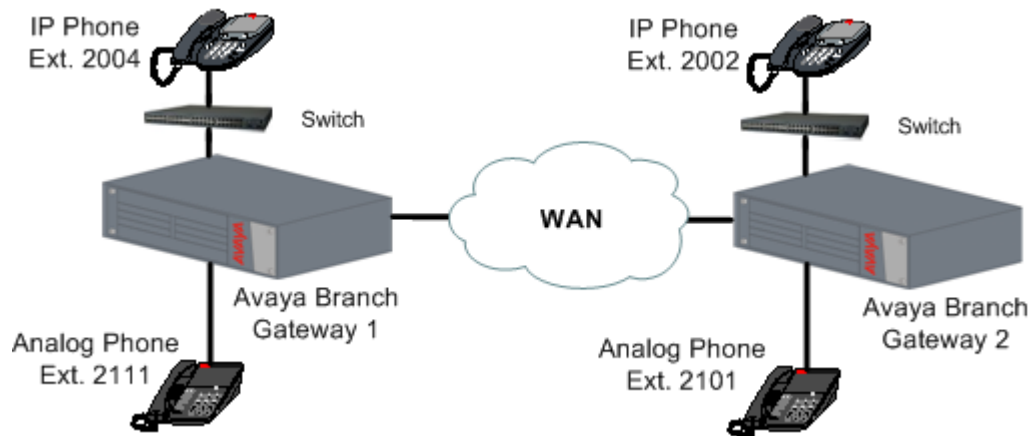
Name	Description
Session ID	The RTP statistics index for the RTP session
From	The IP address of the Branch Gateway
To	The IP address of the session destination (in this case, a destination within the specified subnet)
At	The time the traceroute is performed
TTL	The hop count and TTL field value of probe 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.

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
```



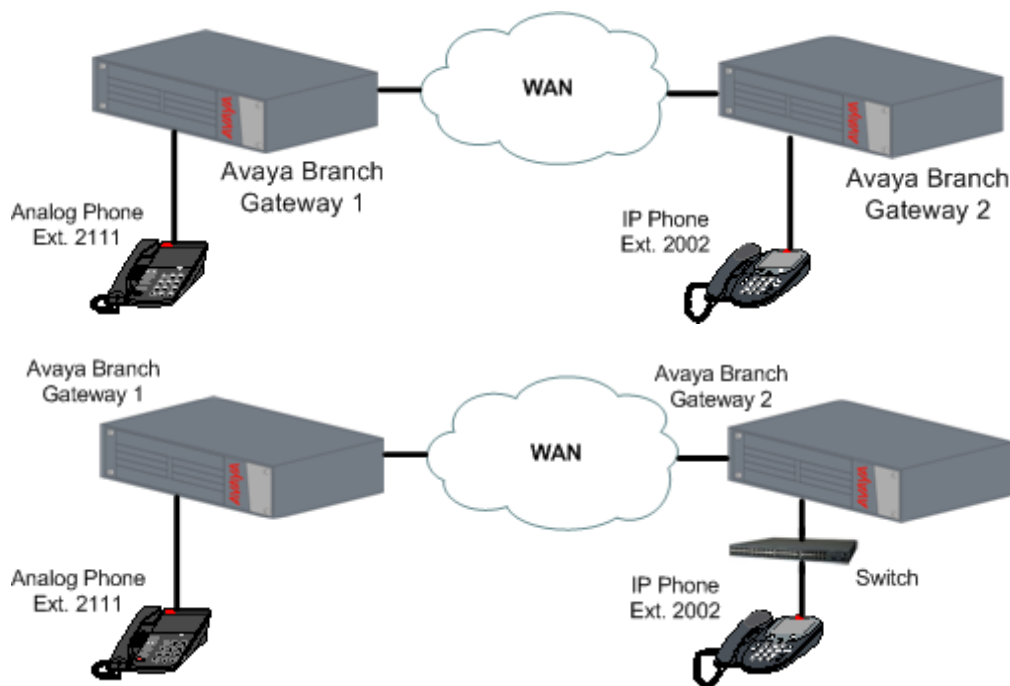
```
Gxxx-001(super)# rtp-stat thresholds rtt 500
Gxxx-001(super)# rtp-stat event-threshold echo-return-loss 0
Gxxx-001(super)# rtp-stat event-threshold loss 1
Gxxx-001(super)# rtp-stat event-threshold remote-loss 0
Gxxx-001(super)# rtp-stat event-threshold jitter 0
Gxxx-001(super)# rtp-stat event-threshold 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
```

Remote calls from analog to IP telephone

At 00:39 on August 23, 2015, an analog phone with an extension 2111 establishes a call with an IP phone with an extension 2002 in the network described in [Four telephones in a sample network](#) on page 351.



You must configure the RTP statistics application as described in [Four telephones in a sample network](#) on page 351. Following complaints related to QoS problems during the call, the administrator performs a check as follows:

```
//to see if the RTP statistics application registered QoS problems for the call:
Gxxx-001 (super)# show rtp sessions
ID      QoS Start date and time End Time Type      Destination
-----
00001   *1
        2015-08-23,00:39:26 00:41:01 G711U      20.20.20.2
//to display more details on the session:
Gxxx-001 (super)# show rtp-stat detailed 1
Session-ID: 1
Status: Terminated, QOS: Faulted2
, EngineId: 0
Start-Time: 2015-08-23,00:39:26, End-Time: 2015-08-23,00:41:01
Duration: 00:01:35
CName: gwp@30.30.30.1
Phone: 199:2111
Local-Address: 30.30.30.1:2329 SSRC 2764463979
Remote-Address: 20.20.20.2:2329 SSRC 1260226 (0)
Samples: 19 (5 sec)
Codec:
G711U 200B 20mS Off, Silence-suppression(Tx/Rx) Disabled/Disabled, Play-Time 63.
916sec, Loss 11.0% #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
```

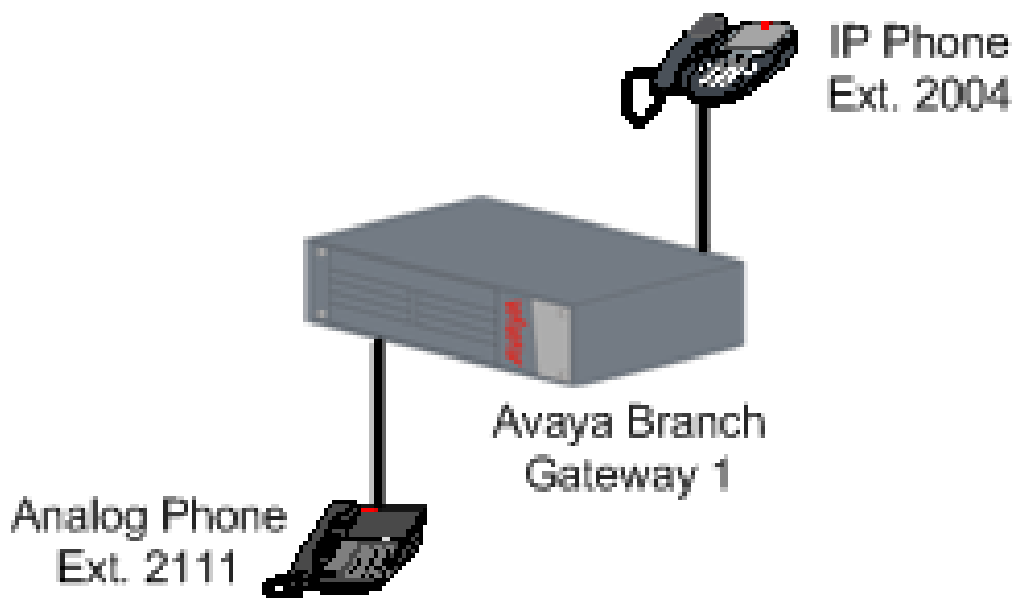
```
, Avg-Loss 8.4%, RTT 124mS #0, Avg-RTT 96mS, Jitter 11
mS #0, Avg-Jitter 9mS, TTL(last/min/max) 63/63/63, Duplicates 0, Seq-Fall 0, DSC
P 46, L2Pri 12, RTCP 9
Transmitted-RTP:
VLAN 1, DSCP 46, L2Pri 6, RTCP 17
Remote-Statistics:
Loss 11.6% #145
, Avg-Loss 8.9%, Jitter 33mS #0, Avg-Jitter 26mS
Echo-Cancellation:
Loss 49dB #0, Len 32mS
RSVP:
Status Disabled, Failures 0
```

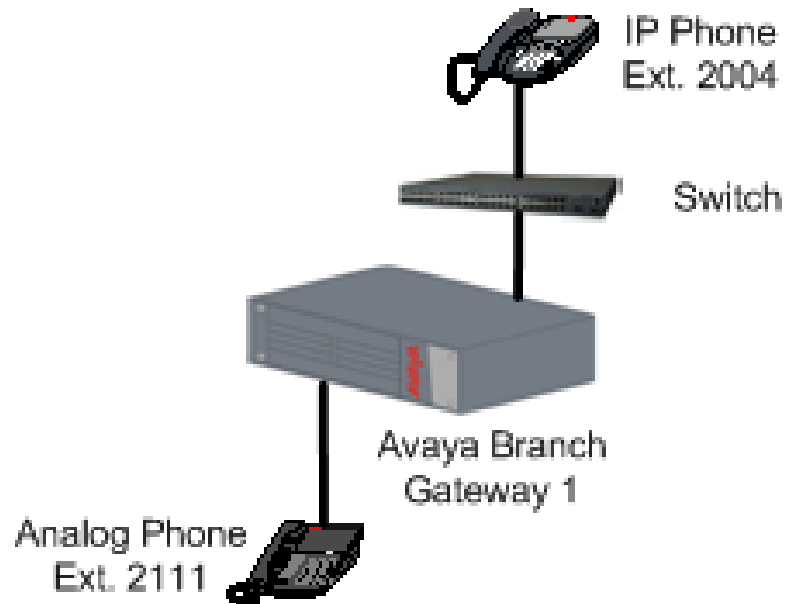
A few points to note:

- The asterisk in the `show rtp sessions` output indicates that session 1 has QoS faults [1]
- The QoS is described as Faulted because of QoS faults [2]
- QoS faults that can be seen in the output are:
 - The codec loss event counter indicates that the codec loss exceeded the threshold 15 times [3]
 - The received-RTP packet loss event counter indicates that packet loss exceeded the threshold nine times [4]
 - The remote packet loss event counter indicates that remote packet loss exceeded the threshold 14 times [5]

Local calls between an IP and an analog telephone

At 00:57, a local call is placed between an IP telephone with an extension 2004 and an analog telephone with an extension 2111 in the network described in [Four telephones in a sample network](#) on page 351. The call ends at 00:59:19.





After the call ends, the administrator uses the CLI to view the QoS statistics:

```

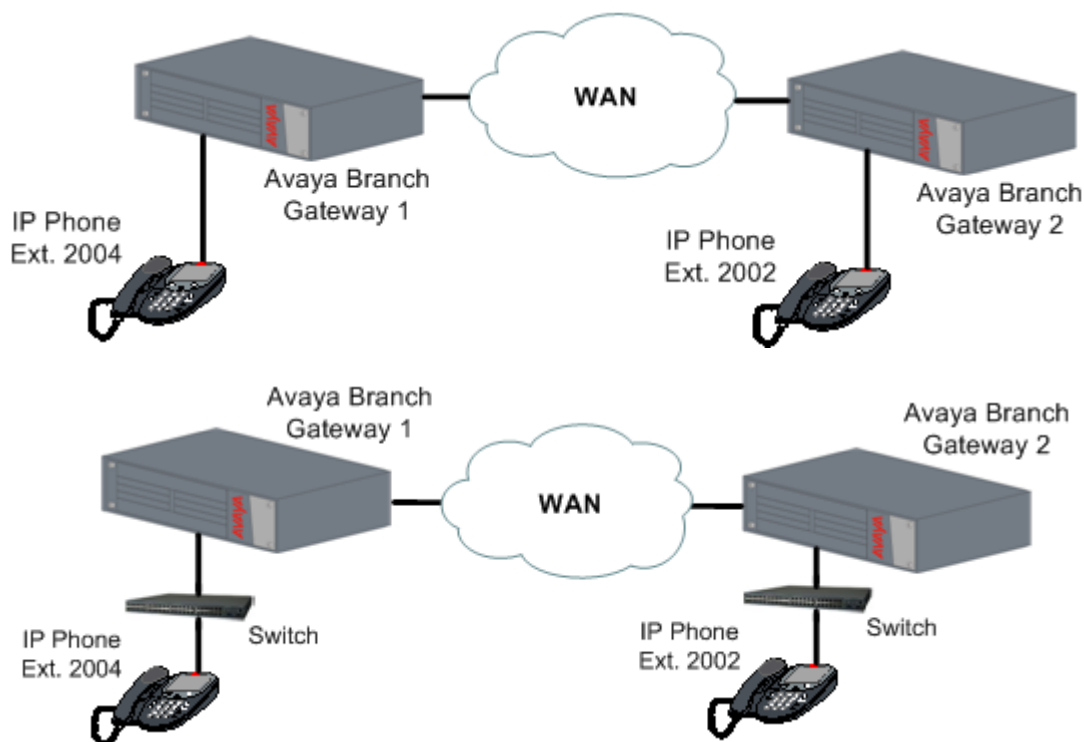
Oct 201
11:10:542
LZ-SIT-SR1 snmptrapd[9407]: 135.8.118.252
[135.8.118.252]: TrapsysUpTime.0 = Timeticks: (43131114) 4 days,
23:48:31.143
, snmpTrapOID.0 = OID: avRtpQoSFault4
, avRtpQoSFaultTh.0 =
INTEGER: 15
, avRtpQoSClearTh.0 = INTEGER: 06
Oct 201
11:13:402
LZ-SIT-SR1 snmptrapd[9407]: 135.8.118.252
[135.8.118.252]: TrapsysUpTime.0 = Timeticks: (43147723) 4 days,
23:51:17.233
, snmpTrapOID.0 = OID: avRtpQoSClear4
, avRtpQoSFaultTh.0 =
INTEGER: 15
, avRtpQoSClearTh.0 = INTEGER: 06
  
```

Points to note:

- The QoS column in the `show rtp sessions` output has no asterisk (*), indicating that no metrics exceeded their event thresholds or average thresholds during the session [1].
- The QoS is described as `Ok` because there were no QoS problems [2]
- All average metric values are below the average thresholds [4] [5] [6] [8] [10] [12] [14] [16]
- All event counters are zero [3] [5] [7] [9] [11] [13] [15] [17]

Remote calls from IP telephone to IP telephone

An IP telephone with an extension 2004 establishes an unshuffled call to another IP telephone with an extension 2002 in the network described in [Four telephones in a sample network](#) on page 351.



The following commands are run after call termination:

```
//to display the RTP sessions:
```

```
Gxxx-001 (super)# show rtp sessions
```

ID	QoS	Start date and time	End Time	Type	Destination
00011		2015-08-23,00:57:13	00:59:19	G711U	30.30.30.2
00012	*	2015-08-23,00:39:26	00:41:01	G711U	20.20.20.2
00013	*	2015-08-23,01:02:45	01:05:15	G711U	20.20.20.2
00014		2015-08-23,01:02:50	01:05:15	G711U	30.30.30.2

Both sessions 13 and 14 are part of the call. The call architecture follows this pattern because an unshuffled call between two IP telephones use two VoIP channels: one channel between each telephone and the Branch GatewayVoIP engine.

Session 13 has QoS problems.

```
//to display details of session 13:
```

```
Gxxx-001 (super)# show rtp-stat detailed 13
```

```
Session-ID: 13
```

```
Status: Terminated, QOS: Faulted, EngineId: 0
```

```
Start-Time: 2015-08-23,01:02:45, End-Time: 2015-08-23,01:05:15
```

```
Duration: 00:02:30
```

```
CName: gwp@30.30.30.1
```

```
Phone: 202:2004
```

```
Local-Address: 30.30.30.1:2329 SSRC 3510756141
```

```
Remote-Address: 20.20.20.2:2329 SSRC 1372162 (0)
```

```
Samples: 30 (5 sec)
```

```
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
```

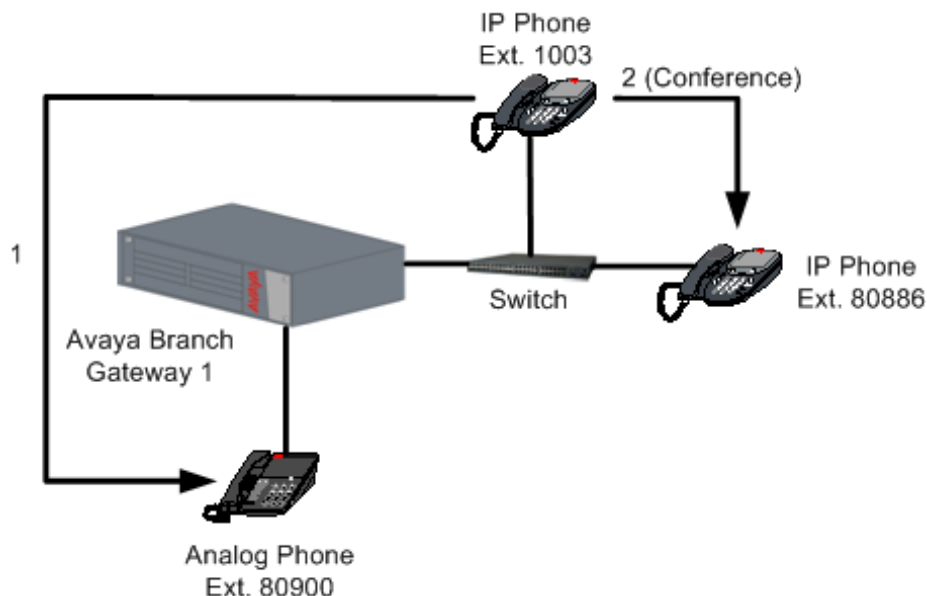
```
#0, Avg-Jitter 6mS, TTL(last/min/max) 63/63/63, Duplicates 0, Seq-Fall 0, DSCP
46, L2Pri 12, RTCP 23
Transmitted-RTP:
VLAN 1, DSCP 46, L2Pri 6, RTCP 27
Remote-Statistics:
Loss 0.4% #17 , Avg-Loss 6.5%, Jitter 3mS #0, Avg-Jitter 22mS
Echo-Cancellation:
Loss 49dB #0, Len 32mS
RSVP:
Status Disabled, 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: 2015-08-23,01:02:50, End-Time: 2015-08-23,01:05:15
Duration: 00:02:25
CName: gwp@30.30.30.1
Phone: 202:2002
Local-Address: 30.30.30.1:2165 SSRC 247950253
Remote-Address: 30.30.30.2:2165 SSRC 120077 (0)
Samples: 29 (5 sec)
Codec:
G711U 200B 20mS Off, Silence-suppression(Tx/Rx) Disabled/Disabled, Play-Time 151
.140sec, Loss 0.0% #0, Avg-Loss 0.0%, RTT 95mS #0, Avg-RTT 106mS, JBuf-under/ove
rruns 0.0%/0.0%, Jbuf-Delay 11mS, Max-Jbuf-Delay 27mS
Received-RTP:
Packets 7556, Loss 0.0% #0, Avg-Loss 0.0%, RTT 0mS #0, Avg-RTT 0mS, Jitter 0mS #
0, Avg-Jitter 0mS, TTL(last/min/max) 64/64/64, Duplicates 0, Seq-Fall 0, DSCP 46
, L2Pri 12, RTCP 31
Transmitted-RTP:
VLAN 1, DSCP 46, L2Pri 6, RTCP 25
--type q to quit or space key to continue--
Remote-Statistics:
Loss 0.0% #0, Avg-Loss 0.0%, Jitter 7mS #0, Avg-Jitter 7mS
Echo-Cancellation:
Loss 49dB #0, Len 32mS
RSVP:
Status Disabled, Failures 0
```

Conference Calls

A conference call is placed between two IP phones with extensions 1003 and 80886, and an analog phone with an extension 80900. The IP phone with extension 1003 connects to the analog phone with an extension 80900. The conference function of the IP phone with an extension 1003 is used to add the IP phone with an extension 80886 to the conference.



During the call, the system runs the following commands:

```
//to display the RTP sessions:
Gxxx-001(super)# show rtp sessions
ID      QoS Start date and time End Time Type           Destination
-----
00001    2015-08-23,09:55:17      -           G729 16.16.16.101
00002    2015-08-23,09:55:20      -           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: 2015-08-23,09:55:17, End-Time: -
Duration: 00:00:48
CName: gwp@33.33.33.33
Phone: 1401
: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: 2015-08-23,09:55:20, End-Time: -
Duration: 00:00:50
CName: gwp@33.33.33.33
Phone: 1402
:80886:1003
Local-Address: 33.33.33.33:61175 SSRC 3702564610
Remote-Address: 149.49.41.50:61175 SSRC 15161893 (0)
Samples: 10 (5 sec)
Codec:
G711U 40B 0mS Off, Silence-suppression(Tx/Rx) Disabled/Disabled, Play-Time 161.9
00sec, Loss 0.0% #0, Avg-Loss 0.0%, RTT 103mS #0, Avg-RTT 105mS, JBuf-under/over
runs 0.0%/0.0%, Jbuf-Delay 11mS, Max-Jbuf-Delay 13mS
Received-RTP:
Packets 8094, Loss 0.0% #0, Avg-Loss 0.0%, RTT 8mS #0, Avg-RTT 9mS, Jitter 0mS #
0, Avg-Jitter 0mS, TTL(last/min/max) 0/64/64, Duplicates 0, Seq-Fall 0, DSCP 0,
L2Pri 6, RTCP 30
Transmitted-RTP:
VLAN 400, DSCP 46, L2Pri 6, RTCP 30
Remote-Statistics:
Loss 0.0% #0, Avg-Loss 0.0%, Jitter 1mS #0, Avg-Jitter 0mS
Echo-Cancellation:
Loss 49dB #0, Len 0mS
RSVP:
Status Reserved, Failures 0

```

For clarity, suggest: The conference ID that appears in the Phone string for session 1 and for session 2 is identical and indicates that the two sessions belong to the same conference call [1] [2].

Summary of RTP statistics commands

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

Command	Description
rtp-stat clear	Reset the RTP statistics application
rtp-stat event-threshold	Set a QoS event-threshold for RTP streams
rtp-stat fault	Configure the RTP statistics application to send QoS fault and/or clear traps
rtp-stat min-stat-win	Set the RTP statistics minimum statistic window
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

Table continues...

Command	Description
<code>show rtp-stat traceroute</code>	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 enables you to analyze packets that pass through the Branch Gateway's interfaces. Packets are captured to a buffer based on the criteria that you specify. You can use the Ethereal or Wireshark analysis tool to upload and analyze the buffer.

The packet sniffing service on the Branch Gateway offers several advantages to the network administrator. The capture file is saved in the libpcap format, which is the industry standard. To read the file, use Tethereal or Tshark software of S8300 and standard versions of Ethereal or Wireshark for Unix, Windows, and Linux (see <http://www.wireshark.org>).

Note:

Ethereal or Wireshark is an open-source application.

In addition, the Branch Gateway's packet sniffing service can capture non-Ethernet packets, such as frame-relay and PPP. Non-Ethernet packets are wrapped in a dummy Ethernet header to enable them to view in a libpcap format. Thus, the Branch Gateway enables you to analyze packets on all the device interfaces.

The Branch Gateway's packet sniffing service gives you full control over the memory usage of the sniffer. You can set a maximum limit for the capture buffer size, configure a circular buffer so that older information is overwritten when the buffer fills up, and specify a maximum number of bytes to capture for each packet.

What can be captured

The Branch Gateway packet sniffing service captures only the packets handled by the Branch Gateway and delivered to the device CPU ("non-promiscuous" mode). This is unlike regular sniffer applications that pick up all traffic on the network.

See [Roadmap for configuring packet sniffing](#) on page 362 for a description of how to configure packet sniffing and analyze the resulting capture file.

Streams that can always be captured

- H.248 registration
- RTP from the Branch Gateway
- ARP on the LAN (broadcast)
- All packets that traverse the WAN
- All traffic to/from the Branch Gateway

Streams that can never be captured

The following streams can never be captured because they are switched by the internal Ethernet switch and not by the CPU:

- H.323 Signaling from an IP phone on the LAN to an ICC on the LAN
- RTP stream between IP phones on the LAN

Streams that can sometimes be captured

If the Branch Gateway is the WAN router of the following streams, they can be captured:

- H.323 Signaling from IP phones on the LAN to an ECC over the WAN
- DHCP when the DHCP server is behind the WAN (using the Branch Gateway DHCP relay capability)
- RTP stream on an IP phone on the LAN to a remote IP phone

Roadmap for configuring packet sniffing

About this task

Packet sniffing configuration consists of the following steps:

Procedure

1. [Enabling packet sniffing](#) on page 362.
2. [Limiting packet sniffing to specific interfaces](#) on page 363 (if necessary).
3. [Applying a capture list](#) on page 369 that specifies which packets to capture.
4. [Rule criteria for a capture list](#) on page 364.
5. [Viewing the capture list](#) on page 369.
6. [Applying a capture list](#) on page 369.
7. [Configuring packet sniffing settings](#) on page 370.
8. [Starting the packet sniffing service](#) on page 371.

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 be enabled by an administrator connecting with a serial cable to the Branch Gateway Console port or the Services port.

2. To disable packet sniffing, enter `no capture-service`.

Limiting packet sniffing to specific interfaces

About this task

By default, the packet sniffing service captures packets and Ethernet frames from all the router's interfaces. You can use the `capture interface` command to limit packet sniffing to a specific interface.

For example, the following command limits packet sniffing to the FastEthernet Interface:

```
Gxxx-001(super)# capture interface fastethernet 10/3
Done!
Gxxx-001(super)#
```

The following command enables packet sniffing on all available interfaces:

```
Gxxx-001(super)# capture interface any
Done!
Gxxx-001(super)#
```

Capture lists

By default, the packet sniffing service captures all packets passing through the interfaces on which it is enabled. Use a capture list to selectively filter the packets that are captured by the service.

A capture list contains an ordered list of rules and actions. A rule specifies criteria against which packets are tested. The action tells the Branch Gateway whether to capture or not capture packets matching the rule criteria. Only packets that match the specified criteria and have an action of `capture` are captured to the capture file. The rules are evaluated one by one, according to their number. If none of the rules match the packet, the default action is executed. You can set the default action as desired. Use the command `ip-rule default` to set the default action.

* Note:

ARP frames are not IP packets and therefore cannot be filtered by capture lists. However, in a healthy network, the ARP frames rate is relatively low.

Configuring capture lists

Procedure

Use the `ip capture-list` command, followed by the list number, to enter the context of a capture list (and to create the capture list if it does not exist).

Capture lists are numbered from 501 to 599.

For example:

```
Gxxx-001(super)# ip capture-list 510
Gxxx-001(super-Capture 510)#
```

Example

You can use the following commands to set the parameters of the capture list:

- Use the `name` command to assign a name to the capture list.

- Use the **owner** command to record the name of the person that created the list.
- Use the **ip-rule** command to define rule criteria for the capture list.

*** Note:**

You can use the **cookie** command to set the list cookie for the capture list. However, capture list cookies are not currently used by any application.

Rule criteria for a capture list

Once in the capture list context, use the **ip-rule** command, followed by a number from 1 to 9999, to define a set of criteria against which to test packets. In addition to the rule criteria, each rule must include a composite operation. The composite operation determines the action the rule takes with respect to packets that match the rule criteria, and can be one of the following:

- capture
- no-capture

Configuring rule criteria for a capture list

Procedure

Use the **composite-operation** command to include a composite operation in a rule for a capture list.

For example, the following commands create a rule (rule 10 in capture list 510) that determines that TCP packets are not captured:

```
Gxxx-001(super)# ip capture-list 510
Gxxx-001(super-Capture 510)# ip-rule 10
Gxxx-001(super-Capture 510/ip rule 10)# composite-operation no-capture
Done!
Gxxx-001(super-Capture 510/ip rule 10)# ip-protocol tcp
Done!
Gxxx-001(super-Capture 510/ip rule 10)#
```

Rule applications

Rules work in the following ways, depending on the type of information in the packet, and the number of criteria in the rule:

- L4 rules with a *Permit* operation are applied to non-initial fragments
- L4 rules with a *Deny* operation are not applied to non-initial fragments, and the device continues checking the next IP rule. This is to prevent cases in which fragments that belong to other L4 sessions may be blocked by the other L4 session which is blocked.
- L3 rules apply to non-initial fragments
- L3 rules that include the fragment criteria do not apply to initial fragments or non-fragment packets
- L3 rules that do not include the fragment criteria apply to initial fragments and non-fragment packets
- L4 rules apply to initial fragments and non-fragment packets

Rule criteria commands

You can use the following rule criteria commands. These commands are described in more detail below.

- **dscp**
- **ip protocol**
- **source ip address**
- **destination ip address**
- **tcp source-port**
- **tcp destination-port**
- **udp source-port**
- **udp destination-port**
- **icmp**
- **fragment**

Note:

You can also use the **description** command in the rule context to add a description of the rule.

Applying rules to packets with DSCP values

Procedure

Use the **dscp** command, followed by a DSCP value (from 0 to 63) to apply the rule to all packets with the specified DSCP value.

For example, the following rule is defined to capture all VoIP Bearer packets (DSCP = 46):

```
Gxxx-001(super)# ip capture-list 520
Gxxx-001(super-Capture 520)# ip-rule 20
Gxxx-001(super-Capture 520/ip rule 20)# composite-operation capture
Done!
Gxxx-001(super-Capture 520/ip rule 20)# dscp 46
Done!
Gxxx-001(super-Capture 520/ip rule 20)#
```

Applying rules to packets with IP protocols

Procedure

1. Use the **ip-protocol** command, followed by the name of an IP protocol, to apply the rule to all packets with the specified IP protocol.
2. If you want the rule to apply to all protocols, use **any** after the command (**ip-protocol any**).

For example, the following rule is defined to capture all TCP packets:

```
Gxxx-001(super)# ip capture-list 520
Gxxx-001(super-Capture 520)# ip-rule 20
Gxxx-001(super-Capture 520/ip rule 20)# composite-operation capture
```

```
Done!
Gxxx-001(super-Capture 520/ip rule 20)# ip-protocol tcp
Done!
Gxxx-001(super-Capture 520/ip rule 20)#
```

3. To apply the rule to all protocols except the specified protocol, use the **no** form of this command.

For example:

```
Gxxx-001(super-Capture 520/ip rule 20)# no ip-protocol tcp
Done!
Gxxx-001(super-Capture 520/ip rule 20)#
```

Applying rules to source or destination IP address

Procedure

1. Use the **source-ip** command to apply the rule to packets from the specified IP address or range of addresses.
2. Use the **destination-ip** command to apply the rule to packets going to the specified IP address or range of addresses.

IP range criteria

Range: Type two IP addresses to set a range of IP addresses to which the rule applies. You can use wildcards in setting the range. For example:

```
Gxxx-001(super-Capture 520/ip rule 20)# source-ip 135.64.102.0 0.0.255.255
Done!
Gxxx-001(super-Capture 520/ip rule 20)#
```

Single address: Type **host**, by an IP address, to set a single IP address to which the rule applies. For example:

```
Gxxx-001(super-Capture 520/ip rule 20)# destination-ip host 135.64.104.102
Done!
Gxxx-001(super-Capture 520/ip rule 20)#
```

Wildcard: Type **host**, followed by an IP address using wildcards, to set a range of IP addresses to which the rule applies. For example:

```
Gxxx-001(super-Capture 520/ip rule 20)# source-ip host 135.0.0.0
Done!
Gxxx-001(super-Capture 520/ip rule 20)#
```

Any: Type **any** to apply the rule to all IP addresses. For example:

```
Gxxx-001(super-Capture 520/ip rule 20)# destination-ip any
Done!
Gxxx-001(super-Capture 520/ip rule 20)#
```

To apply the rule to all source or destination IP addresses except the specified address or range of addresses, use the **not** form of the applicable command. For example:

```
Gxxx-001(super-Capture 520/ip rule 20)# not destination-ip 135.64.102.0 0.0.255.255
Done!
Gxxx-001(super-Capture 520/ip rule 20)#
```

Commands used to specify a range of source and destination ports

To specify a range of source and destination ports to which the rule applies, use the following commands, followed by either port name or port number range criteria:

- **tcp source-port**. The rule applies to TCP packets from ports that match the defined criteria
- **tcp destination-port**. The rule applies to TCP packets to ports that match the defined criteria
- **udp source-port**. The rule applies to UDP packets from ports that match the defined criteria
- **udp destination-port**. The rule applies to UDP packets to ports that match the defined criteria

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

Port name or number range criteria

The port name or number range criteria can be any of the following:

Range: Type **range**, followed by two port numbers, to set a range of port numbers to which the rule applies. For example:

```
Gxxx-001(super-Capture 520/ip rule 20)# tcp destination-port range 1 3
Done!
Gxxx-001(super-Capture 520/ip rule 20)#
```

Equal: Type **eq**, followed by a port name or number, to set a port name or port number to which the rule applies. For example:

```
Gxxx-001(super-Capture 520/ip rule 20)# tcp source-port eq ftp
Done!
Gxxx-001(super-Capture 520/ip rule 20)#
```

Greater than: Type **gt**, followed by a port name or port number, to apply the rule to all ports with a name or number greater than the specified name or number. For example:

```
Gxxx-001(super-Capture 520/ip rule 20)# udp destination-port gt 10
Done!
Gxxx-001(super-Capture 520/ip rule 20)#
```

Less than: Type **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 "telnet" (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 "telnet" (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 KB. 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 command is useful, since in most cases, the packet headers contain the relevant information. Available values are 14 to 4096. The default value is 128 bytes.

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 command is valuable since it is the packets headers that contain the interesting information.
- Use capture lists to select specific traffic.

Starting the packet sniffing service

About this task

Use this procedure to enable the packet sniffing service.

You must apply a capture list using the **capture filter-group** command in order for the capture list to be active. If you do not use the **capture filter-group** command, the packet sniffing service captures all packets.

*** Note:**

The capture start command resets the buffer before starting the sniffer.

Procedure

Once you have defined and applied the packet capture lists, use the **capture start** command in general context to instruct the packet sniffing service to start capturing packets.

Result

If packet sniffing has been enabled by the administrator, the following appears:

```
Gxxx-001(super)# capture start
Starting the packet sniffing process
Gxxx-001(super)#
```

If packet sniffing has not been enabled by the administrator, the following appears:

```
Gxxx-001(super)# capture start
Capture service is disable
To enable, use the `capture-service` command in supervisor mode.
Gxxx-001(super)#
```

Decrypted IPsec VPN packets

IPsec VPN packets are encrypted packets. The contents of encrypted packets cannot be viewed when captured. However, you can use the **capture ipsec** command to specify that IPsec VPN packets, handled by the internal VPN Branch Gateway process, should be captured in plain text format.

Analyzing captured packets

Procedure

Analyze the captured packets by stopping the packet sniffing service, uploading the capture file, and analyzing the capture file.

Stopping the packet sniffing service

Procedure

Enter **capture stop** to stop the packet sniffing service.

Stop the service in order to upload a capture file.

* Note:

The **capture stop** command is not saved in the startup configuration file.

Viewing packet sniffing information

Procedure

1. You can enter **show capture** to view information about the packet sniffing configuration and the capture state.

For example:

```
Gxxx-001> show capture
Capture service is enabled and inactive
Capture start time 23/08/2015-13:57:40
Capture stop time 23/08/2015-13:58:23
Current buffer size is 1024 KB
Buffer mode is cyclic
Maximum number of bytes captured from each frame: 1515
Capture list 527 on interface "FastEthernet 10/3"
Number of captured frames in file: 3596 (out of 3596 total captured frames)
Size of capture file: 266 KB (26.6 %)
```

* Note:

The number of captured frames can be larger than the number of the frames in the buffer because the capture file may be in cyclic mode.

2. You can use the **show capture-buffer hex** command to view a hex dump of the captured packets.

However, for a proper analysis of the captured packets, you should upload the capture file and analyze it using a sniffer application, as described in the following sections.

Example

The following is an example of the **show capture-buffer hex** command:

```
Gxxx-001> show capture-buffer hex
Frame number: 1
Time relative to first frame (D H:M:S:Micro-S): 0, 0:0:0.0
Packet time: 14/01/1970-13:24:55.583598
Frame length: 60 bytes
Capture Length: 60 bytes
00000000:ffff ffff ffff 0040 0da9 4201 0806 0001      .....@..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.

Uploading the capture file to a remote server or USB mass storage device

Procedure

Use one of the following commands to upload the capture file:

- **copy capture-file ftp**
- **copy capture-file tftp**
- **copy capture-file scp**
- **copy capture-file usb**
- **copy capture-file https**
- **copyedge capture-file scp**

Result

Note:

The use of the **copy capture-file scp** command is limited to uploading files of 1 MB or less.

For example:

```
Gxxx-001(super)# copy capture-file ftp myCature.cap 135.64.103.66
This command will stop the capture if capturing is started
Confirmation - do you want to continue (Y/N)? y
Username: xxxx
Password: xxxx
Beginning upload operation ...
This operation may take up to 20 seconds.
Please refrain from any other operation during this time.
For more information , use 'show upload status 10' command
Gxxx-001(super)#
```

Uploading the capture file to an S8300 Server

Procedure

1. As root update `/etc/ssh/sshd_config` changing to: **PasswordAuthentication yes**.
2. As root update `/etc/ecs.conf` changing to: **CustomSSHFiles enabled**.
3. As root run the **systemctl restart sshd**.
4. Log on to Branch Gateway.
5. Use the **copy capture file scp** command to upload the capture file.

For example:

```
Gxxx-001(super)# copy capture-file scp capfile.cap 149.49.43.96
```

6. At the SCP login prompt, enter a valid S8300 user (not a service user).
7. At the SCP password prompt, enter the user password.
8. 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 : 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, Wireshark and Tshark.

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.wireshark.com>.

*** Note:**

Ethereal enables you to create filter expressions to filter the packets in the capture file and display required 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 375.

Interface identification

The Branch Gateway's packet sniffing service can capture also non-Ethernet packets, such as frame-relay and PPP, into the capture file. This is achieved by wrapping non-Ethernet packets in a dummy Ethernet header to allow the packets to be stored in a libpcap format. This enables you to analyze packets on all the device interfaces.

The dummy Ethernet headers are allocated according to the original packet type. Dummy Ethernet headers start with 00:00. Therefore, if the source or destination address of a packet you are viewing in Ethereal starts with 00:00, this indicates the packet is a non-Ethernet packet.

The dummy Ethernet header is identified by special MAC addresses. Packets sent from a non-Ethernet interface are identified with an SA address in the format 00:01:00:00:xx and a DA address which holds the interface index. Packets received over a non-Ethernet interface are identified with DA address in the format 00:01:00:00:xx and an SA address which holds the interface index. The **show capture-dummy-headers** command displays the dummy header addresses and their meaning according to the current configuration.

*** Note:**

Ethernet packets received on a VLAN interface are identified by their VLAN tag. However, decrypted IPsec packets received on a VLAN interface are stored with a dummy header.

```
Gxxx-001> show capture-dummy-headers
      MAC                Description
-----
00:00:01:00:00:00      Src/dst address of Packet to/from frame-relay or PPP
00:00:01:00:00:01      Decrypted IPsec packet
00:00:0a:00:0a:02      interface fastethernet 10/3
00:00:0c:a0:b0:01      interface vlan 1
00:00:21:20:10:01      interface serial 3/1:1
00:00:21:40:10:02      interface serial 4/1:2
00:00:31:00:00:01      interface dialer 1
```

About simulating packets

Capture lists support the IP simulate command. Refer to [Simulating packets](#) on page 522.

Summary of packet sniffing commands

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

Root level command	First level command	Second level command	Description
<code>capture buffer-mode</code>			Set the capture buffer to cyclic mode
<code>capture buffer-size</code>			Change the size of the capture file
<code>capture filter-group</code>			Activate a capture list
<code>capture interface</code>			Specify a capture interface (by default, the service captures from all interfaces simultaneously)
<code>capture ipsec</code>			Set whether to capture IPSec VPN packets, handled by the internal VPN process, decrypted (plaintext) or encrypted (cyphertext)
<code>capture max-frame-size</code>			Set the maximum octets that are captured from each frame
<code>capture start</code>			Start capturing packets
<code>capture stop</code>			Stop capturing packets
<code>capture-service</code>			Enable or disable the capture service
<code>clear capture-buffer</code>			Clear the capture buffer (useful in case it holds sensitive information)
<code>copy capture-file ftp</code>			Upload the packet sniffing buffer to a file on a remote FTP server
<code>copy capture-file scp</code>			Upload the packet sniffing buffer to a file on a remote SCP server
<code>copy capture-file tftp</code>			Upload the packet sniffing buffer to a file on a remote TFTP server
<code>copy capture-file usb</code>			Upload the capture file to a USB mass storage device
<code>copy capture-file https</code>			Upload the packet sniffing buffer to a file on a remote HTTP server
<code>copyedge capture-file scp</code>			Upload the packet sniffing buffer to a file on a remote SCP server via Avaya SBC tunnel
<code>ip capture-list</code>			Enter the capture list configuration context, create a capture list, or delete a capture list

Table continues...

Root level command	First level command	Second level command	Description
	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
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 258.

For example, if an interface is enabled but normal keepalive packets are failing, show interfaces displays:

```
FastEthernet 10/3 is up, line protocol is down
```

However, if normal keepalive reports that the connection is up but ICMP keepalive fails, the following is displayed:

```
FastEthernet 10/3 is up, line protocol is down (no KeepAlive)
```

Reporting of interface status

Port status	Keepalive status	Show interfaces output	Administrative state	Operational state	Extended operational state
Up	No Keepalive	FastEthernet 10/3 is up, line protocol is up	Up	Up	Up
Up	Keepalive Up	FastEthernet 10/3 is up, line protocol is up	Up	Up	Up
Up	Keepalive down	FastEthernet 10/3 is up, line protocol is down (no keepalive)	Up	Up	KeepAlive-Down
Down	N/A	FastEthernet 10/3 is up, line protocol is down	Up	Down	FaultDown
Standby	N/A	FastEthernet 10/3 is in standby mode, line protocol is down	Up	Dormant	DormantDown
Shutdown	N/A	FastEthernet 10/3 is administratively down, line protocol is down	Down	Down	AdminDown

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

Summary of interface status commands

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

Command	Description
show interfaces	Display interface information

Echo cancellation

Echo canceller control is intended to improve voice quality on a call by call basis.

The Branch Gateway has multiple echo cancellers of various capabilities. For best echo cancellation performance, the general rule is to enable only one echo canceller in any direction -- the one with the greater capacity in terms of echo tail control in the steady state. Tandeming echo cancellers in the same direction in a media path results in poorer performance in terms of echo control, double-talk performance, noise, etc. In addition, if a smaller tail echo canceller is in the echo path of a longer tail canceller, audible echo can result when echo exists partly in one canceler's window and partly in the other.

For cases where there is no echo to cancel, it is usually best to disable any echo canceller in the path. Echo cancellers are not totally transparent and sometimes introduce undesirable artifacts.

However, the best echo cancellation policy varies depending on each specific call configuration. The Branch Gateway has an internal table for determining which VoIP engine and analog card echo cancellers to enable on a case-by-case basis. This table is consulted when the default auto mode is specified in the echo cancellation CLI commands. The CLI commands also offer the option of overriding the default automatic mode, but those alternative modes are intended for debugging and diagnostics purposes only.

 Note:

DS1 echo cancellation can only be administered via the CM SAT, and these settings are always honored by the Branch Gateway. Therefore, the Branch Gateway CLI controls only the operation of the VoIP engine and analog trunk/line echo cancellers in relation to the DS1 echo canceller and between themselves.

Summary of echo cancellation commands

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

Command	Description
<code>set echo-cancellation analog</code>	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.
<code>set echo-cancellation config analog</code>	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.

Table continues...

Command	Description
<code>set echo-cancellation config voip</code>	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.
<code>set echo-cancellation voip</code>	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.
<code>show echo-cancellation</code>	Display echo cancellation settings and configuration information

Integrated analog testing – Test and Heal

The analog trunk ports of the Branch Gateway are designed to meet certain standards. However, loop characteristics such as signal loss, noise, and crosstalk can cause deviation from those standards.

External testing of the loop typically involves removing the line from the Branch Gateway and connecting it to measurement equipment, dialing into the Local Exchange Carrier's test facility, and taking measurements locally. Alternatively, a technician can dial into a remote location that terminates in additional measurement equipment.

The Branch Gateway's integrated analog testing feature provides a simpler procedure in which the necessary testing is integrated into the Branch Gateway's analog ports, and the Branch Gateway plays the role of the measurement equipment. Using CLI commands, you can:

- Dial out on a specific trunk port to measure noise, receive-loss, crosstalk, trans-hybrid loss, or hybrid balance match
- Display the results of the measurements
- Take corrective action by manually setting a port's balance, receive-gain, or transmit-gain

The integrated analog testing feature enables quick and accurate testing of the loops at installation, and custom modifications to the analog ports that require correction for the actual loop characteristics. After installation, you can run additional tests whenever needed and correct each port that requires tuning.

Hardware support for integrated analog testing

- The MM711 hardware vintage 30 and above
- The MM714 hardware vintage 10 and above, and the MM716

For detailed information about accepted values and recommended corrections, see *Analog Test and Heal User Guide*.

Types of tests

Tests typically make a series of measurements in frequencies between 100Hz and 3400Hz in 100Hz increments. You can run the following tests:

Noise test: Noise is the measure of unwanted signals in the transmission path. After the call is established and while the far end is silent, the Branch Gateway collects the noise level.

Receive-loss test: After the call is established and while the tone (or tones) specific to the responder sequence is being received, the Branch Gateway collects the signal level at the reference frequency and compares it with the reference level. The difference in decibel between the level sent and the level received is the loss.

Crosstalk test: While the analog port under test is in a call and both ends of the call are silent, the crosstalk port establishes another call and plays a sequence of tones. The Branch Gateway collects during that time the tone level for different frequencies on the port under test.

Balance test: This test measures trans-hybrid loss. After the call is established and while the far end is silent, the Branch Gateway transmits a tone and measures the reflected signal level. The transmitted tone level minus the reflected tone level is the trans-hybrid loss at that frequency.

Match test: This test matches hybrid balance. Stored in the integrated analog testing firmware is a group of hybrid balance coefficient sets. Each entry in the group balances the hybrid against a different loop impedance. The match test executes a balance test for each set of coefficients and determines which set best matches the loop.

Types of test lines

The measurements performed by the analog trunk ports in the Branch Gateway are based on some of the more common Centralized Automatic Reporting On Trunks (CAROT) test lines: Test 100, Test 102, and Test 105.

- The Test 100 line answers an incoming call, sends a 1004 Hz tone at 0 dBm for 5.5 seconds, and then remains quiet until it is disconnected.
- The Test 102 line answers an incoming call, sends a 1004 Hz tone at 0 dBm for 9 seconds, and then remains quiet for 1 second. The line repeats the 1004Hz/quiet sequence until disconnected.
- The Test 105 line answers an incoming call, then:
 - Sends a 1004 Hz tone at -16 dBm for 9 seconds
 - Remains quiet for 1 second
 - Sends a 404 Hz tone at -16 dBm for 9 seconds
 - Remains quiet for 1 second
 - Sends a 2804 Hz tone at -16 dBm for 9 seconds
 - Remains quiet for 30 second
 - Sends a 2225 Hz tone (progress tone) at -16 dBm for half a second

- Forces disconnect

Setting up a test profile

About this task

A test profile is a set of definitions for running a particular test. In essence, it specifies what measurements to run on which port. Once you set up a test profile, you can run it whenever necessary using the single **launch** command. You can define up to 30 profiles.

Procedure

1. Enter **analog-test** to enter the analog-test context.
2. Use the **profile** command to enter the analog-test-profile context, for configuring a specific test profile.
3. In the analog-test-profile context, setup the test profile:
 - Use the **set type** command to specify what type of test to run, that is, what type of measurements to run.
 - Use the **set port** command to specify which port to test. Note that only analog trunk ports are accepted.
 - Use the **set destination** command to set the Local Exchange Carrier (LEC) number destination of the measurement call. This number is called by the port being tested.

Note:

If you enter **set destination none**, the port does not attempt to make a call toward any destination but makes the measurement on the current call. The test is performed while the port is in use. Remember to start the call before launching the test.

4. Use the **set responder** command to specify a responder port.

A responder is an analog trunk port that answers an incoming call and then plays a sequence of tones. The analog media module or the LEC collect the measurements while the responder plays its specific sequence. The responder can be a port in the media module, or the Local Exchange Carrier (LEC).

5. Use the **set responder-type** command to specify the responder type.

The different types send different sequences of tones, as explained in [Types of test lines](#) on page 381.

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 fails if the port specified for the test is in use for a call, unless you specify `set destination none` for this test profile.

Procedure

1. Enter `analog-test` to enter the `analog-test` context.
2. Use the `launch` command to launch a specific test.

The port specified in the test profile must be busied out from CM before the test is launched.

As soon as `launch` is issued, the results of previous measurements on the port are cleared.

3. **(Optional)** To abort a currently running analog test, use the `cancel` command.

Displaying test results

Procedure

Use any of the following commands to display test results:

- In the analog-test context, use the **show result** command to display the result of the latest measurements performed for a particular profile.
- In the analog-test-profile context, use the **show result** command to display the results of the latest measurements performed by the test profile.

Result

If a test did not succeed, the output indicates the reason for the test failure.

Healing trunks

About this task

You can manually tune three parameters on each analog trunk port: balance, receive-gain, and transmit gain.

Procedure

1. Enter **analog-test** to enter the analog-test context.
2. Correct the balance, receive-gain, or transmit-gain of a port using the following commands:
 - Use the **set balance** command to set the balance on a specific port.
 - Use the **set receive-gain** command to set the receive-gain on a specific port.
 - Use the **set transmit-gain** command to set the transmit-gain on a specific port.

Displaying corrections

About this task

After correcting the balance, receive-gain or transmit-gain, you can view the corrections applied to each port.

Procedure

1. Enter **analog-test** to enter the analog-test context.
2. Use the **show correction** command to display the balance, receive-gain, and transmit-gain corrections applied to each port.

Summary of integrated analog testing commands

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

Root Level Commands	First level command	Second level command	Description
analog-test			Enter the analog-test context
	cancel		Abort an analog test if it is already running
	clear profile		Delete a test profile
	launch		Launch a specific test
	profile		Enter the analog-test-profile context to setup or edit a test profile
		set crosstalk-destination	Set the Local Exchange Carrier number destination of the call from the crosstalk port
		set crosstalk-port	Specify the crosstalk port
		set crosstalk-responder	Specify the responder port for the crosstalk port
		set destination	Set the Local Exchange Carrier number destination of the measurement call
		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

Table continues...

Root Level Commands	First level command	Second level command	Description
	<code>show result</code>		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
	<code>copy scp root-ca sla</code>		Copy and install a trusted CA certificate to be used for the TLS connection to the SLA server.
	<code>copy usb root-ca sla</code>		Copy and install a trusted CA certificate to be used for the TLS connection to the SLA server.
	<code>set sla-monitor</code>		Enables or disables the SLA Monitor Agent.
	<code>show root-ca sla</code>		Display the trusted CA certificates to be used for the SLA TLS connection.
	<code>show sla-monitor</code>		Displays the state of the SLA Monitor Agent for example, enabled or disabled. The command also displays all gateway parameters pertaining to the SLA Monitor Agent.

Chapter 20: Router

The Branch Gateway has an internal router. You can configure the following routing features on the router:

 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 393 for an explanation of the priority considerations employed by the Branch Gateway to determine the next hop source.

Enabling and disabling the router

Procedure

1. Use the `ip routing` command to enable the router.

2. Use the `no ip routing` command to disable the router.

Interface configuration

You can use the CLI to configure interfaces on the router.

Router interface concepts

The router in the Branch Gateway includes the following interface categories:

- Physical
- Layer 2 virtual
- Layer 3 routing

Physical router interfaces

The physical interfaces of the Branch Gateway router include:

WAN Interfaces: When you add a WAN media module to the Branch Gateway, the media module provides a WAN interface. You can add one of the following types of WAN media modules:

- The Avaya MM340 media module provides an E1/T1 WAN interface
- The Avaya MM342 media module provides a USP WAN interface

FastEthernet Interface: The 10/3 and 10/4 Fast Ethernet ports on the front panel of the Branch Gateway provide a FastEthernet interface. This interface is an autosensing 10/100 Mbps Fast Ethernet port. It can be used to connect to a LAN, an external firewall, an external Virtual Private Network (VPN), or a DeMilitarized Zone (DMZ). This interface can also be used as a WAN interface when configured for PPPoE. For more information, see [Configuring PPPoE](#) on page 232.

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 398.

Layer 2 logical interfaces

VLAN (on the Switching Interface): The Branch Gateway switch can have multiple VLANs defined within its switching fabric. The Branch Gateway router supports up to 64 VLANs that can be configured over their internal switching interface connections.

Serial Interface: The Serial interface is a virtual interface that is created over a portion of an E1/T1 or USP port. Serial interfaces support PPP and frame relay encapsulation protocols. For more information about configuring Serial interfaces for a WAN, see [Configuring the initial WAN](#) on page 222.

Dialer Interface: The Dialer interface is used for the modem dial-backup feature. Refer to [Modem dial backup](#) on page 241.

* Note:

One or more IP interfaces can be defined over each Serial, FastEthernet, switching, and Loopback interface.

Configuring an IP interface

Procedure

1. To create an interface, enter **interface** followed by the type of interface you want to create.

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

For example:

```
interface vlan 1
interface serial 3/1
interface fastethernet 10/2
```

2. Enter **ip address**, followed by an IP address and subnet mask, to assign an IP address to the interface.

Use the **no** form of this command to delete the IP interface.

Interface configuration examples

Use the following commands to configure the fixed router port with IP address 10.20.30.40 and subnet mask 255.255.0.0:

```
Gxxx-001# interface fastethernet 10/3
Gxxx-001(if:FastEthernet 10/3)# ip address 10.20.30.40 255.255.0.0
Done!
```

Use the following commands to create VLAN 2 on the switching interface and configure it with IP address 10.30.50.70 and subnet mask 255.255.0.0:

```
Gxxx-001# interface Vlan 2
Gxxx-001(if:Vlan 2)# ip address 10.30.50.70 255.255.0.0
Done!
```

Summary of basic interface configuration commands

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

Root level command	Command	Description
interface console		Enter the Console interface configuration context, create the interface if it does not exist, or delete the Console interface
	ip address	Assign an IP address and mask to an interface or delete an interface
interface dialer		Enter the Dialer interface context, create the Dialer interface if it does not exist, or delete the Dialer interface
	ip address	Assign an IP address and mask to an interface or delete an interface
	ip admin-state	Set the administrative state of an IP interface
	ip broadcast-address	Update the interface broadcast address
interface fastethernet		Enter FastEthernet interface configuration context, create a FastEthernet interface if it does not exist, or delete a FastEthernet interface
	ip address	Assign an IP address and mask to an interface or delete an interface
	ip admin-state	Set the administrative state of an IP interface
	ip broadcast-address	Update the interface broadcast address
interface loopback		Enter loopback interface configuration context, create a Loopback interface if it does not exist, or delete a Loopback interface or sub-interface
	ip address	Assign an IP address and mask to an interface or delete an interface
	ip admin-state	Set the administrative state of an IP interface
interface serial		Enter Serial interface or sub-interface configuration context, create a serial interface if it does not exist, or delete a serial interface or sub-interface
	ip address	Assign an IP address and mask to an interface or delete an interface

Table continues...

Root level command	Command	Description
	<code>ip admin-state</code>	Set the administrative state of an IP interface
	<code>ip broadcast-address</code>	Update the interface broadcast address
<code>interface tunnel</code>		Enter tunnel interface configuration context, create a tunnel interface if it does not exist, or delete a tunnel interface or sub-interface
	<code>ip address</code>	Assign an IP address and mask to an interface or delete an interface
	<code>ip admin-state</code>	Set the administrative state of an IP interface
<code>interface usb-modem</code>		Enter the USB-modem interface configuration context, reset the USB-modem interface settings to their factory defaults
	<code>ip address</code>	Assign an IP address and mask to an interface or delete an interface
<code>interface vlan</code>		Enter VLAN interface configuration context, create a VLAN interface if it does not exist, or delete a VLAN interface
	<code>ip address</code>	Assign an IP address and mask to an interface or delete an interface
	<code>ip admin-state</code>	Set the administrative state of an IP interface
	<code>ip broadcast-address</code>	Update the interface broadcast address
<code>show ip interface brief</code>		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 241. Modem dial-backup is a feature that sets up a backup dialing destination for a Branch Gateway. Modem dial-backup requires unnumbered IP to be configured on the Dialer interface of the Branch Gateway and at both the default and the backup dialing destinations.

Related links

[Modem dial backup](#) on page 241

Unnumbered IP on an interface configuration

To configure unnumbered IP on an interface, you must specify the interface from which to borrow the IP address. The borrowed interface must already exist and have an IP address configured on it.

The status of an unnumbered IP interface is down whenever the borrowed interface is down. Therefore, it is recommended to borrow the IP address from an interface that is always up, such as the Loopback interface.

Routes discovered on an unnumbered interface by the RIP and OSPF routing protocols are displayed as `via routes` in the routing table. The next hop is listed as `via` the IP unnumbered interface instead of the source address of the routing update.

Configuring IP on an interface configuration

Procedure

1. Decide which interface from which to borrow the IP address.
If necessary, configure the interface. You can use the `show interfaces` command to display existing interface configuration.
2. Enter the context of the interface on which you want to configure an unnumbered IP address (usually the Dialer interface).
3. Use the `ip unnumbered` command, specifying the interface from which to borrow the IP address.

Unnumbered IP examples

In the following example, a VLAN interface is configured, and then the Dialer interface is configured with an unnumbered IP address, borrowing the IP address from the VLAN interface.

```
//enter the context of vlan interface 1:
Gxxx-001(super)# interface Vlan 1
//to configure the IP address of the vlan interface:
Gxxx-001(super-if:Vlan 1)# ip address 180.0.0.1 255.255.255.0
Gxxx-001(super-if:Vlan 1)# exit
Gxxx-001# !
//enter the context of the Dialer interface:
Gxxx-001(super)# interface dialer 1
Gxxx-001(super-if:Dialer 1)# dialer string 1 3001
Gxxx-001(super-if:Dialer 1)# dialer persistent delay 1
Gxxx-001(super-if:Dialer 1)# dialer modem-interface USB-modem
//to configure IP unnumbered on the Dialer interface, borrowing the IP address from
vlan interface 1, configured above:
Gxxx-001(super-if:Dialer 1)# ip unnumbered 1 Vlan 1
Gxxx-001(super-if:Dialer 1)# exit
Gxxx-001(super)# !
```

The following sample routing table shows how routes discovered on unnumbered interfaces by routing protocols are listed as `via routes` in the Next-Hop column:

Network	Mask	Interface	Next-Hop	Cost	TTL	Source
-----	-----	-----	-----	-----	-----	-----
0.0.0.0	0	FastEth10/3	149.49.54.1	1	n/a	STAT-HI
2.2.2.0	24	Vlan15	2.2.2.1	1	n/a	LOCAL
10.0.0.0	8	Vlan1	0.0.0.40	1	n/a	LOCAL
3.0.0.0	8	Tunnel1	Via Dia.1	2	172	RIP
4.0.0.0	8	Tunnel 1	Via Dia.1	2	172	RIP
20.0.0.0	8	Tunnel 1	Via Dia.1	11112	n/a	OSPF
20.0.0.1	32	Tunnel 1	Via Dia.1	22222	n/a	OSPF
26.0.0.0	8	Vlan 15	2.2.2.2	3	n/a	STAT-LO
31.0.0.0	8	Serial 3/1:1.1	31.0.0.1	1	n/a	LOCAL
32.0.0.0	8	Serial 3/1:1.2	32.0.0.1	1	n/a	LOCAL
33.0.0.0	8	Serial 3/1:1.3	33.0.0.1	1	n/a	LOCAL
99.0.0.0	8	Vlan 99	99.1.1.1	1	n/a	LOCAL
135.64.0.0	16	FastEth 10/3	149.49.54.1	1	n/a	STAT-HI
138.0.0.0	8	Serial 3/1:1.1	Via Ser.3/1:1.1	2	n/a	STAT-LO
139.0.0.0	8	Serial 3/1:1.1	Via Ser.3/1:1.1	1	n/a	STAT-LO
149.49.54.0	24	FastEth 10/3	149.49.54.112	1	n/a	LOCAL
180.0.0.0	8	Loopback 1	180.0.0.1	1	n/a	LOCAL

Summary of unnumbered IP interface configuration commands

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

Root level command	Command	Description
interface (dialer fastethernet serial tunnel)		Enter the Dialer , FastEthernet , Serial , or Tunnel interface context
	ip unnumbered	Configure an interface to borrow an IP address from another interface or remove an unnumbered IP configuration from an interface

Routing sources

The Branch Gateway router supports both static and dynamic routing per interface. You can configure static routes with two levels of priority, high and low, and you can enable and configure Open Shortest Path First (OSPF) and Routing Information Protocol (RIP) dynamic routing protocols. Additionally, when DHCP client is configured on an interface, you can configure DHCP client to request a default router address from the DHCP server (DHCP option 3).

The actual source from which the router learns the next hop for any given interface is determined as follows: The router seeks the best match to a packet's destination IP address from all enabled routing sources. If there is no best match, the next hop source is determined according to the following priority order:

1. High priority static route (highest)

If a high priority static route is configured on the interface, this route overrides all other sources.

2. OSPF

If no high priority static route is configured on the interface, but OSPF is enabled, then OSPF determines the next hop.

3. RIP

If no high priority static router is configured on a given interface, and OSPF is not enabled, but RIP is enabled, RIP determines the next hop.

4. EXT OSPF

5. DHCP

If no high priority static router is configured on a given interface, and neither OSPF nor RIP are enabled, and DHCP client is configured on the interface with a default router requested from the DHCP server (DHCP option 3), then the default router provided by DHCP is used.

6. Low priority static route (lowest)

When more than one next hop is learned from the same source, the router uses an equal cost multi path algorithm that performs load balancing between routes.

- For information about configuring static routes, see [Routing table configuration](#) on page 394.
- For information about configuring OSPF, see [OSPF](#) on page 426.
- For information about configuring RIP, see [RIP](#) on page 421.
- For information about configuring DHCP client, see [DHCP client configuration](#) on page 183.

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 396. 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 263.

Static routes can be advertised by routing protocols, such as RIP and OSPF. For more information, see [Route redistribution](#) on page 429. Static routes also support load-balancing similar to OSPF.

Next hops

Static routes can be configured with the following as next hops:

Via-interface route: Specifies a Serial interface as the next hop, without a specific next hop IP address.

Next-hop IP address: Specifies the IP address of a router as a next hop. The next hop router must belong to one of the directly attached networks for which the Branch Gateway has an IP interface.

Static route types

Two kinds of static routes can be configured:

High Preference static routes: Preferred to routes learned from any routing protocol

Low Preference static routes: Used temporarily until the route is learned from a routing protocol

By default, a static route has low preference.

Configuring multiple next hops

Procedure

You can configure up to three next hops for each static route in one of the following manners:

- Enter all of the next hops using a single `ip route` command. To add a new next hop to an existing static route, enter the new next hop individually, as in the following option.
- Enter each next hop individually with its own `ip route` command

* Note:

If you apply tracking to a static route, you can only configure one next hop for the route.

Metrics are used to choose between routes of the same protocol. Preferences are used to choose between routes of different protocols.

Deleting a route and its next hops

Procedure

Use the `no ip route` command to delete the route including all of its next-hops.

This deletes all of the next-hops, whether entered individually or with a single command. For example, to specify next hops 149.49.54.1 and 149.49.75.1 as a static route to the network 10.1.1.0, do one of the following:

- Enter `ip route 10.1.1.0 24 149.49.54.1 149.49.75.1`, specifying all next hops together
- Enter both `ip route 10.1.1.0 24 149.49.54.1` and `ip route 10.1.1.0 24 149.49.75.1`

Via-interface static route

PPP and frame relay allow for a Layer 3 interface to be established without knowing in advance the next-hop on the other side of a serial link. In this case, you can specify a Serial Layer 2 interface or a GRE tunnel as a next-hop instead of providing a specific next hop IP address. This is equivalent to specifying the node on the other side of the serial link as the next hop when its IP address is unknown. The via interface option is configured by specifying the type and the number of the Serial interface using the `ip route` command.

* Note:

The interface used in the via route must have an IP address attached to it.

For example, the command `ip route 193.168.10.0 24 serial 3/1:1` creates a static route to the network 193.168.10.0 24 via the Serial 3/1:1 interface.

A static route can have both via interface and IP addressed next hops, with a maximum of three next-hops. If such a combination is required, separate `ip route` commands should be used for the via interface static route and the IP addressed next hop routes. Also, if more than one via interface next hop is required, each must be configured by separate `ip route` commands.

* Note:

You cannot define a static route through the FastEthernet Interface unless the interface was previously configured to use PPPoE encapsulation or was configured as a DHCP Client. See [Configuring PPPoE](#) on page 232 and [DHCP client configuration](#) on page 183.

Permanent static route

The Branch Gateway enables you to configure a static route as a permanent route. Configuring this option prevents the static route from becoming inactive when the underlying Layer 2 interface is down. This prevents routing table updates from being sent each time an interface goes up or

down when there is a fluctuating Layer 2 interface on the static route. Configure the permanent option using the **ip route** command.

For example, the command **ip route 193.168.10.0 24 serial 3/1:1 permanent** creates a permanent static route to the network 193.168.10.0 24 via the serial 3/1:1 interface.

The command **ip route 132.55.0.0 255.255.0.0 132.55.4.45 3 high** creates a high static route to the network 132.55.0.0/255.255.0.0 using next-hop ip address 132.55.4.45 and with cost 3.

Permanent static routes should not be configured over Serial Layer 2 interfaces that participate in a Primary-Backup pair.

For more information on Backup interfaces, see [Backup interfaces](#) on page 239.

*** 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 *Avaya Branch Gateway G450 CLI Reference*.

Command	Description
clear ip route	Delete all the dynamic routing entries from the routing table
ip default-gateway	Define a default gateway for the router
no ip default-gateway	Removes a default gateway for the router
ip netmask-format	Specify the format of subnet masks in the output of show commands
ip redirects	Enable the sending of redirect messages on the current interface
no ip redirects	Disable the sending of redirect messages on the current interface

Table continues...

Command	Description
<code>ip route</code>	Establish a static route
<code>no ip route</code>	Removes a static route
<code>ip routing</code>	Enable IP routing
<code>show ip route</code>	Display information about the IP routing table
<code>show ip route best-match</code>	Display a routing table for a destination address
<code>show ip route static</code>	Display static routes
<code>show ip route summary</code>	Display the number of routes known to the device
<code>show ip route track-table</code>	Display all routes with configured object trackers
<code>traceroute</code>	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 239.

For an example of a GRE tunneling application, see [GRE tunnel application example](#) on page 404.

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 394.
- The packet is routed to the Tunnel interface dynamically by a routing protocol (RIP or OSPF)
- The packet is routed to the Tunnel interface via policy-based routing. See Policy-based routing section.

Prevention of nested tunneling in GRE tunnels

Nested tunneling occurs when the tunnel's next hop for its destination is another tunnel, or the tunnel itself. When the next hop is the tunnel itself, a tunnel loop occurs. This is also known as recursive routing.

When the Branch Gateway recognizes nested tunneling, it brings down the Tunnel interface and produces a message that the interface is temporarily disabled due to nested tunneling. The tunnel remains down until the tunnel is re-configured to eliminate the nested tunneling.

In addition to checking for nested tunneling, the Branch Gateway prevents loops in connection with GRE tunnels by preventing the same packet from being encapsulated more than once in the Branch Gateway.

Reasons for nested tunneling in a GRE tunnel

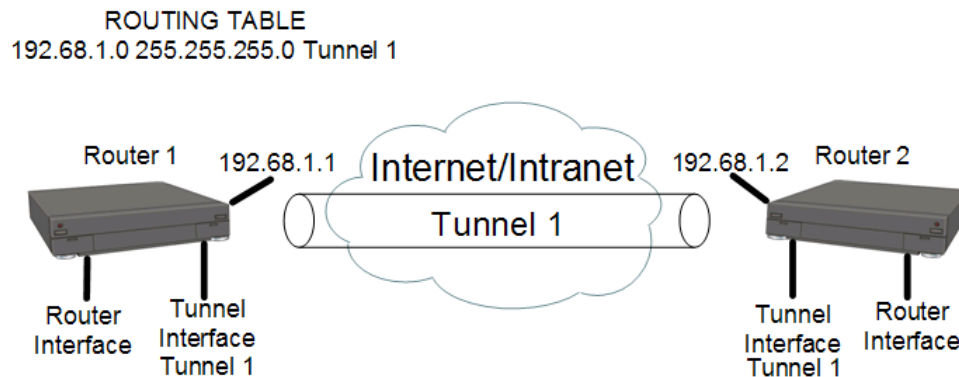
- A static route exists on the source tunnel endpoint that tells the tunnel to route packets addressed to the receiving tunnel endpoint via the tunnel itself
- The local endpoint of the tunnel learns the tunnel as a route to the tunnel's remote endpoint via OSPF or RIP

- A combination of static routes via parallel tunnels lead to a situation in which each tunnel is routing packets via another tunnel. For example:

```
Gxxx-001(super)# interface tunnel 1
Gxxx-001(super-if:Tunnel 1)# tunnel source x.x.x.x
Gxxx-001(super-if:Tunnel 1)# tunnel destination 1.0.0.1
Done!
Gxxx-001(super-if:Tunnel 1)# exit
Gxxx-001(super)# interface tunnel 2
Gxxx-001(super-if:Tunnel 2)# tunnel source x.x.x.x
Gxxx-001(super-if:Tunnel 2)# tunnel destination 2.0.0.1
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 400 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 400 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 400 as an illustration, you would configure the following policy rule on router 1 and activate it on the router RIP with the matching interface:

```

Gxxx-001(super)# ip distribution access-list-name 1 "list #1"
Done!
Gxxx-001(super)# ip distribution access-default-action 1 default-action-permit
Done!
Gxxx-001(super)# ip distribution access-list 1 10 "deny"
192.68.1.0 0.0.0.255
Done!
Gxxx-001(super)# router rip
Gxxx-001(super router:rip)# distribution-list 1 in FastEthernet 10/3
Done!
Gxxx-001(super router:rip)# exit
Gxxx-001(super)#

```

Static route: Configure a static rule on router 1 telling it the route for packets destined to the tunnel's receiving endpoint (192.68.1.2). This route should be configured with a high route preference. For example:

```

Gxxx-001(super)# ip route 192.68.1.2 255.255.0.0 192.68.1.3 high permanent
Done!
Gxxx-001(super)#

```

Optional GRE tunnel features

You can configure optional features in GRE tunnels. The tunnel keepalive feature enables periodic checking to determine if the tunnel is up or down. The dynamic MTU discovery feature determines and updates the lowest MTU on the current route through the tunnel.

Keepalive feature

The tunnel keepalive feature sends keepalive packets through the Tunnel interface to determine whether the tunnel is up or down. This feature enables the tunnel's source interface to inform the host if the tunnel is down. When the tunnel keepalive feature is not active, if the tunnel is down, the tunnel's local endpoint continues to attempt to send packets over the tunnel without informing the host that the packets are failing to reach their destination.

Enabling the keepalive feature

Procedure

Use the **keepalive** command in the GRE Tunnel interface context to enable the tunnel keepalive feature.

 Note:

You do not have to configure tunnel keepalive on both sides of the tunnel.

Use the **no** form of this command to deactivate the feature.

Example

The following example configures Tunnel 1 to send keepalive packets every 20 seconds. If the tunnel's destination interface fails to respond to three consecutive packets, the tunnel's source interface concludes that the tunnel is down. The source interface continues to send keepalive packets, but until it receives a response from the tunnel's destination interface, the tunnel informs hosts that send packets to the tunnel that the tunnel is down.

```
Gxxx-001# interface tunnel 1
Gxxx-001(if:Tunnel 1)# keepalive 20 3
Done!
```

Keepalive command parameters

The **keepalive** command includes the following parameters:

seconds: The length, in seconds, of the interval at which the source interface sends keepalive packets. The default value is 10.

retries: The number of retries after which the source interface declares that the tunnel is down. The default value is 3.

Dynamic MTU discovery

The size of packets that can travel through a GRE tunnel is limited by the lowest MTU of any router along the route through the tunnel. When dynamic MTU discovery is enabled, the tunnel maintains an MTU limit.

When a large packet is sent from the host with the DF bit on, and a router in the tunnel path has an MTU that is smaller than the size of the packet, since the DF bit is set, the router sends an ICMP unreachable message back in the originator (in this case, the GRE router). The GRE router then updates the tunnel's MTU limit accordingly. When a packet larger than the MTU arrives at the tunnel, if the packet is marked "do not fragment", the tunnel's source interface sends the packet back to the host requesting the host to fragment the packet. When dynamic MTU discovery is disabled, the tunnel's source interface marks each packet as *may be fragmented*, even if the packet's original setting is *do not fragment*. For more information on MTU and fragmentation, refer to [Fragmentation](#) on page 433.

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 401.

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 402.

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**.

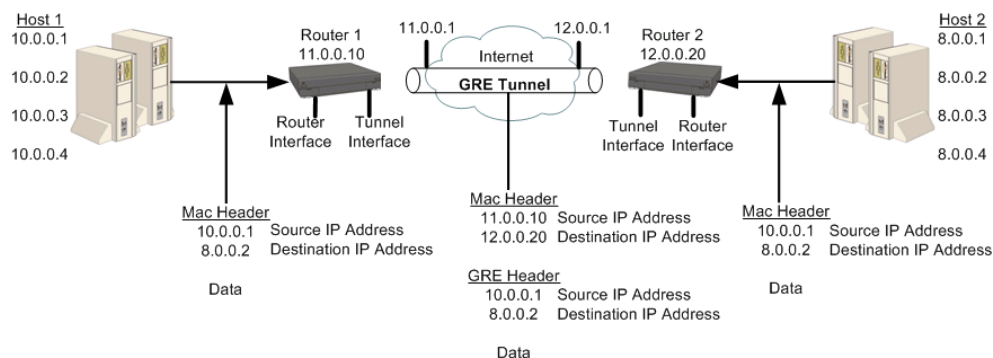
This saves the new Tunnel interface configuration in the startup configuration file.

Result

For a list of optional GRE tunnel features, refer to [Optional GRE tunnel features](#) on page 401. For a list of additional GRE tunnel CLI commands, refer to [Summary of GRE tunneling commands](#) on page 405.

GRE tunnel application example

This section provides an example of a GRE tunnel application and its configuration.



In the example shown in this figure, Host 1 and Host 2 are private networks using a GRE tunnel to connect them via the Internet. 11.0.0.10 and 12.0.0.20 are public IP addresses used by the GRE tunnel for the tunnel encapsulation.

A packet originating from 10.0.0.1 on Host 1 is sent to the destination 8.0.0.2 on Host 2. Since the destination IP address is a private IP address, the packet cannot be routed as is over the Internet. Instead, Router 1 receives the packet from host 1, looks up the packet's destination address in its

routing table, and determines that the next hop to the destination address is the remote end of the GRE tunnel.

Router 1 encapsulates the packet with a GRE header and a new IP header that assigns the IP address of Router 2 (12.0.0.20) as the destination IP address and the IP address of Router 1 (11.0.0.10) as the source IP address. When the packet arrives at Router 2, which is the end point of the GRE tunnel, Router 2 removes the outer IP header and the GRE header and sends the packet to its original destination at IP address (8.0.0.2).

You can use the following commands to configure GRE tunneling (with OSPF) in this example:

Example

Router 1 configuration

```
Gxxx-001(super)# interface fastethernet 10/3
Gxxx-001(super-if:FastEthernet 10/3)# ip address 11.0.0.10 255.255.255.0
Gxxx-001(super-if:FastEthernet 10/3)# exit
Gxxx-001(super)# interface tunnel 1
Gxxx-001(super-if:Tunnel 1)# keepalive 10 3
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 *Avaya Branch Gateway G450 CLI Reference*.

Root level command	Command	Description
<code>interface tunnel</code>		Enter tunnel interface configuration context, create a Tunnel interface if it does not exist, or delete a Tunnel interface or sub-interface
	<code>keepalive</code>	Enable the tunnel keepalive feature
	<code>tunnel checksum</code>	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.
	<code>no tunnel checksum</code>	Disables checksums
	<code>tunnel destination</code>	Set the destination address of the tunnel
	<code>tunnel dscp</code>	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.
	<code>tunnel key</code>	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.
	<code>no tunnel key</code>	Disables key checking
	<code>tunnel path- mtu- discovery</code>	Enable dynamic MTU discovery by the tunnel
	<code>tunnel source</code>	Set the source address of the tunnel
	<code>tunnel ttl</code>	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.

Table continues...

Root level command	Command	Description
<code>show interfaces tunnel</code>		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 409. For information about configuring DHCP client on the Branch Gateway, see [DHCP client configuration](#) on page 183.

DHCP

DHCP assigns dynamic IP addresses to devices on a network. With dynamic addressing, a device can have a different IP address whenever the device connects to the network. In some systems, the device's IP address can even change while it is still connected. DHCP also supports a mix of static and dynamic IP addresses.

Dynamic addressing simplifies network administration because the software keeps track of IP addresses rather than requiring an administrator to manage the task. This means you can add a new computer to a network without needing to manually assign a unique IP address. Many ISPs use dynamic IP addressing for dial-up users. However, dynamic addressing may not be desirable for a network server.

BOOTP

BOOTP is an Internet protocol that allows a diskless workstation to discover the following:

- Its own IP address
- The IP address of a BOOTP server on the network
- A file to be loaded into memory to boot the workstation

BOOTP allows the workstation to boot without requiring a hard disk or floppy disk drive. It is used when the user or station location changes frequently. The protocol is defined by RFC 951.

DHCP/BOOTP relay

The Branch Gateway supports the DHCP/BOOTP relay agent function. This is an application that accepts DHCP/BOOTP requests that are broadcast on one VLAN. The application sends them to

a DHCP/BOOTP server. That server connects to another VLAN or a server that might be located across one or more routers that might otherwise not get the broadcast request. The relay agent handles the DHCP/BOOTP replies as well. The relay agent transmits the replies to the client directly or as broadcast, according to a flag in the reply message.

*** Note:**

The same DHCP/BOOTP relay agent serves both the BOOTP and DHCP protocols.

When there is more than one IP interface on a VLAN, the Branch Gateway chooses the lowest IP address on this VLAN when relaying DHCP/BOOTP requests. The DHCP/BOOTP server then uses this address to decide the network from which to allocate the address. When there are multiple networks configured, the Branch Gateway performs a round-robin selection process.

When the DHCP/BOOTP server is configured to allocate addresses only from a single subnetwork among the different subnetworks defined on the VLAN, you might need to configure the Branch Gateway with the relay address on that subnet so the DHCP/BOOTP server can accept the request.

DHCP/BOOTP Relay in the Branch Gateway is configurable per VLAN and allows for two DHCP/BOOTP servers to be specified. In this case, the Branch Gateway duplicates each request, and sends it to both servers. This duplication provides redundancy and prevents the failure of a single server from blocking hosts from loading. You can enable or disable DHCP/BOOTP Relay in the Branch Gateway.

Summary of DHCP and BOOTP relay commands

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

Root level command	Command	Description
interface (fastethernet VLAN)		Enter the FastEthernet or VLAN interface configuration context
	ip bootp-dhcp network	Select the network from which the BOOTP/DHCP server should allocate an address This command is required only when there are multiple IP interfaces over the VLAN. You must be in an interface context to use this command
	no ip bootp-dhcp network	Restores the default value.
	ip bootp-dhcp server	Add or remove a BOOTP/DHCP server to handle BOOTP/DHCP requests received by the current interface A maximum of two servers can be added to a single interface. You must be in an interface context to use this command

Table continues...

Root level command	Command	Description
	<code>no ip bootp-dhcp server</code>	Removes a server.
<code>ip bootp-dhcp relay</code>		Enable or disable relaying of BOOTP and DHCP requests to the BOOTP/DHCP server You must be in general context to use this command.
<code>no ip bootp-dhcp relay</code>		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 for WAN failure.

The Branch Gateway supports the following DHCP server features:

- Up to 32 DHCP pools
- Up to 120 users
- Up to 1024 IP addresses for all DHCP pools together
- Automatic and reservation pools
- Standard DHCP options and IP phone and wireless special options
- Vendor specific information option
- DHCP relay packets
- Global statistics
- Syslog/traps for special events

The Branch Gateway can function as a DHCP server, as a DHCP relay, or both simultaneously, with each interface configured in either DHCP server mode or DHCP relay mode. For example, you can configure the Branch Gateway to provide DHCP service to voice devices while DHCP requests by data devices are routed to a central remote DHCP server using DHCP relay.

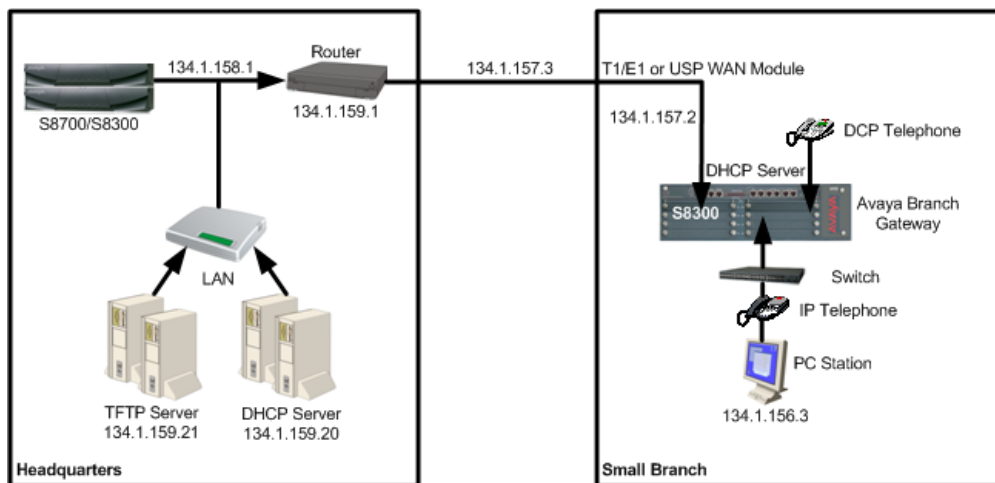
The Branch Gateway can function as a DHCP server or as a DHCP client, or both simultaneously. For information about configuring DHCP client on the Branch Gateway, see [DHCP client configuration](#) on page 183.

Related links

[DHCP client configuration](#) on page 183

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 pool1`, 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 412 and, for vendor specific options, [Configuring vendor-specific options](#) on page 413.

8. Repeat steps 1 to 7 to configure as many DHCP pools as you require.

You can configure up to 32 DHCP pools. By default, all pools are inactive until you activate them. This enables you to modify each pool's configuration without affecting network devices.

9. Activate each of the DHCP pools you configured using the **ip dhcp activate pool** command in general context, followed by the pool number.
10. Enter **ip dhcp-server** to activate DHCP server.

DHCP server is now active. If you change the pool configuration, it is recommended to do so while the pool is active.

 Note:

If you try to configure a new start and end IP address that is not part of the current network and beyond the allowed maximum of 256 IP addresses, first use the **no**

`start ip address` and `no end ip address` commands before configuring the new start and end IP addresses.

Configuring options

About this task

DHCP options are various types of network configuration information that the DHCP client can receive from the DHCP server. The Branch Gateway supports all DHCP options. The most common options used for IP phones are listed in [Common user-configurable DHCP options](#) on page 412. Some options are configured with specific CLI commands that are also listed in [Common user-configurable DHCP options](#) on page 412. 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 412 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	<code>subnet-mask</code>
3	Router	<code>default-router</code>
6	Domain name server	<code>dns_server</code>
7	Log Server	
15	Domain Name	<code>domain-name</code>
43	vendor-specific information	<code>vendor-specific-option</code>
44	Wins/NBNS server	
46	Wins/NBT Node Type	
51	IP Address Lease Time	<code>lease</code>
66	TFTP server name	
69	SMTP server	
242	Avaya Site Specific Option Numbers (SSON) for IP phones	

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. 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 242
Gxxx-001(super-DHCP 1/option 242)# name "Avaya IP phone option"
Done!
Gxxx-001(super-DHCP 1/option 242)# value ascii "MCIPADD=10.10.2.140,
MCPORT=1719, TFTP SRVR=10.10.5.188"
Done!
Gxxx-001(super-DHCP 1/option 242)# 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 242
Gxxx-001(super-DHCP 2/option 242)# value ascii "MCIPADD=192.168.50.17,
192.168.50.15, MCPORT=1719, TFTPSPVR=192.168.50.1, TFTPDIR=/phonedir/"
Done!
Gxxx-001(super-DHCP 2/option 242)# 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 415 or the *Avaya Branch Gateway G450 CLI Reference*.

Summary of DHCP Server commands

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

Root level command	First level command	Second level command	Description
<code>clear ip dhcp-server binding</code>			Delete IP address binding
<code>clear ip dhcp-server statistics</code>			Clear the statistics of the DHCP server
<code>ip dhcp activate pool</code>			Activate configured DHCP pools
<code>ip dhcp ping packets</code>			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
<code>ip dhcp ping timeout</code>			Set the time the DHCP server waits for a reply to a sent ping packet before allocating an IP address to a DHCP client
<code>ip dhcp pool</code>			Create a DHCP pool
	<code>bootfile</code>		Provide startup parameters for the DHCP client device
	<code>client-identifier</code>		Reserve the pool's IP address for assignment to a specific client
	<code>default- router</code>		Set up to eight default router IP addresses in order of preference
	<code>dns-server</code>		Set up to eight Domain Name Server (DNS) IP addresses
	<code>domain-name</code>		Set a domain name string for the client
	<code>end-ip-addr</code>		Set the end IP address of the range of available IP addresses that the DHCP server may assign to clients

Table continues...

Root level command	First level command	Second level command	Description
	lease		Configure the lease period for IP address assignment
	name		Configure the pool's name
	next-server		Specify the IP address of the next server in the boot process of a DHCP client
	option		Enter the context of a DHCP option
		name	Configure a name for the DHCP option
		value	Enter the option data type and the option data
	server-name		Specify the optional server name in the boot process of a DHCP client
	show ip dhcp-pool		Display DHCP pool configurations
	start-ip-addr		Set the start IP address of the range of available IP addresses that the DHCP server may assign to clients
	subnet-mask		Configure the subnet mask of the pool
	vendor-specific-option		Create a vendor-specific option with a unique index
		name	Name the vendor-specific option
		class-identifier	Set a vendor-specific identifier
		value	Set the data type and value of the vendor-specific option
ip dhcp-server			Activate DHCP server
show ip dhcp-server bindings			Display bindings
show ip dhcp-server statistics			Display DHCP server statistic

Broadcast relay

When you configure broadcast relay, the router forwards broadcast packets across interfaces. You can configure broadcast relay types including directed broadcast forwarding, NetBIOS rebroadcast, DHCP, and BOOTP client broadcast.

For more information about DHCP and BOOTP client broadcast, see [DHCP and BOOTP relay](#) on page 407.

Directed broadcast forwarding

About this task

A directed broadcast is an IP packet whose destination address is the broadcast address of a network or subnet. A directed broadcast causes every host on the network to respond. You can use directed broadcasts to obtain a list of all active hosts on the network. A hostile user can exploit directed broadcasts to launch a denial-of-service attack on the network. For each interface on the Branch Gateway, you can configure whether the Branch Gateway forwards directed broadcast packets to the network address or subnet mask address of the interface.

Procedure

Enter `ip directed-broadcast` to enable directed broadcast forwarding on an interface. Use the `no` form of this command to disable directed broadcast forwarding on an interface.

NetBIOS rebroadcast

Network Basic Input Output System (NetBIOS) is a protocol for sharing resources among desktop computers on a LAN. You can configure the Branch Gateway to relay NetBIOS UDP broadcast packets. This feature is used for applications such as WINS that use broadcast but might need to communicate with stations on other subnetworks or VLANs.

Configuration is performed on a per-interface basis. A NetBIOS broadcast packet arrives from an interface on which NetBIOS rebroadcast is enabled. The packet is distributed to all other interfaces configured to rebroadcast NetBIOS.

- If the NetBIOS packet is a net-directed broadcast, for example, 149.49.255.255, the packet is relayed to all other interfaces on the list, and the IP destination of the packet is replaced by the appropriate interface broadcast address.
- If the NetBIOS broadcast packet is a limited broadcast, for example, 255.255.255.255, it is relayed to all VLANs on which there are NetBIOS-enabled interfaces. In that case, the destination IP address remains the limited broadcast address.

Summary of broadcast relay commands

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

Root level command	Command	Description
<code>interface (dialer fastethernet tunnel vlan)</code>		Enter the Dialer, FastEthernet, Tunnel, or VLAN interface context
	<code>ip directed-broadcast</code>	Enable or disable directed broadcast forwarding on the interface
	<code>ip netbios-rebroadcast</code>	Enable or disable NetBIOS rebroadcasts on the interface

ARP table

When you configure the Address Resolution Protocol (ARP) table, you can:

- View information about the ARP table
- Add entries to the ARP table
- Delete entries from the ARP table
- Configure the ARP timeout

Overview of ARP

IP logical network addresses are independent of physical addresses. The physical address must be used to convey data in the form of a frame from one device to another. Therefore, a mechanism is required to acquire a destination device hardware address from its IP address. This mechanism is called ARP.

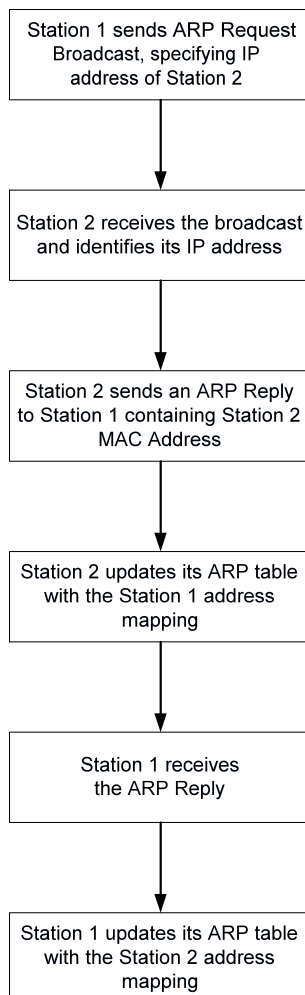
Static and dynamic table entries

The ARP table stores pairs of IP and MAC addresses. This storage saves time and communication costs, since the host looks in the ARP table first when transmitting a packet. If the information is not there, then the host sends an ARP Request.

There are two types of entries in the ARP table:

Static ARP table entries: Static ARP table entries do not expire.

Dynamic ARP table entries: Dynamic ARP table entries are mappings between IP addresses and MAC addresses that the switch used recently. Dynamic ARP table entries expire after a configurable amount of time. The following diagram shows how a switch adds dynamic ARP table entries:



Adding static ARP table entries

Procedure

To add static ARP table entries manually, use the **arp** command.

For example, to add a static ARP table entry for station 192.168.7.8 with MAC address 00:40:0d:8c:2a:01, use the following command:

```
Gxxx-001# arp 192.168.7.8 00:40:0d:8c:2a:01
```

Removing static and dynamic entries

Procedure

To remove static and dynamic entries from the ARP table, use the **no arp** command .

For example, to remove the ARP table entry for the station 192.168.13.76:

```
Gxxx-001# no arp 192.168.13.76
```

Changing an entry in the ARP table

Procedure

To change an entry in the ARP table, delete the entry and reinsert it with revised parameters.

Summary of ARP table commands

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

Command	Description
arp	Add a permanent entry to the ARP table
no arp	Remove either a static entry or a dynamically-learned entry from the ARP table
arp timeout	Configure the amount of time, in seconds, that an entry remains in the ARP table Entering this command without a time parameter displays the current timeout value.
no arp timeout	Restore the default value (four hours)
clear arp-cache	Delete all dynamic entries from the ARP table and the IP route cache
ip max-arp-entries	Specify the maximum number of ARP table entries allowed in the ARP table
no ip max-arp-entries	Restore the maximum number of ARP table entries allowed in the ARP table to default value
show ip arp	Display a list of the ARP resolved MAC to IP addresses in the ARP table
show ip reverse-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 identity, the router accepts responsibility for routing packets to their true destination.

Proxy ARP can help devices on a subnet to reach remote subnets without the need to configure routing or a default gateway.

Summary of Proxy ARP commands

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

Root level command	Command	Description
interface (fastethernet vlan)		Enter the FastEthernet or VLAN interface context

Table continues...

Root level command	Command	Description
	<code>ip proxy-arp</code>	Enable proxy ARP on an Branch Gateway interface
	<code>no ip proxy-arp</code>	Disable proxy ARP on an interface

ICMP errors

You can control whether the router sends Internet Control Message Protocol (ICMP) error messages. The router sends an ICMP error message to the source of a packet if the router rejects the packet.

Summary of ICMP errors commands

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

Command	Description
<code>ip icmp-errors</code>	Set ICMP error messages to ON or OFF
<code>show ip icmp</code>	Display the status (enabled or disabled) of ICMP error messages

Routing information protocol (RIP)

The Routing information protocol (RIP) enables routers to compute the path that an IP packet must 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 426.

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 429.

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, require to gather information on how to reach each destination in the Internet. However the simplicity of RIP has a disadvantage. This protocol does not consider network bandwidth, physical cost, and data priority. The Branch Gateway supports two versions of RIP:

- [RIPv1](#) on page 422
- [RIPv2](#) on page 422

 Note:

RIP is not supported in FIPS mode.

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 (VLSM). 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 422.

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 422

Commands used to prevent routing loops in RIP

Split-horizon technique

- Enter `ip rip split-horizon` to enable the split-horizon mechanism.

- Use the **no** form of this command to disable the split-horizon mechanism. By default, split-horizon is enabled.

Poison-reverse updates

- Enter **ip rip poison-reverse** to enable split-horizon with poison-reverse on an interface.
- Use the **no** form of this command to disable the poison-reverse mechanism.

RIP distribution access lists

RIP distribution access lists consist of rules that specify how a router distributes and accepts RIP routing information from other routers. Before sending an update, the router consults an access list to determine if it should include specific routes in the update. When receiving an update, the router first checks a set of rules which apply to incoming updates to determine if it should insert those routes into its routing table. You can assign the rules per interface and per direction.

You can configure up to 99 RIP distribution access lists on the Branch Gateway.

Configuring a distribution access list example

About this task

For example, to configure RIP distribution access list number 10 permitting distribution and learning of network 10.10.0.0, do the following:

Procedure

1. Enter the command: **ip distribution access-list 10 1 permit 10.10.0.0 0.0.255.255**

The default action of the access list is deny and can be changed using the **ip distribution access-default-action** command.

Note:

Whenever at least one permit rule exists, distributing and learning of all the remaining networks is denied, unless specifically permitted by another rule.

2. Apply the distribution access list created in Step 1 by performing the following procedure within the Router RIP context:
 - a. Enter the **distribution-list 10 in** command to apply list number 10 created in Step 1 on all updates received on all interfaces.
 - b. Enter the **distribution-list 10 in FastEthernet 10/3** command to apply Access List 10 on updates received on interface 'FastEthernet 10/3'.
 - c. Enter the **distribution-list 10 out** command to apply Access List 10 to all advertised updates.
 - d. Enter the **distribution-list 10 out ospf** command to apply Access List 10 to all advertised updates that were learned from OSPF (redistributed from OSPF into RIP).

Result

If no distribution access list is defined, learning and advertising is allowed for all of the routing information. This is the default.

RIP limitations

Configuration of RIPv1 and RIPv2 is per IP interface. Configuration must be homogeneous on all routers on each subnetwork. That is, RIPv1 and RIPv2 routers should not be configured on the same subnetwork. However, you can configure different IP interfaces of the Branch Gateway with different RIP versions. This configuration is valid as long as all routers on the subnet are configured with the same version.

RIPv2 and RIPv1 are considered the same protocol with regard to redistribution to and from OSPF and static route preferences.

Summary of RIP commands

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

Root level command	Command	Description
<code>ip distribution access-default-action</code>		Set the default action for a specific RIP distribution access list
<code>ip distribution access-list</code>		Create a RIP distribution access list
<code>ip distribution access-list-cookie</code>		Set the access list cookie
<code>ip distribution access-list-copy</code>		Copy the distribution access list
<code>ip distribution access-list-name</code>		Set the name of the distribution list
<code>ip distribution access-list-owner</code>		Set the owner of the distribution list
<code>interface (dialer fastethernet loopback serial vlan tunnel)</code>		Enter the Dialer, FastEthernet, Loopback, Serial, Tunnel, or VLAN interface context
	<code>ip rip authentication key</code>	Set the authentication string used on the interface
	<code>no ip rip authentication key</code>	Clear the password
	<code>ip rip authentication mode</code>	Specify the type of authentication used in RIP v2 packets
	<code>no ip rip authentication mode</code>	Restore the default value, none

Table continues...

Root level command	Command	Description
	ip rip default-route-mode	Enable learning of the default route received by the RIP protocol. The default state is talk-listen. The default state is talk-listen.
	no ip rip default-route-mode	Disable listening to default routes.
	ip rip poison-reverse	Enable or disable split-horizon with poison-reverse on an interface
	no ip rip poison-reverse	Disable the poison-reverse mechanism
	ip rip rip-version	Specify the RIP version running on the interface
	ip rip send-receive-mode	Set the RIP send and receive modes on an interface
	no ip rip send-receive-mode	Set the RIP to talk, that is, to send reports
	ip rip split-horizon	Enable or disable the split-horizon mechanism
	no ip rip split-horizon	Disable the split-horizon mechanism. By default split-horizon is enabled.
router rip		Enable the RIP and enter the router configuration context or disable the RIP
no router rip		Restore the default value by disabling RIP
	default-metric	Set or reset the interface RIP route metric value
	no default-metric	restore the interface RIP route metric default value.
	distribution-list	Apply a distribution access list for incoming or outgoing routing information in route updates or deactivate the list
	no distribution-list	Deactivate the distribution access list
	network	Specify a list of networks on which the RIP is running
	no network	Remove an entry from the list of networks
	redistribute	Redistribute routing information from other protocols into RIP
	no redistribute	Restore the default value, disable redistribution by RIP

Table continues...

Root level command	Command	Description
	<code>timers basic</code>	Set RIP timers
	<code>no timers basic</code>	Set the RIP timers to their default value
<code>show ip distribution access-lists</code>		Display the contents of all current distribution lists or of a specific list
<code>show ip protocols</code>		Display parameters and statistics of a given IP routing protocol

Open shortest path first (OSPF)

The Open Shortest Path First (OSPF) protocol enables routers to compute the path that an IP packet must 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 421.

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 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 429.

Note:

OSPF is not supported in FIPS mode.

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: $\text{Cost} = 100,000 / \text{bandwidth (in kbps)}$

The result is that the higher the bandwidth, the lower the Cost.

When manually configuring the Cost of an OSPF interface (**ip ospf cost** command), dynamic bandwidth updates do not change the Cost.

When manually adjusting the interface's bandwidth, (**bandwidth** command), if Cost is being determined dynamically, it is this configured bandwidth and not the actual interface bandwidth that is used to calculate Cost.

OSPF limitations

You can configure the Branch Gateway as an OSPF Autonomous System Boundary Router (ASBR) using route redistribution. The Branch Gateway can be installed in the OSPF backbone area (area 0.0.0.0) or in any OSPF area that is part of a multiple areas network. However, the Branch Gateway cannot be configured to be an OSPF area border router itself.

The Branch Gateway supports the ECMP equal-cost multipath (ECMP) feature which allows load balancing by splitting traffic between several equivalent paths.

While you can activate OSPF with default values for each interface using a single command, you can configure many of the OSPF parameters.

Summary of OSPF commands

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

Root level command	Command	Description
interface (dialer fastethernet loopback serial tunnel vlan)		Enter the Dialer, FastEthernet, Loopback, Serial, Tunnel, or VLAN interface context
	bandwidth	Set the bandwidth parameter manually for this interface
	ip ospf authentication	Specify the authentication type for an interface
	no ip ospf authentication	Remove the authentication type for an interface.
	ip ospf authentication-key	Configure the interface authentication password
	no ip ospf authentication-key	Remove the OSPF password
	ip ospf cost	Configure the Cost of an OSPF interface, for the purpose of determining the shortest path
	no ip ospf cost	Set the cost to its default value

Table continues...

Root level command	Command	Description
	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
	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.

Table continues...

Root level command	Command	Description
	<code>passive-interface</code>	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 <code>network</code> command with this command to make the network passive.
	<code>redistribute</code>	Redistribute routing information from other protocols into OSPF
	<code>no redistribute</code>	Disable redistribution by OSPF
	<code>timers spf</code>	Configure the delay between runs of OSPFs (SPF) calculation
	<code>no timers spf</code>	Restore the default value
<code>show ip ospf</code>		Display general information about OSPF routing
<code>show ip ospf database</code>		Display lists of information related to the OSPF database for a specific router
<code>show ip ospf interface</code>		Display the OSPF-related interface information
<code>show ip ospf neighbor</code>		Display OSPF neighbor information on a per-interface basis
<code>show ip protocols</code>		Display OSPF parameters and statistics

Route redistribution

Route redistribution is the interaction of multiple routing protocols. OSPF and RIP can be operated concurrently in the Branch Gateway. In this case, you can configure the Branch Gateway to redistribute routes learned from one protocol into the domain of the other routing protocol. Similarly, static routes can be redistributed to RIP and OSPF.

* **Note:**

Take care when you configure route redistribution. It involves metric changes and might cause routing loops in the presence of other routes with incompatible schemes for route redistribution and route preferences.

The Branch Gateway scheme for metric translation in route redistribution is as follows:

- Static to RIP metric configurable (default 1)
- OSPF internal metric N to RIP metric (default 1)

- OSPF external type 1 metric N to RIP metric (default 1)
- OSPF external type 2 metric N to RIP metric (default 1)
- Static to OSPF external type 2, metric configurable (default 20)
- RIP metric N to OSPF external type 2, metric (default 20)
- Direct to OSPF external type 2, metric (default 20)

By default, the Branch Gateway does not redistribute routes between OSPF and RIP. Redistribution from one protocol to the other can be configured. Static routes are, by default, redistributed to RIP and OSPF. The Branch Gateway allows the user to globally disable redistribution of static routes to RIP, and separately to globally disable redistribution of static routes to OSPF. In addition you can configure, on a per static route basis, whether the route is to be redistributed to RIP and OSPF, and what metric to use (in the range of 1-15). The default state is to allow the route to be redistributed at metric 1. When static routes are redistributed to OSPF, they are always redistributed as external type 2.

Export default metric

The Branch Gateway enables you to configure the metric to be used in updates that are redistributed from one routing protocol to another.

In RIP, the default is 1 and the maximum value is 16. In OSPF, the default is 20.

Set the default metric value before redistribution, using the **default-metric** command from within the Router RIP or Router OSPF contexts. This value is used for all types of redistributed routes, regardless of the protocol from which the route was learned.

Summary of route redistribution commands

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

Root level command	Command	Description
router ospf		Enable OSPF and enter the router configuration context
	redistribute	Redistribute routing information from other protocols into OSPF • Use in the Router RIP context to configure route redistribution into RIP. • Use in the Router OSPF context to configure route redistribution into OSPF.
	default-metric	Configure the metric to be used in updates that are redistributed from one routing protocol to another
router rip		Enable RIP and enter the router configuration context

Table continues...

Root level command	Command	Description
	<code>redistribute</code>	Redistribute routing information from other protocols into RIP
	<code>default-metric</code>	Configure the metric to be used in updates that are redistributed from one routing protocol to another

VRRP

Virtual Router Redundancy Protocol (VRRP) is an IETF protocol designed to support redundancy of routers on the LAN and load balancing of traffic. VRRP is open to host stations, making it an ideal option when redundancy, load balancing, and ease of configuration are required.

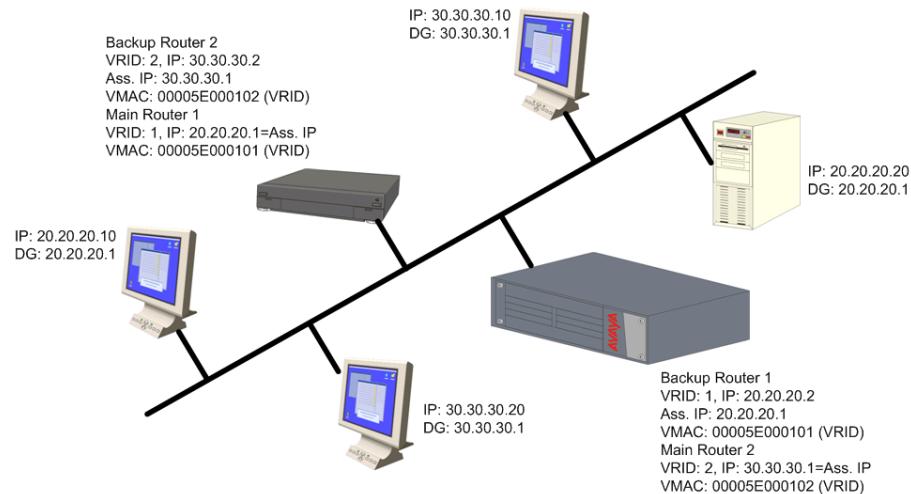
The concept underlying VRRP is that a router can back up other routers, in addition to performing its primary routing functions. This redundancy is achieved by introducing the concept of a virtual router. A virtual router is a routing entity associated with multiple physical routers. One of the physical routers with which the virtual router is associated performs the routing functions. This router is known as the master router. For each virtual router, VRRP selects a master router. If the selected master router fails, another router is selected as master router.

In VRRP, two or more physical routers can be associated with a virtual router, thus achieving extreme reliability. In a VRRP environment, host stations interact with the virtual router. The stations are not aware that this router is a virtual router, and are not affected when a new router takes over the role of master router. Thus, VRRP is fully interoperable with any host station.

You can activate VRRP on an interface using a single command while allowing for the necessary fine-tuning of the many VRRP parameters. For a detailed description of VRRP, see VRRP standards and published literature.

VRRP configuration example

The following diagram illustrates an example of a VRRP configuration:



There is one main router on IP subnet 20.20.20.0, such as a Branch Gateway, switch, or any router that supports VRRP, and a backup router. You can configure more backup routers.

- The Branch Gateway itself must have an interface on the IP subnetwork, for example, 20.20.20.2
- Configure all the routers under the same VRID, for example, 1. You must configure the routers per VLAN.
- An assigned VRID must not be used in the network, even in a different VLAN
- When router configuration is complete and the network is up, the main router for each virtual router is selected according to the following order of preference:
 - The virtual router IP address is also the router's interface IP address
 - It has the highest priority (you can configure this parameter)
 - It has the highest IP address if the previous conditions do not apply
- The virtual router IP address needs to be configured as the default gateway on the stations
- The Main router advertises a six-byte Virtual MAC address, in the format 00.00.5E.00.01.02 VRID, as a response to the stations' ARP requests
- The redundant router uses a VRRP polling protocol to check the Main router integrity at one-second intervals (default). Otherwise, it is idle.
- If the Main router fails, the redundant router that does not receive a response from four consecutive polling requests (default) takes over and starts to advertise the same Virtual MAC for ARP requests. Therefore, the stations will not detect any change either in the configured default gateway or at the MAC level.
- VRRP has no provisions for routing database synchronization among the redundant routers. You must perform this manually, if needed.

Summary of VRRP commands

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

Root level command	Command	Description
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)
	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

Branch Gateway supports IP fragmentation and reassembly. The Branch Gateway router can fragment and reassemble IP packets according to RFC 791. This feature allows the router to send and receive large IP packets where the underlying data link protocol constrains the Maximum Transport Unit (MTU).

IP fragmentation involves breaking a datagram into a number of pieces that can be reassembled later. The IP source, destination, identification, total length, and fragment offset fields, along with the more fragment and don't fragment flags in the IP header, are used for IP fragmentation and reassembly.

IP fragmentation works as follows:

- Each IP packet is divided into fragments
- Each fragment becomes its own IP packet
- Each packet has same identifier, source, and destination address

Fragments are usually not reassembled until final destination. The Branch Gateway supports fragmentation of IP packets according to RFC 791, and reassembly of IP packets destined only to its interfaces.

Summary of fragmentation commands

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

Command	Description
<code>clear fragment</code>	Clear the fragment database and restore its default values
<code>fragment chain</code>	Set the maximum number of fragments that can comprise a single IP packet destined to the router
<code>no fragment chain</code>	Set the fragment chain to its default value
<code>fragment size</code>	Set the maximum number of fragmented IP packets destined to the router to reassemble at any given time
<code>no fragment size</code>	Set the fragment size to its default value
<code>fragment timeout</code>	Set the maximum number of seconds to reassemble a fragmented IP packet destined to the router
<code>no fragment timeout</code>	Set the fragment timeout to its default value.
<code>show fragment</code>	Display information regarding fragmented IP packets that are destined to a router

Chapter 21: IPSec VPN

VPN (Virtual Private Network) defines a private secure connection between two nodes on a public network such as the Internet. VPN at the IP level is deployed using IP Security (IPSec). IPSec is a standards-based set of protocols defined by the IETF that provide privacy, integrity, and authenticity to information transferred across IP networks.

The standard key exchange method employed by IPSec uses the Internet Key Exchange (IKE) protocol to exchange key information between the two nodes (referred to as peers). Each peer maintains Security Associations (SAs) to maintain the private secure connection. IKE operates in two phases:

- The Phase-1 exchange negotiates an IKE SA
- The IKE SA created in Phase-1 secures the subsequent Phase-2 exchanges, which in turn generate IPSec SAs

IPSec SAs secure the actual traffic between the protected networks behind the peers, while the IKE SA only secures the key exchanges that generate the IPSec SAs between the peers.

The Branch Gateway IPSec VPN feature is designed to support site-to-site topologies, in which the two peers are gateways.

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 must define and the order in which you require to define them.

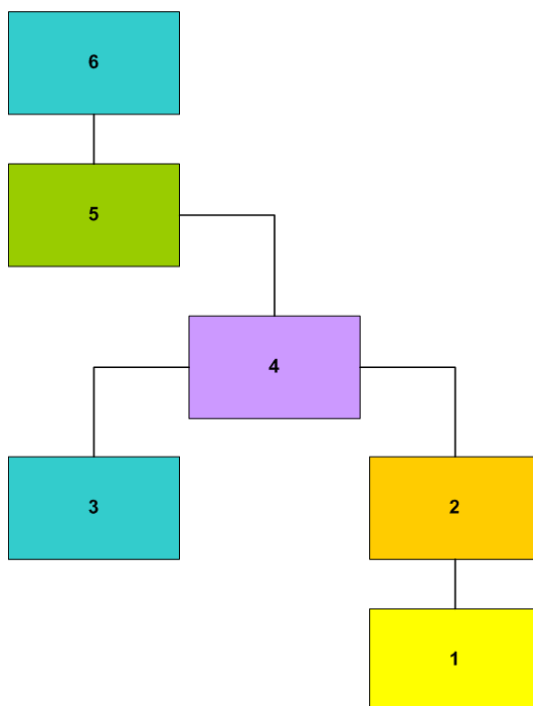


Table 4: IPSec VPN components configuration

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

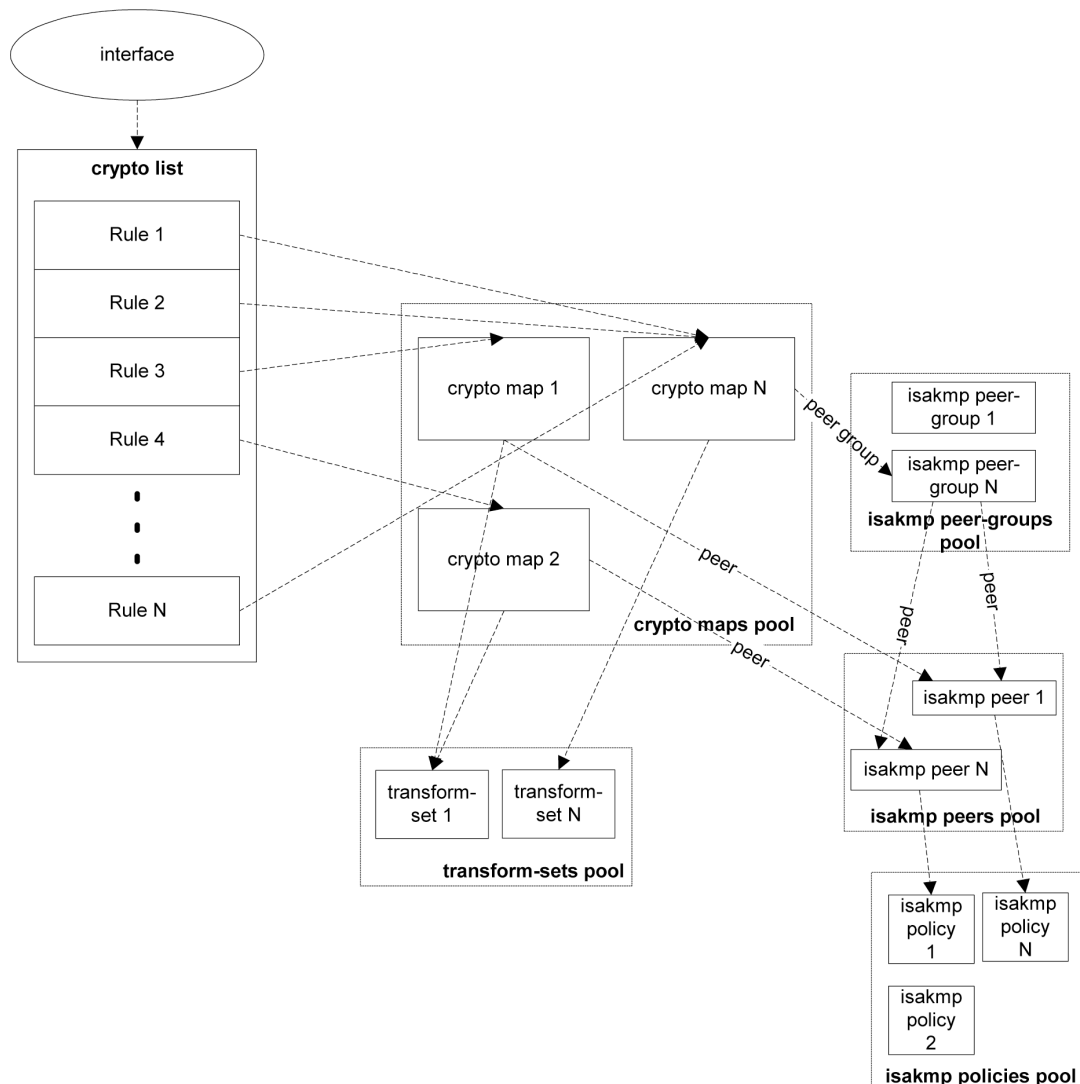
Transform-sets: Define parameters for IKE phase 2 negotiation

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 439.

* 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 440
 - description
 - authentication pre-share
 - encryption

- hash
- group
- lifetime
- IPSEC transform-set – [crypto ipsec transform-set](#) on page 441
 - set pfs
 - et security-association lifetime seconds
 - set security-association lifetime kilobytes
 - mode (tunnel/transport)
- ISAKMP peer – [crypto isakmp peer](#) on page 442
 - 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 445
 - description
 - set peer
- Crypto map – [crypto map](#) on page 446
 - description
 - set transform-set
 - set peer or set peer-group
 - set dscp
 - continuous-channel
- IP crypto list – [ip crypto-list](#) on page 448
 - 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 451
- [global parameters](#) on page 451
 - `crypto isakmp invalid-spi-recovery`
 - `crypto ipsec nat-transparency udp-encapsulation`
 - `crypto isakmp nat keepalive`
- [assigning a crypto-list to an interface](#) on page 452
 - `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 451).

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.

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 440)
- The IKE phase 2 parameters (as defined in the transform-set, see [Configuring transform-sets](#) on page 441)
- The ISAKMP peer parameters (see [Configuring ISAKMP peer information](#) on page 442)
- Which packets should be secured (as defined in the crypto list, see [Configuring crypto lists](#) on page 448)
- The peer addresses. For each peer, the local address entered in the crypto list (see [Configuring crypto lists](#) on page 448) should match the ISAKMP peer address in the other peer (see [Configuring ISAKMP peer information](#) on page 442).
- NAT Traversal, if your installation includes one or more NAT devices between the local and remote VPN peers. See [Configuring global parameters](#) on page 451.

See [Configuring IPSec VPN logging](#) on page 455 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 aes (default), 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. The only value allowed is 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 aes
Done!
Gxxx-001(config-isakmp:1)# hash md5
Done!
Gxxx-001(config-isakmp:1)# group 14
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-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:

```
crypto ipsec transform-set ts1 esp-aes esp-sha-hmac comp-lzs
```

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 GNPilodGNBrB5z4GJL
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 460.

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 463.

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 460.

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 263.

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 463.

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 478.

*** 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 442).

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 446 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 463.

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 460.

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 446.

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 to 6 for every ip-rule you wish to define in the crypto list.

8. Exit crypto list context with the **exit** command.

For example:

```

Gxxx-001(Crypto 901)# exit
Gxxx-001#

```

Deactivating crypto lists to modify IPSec VPN parameters

About this task

Most IPSec VPN parameters cannot be modified if they are linked to an active crypto list.

Procedure

1. To modify a parameter linked to an active crypto list, you must first deactivate the list using the **no ip crypto-group** command in the context of the interface on which the crypto list is activated.

Note:

If the crypto list is activated on more than one interface, deactivate the crypto list for each of the interfaces on which it is activated.

For example:

```

Gxxx-001# interface serial 3/1
Gxxx-001(if:serial 3/1)# no ip crypto-group
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:

```
Gxxx-001# interface serial 3/1
Gxxx-001(if:serial 3/1)# 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 456.

Configuring global parameters

Enabling invalid SPI recovery

About this task

Invalid SPI Recovery enables an IKE SA to be established when an invalid security parameter index error occurs during packet processing. A notification of the invalid SPI error is sent to the originating peer so that the SA databases can be re-synchronized, and successful packet processing can be resumed.

Note:

Invalid SPI recovery is enabled by default. Configure invalid SPI recovery only if you wish to re-enable it after it was disabled.

Procedure

1. Enable invalid SPI recovery with the `crypto isakmp invalid-spi-recovery` command.

For example:

```
Gxxx-001# crypto isakmp invalid-spi-recovery
Done!
```

2. Configure NAT Traversal global parameters as described in [NAT Traversal](#) on page 452

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.

Configuring NAT Traversal Procedure

1. Enable NAT Traversal by entering **crypto ipsec nat-transparency udp-encapsulation**.

For example:

```
Gxxx-001# crypto ipsec nat-transparency udp-encapsulation
Done!
```

2. Enable NAT Traversal keepalives and configure the keepalive interval in seconds by entering **crypto isakmp nat keepalive**, followed by a number from 5 to 3600.

NAT Traversal keepalives are empty UDP packets that the device sends on a periodic basis at times of inactivity when a dynamic NAT is detected along the way. These keepalives are intended to maintain the NAT translation alive in the NAT device, and not let it age-out due to periods of inactivity. Set the NAT Traversal keepalive interval on the Branch Gateway to be less than the NAT translation aging time on the NAT device.

For example:

```
Gxxx-001# crypto isakmp nat keepalive 60
Done!
```

Assigning a crypto list to an interface

About this task

A crypto list is activated on an interface. You can assign multiple crypto lists to different interfaces on the Branch Gateway.

Procedure

1. Enter interface context using the **interface** command.

For example:

```
Gxxx-001# interface fastethernet 10/3
Gxxx-001(config-if:FastEthernet 10/3)#
```

2. Configure the IP address of the interface.

You can configure either a static or a dynamic IP address.

- To configure a static IP address:
 - Be sure to specify an IP address (not an interface name) as the **local-address** in the crypto list (see [Configuring crypto lists](#) on page 448)
 - 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 460
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 499 or *Avaya Branch Gateway G450 CLI Reference*.

Commands used to display an IPSec VPN configuration

- **show crypto ipsec transform-set**
- **show crypto isakmp policy**
- **show crypto isakmp peer**
- **show crypto isakmp peer-group**
- **show crypto map**
- **show ip crypto-list list#**
- **show ip crypto-list**
- **show ip active-lists**

For a description of these commands, see [Summary of VPN commands](#) on page 499

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

Commands used to display IPSec VPN status

The following **show** commands show runtime IPSec VPN database status and statistics, and clear runtime statistics.

- **show crypto isakmp sa**
- **show crypto ipsec sa**
- **show crypto ipsec sa address**
- **show crypto ipsec sa list**

+ Tip:

The **detail** option in the various **show crypto ipsec sa** commands, provides detailed counters information on each IPsec SA. To pinpoint the source of a problem, check for a counter whose value grows with time.

- **clear crypto sa counters**

For a description of these commands, see [Summary of VPN commands](#) on page 499 .

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

Clearing both ISAKMP connection and IPsec SAs

Procedure

1. Clear the IPsec SAs with the **clear crypto sa all** command.
2. Clear the ISAKMP SA with the **clear crypto isakmp** command.

Configuring IPsec VPN logging

About this task

IPsec VPN logging allows you to view the start and finish of IKE phase 1 and IKE phase 2 negotiations. Most importantly, it displays the configuration of both peers, so that you can pinpoint the problem in case of a mismatch between the IPsec VPN configuration of the peers.

*** Note:**

For more information about logging, see [System logging](#) on page 191.

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

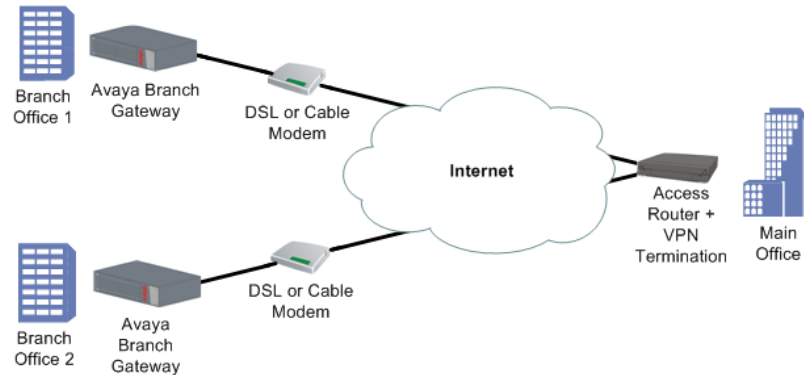
Included in the typical installations, are examples of installing VPN hub and spokes, full or partial mesh, and a hub-and-spoke with VPN for data and VoIP control backup.

Simple VPN topology – VPN hub and spokes

The simple VPN topology consists of several VPN spokes (branch offices) connected via the Internet to the VPN hub (Main Office).

In this topology:

- The Broadband Internet connection uses cable or DSL modem, with a static public IP address
- There is a VPN tunnel from each spoke to the VPN hub over the Internet
- Only VPN traffic is allowed via the Internet connection



Configuring the simple VPN topology

Procedure

1. Configure each branch as follows:
 - The default gateway is the Internet interface
 - VPN policy is configured on the Internet interface egress as follows:
 - Traffic from the local subnets to any IP address is encrypted, using tunnel mode IPSec
 - The remote peer is the Main Office (the VPN Hub)
 - An access control list (ACL) is configured on the Internet interface to allow only the VPN / ICMP traffic. See [Simple VPN topology](#) on page 457 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 504.

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

Table continues...

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 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 Office Main 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
        destination-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 463).
- Maintain a steady transmission of traffic by sending GRE keepalives or employing object tracking.

Prerequisites for dynamic local peer IP

- Specify IKE aggressive mode with the **initiate mode aggressive** command when entering the ISAKMP peer information (see [Configuring ISAKMP peer information](#) on page 442).

```
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 442). 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 448). 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**

- Enter the context of the FastEthernet interface.

For example:

```
Gxxx-001(config)# interface fastethernet 10/3
Gxxx-001(config-if:FastEthernet 10/3)#
```

- 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!
```

- 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 232.

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 512).
- 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 183.

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 442).

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 446.

For example:

```
Gxxx-001# crypto map 1
Gxxx-001(config-crypto:1)# continuous-channel
Done!
```

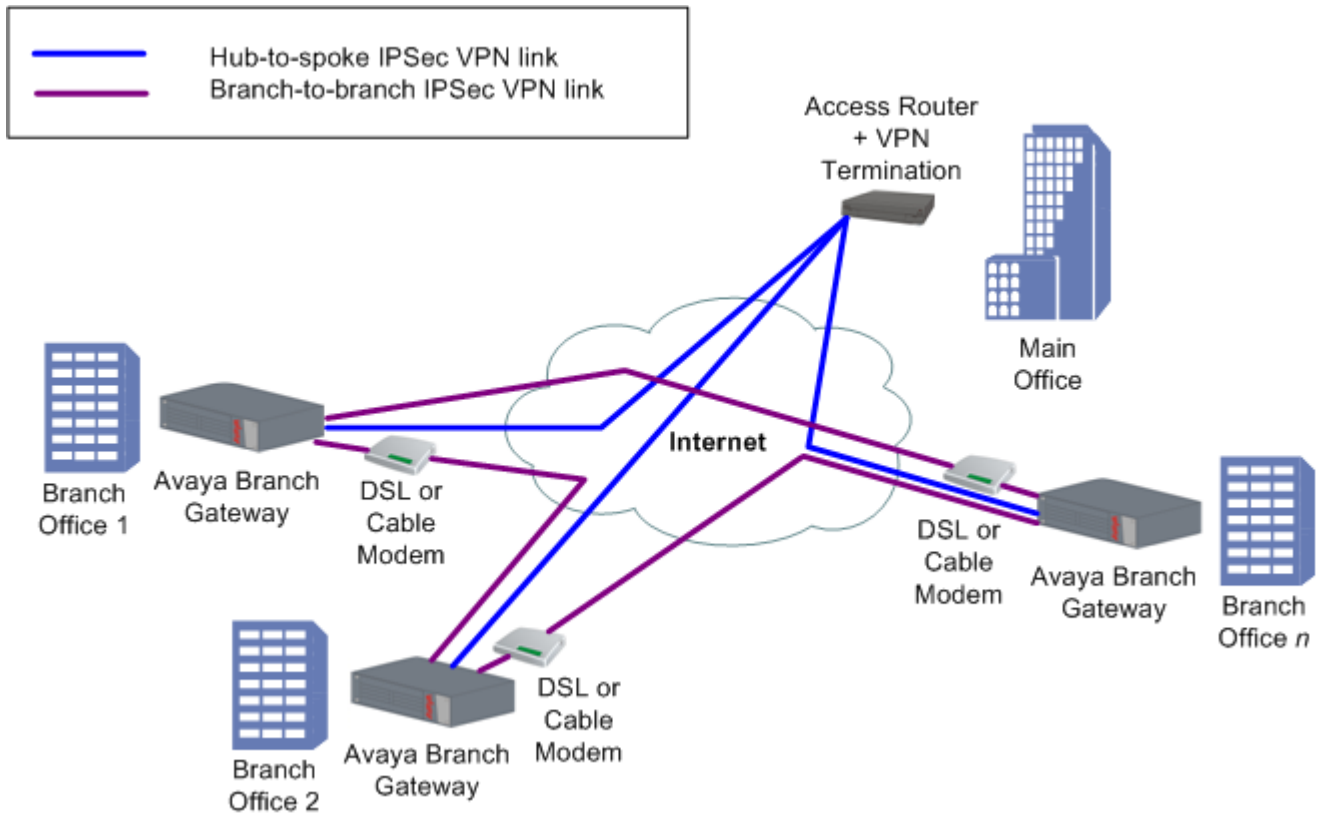
Full or partial mesh

This installation is very similar to the simple hub and spokes installation, but instead of connecting to a single central site, the branch is also connected to several other branch sites by direct IPSec VPN tunnels. The configuration is therefore very similar to the previous one, duplicated several times.

In this topology:

- The Broadband Internet connection uses cable or DSL modem, with a static public IP address
- There is a VPN tunnel from each spoke to the VPN hub over the Internet
- There is a VPN tunnel from one spoke to another spoke
- Only VPN traffic is allowed via the Internet connection

Full or partial mesh diagram



Configuring the mesh VPN topology Procedure

1. Configure Branch Office 1 as follows:
 - The default gateway is the Internet interface
 - VPN policy is configured on the Internet interface egress as follows:
 - Traffic from the local subnets to the second spoke subnets -> encrypt, using tunnel mode IPSec, with the remote peer being the second spoke
 - Traffic from the local subnets to any IP address -> encrypt, using tunnel mode IPSec, with the remote peer being the main office (VPN hub)
 - An access control list (ACL) is configured on the Internet interface to allow only the VPN / ICMP traffic. See step 2 for configuration settings.

*** Note:**

For information about using access control lists, see [Policy lists](#) on page 504.

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 467 for configuration settings.

*** Note:**

For information about using access control lists, see [Policy lists](#) on page 504.

3. Configure the VPN Hub (Main Office) as follows:

- Static routing: Branch subnets -> Internet interface
- The VPN policy portion for the branch is configured as a mirror image of the branch, as follows:
 - Traffic from any IP address to branch local subnets -> encrypt, using tunnel mode IPSec
 - The remote peer is the VPN Spoke (Branch Internet address)

Mesh VPN topology – Branch Office 1

Traffic direction	ACL parameter	ACL value	Description
Ingress	IKE from Main Office IP to Branch IP	Permit	-
Ingress	ESP from Main Office IP to Branch IP	Permit	-
Ingress	IKE from Second Branch IP to Branch IP	Permit	-
Ingress	ESP from Second Branch IP to Branch IP	Permit	-
Ingress	ICMP from any IP address to local tunnel endpoint	Permit	This enables the PMTUD application to work
Ingress	All allowed services from any IP address to any local subnet	Permit	Due to the definition of the VPN Policy, this will be allowed only if traffic comes over ESP
Ingress	Default	Deny	-
Egress	IKE from Branch IP to Main Office IP	Permit	-
Egress	ESP from Branch IP to Main Office IP	Permit	-

Table continues...

Traffic direction	ACL parameter	ACL value	Description
Egress	IKE from Branch IP to Second Branch IP	Permit	This enables the PMTUD application to work
Egress	ESP from Branch IP to Second Branch IP	Permit	This traffic is tunnelled using VPN
Egress	ICMP from local tunnel endpoint to any IP address	Permit	This enables the PMTUD application to work
Egress	All allowed services from any local subnet to any IP address	Permit	This traffic is tunnelled using VPN
Egress	Default	Deny	-

Mesh VPN topology – Branch Office 2

Traffic direction	ACL parameter	ACL value	Description
Ingress	IKE from Main Office IP to Branch IP	Permit	-
Ingress	ESP from Main Office IP to Branch IP	Permit	-
Ingress	IKE from First Branch IP to Branch IP	Permit	-
Ingress	ESP from First Branch IP to Branch IP	Permit	-
Ingress	ICMP from any IP address to local tunnel endpoint	Permit	This enables the PMTUD application to work
Ingress	All allowed services from any IP address to any local subnet	Permit	Due to the definition of the VPN Policy, this will be allowed only if traffic comes over ESP
Ingress	Default	Deny	-
Egress	IKE from Branch IP to Main Office IP	Permit	-
Egress	ESP from Branch IP to Main Office IP	Permit	-
Egress	IKE from Branch IP to First Branch IP	Permit	This enables the PMTUD application to work
Egress	ESP from Branch IP to First Branch IP	Permit	This traffic is tunnelled using VPN
Egress	ICMP from local tunnel endpoint to any IP address	Permit	This enables the PMTUD application to work
Egress	All allowed services from any local subnet to any IP address	Permit	This traffic is tunnelled using VPN
Egress	Default	Deny	-

Mesh VPN topology example

Branch Office 1 configuration

```
crypto isakmp policy 1
  encryption aes
  hash sha
  group 2
  exit
```

```

crypto isakmp peer address <Main Office Public Internet Static IP 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
        destination-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
        destination-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

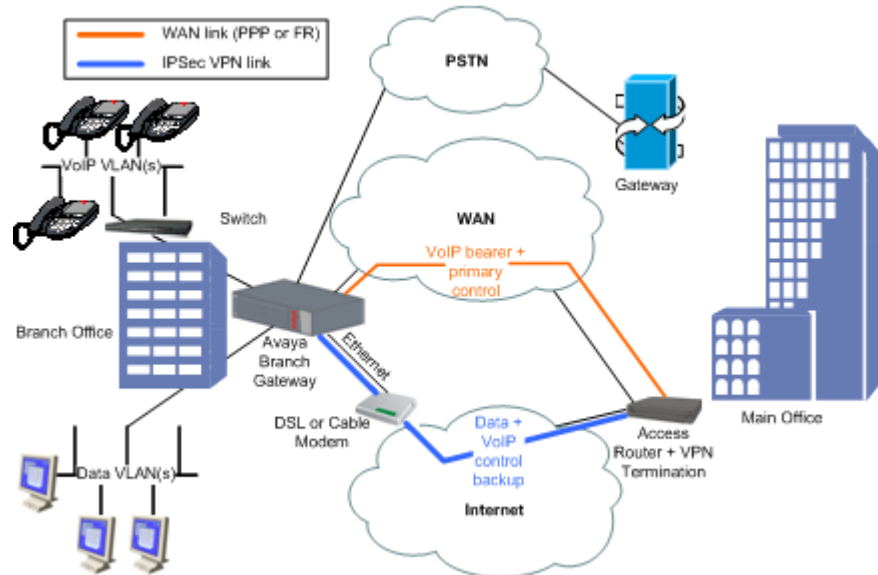
The full solution consists of a hub-and-spoke with VPN for data and VoIP control backup.

In this topology:

- There is a direct WAN connection to the Main Office for VoIP bearer and as primary VoIP control connection.
- The Broadband Internet connection uses cable or DSL modem, with a static public IP address
- There is a VPN tunnel to the hub over the Internet for intranet data, and as backup connection for VoIP control

- The local hosts access the Internet directly through the local broadband connection
- The PSTN connection backs up the voice bearer

Full solution: hub-and-spoke with VPN for data and VoIP control backup



Configuring hub-and-spoke with VPN for data and VoIP control backup Procedure

1. Configure the Branch Office as follows:
 - The default gateway is the Internet interface.
 - VPN policy is configured on the Internet interface egress as follows: Traffic from the local GRE tunnel endpoint to the remote GRE tunnel endpoint > encrypt, using IPSec tunnel mode, with the remote peer being the Main Office.
 - An access control list (ACL) is configured on the Internet interface to allow only the VPN tunnel and ICMP traffic. See [Configuring hub-and-spoke with VPN for data and VoIP control backup](#) on page 474 for configuration settings.

* Note:

For information about using access control lists, see [Policy lists](#) on page 504.

- 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 section.

2. Configure the VPN Hub (Main Office) as follows:

- The VPN policy portion for the branch is configured as a mirror image of the branch
- The ACL portion for the branch is a mirror image of the branch, with some minor modifications
- Static routing is configured as follows:
Branch subnets > Internet interface
- The PBR portion for the branch is configured as follows, on most interfaces:
 - Destination IP = branch VoIP subnets or GW address (PMI), DSCP = bearer > Route: WAN
 - Destination IP = branch VoIP subnets or GW address (PMI), DSCP = control > Route: 1. WAN 2. DBR
- ACM is configured to route voice calls through PSTN when the main VoIP trunk is down.

Hub-and-spoke with VPN

Traffic direction	ACL parameter	ACL value
Ingress	IKE (UDP/500) from remote tunnel endpoint to local tunnel endpoint	Permit
Ingress	ESP/AH from remote tunnel endpoint to local tunnel endpoint	Permit
Ingress	Remote GRE tunnel endpoint to local GRE tunnel endpoint	Permit
Ingress	Allowed ICMP from any IP address to local tunnel endpoint	Permit
Ingress	Default	Deny
Egress	IKE (UDP/500) from local tunnel endpoint to remote tunnel endpoint	Permit
Egress	Local GRE tunnel endpoint to remote GRE tunnel endpoint	Permit
Egress	All allowed services from any local subnet to any IP address	Permit
Egress	Allowed ICMP from local tunnel endpoint to any IP address	Permit
Egress	Default	Deny

Hub-and-spoke with VPN example

```
crypto isakmp policy 1
  encryption aes
  hash sha
  group 2
  authentication pre-share
  exit
crypto isakmp peer address <Main Office Internet public Static IP 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 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 serial 3/1 ip address <Branch Office serial IP address> <Branch Office
serial
                                net mask>      exit
        ip next-hop-list 1      next-hop-interface 1 serial 3/1
        exit
ip next-hop-list 2
    next-hop-interface 1 FastEthernet 10/3      next-hop-interface 2 serial 3/1
    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
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 479), 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 485). 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 490):
 - 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

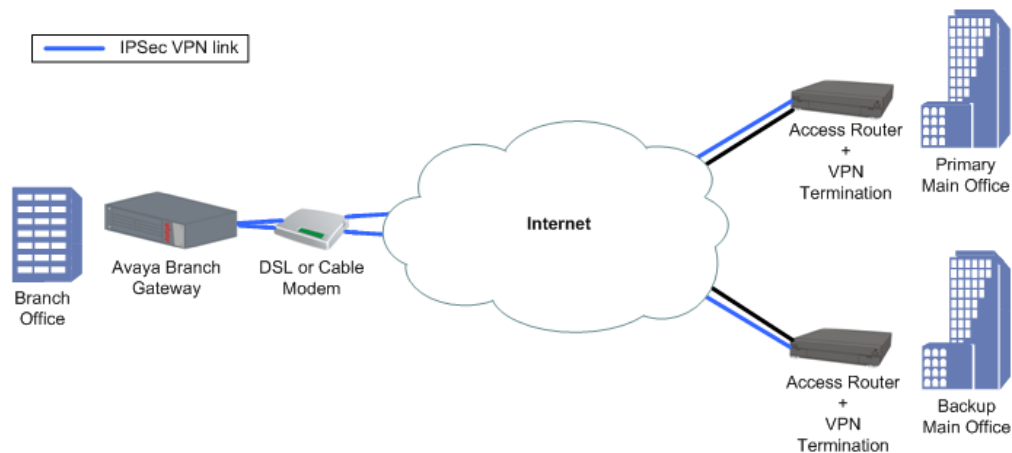
The two GRE tunnels can then be used for branch to Primary/Backup Main Office in either Redundancy or Load sharing mode:

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 481 for configuration settings.

For information about using access control lists, see [Policy lists](#) on page 504.
 - 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-vsuo
        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 Office GRE Tunnel end point IP Address>
255.255.255.255 FastEthernet 10/3 high
ip route <Backup Main Office 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

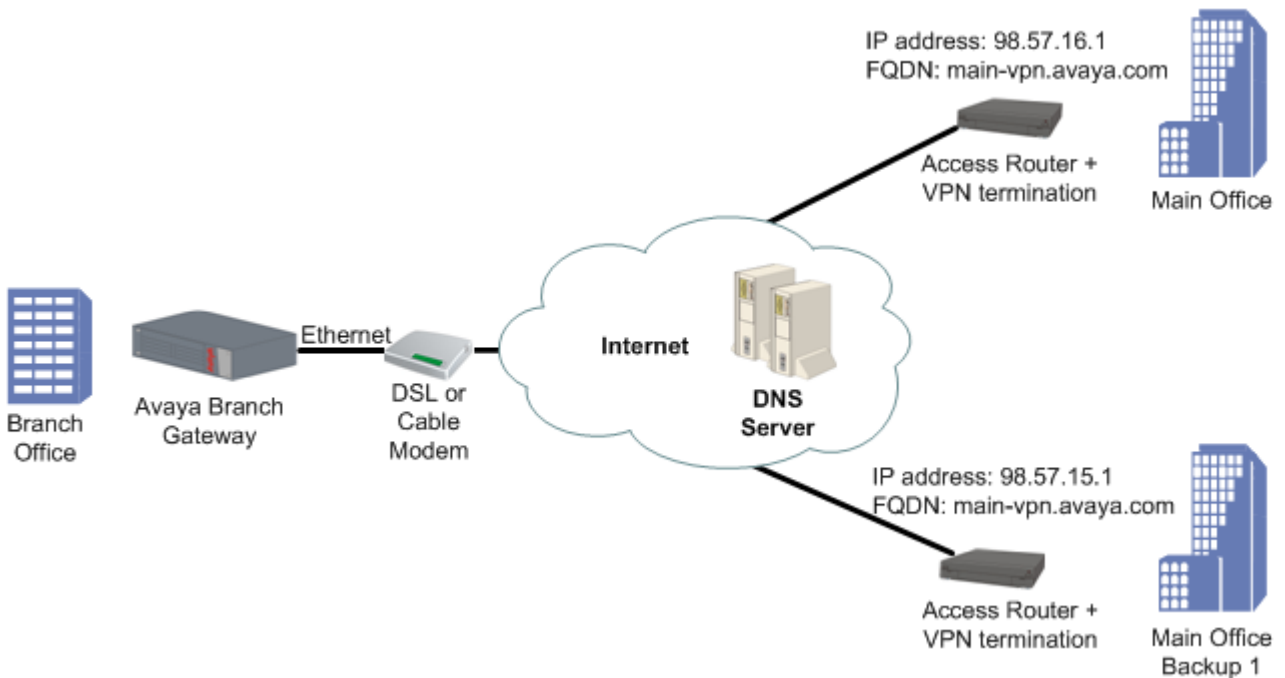
```

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 mask>`. 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

```

```

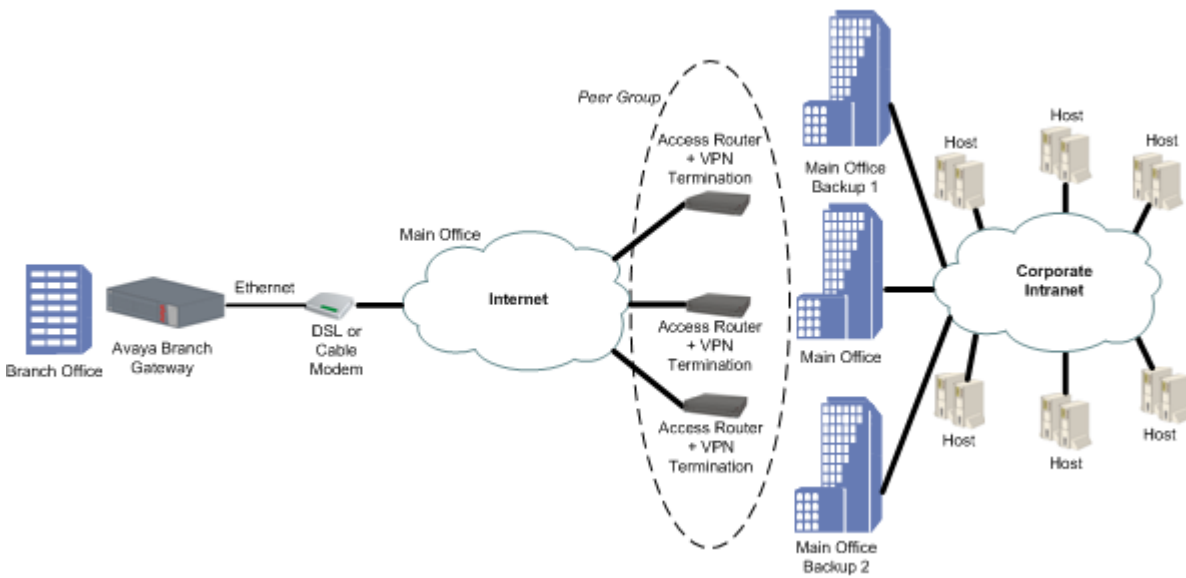
        udp destination-port eq Ike-nat-t-vsu
        composite-operation permit
        exit
    ip-rule 20
        source-ip            any
        destination-ip       any
        ip-protocol          esp
        composite-operation   Permit
        exit
    ip-rule 30
        source-ip            any
        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 263.

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
  icmp-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 interface
!
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	

Table continues...

Parameter	Possible values	Actual value
3. VPN Local IP Address	Type: • Static – If static, provide: IP Address Mask Next-hop Router • Dynamic (DHCP/PPPoE)	
4. Coordinating with the VPN Remote 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		
— 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	

Table continues...

Parameter	Possible values	Actual value
— PFS Group	• no pfs (default) • 1 • 2 • 5 • 14	
— Lifetime seconds	• 120 to 86,400 default: 3,600 (1 hour)	
— Lifetime kilobytes	• 2,560 to 536,870,912 default: 4,608,000 kb • disable	
5. Which packets should be secured		
a. Protect rules matching options	• IP source address • IP destination address	
b. Bypass rules matching options	• IP source address • IP destination address • udp • tcp • dscp • fragment • icmp • IP protocol	
6. The remote peer (crypto isakmp peer) parameters		
a. Remote peer	• IP address • FQDN (dns name)	
b. Pre-shared key	• 1 to 127 alphanumerical characters. 1 to 64 bytes in hexadecimal notation	
7. If the branch IP is dynamic		
	• If the branch IP is an initiator, set initiate mode to none (device is a responder) • If the branch IP is a responder, set initiate mode to aggressive (device is an initiator) • Set self identity to identify the device in the remote peer	

Summary of VPN commands

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

Root level command	First level command	Second level command	Description
<code>clear crypto isakmp</code>			Flush a specific ISAKMP SA or all the ISAKMP SAs
<code>clear crypto sa</code>			Clear all or specific IPsec SAs
<code>clear crypto sa counters</code>			Clear the crypto SA counters
<code>crypto ipsec nat-transparency udp-encapsulation</code>			Re-enable NAT Traversal if it was disabled
<code>crypto ipsec transform-set</code>			Enter the IKE phase 2 (IPsec) transform-set context and create or edit IPsec parameters for the VPN tunnel
	<code>mode</code>		Set security-association lifetime
	<code>set pfs</code>		Specify whether each IKE phase 2 negotiation will employ PFS and, if yes, which Diffie-Hellman group to employ
	<code>set security-association lifetime</code>		Set the IKE phase 2 (IPsec) SA lifetime
<code>crypto isakmp invalid-spi-recovery</code>			Enable invalid SPI recovery (default setting)
<code>crypto isakmp nat keepalive</code>			Re-enable NAT Traversal keepalive if it was disabled, and configure the keepalive interval. This command keeps the NAT devices tables updated.
<code>crypto isakmp peer</code>			Enter the crypto ISAKMP peer context and create or edit an ISAKMP peer
	<code>continuous-channel</code>		Enable continuous-channel IKE, which keeps the IKE phase1 session always up and running, even if there is no traffic
	<code>description</code>		Enter a description for the ISAKMP peer

Table continues...

Root level command	First level command	Second level command	Description
	initiate mode		Specify which IKE Phase-1 mode to use when communicating with the peer: aggressive or none
	isakmp- policy		Set the ISAKMP policy for the ISAKMP peer
	keepalive		Enable DPD keepalives that check whether the remote peer is up
	keepalive- track		Bind an object tracker to a remote VPN peer or to an interface, to check whether the remote peer or the interface is up
	pre-shared- key		Configure the IKE pre-shared key
	self- identity		Set the identity of this device
	suggest-key		Generate a random string which you can use as a pre-shared key for IKE. You must use the same key on both peers.
crypto isakmp peer-group			Enter the crypto ISAKMP peer-group context and create or edit an ISAKMP peer group
	description		Enter a description for the ISAKMP peer group
	set peer		Add a peer to the peer-group
crypto isakmp policy			Enter the crypto ISAKMP policy context and create or edit IKE Phase 1 parameters
	authentication		Set the authentication of ISAKMP policy to pre-shared secret
	description		Enter a description for the ISAKMP policy
	encryption		Set the encryption algorithm for an ISAKMP policy
	group		Set the Diffie-Hellman group for an ISAKMP policy
	hash		Set the hash method for an ISAKMP policy
	lifetime		Set the lifetime of the ISAKMP SA in seconds

Table continues...

Root level command	First level command	Second level command	Description
crypto isakmp suggest-key			Generate a random string which you can use as a pre-shared key for IKE. You must use the same key on both peers.
crypto map			Enter crypto map context and create or edit a crypto map
	continuous-channel		In a crypto ISAKMP peer context, enable continuous-channel IKE, which keeps the IKE phase1 session always up and running, even if there is no traffic
	description		Enter a description for the crypto map
	set dscp		Set the DSCP value in the tunneled packet
	set peer		Attach a peer to a crypto map
	set peer-group		Attach a peer-group to a crypto map
	set transform-set		Configure the transform-set
interface (fastethernet dialer serial vlan)			Enter the FastEthernet, Dialer, Serial, or VLAN interface context
	crypto ipsec df-bit		Set the Don't-Fragment bit to clear mode or copy mode
	crypto ipsec minimal-pmtu		Set the minimal PMTU value that can be applied to an SA when the Branch Gateway participates in PMTUD for the tunnel pertaining to that SA
	ip crypto-group		Activate a crypto list in the context of the interface on which the crypto list is activated
ip crypto-list			Enter crypto list context and create or edit a crypto list
	ip-rule		Enter ip-rule context and create or modify a specific rule
		description	Enter a description for the ip-rule in the ip crypto list

Table continues...

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
show ip active-lists			Display information about a specific policy list or all lists

Table continues...

Root level command	First level command	Second level command	Description
<code>show ip crypto-list</code>			Display all or specific crypto list configurations

Chapter 22: Policy lists

Policy lists enable you to control the ingress and egress of traffic to a router or port. You can use policies to manage security, determine packet priority through an interface, implement quality of service, or determine routing for a specific application or user. Each policy list consists of a set of rules determining the behavior of a packet entering or leaving the interface on which the list is applied.

 Note:

Policy lists are supported on IPv4 only.

Types of policy lists

There are various policy lists on the Branch Gateway, including access control lists, QoS lists, and Policy-based routing.

Access control lists

Access lists include the following:

Global rules: A set of rules that are executed before the list is evaluated.

Rule list: A list of filtering rules that determine the action taken by Branch Gateway. These actions are pointers to the composite operation table.

Actions (composite operation table): A table that describes actions to be performed when a packet matches a rule. The table includes predefined actions, such as permit and deny. To configure more complex rules, see [Composite operations](#) on page 517.

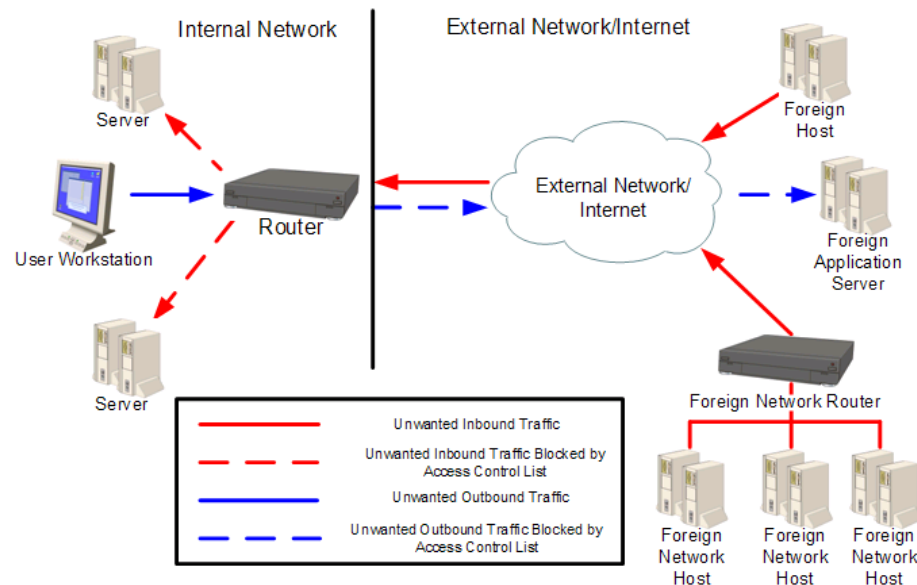
Access control list rule specifications

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 506.

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 517.

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 520.

Allowed values on QoS fields

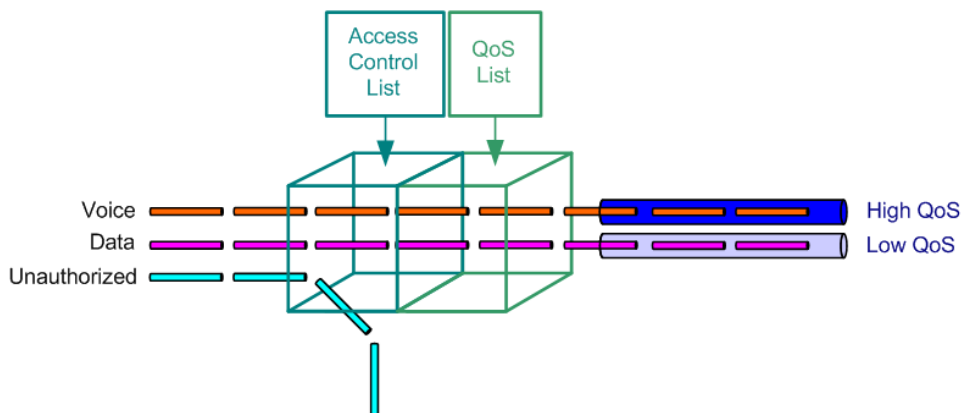
Layer	QoS field	Allowed values
2	802.1p	0–7
3	DSCP	0–63

Use of policy-based routing

You can use policy-based routing to determine the routing path a packet takes based on the type of packet, or the packet's source or destination IP addresses, or its DSCP field. This enables you to route different types of traffic over different routes or interfaces. For example, you use policy-based routing to route voice traffic over a WAN interface and data traffic over the Internet. Policy-based routing is implemented by means of policy-based routing (PBR) lists. PBR lists are similar in many respects to access control lists and QoS lists. However, since there are also some key differences, policy-based routing is explained in a separate chapter. Refer to Policy-based routing section.

Policy list management

You can manage policy lists on the Branch Gateway with CLI commands. You can also manage policy lists throughout your network with Avaya QoS Manager. Avaya QoS Manager is part of Avaya Integrated Management. The following figure illustrates the operation of policy lists on the Branch Gateway:



Policy list configuration

You can create and edit policy lists, and define the list identification attributes. You can also delete an unnecessary policy list.

Creating or editing a policy list

Procedure

To create or edit a list, do one of the following tasks:

- To create or edit a policy list, enter the context of the list.

If the list already exists, you can edit the list from the list context. If the list does not exist, entering the list context creates the list.

- To create or edit an access control list, enter **ip access-control-list** followed by a list number in the range 300-399. The Branch Gateway includes one pre-configured access control list. The pre-configured access control list is list number 300.

For example, to create access control list 301, enter the following command:

```
ip access-control-list 301
```

- To create or edit a QoS list, enter **ip qos-list** followed by a list number in the range 400-499. The Branch Gateway includes one pre-configured QoS list. The pre-configured QoS list is list number 400.

For example, to create a new QoS list 401, enter the following command:

```
ip qos-list 401
```

Creating a list based on an existing list

Procedure

1. To create a new policy list based on an existing list, use the **ip policy-list-copy** command followed by the name of the list from which you want to copy.

The source and destination lists must be of the same type. For example, you cannot copy an access control list to a QoS list.

The following example creates a new access control list, number 340, based on access control list 330. You can then enter the context of access control list 340 to modify it.

```
Gxxx-001(super)# ip policy-list-copy 330 340
Done!
```

2. Once you have entered the list context, you can perform the following actions:

- Configure rules - see [Policy rule configuration](#) on page 512
- Configure composite operations - see [Composite operations](#) on page 517
- Configure DSCP mapping (QoS lists only) - see [DSCP table](#) on page 520

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# <i><listnumber></i> .
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.

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

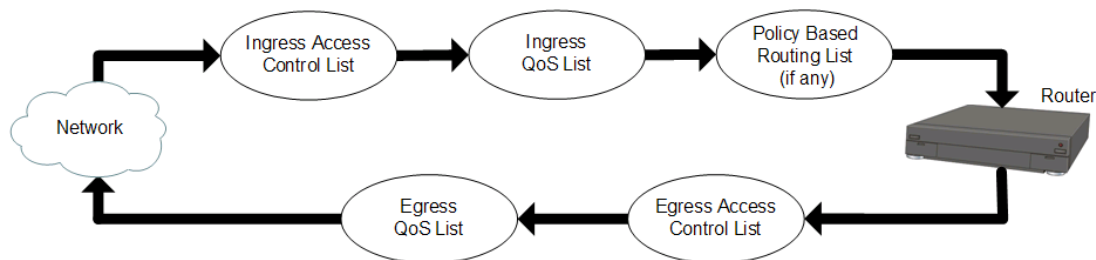
When a packet exits the Branch Gateway through an interface, the Branch Gateway applies the policy lists in the following order:

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 509.

* Note:

If you attach a policy list to a Loopback interface other than Loopback 1, the policy list has no effect.

When you attach a policy list to the Loopback 1 interface, thereby creating a device-wide policy list, and you also attach policy lists to specific interfaces, the Branch Gateway applies the lists in the following order:

- Incoming packets:
 1. Apply the ingress policy lists that are attached to the interface
 2. Apply the device-wide ingress policy lists
- Outgoing packets:
 1. Apply the device-wide egress policy lists
 2. Apply the egress policy lists that are attached to the interface

Defining global rules

About this task

In an access control list, you can define global rules for packets that contain IP fragments and IP options. These rules apply to all packets. This is in contrast to individual rules, which apply to packets that match certain defined criteria. See [Policy rule configuration](#) on page 512.

The Branch Gateway applies global rules before applying individual rules.

Procedure

1. Enter the context of the access control list in which you want to define the rule.
2. Enter one of the following commands, followed by the name of a composite command:
 - **ip-fragments-in**. Applies to incoming packets that contain IP fragments
 - **ip-option-in**. Applies to incoming packets that contain IP options

Result

The composite command can be any command defined in the composite operation list. These commands are case-sensitive. To view the composite operation list for the access control list you are working with, use the command **show composite-operation** in the context of the access control list.

Example

The following example defines a rule in access control list 301 that denies access to all incoming packets that contain IP fragments:

```
Gxxx-001(super)# ip access-control-list 301
Gxxx-001(super/ACL 301)# ip-fragments-in Deny
Done!
```

Policy rule configuration

You can configure policy rules to match packets based on one or more of the following criteria:

- Source IP address, or a range of addresses
- Destination IP address, or a range of addresses
- IP protocol, such as TCP, UDP, ICMP, or IGMP
- Source TCP or UDP port or a range of ports
- Destination TCP or UDP port or a range of ports
- ICMP type and code
- Fragment
- DSCP

Use IP wildcards to specify a range of source or destination IP addresses. The zero bits in the wildcard correspond to bits in the IP address that remain fixed. The one bits in the wildcard

correspond to bits in the IP address that can vary. Note that this is the opposite of how bits are used in a subnet mask.

For access control lists, you can require the packet to be part of an established TCP session. If the packet is a request for a new TCP session, the packet does not match the rule. You can also specify whether an access control list accepts packets that have an IP option field.

Editing and creating rules

About this task

To create or edit a policy rule, you must enter the context of the rule. If the rule already exists, you can edit the rule from the rule context. If the rule does not exist, entering the rule context creates the rule.

Procedure

1. Enter the context of the list in which you want to create or edit a rule.
2. Enter **ip-rule** followed by the number of the rule you want to create or edit.

For example, to create rule 1, enter **ip-rule 1**.

Policy lists rule criteria

Rules work in the following ways, depending on the type of list and the type of information in the packet:

- Layer 4 rules in an access control list with a *Permit* operation are applied to non-initial fragments
- Layer 4 rules in an access control list with a *Deny* operation are not applied to non-initial fragments, and the device continues checking the next IP rule. This is to prevent cases in which fragments that belong to other L4 sessions may be blocked by the other L4 session which is blocked.
- Layer 3 rules apply to non-initial fragments
- Layer 3 rules that include the fragment criteria do not apply to initial fragments or 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

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 523, [Summary of QoS list commands](#) on page 525, 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 519.

Composite operations

A composite operation is a set of operations that the Branch Gateway can perform when a rule matches a packet. Every rule in a policy list has an **operation** field that specifies a composite operation. The **operation** field determines how the Branch Gateway handles a packet when the rule matches the packet.

There are different composite operations for access control list rules and QoS list rules. For each type of list, the Branch Gateway includes a pre-configured list of composite operations. You cannot change or delete pre-configured composite operations. You can define additional composite operations.

Pre-configured composite operations for access control lists

The following table lists the pre-configured entries in the composite operation table for rules in an access control list:

No	Name	Access	Notify	Reset Connection
0	Permit	forward	no trap	no reset
1	Deny	deny	no trap	no reset
2	Deny-Notify	deny	trap all	no reset
3	Deny-Rst	deny	no trap	reset
4	Deny-Notify-Rst	deny	trap all	reset

Each column represents the following:

No: A number identifying the operation

Name: A name identifying the operation. Use this name to attach the operation to a rule.

Access: Determines whether the operation forwards (forward) or drops (deny) the packet

Notify: Determines whether the operation causes the Branch Gateway to send a trap when it drops a packet

Reset Connection: Determines whether the operation causes the Branch Gateway to reset the connection when it drops a packet

Pre-configured composite operations for QoS lists

The following table lists the pre-configured entries in the composite operation table for rules in a QoS list:

No	Name	CoS	DSCP	Trust
0	CoS0	cos0	no change	No
1	CoS1	cos1	no change	No
2	CoS2	cos2	no change	No
3	CoS3	cos3	no change	No
4	CoS4	cos4	no change	No
5	CoS5	cos5	no change	No
6	CoS6	cos6	no change	No
7	CoS7	cos7	no change	No
9	No-Change	no change	no change	No
10	Trust-DSCP	-	-	DSCP
11	Trust-DSCP-CoS	-	-	DSCP and CoS

Each column represents the following:

No: A number identifying the operation

Name: A name identifying the operation. Use this name to attach the operation to a rule.

CoS: The operation sets the **Ethernet IEEE 802.1p CoS:** field in the packet to the value listed in this column

DSCP: The operation sets the **DSCP:** field in the packet to the value listed in this column

Trust: Determines how to treat packets that have been tagged by the originator or other network devices. If the composite operation is set to Trust-DSCP, the packet's CoS tag is set to 0 before the QoS list rules and DSCP map are executed. If the composite operation is set to CoSX, the DSCP map is ignored, but the QoS list rules are executed on the **Ethernet IEEE 802.1p CoS** field. (For example, the composite operation CoS3 changes the **CoS** field to 3.) If the composite operation is set to Trust-DSCP-CoS, the operation uses the greater of the CoS or the DSCP value. If the composite operation is set to No Change, the operation makes no change to the packet's QoS tags.

Configuring composite operations

About this task

You can configure additional composite operations for QoS lists. You can also edit composite operations that you configured. You cannot edit pre-configured composite operations.

Note:

You cannot configure additional composite operations for access control lists, since all possible composite operations are pre-configured.

Procedure

1. Enter the context of a QoS list.
2. Enter **composite-operation** followed by an index number.

The number must be 12 or higher, since numbers 1 through 11 are assigned to 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 519.

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 518.

QoS rules on the list take precedence over the DSCP table. If a QoS rule other than the default matches the packet, the Branch Gateway does not apply the DSCP table to the packet. The Branch Gateway applies only the operation specified in the QoS rule.

Changing an entry in the DSCP table

Procedure

1. Enter the context of a QoS list.
2. Enter **dscp-table** followed by the number of the DSCP value for which you want to change its composite operation.
3. Enter **composite-operation** followed by the name of the composite operation you want to execute for packets with the specified DSCP value.

Result

The following commands specify the pre-configured composite operation CoS5 for DSCP table entry 33 in QoS list 401. Every packet with DSCP equal to 33 is assigned CoS priority 5.

```
Gxxx-001# ip qos-list 401
Gxxx-001(QoS 401)# dscp-table 33
Gxxx-001(QoS 401/dscp 33)# composite-operation CoS5
Done!
```

The following commands create a new composite operation called dscp5 and assign the new composite operation to DSCP table entry 7 in QoS list 402. Every packet with DSCP equal to 7 is assigned a new DSCP value of 5.

```
Gxxx-001(super)# ip qos-list 402
Gxxx-001(super/QoS 402)# composite-operation 12
Gxxx-001(super/QoS 402/CompOp 12)# name dscp5
Done!
Gxxx-001(super/QoS 402/CompOp 12)# dscp 5
Done!
Gxxx-001(super/QoS 402/CompOp 12)# cos No-Change
Done!
Gxxx-001(super/QoS 402/CompOp 12)# exit
Gxxx-001(super/QoS 402)# dscp-table 7
Gxxx-001(super/QoS 402/dscp 7)# composite-operation dscp5
Done!
```

Composite operation dscp5 changes the mapping of packets entering the router with a DSCP values of 7. DSCP value 5 is most likely to be mapped to a different CoS, making these packets subject to a different set of behavioral rules.

Policy list displays and tests

To verify access control lists, QoS lists, and policy-based routing (PBR) lists, you can view the configuration of the lists. You can also test the effect of the lists on simulated IP packets.

Policy list commands in context

When viewing information about policy lists and their components, these commands produce different results in different contexts.

- In general context:
 - **show ip access-control-list**. Displays a list of all configured access control lists, with their list numbers and owners
 - **show ip access-control-list list number detailed**. Displays all the parameters of the specified access control list
 - **show ip qos-list**. Displays a list of all configured QoS lists, with their list numbers and owners
 - **show ip qos-list detailed**. Displays all the parameters of the specified QoS list.

- In ip access-control-list context:
 - **show composite-operation**
 - **show ip-rule**. Displays a list of all rules configured for the list
 - **show list**. displays the parameters of the current list, including its rules
- In ip access-control-list/ip-rule context:
 - **show composite-operation**. Displays the parameters of the composite operation assigned to the current rule
 - **show ip-rule**. Displays the parameters of the current rule
- In ip qos-list context:
 - **show composite-operation**. Displays a list of all composite operations configured for the list
 - **show dscp-table**. Displays the current list's DSCP table
 - **show ip-rule**. Displays a list of all rules configured for the list
 - **show list**. Displays the parameters of the current list, including its rules
- In ip qos-list/ip-rule context:
 - **show composite-operation**. Displays the parameters of the composite operation assigned to the current rule
 - **show dscp-table**. Displays the current list's DSCP table
 - **show ip-rule**. Displays the parameters of the current rule
- In ip 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 G450 CLI Reference*.

Example

For example, the following command simulates the effect of applying QoS list number 401 to a packet entering Branch Gateway through interface VLAN 2:

```
Gxxx-001(if:VLAN 2)# ip simulate 401 in CoS1 dscp46 10.1.1.1
10.2.2.2 tcp 1182 20
```

When you use the **ip simulate** command, the Branch Gateway displays the effect of the policy rules on the simulated packet. For example:

```
Gxxx-001(super-if:VLAN 2)# ip simulate 401 in CoS1 dscp46 10.1.1.1
10.2.2.2 tcp 1182 20
Rule match for simulated packet is the default rule
Composite action for simulated packet is CoS6
New priority value is fwd6
Dscp value is not changed
```

Simulated packet properties

- CoS priority is 1
- DSCP is 46
- source IP address is 10.1.1.1
- destination IP address is 10.2.2.2
- IP protocol is TCP
- source TCP port is 1182
- destination TCP port is 20

Summary of access control list commands

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

Root level command	Command	Command	Description
interface {dialer loopback fastethernet tunnel vlan}			Enter the Dialer, Loopback, FastEthernet, Tunnel or VLAN interface configuration context
	ip access-group		Activate a specific Access Control list, for a specific direction, on the current interface
	ip simulate		Test the action of a policy on a simulated packet

Table continues...

Root level command	Command	Command	Description
	show ip access-control-list		Display the attributes of a specific access control list or of all access control lists on the current interface
ip access-control-list			Enter configuration mode for the specified policy access control list, and create the list if it does not exist
	cookie		Set the cookie for the current list
	ip-fragments-in		Specify the action taken on incoming IP fragmentation packets for the current access control list
	ip-option-in		Specify the action taken on incoming packets carrying an IP option for the current access control list
	ip-rule		Enter configuration mode for a specified policy rule or, if the rule doesn't exist, create it and enter its configuration mode
		composite-operation	Assign the specified composite operation to the current rule
		destination-ip	Apply the current rule to packets with the specified destination IP address
		dscp	Apply the current rule to packets with the specified DSCP value
		fragment	Apply the current rule for non-initial fragments only
		icmp	Apply the current rule to a specific type of ICMP packet
		ip-protocol	Apply the current rule to packets with the specified IP protocol
		show composite-operation	Display the parameters of the composite operation assigned to the current rule
		show ip-rule	Display the attributes of the current rule
		source-ip	Apply the current rule to packets from the specified source IP address

Table continues...

Root level command	Command	Command	Description
		<code>tcp destination-port</code>	Apply the current rule to TCP packets with the specified destination port
		<code>tcp established</code>	Apply the current rule only to packets that are part of an established TCP session
		<code>tcp source-port</code>	Apply the current rule to TCP packets from ports with specified source port
		<code>udp destination-port</code>	Apply the rule to UDP packets with the specified destination port
		<code>udp source-port</code>	Apply the rule to UDP packets from the specified source port
	<code>name</code>		Assign a name to the current list
	<code>owner</code>		Specify the owner of the current list
	<code>show composite-operation</code>		Display the composite operations configured for the list
	<code>show ip-rule</code>		Display the rules configured for the current list attributes of a specific rule
	<code>show list</code>		Display the attributes of the current list, including its rules
<code>ip policy-list-copy</code>			Copy an existing policy list to a new list
<code>show ip access-control-list</code>			Display the attributes of a specific access control list or of all access control lists

Summary of QoS list commands

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

Root level command	Command	Command	Description
interface {dialer loopback fastethernet tunnel vlan}			Enter the Dialer, Loopback, FastEthernet, Tunnel, or VLAN interface configuration context
	ip qos-group		Activate a specific QoS list, for a specific direction, on the current interface
	ip simulate		Test the action of a policy on a simulated packet
	show ip qos-list		Display the attributes of a specific QoS list or all QoS lists for the current interface
ip policy-list-copy			Copy an existing policy list to a new list
ip qos-list			Enter configuration mode for the specified QoS list, and create the list if it does not exist
	composite-operation		Enter the configuration mode for one of the current list's composite operations
		cos	Set the CoS priority value for the current composite operation
		dscp	Set the DSCP value for the current composite operation
		name	Assign a name to the current composite operation
		show composite-operation	Display the attributes of the current composite operation
	cookie		Set the cookie for the current list
	dscp-table		Enter the DSCP table entry context for a particular DSCP value for the current QoS list
		composite-operation	Specify the composite operation to execute for packets with the specified DSCP value
		name	Assign a name to the current DSCP table entry
		show dscp-table	Display the parameters of the current DSCP table entry

Table continues...

Root level command	Command	Command	Description
	ip-rule		Enter configuration mode for a specified policy rule or, if the rule does not exist, create it and enter its configuration mode
		composite-operation	Assign the specified composite operation to the current rule
		destination-ip	Apply the current rule to packets with the specified destination IP address
		dscp	Apply the current rule to packets with the specified DSCP value
		fragment	Apply the current rule for non-initial fragments only
		icmp	Apply the current rule to a specific type of ICMP packet
		ip-protocol	Apply the current rule to packets with the specified IP protocol
		show composite-operation	Display the parameters of the composite operation assigned to the current rule
		show dscp-table	Display the current list's DSCP table
		show ip-rule	Display the attributes of the current rule
		source-ip	Apply the current rule to packets from the specified source IP address
		tcp destination-port	Apply the current rule to TCP packets with the specified destination port
		tcp source-port	Apply the current rule to TCP packets from ports with specified source port
		udp destination-port	Apply the rule to UDP packets with the specified destination port
		udp source-port	Apply the rule to UDP packets from the specified source port
	name		Assign a name to the current list
	owner		Specify the owner of the current list

Table continues...

Root level command	Command	Command	Description
	<code>pre-classification</code>		Specify which priority tag the current QoS list uses for data flows
	<code>show composite-operation</code>		Display all composite operations configured for the list
	<code>show dscp-table</code>		Display the current list's DSCP table
	<code>show ip-rule</code>		Display the rules configured for the current list attributes of a specific rule
	<code>show list</code>		Display the attributes of the current list, including its rules
<code>show ip qos-list</code>			Display the attributes of a specific QoS list or all QoS lists

Chapter 23: Policy-based routing

Policy-based routing

Policy-based routing enables you to configure a routing scheme based on traffic's source IP address, destination IP address, IP protocol, and other characteristics. You can use policy-based routing (PBR) lists to determine the routing of packets that match the rules defined in the list. Each PBR list includes a set of rules, and each rule includes a next hop list. Each next hop list contains up to 20 next hop destinations to which the Branch Gateway sends packets that match the rule. A destination can be either an IP address or an interface.

Policy-based routing takes place only when the packet enters the interface, not when it leaves. Policy-based routing takes place after the packet is processed by the Ingress Access Control List and the Ingress QoS list. Thus, the PBR list evaluates the packet after the packet's DSCP field has been modified by the Ingress QoS List. See [Policy lists to packets](#) on page 509.

 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 258.

 Note:

Policy-based routing is supported on IPv4 only.

Policy-based routing only operates on routed packets. Packets traveling within the same subnet are not routed, and are, therefore, not affected by policy-based routing.

The Loopback interface is a logical interface which handles traffic that is sent to and from the Branch Gateway itself. This includes ping packets to or from the Branch Gateway, as well as Telnet, SSH, FTP, DHCP Relay, TFTP, HTTP, NTP, SNMP, H.248, and other types of traffic. The Loopback interface is also used for traffic to and from analog and DCP phones connected to the device via IP phone entities.

The Loopback interface is always up. You should attach a PBR list to the Loopback interface if you want to route specific packets generated by the Branch Gateway to a specific next-hop.

Unlike the case with other interfaces, PBR lists on the Loopback interface are applied to packets when they leave the Branch Gateway, rather than when they enter.

Certain types of packets are not considered router packets (on the Loopback interface only), and are, therefore, not affected by policy-based routing. These include RIP, OSPF, VRRP, GRE, and keepalive packets. On the other hand, packets using SNMP, Telnet, Bootp, ICMP, FTP, SCP, TFTP, HTTP, NTP, and H.248 protocols are considered routed packets, and are, therefore, affected by policy-based routing on the Loopback interface.

Chapter 24: Synchronization

If the Branch Gateway contains an MM710 T1/E1 media module, it is advisable to define the MM710 as the primary synchronization source for the Branch Gateway. In so doing, clock synchronization signals from the Central Office (CO) are used by the MM710 to synchronize all operations of the Branch Gateway. ISDN BRI trunks Media Modules (MM721, MM722) can also use signals from the Central Office, to synchronize all operations of the Branch Gateway.

Where traditional synchronization is not available, you can use Clock Synchronization over IP (CSolP). CSolP to provide timing information across IP networks. CSolP is also needed to support TDM-based devices, such as an H.320 video device, that customers would retain and transmit within an IP infrastructure. Use the CM SAT Administration forms to administer Synchronization over IP.

The relevant screens are the following:

- **change system features** to enable the synchronization over the IP feature
- **change media gateway** <n> to enable synchronization over IP for the gateway.
- **change synchronization media-gateway** <n> to configure synchronization sources on the gateway

Defining a clock source

Procedure

To define a potential clock source (T1/E1 Media Module, ISDN-BRI), run the following command:

```
set sync interface primary|secondary mmID portID,
```

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 port number. You can set up multiple ports. For example, v2 1, 3, and 5-8.

Note:

The port ID parameter only applies if the source is a BRI module.

Setting the clock source to primary, normal failover occurs. The identity of the current synchronization source is not stored in persistent storage. Persistent storage is used to preserve the parameters set by this command.

 Note:

Setting the source to secondary overrides normal failover, generates a trap, and asserts a fault. Thus, it is only recommended to set the clock source to secondary for testing purposes.

Setting the synchronization source

Procedure

To determine which reference source is the active source, use the `set sync source primary|secondary` command.

If you choose secondary, the secondary source becomes active, and the primary source goes on standby. In addition, fallback to the primary source does not occur even when the primary source becomes available.

Result

If neither primary nor secondary sources are identified, the local clock becomes the active source.

Example

The following example sets the MM710 media module located in slot 2 of the Branch Gateway chassis as the primary clock synchronization source for the Branch Gateway.

```
set sync interface primary v2
set sync source primary
```

If the Branch Gateway includes a second MM710 media module, enter the following command:

```
set sync interface secondary v3
set sync source secondary
```

If, for any reason, the primary MM710 media module cannot function as the clock synchronization source, the system uses the MM710 media module located in slot 3 of the Branch Gateway chassis as the clock synchronization source. If neither MM710 media module can function as the clock synchronization source, the system defaults to the local clock running on the chassis.

Disassociating a clock source

Procedure

To disassociate an interface previously specified as the primary or secondary clock synchronization source, enter `clear sync interface primary` or `clear sync interface secondary`.

Enabling and disabling automatic failover and failback

Procedure

To enable or disable automatic failover and failback between designated primary and secondary synchronization sources, enter **set sync switching enable** or **set sync switching disable**.

Synchronization status

The yellow ACT LED on the front of the MM710 media module displays the synchronization status of that module.

- If the yellow ACT LED is solidly on or off, it has not been defined as a synchronization source. If it is on, one or more channels is active. If it is an ISDN facility, the D-channel counts as an active channel and causes the yellow ACT LED to be on.
- When the MM710 is operating as a clock synchronization source, the yellow ACT LED indicates that the MM710 is the clock synchronization source by flashing at three second intervals, as follows:
 - The yellow ACT LED is on for 2.8 seconds and off for 200 milliseconds if the MM710 media module has been specified as a clock synchronization source and is receiving a signal that meets the minimum requirements for the interface
 - The yellow ACT LED is on for 200 milliseconds and off for 2.8 seconds if the MM710 media module has been specified as a synchronization source and is not receiving a signal, or is receiving a signal that does not meet the minimum requirements for the interface

Displaying synchronization status

Procedure

Enter **show sync timing** to display the status of the local and remote primary, secondary, and local clock sources.

The status can be Active, Standby, or Not Configured. The status is Not Configured when a source has not been defined, for example, when there are no T1 cards installed.

Example

```
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 G450 CLI Reference*.

Command	Description
clear sync interface	Disassociate a previously specified interface as the primary or secondary clock synchronization source
set sync interface	Define the specified module and port as a potential source for clock synchronization for the Branch Gateway
set sync source	Specify which clock source is the active clock source. The identity of the current synchronization source is not stored in persistent storage.
set sync switching	Toggle automatic sync source switching
show sync timing	Display the status of the primary, secondary, and local clock sources

Chapter 25: TLS / Certificate Management

TLS

Avaya recommends TLS protocol for H.248 communications between Branch Gateway and Communication Manager. The Branch Gateway SLA Monitor Agent also uses TLS to communicate with the SLA Monitor Server and Avaya Diagnostic Server (ADS).

To use TLS with Communication Manager, set the **link-encryption** type on Communication Manager and Branch Gateway.

On Communication Manager, you can specify whether to use TLS for H.248 communication. Selecting **tls-only** restricts the TLS communication use, whereas when you select **any**, Communication Manager can use TLS or PTLS. Avaya recommends TLS as it is more secure, whereas PTLS is an older proprietary protocol that older gateway releases used before introducing TLS.

Similarly, using the **set link-encryption** CLI command, the administrator can specify the link-encryption type the gateway uses. When using this command, ensure that at least one TLS version is enabled and that Communication Manager supports the selected version. By default, the gateway has TLS version 1.2 enabled. Only TLS 1.2 is supported when FIPS mode is enabled.

For more information on TLS administration, see *Administering Avaya Aura® Communication Manager* and *Avaya Aura® G450 Branch Gateway CLI Reference*.

TLS certificate stores

The Gateway maintains two certificate stores to hold TLS CA and Identity certificates for the following applications:

- **h248reg**: Used for H.248 Media Gateway TLS communication with Communication Manager operating in the following modes:
 - Enterprise: The default mode of the gateway in which the gateway operates with the local enterprise IP address and is connected to the Communication Manager.
 - Edge: Media Gateway uses h248reg certificate store to set up a TLS connection with Avaya SBC. Edge gateway mode operates with the NATed IP address.

Media Gateway uses this connection to send the H.248 signaling messages to Avaya SBC H.248 proxy server application, which forwards the messages to Communication Manager.

In the Edge gateway mode, MGSBC management link uses h248reg certificate store and TCP port 2946 to create a TLS connection with Avaya SBC.

- **sla:** For providing diagnostic information to the SLA Monitor Server.
- **syslog:** For syslog certificates.
- **web:** For HTTPS data transfers to and from web servers.

 Note:

The HTTP or HTTPS upload and download commands use the web trust store. For more information about the HTTPS commands, see *Avaya Branch Gateway G430 CLI Reference* and *Avaya Branch Gateway G450 CLI Reference*.

 Note:

TLS connections can only be established if valid certificates are installed on both the gateway and the server it communicates with. Specifically, TLS communication on the gateway requires the following:

- A CM Identity certificate must be installed on Communication Manager, and a corresponding CM CA certificate must be installed on the Gateway.
- To use SLA Monitor Agent, a SLA Monitor Server Identity certificate must be installed on the SLA Monitor Server and a corresponding SLA Monitor CA certificate must be installed on the Gateway.
- When the gateway is operating in the Edge mode and therefore connected to Avaya SBC, it is recommended to use an identity certificate.
- If an Identity certificate is installed on the Gateway, a corresponding Gateway CA certificate must be installed on CM.

 Note:

A Gateway Identity certificate needs to be installed if mutual authentication is set to **Required** on the Communication Manager Media Gateway form.

The commands used to copy, show, and erase certificates on the Gateway are provided through the Gateway CLI interface. For more information, see *Avaya Branch Gateway G430 CLI Reference* and *Avaya Branch Gateway G450 CLI Reference*.

The forms and commands used to copy, show, and erase certificates on CM and the ADS SLA Monitor Server are available in their corresponding administration guides.

Monitoring Certificate Expiration shall be extended to include the user provided certificates in the Web Trust store as follows:

- When the certificate expiration date reaches 60 days before expiration, Media Gateway shall raise a minor trap alarm.
- When the certificate expiration date is reached, Media Gateway shall raise a major trap alarm.

Certificate validation

The gateway provides a variety of options for certificate validation, including Common Name Validation, Subject Alternate Name validation, and the degree of Certificate Revocation checking to be performed using CRLs and/or OCSP.

For more information about the types of certificate validation that can be enabled on the gateway, see *Avaya Aura® G430 Branch Gateway CLI Reference* and *Avaya Aura® G450 Branch Gateway CLI Reference*.

Mutual authentication

Mutual Authentication is required when Media Gateway is operating in the Edge mode and is connected to Avaya SBC.

Requiring mutual authentication sets a condition where both CM and the gateway are required to exchange and validate each other's identity certificates.

The **Mutual Authentication** field on the **Communication Manager Media Gateway** form supports the following keyword options:

- Optional
- Required

Avaya recommends administrators to select the **Required** option because it provides a higher degree of security. If **Optional** is selected, and no identity certificate is loaded in the gateway's H248 application directory; CM establishes a TLS connection without the gateway having to offer an identity certificate. For more information, see *Administering Avaya Aura® Communication Manager*.

Chapter 26: Federal Information Processing Standards (FIPS)

Federal Information Processing Standards

Federal Information Processing Standards (FIPS) are a set of publicly announced standards developed by the National Institute of Standards and Technology (NIST) that describe document processing, encryption algorithms and other information technology standards for use within non-military government agencies and by government contractors and vendors who work with the agencies.

G430 or G450 gateways with FIPS approved mode enabled will operate as a FIPS 140-2 Cryptographic Module (Level 1) if and only if your organization complies with all policies defined in the following Security Policy publications:

- Avaya G430 FIPS 140-2 Cryptographic Module Security Policy
- Avaya G450 FIPS 140-2 Cryptographic Module Security Policy

These documents are later referred in this administration guide as the “Security Policy”.

Strict adherence to the Security Policy is necessary to assure FIPS 140-2 compliance. Therefore, it is recommended that you do not enable FIPS approved mode until the Security Policy has been completely read and its requirements fully understood.

FIPS Security Level of the Cryptographic Module

The gateway’s cryptographic module meets the overall requirements applicable to Level 1 security of FIPS 140-2. The following are security rules enforced by the cryptographic module to implement the security requirements of this FIPS 140-2 Level 1 module:

1. When entering or exiting FIPS-140-2 approved mode, the gateway will be zeroized. Zeroization will erase the entire existing gateway configuration including Critical Security Parameters (CSPs) and the gateway will return to its factory default settings.
2. The cryptographic module performs Power up Self-Tests (POST) to confirm that it can reliably perform FIPS compliant operations. These include:
 - Non-Volatile Random-Access Memory (NVRAM) Integrity Tests
 - Electronically Erasable Programmable Read Only Memory (E2PROM) Integrity Tests

- Cryptographic algorithm Tests
 - Gateway Software/Firmware Integrity Tests
 - Digital Signal Processor (DSP) Power Up Self-Tests (POST)
 - Critical Functions Tests
 - Conditional Self-Tests
3. Users can instruct the module to perform the power-up self-tests at any time by executing the **reset** CLI command or by power cycling the gateway.
 4. Prior to each use, the internal entropy source is tested using FIPS 140-2 approved conditional tests.
 5. Data output is inhibited at power-up during self-tests, zeroization, and error states.
 6. When the gateway is in FIPS approved mode, the gateway's cryptographic module will only provide FIPS approved algorithms and the gateway will be FIPS compliant provided that all policies described in the Security Policy are strictly adhered to.

Determining FIPS Certified Firmware is installed

Procedure

To determine if the cryptographic module of the gateway has FIPS certified firmware installed in both Bank A and Bank B, run the following command:

```
show image version
```

Both gateway firmware banks must be running a FIPS-approved firmware version to be considered FIPS-compliant.

To verify that the version(s) you have installed is certified for FIPS 140-2 compliance, see the *Certificate Module Validation Program (CMVP)* lists on the NIST website at <http://www.nist.gov>.

FIPS Approved Mode of Operation

When the gateway is in FIPS approved mode, the gateway's cryptographic module will only provide FIPS approved algorithms and the gateway will be FIPS compliant provided that all policies described in the Security Policy are strictly adhered to.

When not in FIPS approved mode, the gateway's cryptographic module may provide both approved and unapproved algorithms and the gateway may freely operate in non-FIPS-compliant ways.

Details of the algorithms used in both FIPS approved and unapproved modes are described in the Security Policy.

Prerequisites for entering FIPS Approved Mode

- User type – Cryptographic Officer with administration privileges. For example, root.
- FIPS-approved Media Gateway hardware. G430 or G450 Version 3.0.x or higher.
- FIPS-approved Media Gateway firmware.
- Strict adherence to all policies described in the following publications:
 - Avaya G430 FIPS 140-2 Cryptographic Module Security Policy
 - Avaya G450 FIPS 140-2 Cryptographic Module Security Policy

To verify that the version(s) you have installed is certified for FIPS 140-2 compliance, see the *Certificate Module Validation Program (CMVP)* lists on the NIST website at <http://www.nist.gov>.

Determining FIPS Approved Mode is enabled

Procedure

To determine whether FIPS approved mode is enabled or disabled, run the following command:

```
show fips-mode
```

Determining Configuration is FIPS Compliant

Both gateway firmware banks must be running a FIPS-approved firmware version to be considered FIPS-compliant. To determine if the cryptographic module of the gateway has FIPS certified firmware, run the **show image version** command and verify that both Bank A and Bank B have FIPS-approved firmware versions installed.

To verify that the version(s) you have installed is certified for FIPS 140-2 compliance, see the *Certificate Module Validation Program (CMVP)* lists on the NIST website at <http://www.nist.gov>.

Before enabling FIPS approved mode, the **show fips-mode** command will attempt to detect whether any non-FIPS compliant CLI commands are configured. This can help identify whether any configured CLI commands will automatically be disabled when FIPS approved mode is enabled.

In the example below, the **show fips-mode** command reveals that FIPS approved mode is disabled and that PTLS link encryption for H.248 registration with CM will not be allowed if FIPS approved mode were to be enabled.

```
G4xx(super)# show fips-mode
FIPS Mode: Disabled
These configuration settings are not FIPS-compliant and
will be automatically disabled if FIPS-mode is enabled:
  set link-encryption h248reg ptls yes
```

Be aware that the **show fips-mode** command might not detect all non-compliant configurations. Therefore, the Security Policy must be always used as the definitive source for determining whether a configuration is FIPS compliant.

Backup and restore of Gateway configuration

Backup configuration can only be restored to a gateway that is in the same mode as the one on which the backup is taken. The following rules apply when you backup or restore configuration :

- Backup made in non-FIPS approved mode can only be restored to a gateway in non-FIPS approved mode.
- Backup made in FIPS approved mode can only be restored to the same gateway.
- In addition, backup made in FIPS approved mode can no longer be restored if the **nvram init** or **zeroize** CLI commands are executed, or if FIPS approved mode is disabled at any time after the backup has been made.

Avaya™ recommends that you obtain a complete copy of the gateway's current running configuration before enabling or disabling FIPS approved mode.

For more information about the **backup** and **restore** commands, see *Avaya Branch Gateway G430 CLI Reference* and *Avaya Branch Gateway G450 CLI Reference*.

Before Enabling or Disabling FIPS Approved Mode

Before enabling or disabling FIPS approved mode, it is recommended that you keep a complete copy of the gateway's current running configuration. The gateway's current running configuration can be viewed by executing the following command:

- **show running-config**

Alternatively, the **running-config** command made be saved to an external text file for later viewing by using one of the following commands:

- **copy running-config ftp <destination_file_name> <ip_address>**
- **copy running-config tftp <destination_file_name> <ip_address>**
- **copy running-config scp <destination_file_name> <ip_address>**

This can be especially helpful when enabling or disabling FIPS approved mode since the gateway configuration will not be able to be restored from a backup made in a different mode.

Enabling FIPS Approved Mode

Procedure

To enable the FIPS Approved Mode, run the following CLI command:

- `set fips-mode enable`

Note:

When FIPS approved mode is first enabled, the gateway's existing configuration will be erased and replaced with a basic configuration that is FIPS compliant. The basic FIPS compliant configuration must then be further customized as needed.

Maintaining FIPS Approved Mode

It is imperative that you consult the Security Policy before changing any gateway configuration.

When changing the gateway's configuration via CLI commands, an error or warning will be issued any time a command is entered that is not FIPS compliant. The "show fips-mode" CLI command may be used to verify whether FIPS approved mode is currently enabled. The command will also attempt to detect whether any non-compliant CLI commands are currently configured. However, the Security Policy must be used as the definitive source for FIPS compliance since not all non-compliant configurations may be detected.

Disabling FIPS Approved Mode

Procedure

To disable FIPS Approved Mode, run the following CLI command:

- `set fips-mode disable`

Note:

When FIPS approved mode is first disabled, the gateway's existing configuration will be erased and replaced with a basic configuration. The basic configuration must then be further customized as needed.

Administration procedures

Administration procedures consist of the commands required to enable or disable FIPS approved mode, limitations and the prerequisites. It also includes failure scenarios and repair actions.

FIPS-related CLI commands

- `set fips-mode`
- `show fips-mode`
- `show image version`

For a full description of these commands, see *Avaya Branch Gateway G430 CLI Reference* and *Avaya Branch Gateway G450 CLI Reference*.

Non-compliant CLI Commands in FIPS Approved Mode

The following CLI commands are not permitted in FIPS approved mode:

Command name	Syntax
CHAP	<code>ppp chap</code>
Link Encryption for H.248 Registration (Proprietary TLS)	<code>set link-encryption h248reg ptls</code>
Master Key	<code>key config-key password-encryption</code>
OSPF	<code>router ospf</code>
PAP	<code>ppp pap</code>
PPP	• <code>encapsulation pppoe</code> • <code>interface USB-Modem</code> • <code>interface console</code> • <code>interface Serial</code> • <code>ppp</code>
RADIUS	<code>set radius authentication enable</code>
RIP	<code>router rip</code>
SLA Monitor for Avaya Diagnostic Server (ADS)	<code>set sla-monitor enable</code>
SLS	<code>set sls enable</code>
SNMPv1 and SNMPv2	• <code>set snmp-community</code> • <code>snmp-server remote-user <username> <engineID> <group-name> auth md5</code> • <code>snmp-server remote-user <username> <engineID> <group-name> auth sha priv des56</code> • <code>snmp-server user <username> <group-name> v1</code> • <code>snmp-server user <username> <group-name> v2c</code>
Telnet Client	<code>ip telnet-client</code>
Telnet Server	<code>ip telnet</code>

Table continues...

Command name	Syntax
Telnet Services	<code>ip telnet-services</code>
VPN (IPSEC)	• <code>crypto ipsec</code> • <code>crypto isakmp</code> • <code>crypto map</code> • <code>ip crypto-list</code> • <code>vpn hw</code> • <code>vpn init</code> • <code>vpn memory</code> • <code>vpn monitor</code> • <code>vpn policy</code> • <code>vpn report</code> • <code>vpn show</code>

For a full description of these commands, see *Avaya Branch Gateway G450 CLI Reference* guide.

 Note:

Details about non-compliant CLI commands can be found in the Security Policy.

Warnings for unencrypted communication in FIPS Approved Mode

Although the following commands are all FIPS-compliant, a warning is given and confirmation is requested if any of the following CLI commands are executed while in FIPS approved mode:

- `set link-encryption h248reg unencrypted yes`
- `set link-encryption h248reg all yes`
- `set allow-unencrypted rtp yes`

In addition, the `show fips-mode` command indicates a warning if any of the above commands are enabled. The warning is given to alert the user that an unsecure form of communication is requested.

For a full description of these commands, see *Avaya Branch Gateway G430 CLI Reference* and *Avaya Branch Gateway G450 CLI Reference*.

Enabling FIPS Approved Mode

About this task

The gateway's current configuration will be zeroized anytime FIPS Approved Mode is enabled or disabled.

Procedure

1. Log in to the gateway using a user login account that has administrative privileges.

For example:

```
Login:root
Password: ****
Password accepted
```

 Note:

The gateway's serial console or IP services port can be used when logging onto the gateway to enable FIPS mode. This way FIPS related test results and error states that occur during boot-up can be viewed when the gateway attempts to first enter FIPS mode. The gateway's serial console or IP services port is also required to login to the gateway for the first time after FIPS approved mode is enabled because the zeroization that accompanies the enabling of FIPS mode erases all network configuration.

2. Verify that both firmware banks contain FIPS-approved firmware images using the **show image version** command as shown below.

To verify that the version(s) you have installed is certified for FIPS 140-2 compliance, see the *Certificate Module Validation Program (CMVP)* lists on the NIST website at <http://www.nist.gov>.

```
G4xx-001(super)# show image version
Bank      Version
-----
A          39.27.0
B (current) 41.9.0
```

 Note:

Banks that do not have a FIPS-approved firmware image must be upgraded.

3. To review the impact FIPS Approved Mode will have on the existing configuration, run the **show fips-mode** command as shown below.

```
G4xx(super)# show fips-mode

FIPS Mode:  Disabled

These configuration settings are not FIPS-compliant and
will be automatically disabled if FIPS-mode is enabled:
  set link-encryption h248reg unencrypted yes
  set allow-unencrypted rtp yes
```

4. Run the **show running-config** command and make a copy of its output since the current gateway configuration will be erased after FIPS approved mode is enabled.

```
G4xx(super)# show running-config
```

 Note:

Alternatively, the gateway's current running configuration can be saved to an external text file for later viewing by using the **copy running-config** command.

5. Run the **set fips-mode enable** command to enable FIPS mode as shown below.

```
G4xx(super)# set fips-mode enable

WARNING: This Gateway will be ZEROIZED and RESET if you continue to enable FIPS
mode.
Do you want to continue (Y/N)? Y

Enabling FIPS Mode.

The Gateway will now be Zeroized and Reset...
```

6. The gateway will reset and perform a variety of FIPS related Power On Self Tests (POST) as shown below.

```
FIPS POST TEST - STARTED

NVRAM POST Integrity Test OK
E2PROM POST Integrity Test OK
FIPS Object Module POST Started
    Integrity Test OK
    DRBG AES-256-CTR DF Test OK
    DRBG AES-256-CTR Test OK
    Digest SHA1 Test OK
    Digest SHA1 Test OK
    Digest SHA1 Test OK
    Digest SHA256 Test OK
    Digest SHA256 Test OK
    Digest SHA256 Test OK
    Digest SHA512 Test OK
    Digest SHA512 Test OK
    Digest SHA512 Test OK
    HMAC SHA1 Test OK
    HMAC SHA224 Test OK
    HMAC SHA256 Test OK
    HMAC SHA384 Test OK
    HMAC SHA512 Test OK
    Cipher AES-128-ECB Test OK
    GCM Test OK
    Cipher DES-EDE3-ECB Test OK
    Cipher DES-EDE3-ECB Test OK
    Signature RSA 2048 SHA256 PKCS#1 Test OK
    Signature RSA 3072 SHA256 PKCS#1 Test OK
    Signature ECDSA P-256 Test OK
    Signature ECDSA P-384 Test OK
    Signature ECDSA P-521 Test OK
FIPS Object Module POST Success
SW/FW POST Integrity Test OK
VoIP DSP0 FIPS POST Started
    Core0 AES Test OK
    Core0 HMAC Test OK
    Core0 SHA1 Test OK
    Core1 AES Test OK
    Core1 HMAC Test OK
    Core1 SHA1 Test OK
    Core2 AES Test OK
    Core2 HMAC Test OK
    Core2 SHA1 Test OK
    Core3 AES Test OK
    Core3 HMAC Test OK
    Core3 SHA1 Test OK
VoIP DSP0 FIPS POST Success
VoIP DSP1 FIPS POST Started
    Core0 AES Test OK
    Core0 HMAC Test OK
```

```

Core0 SHA1 Test OK
Core1 AES Test OK
Core1 HMAC Test OK
Core1 SHA1 Test OK
Core2 AES Test OK
Core2 HMAC Test OK
Core2 SHA1 Test OK
Core3 AES Test OK
Core3 HMAC Test OK
Core3 SHA1 Test OK
VoIP DSP1 FIPS POST Success
Generating RSA key, This command may take a few minutes...
.....
Key was created!
Key version: SSH2, RSA
Key Fingerprint: SHA256:X31EqBa0+ikMUASGS0zbFVcjFUCkKzw+U30GYY/aI/o

FIPS POST TEST - COMPLETED

Enabling External Data Ports

```

7. After verifying successful completion of the Power-On Self Tests (POST), the Cryptographic Officer must log in to the gateway using the root login account and default root password as shown below.

```

G450 Login: root
Password: ****
Response accepted

Password accepted

```

 Note:

The root user login can be initially used after enabling FIPS approved mode since all other administrative accounts are deleted during zeroization.

8. The Cryptographic Officer must change the root password from the default password to a new, more secure password as shown below.

```

Enter new password:
Confirm new password:

```

9. The Cryptographic Officer must confirm whether Enhanced Access Security Access (EASG) is to be enabled or disabled as shown below.

```

*****
Enhanced Access Security Gateway (EASG) Confirmation.
*****
Please confirm whether Avaya is granted login access to this system.
You may change this setting any time after confirmation is completed.

Enable EASG:
By enabling Avaya Logins you are granting Avaya access to your system.
This is necessary to maximize the performance and value of your Avaya support
entitlements, allowing Avaya to resolve product issues in a timely manner.

In addition to enabling the Avaya Logins, this product should be registered
with Avaya and technically onboarded for remote connectivity and alarming.
Please see the Avaya support site (support.avaya.com/registration) for
additional information for registering products and establishing remote
access and alarming.

Disable EASG:

```

```

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

Enter 1 to Enable EASG or 2 to Disable EASG? 2

You have requested Avaya Logins be Disabled.
Do you want to continue (Y/N)? Y

Avaya Logins have been Disabled.

```

10. If you use the Gateway Configuration script to complete basic configuration of the gateway complete the required process as shown below. The gateway will then reset.

```

--- Gateway Configuration Script ---
The script will provide you basic gateway connectivity configuration.
Configuration Script - do you want to continue (Y/N)? Y

Default settings are in square brackets '[]'.
Vlan [1] :
IPv4 Enabled (Y/N)? [Y] :

IPv4 address [169.254.0.2] :172.16.1.230
IPv4 Subnet mask [255.255.255.0] :255.255.254.0
IPv4 Default gateway [172.16.1.1] :172.16.1.254
IPv6 Enabled (Y/N)? [N] :

MGC controllers [0.0.0.0] :172.16.1.168
Hostname [G430] :G430
Enable Spanning Tree on LAN ports (Y/N/Help)? [Y] :

The following parameters are about to be configured:
Vlan : 1
IPv4 address : 172.16.1.230
Subnet mask : 255.255.254.0
Default gateway : 172.16.1.254
MGC controllers : 172.16.1.168
Hostname : G430
Spanning Tree Protocol : enabled
The gateway will save those parameters in startup-config and then reset
- do you want to continue (Y/N)? Y

Please connect your gateway to the network via any Ethernet port
Saving configuration...
Resetting the device...

```

11. The Cryptographic Officer must log in to the gateway using a user login account that has administrative privileges as shown below.

```

Login: root
Password: ****
Password accepted

```

12. Run the **show fips-mode** command to verify if FIPS-mode and any non-recommended commands are enabled as shown below.

```

G4xx(super)# show fips

FIPS Mode: Enabled

```

13. Run the **username** command to define new user logins for Crypto-officer, administrators, and users as required.

```

G4xx(super)# username crypto-officer access-type admin
Enter new password: *****

```

```
Confirm password : *****
User account added.
```

14. Run the **show username** command to verify the successful addition of users.

```
G4xx-???(super)# show username
User          Access  Account  Active
account              level      type
-----
root            admin     local    yes
crypto-officer  admin     local    yes
```

15. To define SNMPv3 parameters for SNMPv3 users, run **auth sha priv aes128**.

```
G4xx-001(super)# snmp-server user fips_snmp_user v3ReadWriteG v3 auth sha priv
aes128
Enter authentication password : *****
Confirm authentication password : *****
Enter privacy password : *****
Confirm privacy password : *****
Done!
```

 Note:

Other combinations of auth-type and priv-type are not permitted in FIPS approved mode.

16. If you have saved a copy of your previous configuration before enabling FIPS approved mode, refer to it now to perform any additional configuration as needed. For more information, see [Configuration changes and backup](#) on page 27.

 Note:

When changing the gateway's configuration using CLI commands, the system displays an error or warning, if the entered command is not FIPS compliant. However, it is important that you consult the Security Policy when making changes to the gateway configuration to ensure FIPS compliance.

Disabling FIPS Approved Mode

About this task

The gateway's current configuration will be zeroized anytime FIPS Approved Mode is enabled or disabled.

Procedure

1. The Cryptographic Officer must log in to the gateway using a user login account that has administrative privileges.

For example:

```
Login:root
Password: ****
Password accepted
```

 Note:

The gateway's serial console or IP services port can be used when logging onto the gateway to disable FIPS mode. The gateway's serial console or IP services port is required to login to the gateway for the first time after FIPS approved mode is disabled because the zeroization that accompanies the disabling of FIPS mode erases all network configuration.

2. Run the **set fips-mode disable** command to disable FIPS mode.

```
G4xx(super)# set fips-mode disable

WARNING: This Gateway will be ZEROIZED and RESET if you continue to disable FIPS
mode.
Do you want to continue (Y/N)? Y

Disabling FIPS Mode.

The Gateway will now be Zeroized and Reset...
```

3. The gateway will reset and perform a variety of FIPS related Power On Self Tests (POST) as shown below.

```
FIPS POST TEST - STARTED

NVRAM POST Integrity Test OK
E2PROM POST Integrity Test OK
FIPS Object Module POST Started
    Integrity Test OK
    DRBG AES-256-CTR DF Test OK
    DRBG AES-256-CTR Test OK
    Digest SHA1 Test OK
    Digest SHA1 Test OK
    Digest SHA1 Test OK
    Digest SHA256 Test OK
    Digest SHA256 Test OK
    Digest SHA256 Test OK
    Digest SHA512 Test OK
    Digest SHA512 Test OK
    Digest SHA512 Test OK
    HMAC SHA1 Test OK
    HMAC SHA224 Test OK
    HMAC SHA256 Test OK
    HMAC SHA384 Test OK
    HMAC SHA512 Test OK
    Cipher AES-128-ECB Test OK
    GCM Test OK
    Cipher DES-EDE3-ECB Test OK
    Cipher DES-EDE3-ECB Test OK
    Signature RSA 2048 SHA256 PKCS#1 Test OK
    Signature RSA 3072 SHA256 PKCS#1 Test OK
    Signature ECDSA P-256 Test OK
    Signature ECDSA P-384 Test OK
    Signature ECDSA P-521 Test OK
FIPS Object Module POST Success
SW/FW POST Integrity Test OK
VoIP DSP0 FIPS POST Started
    Core0 AES Test OK
    Core0 HMAC Test OK
    Core0 SHA1 Test OK
    Core1 AES Test OK
    Core1 HMAC Test OK
```

```

Core1 SHA1 Test OK
Core2 AES Test OK
Core2 HMAC Test OK
Core2 SHA1 Test OK
Core3 AES Test OK
Core3 HMAC Test OK
Core3 SHA1 Test OK
VoIP DSP0 FIPS POST Success
VoIP DSP1 FIPS POST Started
Core0 AES Test OK
Core0 HMAC Test OK
Core0 SHA1 Test OK
Core1 AES Test OK
Core1 HMAC Test OK
Core1 SHA1 Test OK
Core2 AES Test OK
Core2 HMAC Test OK
Core2 SHA1 Test OK
Core3 AES Test OK
Core3 HMAC Test OK
Core3 SHA1 Test OK
VoIP DSP1 FIPS POST Success
Generating RSA key, This command may take a few minutes...
.....
Key was created!
Key version: SSH2, RSA
Key Fingerprint: SHA256:X31EqBa0+ikMUASGS0zbFVcjFUCkKzw+U3OGYY/aI/o

FIPS POST TEST - COMPLETED

Enabling External Data Ports

```

4. After verifying successful completion of the Power-On Self Tests (POST), the Cryptographic Officer must log in to the gateway using the root login account and default root password as shown below.

```

G4xx Login: root
Password: ****
Response accepted

Password accepted

```

 Note:

Only the root user login can be initially used after disabling FIPS approved mode since all other administrative accounts are deleted during zeroization.

5. The Cryptographic Officer must change the root password from the default password to a new, more secure password as shown below.

```

Enter new password:
Confirm new password:

```

6. The Cryptographic Officer must confirm whether Enhanced Access Security Access (EASG) is to be enabled or disabled as shown below.

```

*****
Enhanced Access Security Gateway (EASG) Confirmation.
*****
Please confirm whether Avaya is granted login access to this system.
You may change this setting any time after confirmation is completed.

Enable EASG: (Recommended)

```

By enabling Avaya Logins you are granting Avaya access to your system. This is necessary to maximize the performance and value of your Avaya support entitlements, allowing Avaya to resolve product issues in a timely manner.

In addition to enabling the Avaya Logins, this product should be registered with Avaya and technically onboarded for remote connectivity and alarming. Please see the Avaya support site (support.avaya.com/registration) for additional information for registering products and establishing remote access and alarming.

Disable EASG:

By disabling Avaya Logins you are preventing Avaya access to your system. This is not recommended, as it impacts Avaya's ability to provide support for the product. Unless the customer is well versed in managing the product themselves, Avaya Logins should not be disabled.

Enter 1 to Enable EASG (Recommended) or 2 to Disable EASG? 1

You have requested Avaya Logins be Enabled.

Do you want to continue (Y/N)? Y

Avaya Logins have been Enabled.

7. If you use the Gateway Configuration script to complete basic configuration of the gateway complete the required process as shown below. The gateway will then reset.

--- Gateway Configuration Script ---

The script will provide you basic gateway connectivity configuration.

Configuration Script - do you want to continue (Y/N)? Y

Default settings are in square brackets '[]'.

Vlan [1] :

IPv4 Enabled (Y/N)? [Y] :

IPv4 address [169.254.0.2] :172.16.1.230

IPv4 Subnet mask [255.255.255.0] :255.255.254.0

IPv4 Default gateway [172.16.1.1] :172.16.1.254

IPv6 Enabled (Y/N)? [N] :

MGC controllers [0.0.0.0] :172.16.1.168

Hostname [G430] :G430

Enable Spanning Tree on LAN ports (Y/N/Help)? [Y] :

The following parameters are about to be configured:

Vlan : 1

IPv4 address : 172.16.1.230

Subnet mask : 255.255.254.0

Default gateway : 172.16.1.254

MGC controllers : 172.16.1.168

Hostname : G430

Spanning Tree Protocol : enabled

The gateway will save those parameters in startup-config and then reset

- do you want to continue (Y/N)? Y

Please connect your gateway to the network via any Ethernet port

Saving configuration...

Resetting the device...

8. The Cryptographic Officer must log in to the gateway using a user login account that has administrative privileges as shown below.

Login: root

Password: ****

Password accepted

9. Run the **show fips-mode** command to verify if FIPS-mode is disabled.

```
G4xxG4xx(super)# show fips
FIPS Mode: Disabled
```

10. Run the **username** command to define new user logins for Cryptographic officer, administrators and users as shown below.

```
G450(super)# username crypto-officer access-type admin
Enter new password: *****
Confirm password : *****
User account added.
```

11. Run the **show username** command to verify the successful addition of users as shown below.

```
G4xx-??? (super)# show username
```

User account	Access level	Account type	Active
-----	-----	-----	-----
root	admin	local	yes
crypto-officer	admin	local	yes

12. If you have saved a copy of your previous configuration before disabling FIPS approved mode, refer to it to perform any additional configuration as needed. For more information, see [Configuration changes and backup](#) on page 27.

FIPS Error States and LED Status Indicators

The CPU, ALM, MDM, and PWR LED lamps on the gateway's faceplate provide status and error states during power-up self-tests. Status messages and error states may also be viewed on a monitor using the G450 Branch Gateway's serial console port.

Power-up Testing

When the Module is performing Power-up Self-Test, the LED states will be as follows:

- CPU LED: flashing
- ALM LED: on

If FIPS power-up testing completes successfully, the System CPU and ALM LEDs will resume their normal operational state:

- CPU LED: on
- ALM LED: off

If Power-up Self-Test does not complete successfully, the Module will reset and enter the **Error State 1** or **Error State 3** depending on the nature of the failure.

Error States

The gateway's cryptographic module defines three Error States which may be entered due to hard or soft operational failures. Upon entering an Error State, the System CPU and ALM LED lamps will indicate the type of failure by providing a unique pattern of flashing and/or steadily lit lamps on the LEDS of the gateway's faceplate. Additionally, G450 Branch Gateway has a serial console port that allows one to view status and error states using a monitor.

Error State 1

Error State 1 processes hard errors due to failures of the Module's Power-up Self-Tests. Exit is via operator selection of reboot or zeroization with reboot.

LED flash patterns:

- MDM: continuous ON 15 seconds, OFF 15 seconds
- ALM: continuous ON-OFF flash
- CPU: continuous cycles of two ON-OFF flashes separated by 2.25s OFF
- PWR: on if all power supplies are healthy, flashing otherwise

Error State 2

Error State 2 processes soft errors related to conditional self-test failures. Exit is through automatic reboot.

LED flash patterns:

- MDM: on
- ALM: continuous on-off flash
- CPU: continuous cycles of three on-off flashes
- PWR: on if all power supplies are healthy, flashing otherwise

Error State 3

Error State 3 processes hard errors linked to critical function failures. Exit is automatic with immediate zeroization.

LED flash patterns:

- MDM: on
- ALM: continuous on-off flashes
- CPU: continuous cycles of four on-off flashes
- PWR: on if all power supplies are healthy, flashing otherwise

Zeroization Status during Error State 1

When the user is given the option to zeroize as a result of being in Error State 1, the CPU and ALM LEDs will indicate this using the following unique pattern:

- CPU LED: 2 blinks

- ALM LED: flashing

For a 2-hour period, the MDM LED will alternate on and off in 15 second intervals to indicate whether zeroization will occur when the reset button is pressed.

1. MDM LED On: Zeroize and Reset
2. MDM LED Off: Reset only

After 2 hours, the MDM LED will remain off and the user will no longer be given the option to zeroize using the reset button. However, G450 Branch Gateway users may also use the serial console port to select the appropriate action.

Chapter 27: Resources

Branch Gateway documentation

The following table lists the documents related to Branch Gateway. Download the documents from the Avaya Support website at <http://support.avaya.com>.

Title	Description	Audience
Installing and implementing		
<i>Quick Start for Hardware Installation: Avaya G450 Branch Gateway</i>	Describes how to install G450 Branch Gateway in the basic configuration.	Solution architects, implementation engineers, and support personnel
<i>Deploying and Upgrading Avaya G450 Branch Gateway</i>	Describes how to install and upgrade G450 Branch Gateway, perform basic configuration tasks, insert media modules, and connect external devices.	Solution architects, implementation engineers, and support personnel
Administering		
<i>Administering Avaya G450 Branch Gateway</i>	Describes how to configure and manage G450 Branch Gateway after the installation. Contains the detailed information about G450 Branch Gateway features and their implementation.	Solution architects, implementation engineers, and support personnel
<i>Avaya Branch Gateway G450 CLI Reference</i>	Describes the CLI commands for G450 Branch Gateway configuration.	Solution architects, implementation engineers, and support personnel
<i>Avaya Aura® G450 Data Privacy Guidelines</i>	Describes how to administer G450 Branch Gateway to fulfill Data Privacy requirements.	Solution architects, implementation engineers, and support personnel

Finding documents on the Avaya Support website

Procedure

1. Go to <https://support.avaya.com>.
2. To log in, click **Sign In** at the top of the screen and then enter your login credentials when prompted.

3. Click **Product Support > Documents**.
4. In **Search Product**, start typing the product name and then select the appropriate product from the list displayed.
5. In **Select Release**, select the appropriate release number.
This field is not available if there is only one release for the product.
6. **(Optional)** In **Enter Keyword**, type keywords for your search.
7. From the **Select Content Type** list, select one or more content types.
For example, if you only want to see user guides, click **User Guides** in the **Select Content Type** list.
8. Click  to display the search results.

Accessing the port matrix document

Procedure

1. Go to <https://support.avaya.com>.
2. To log in, click **Sign In** at the top of the screen and then enter your login credentials when prompted.
3. Click **Product Support > Documents**.
4. In **Select Release**, select the appropriate release number.
This field is not available if there is only one release for the product.
5. From the **Select Content Type** list, select one or both of the following options:
 - **Application & Technical Notes**
 - **Design, Development & System Mgt**

Avaya Documentation Center navigation

For many programs, the latest customer documentation is available on the Avaya Documentation Center website at <https://documentation.avaya.com>. Some functionality is only available when you log in to the Avaya Documentation Center. The available functionality depends on your role.

Important:

If the documentation you are looking for is not available on the Avaya Documentation Center, you can find it on the [Avaya Support website](#).

While navigating through the Documentation Center, you can click the **Avaya Documentation Center** logo at the top of the screen to return to the home page anytime. On the Avaya Documentation Center, you can do the following:

- Click **Avaya Links** in the top menu bar to access other Avaya websites, including the Avaya Support website.

- Click **Languages** (🌐) in the top menu bar to change the display language and view localized documents.
- In the **Search Documentation** field, search for keywords and click **Filter** to filter by solution category, product, or user role.
You can select multiple items in each filter category. For example, you can select a product and multiple user roles.
- Click **Library** in the top menu bar to access the complete library of documents. Use the filtering options to refine your results.
- After performing a search or accessing the library, you can sort content on the search results page. When you find the item you want to view, click it to open it.
- Use the table of contents in a document for navigation. You can also click < or > next to the document title to navigate to the previous topic or the next topic.
- Click **Share** (➦) to share a topic by email or copy the URL.
- Download a PDF of the current topic in a document, the topic and its subtopics, or the entire document.
- Print the section you are viewing.
- Add content to a collection by clicking **Add to My Topics** (📁). You can add the topic and its subtopics or add the entire publication.
- View the topics in your collections. To access your collections, click your name in the top menu bar and then click **My Topics**.

You can do the following:

- Create, rename, and delete a collection.
 - Set a collection as the default or favorite collection.
 - Save a PDF of the selected content in a collection and download it to your computer.
 - Share content in a collection with others through email.
 - Receive collections that others have shared with you.
- Click **Watch** (👁) to add a topic to your watchlist so you are notified when the content is updated or removed.
 - View and manage your watchlist by clicking **Watchlist** from the top menu with your name.

You can do the following:

- Enable **Email notifications** to receive email alerts.
 - Unwatch the selected content or all topics.
- Send feedback for a topic.

Training

The following courses are available on the Avaya Learning website at <http://www.avaya-learning.com>. After logging in to the website, enter the course code or the course title in the **Search** field and press **Enter** or click **>** to search for the course.

Course code	Course title
70380W	What's New with Avaya Aura® 10.2
70390W	Upgrading to Avaya Aura® 10.2
70410W	Migrating to ASP R6.0.x (KVM on RHEL 8.10) Hypervisor
71301V	Integrating Avaya Aura® Communications Applications
72301V	Supporting Avaya Aura® Communications Applications
20460W	Virtualization and Installation Basics for Avaya Team Engagement Solutions
71201V	Integrating Avaya Aura® Core Components
72201V	Supporting Avaya Aura® Core Components
61131V	Administering Avaya Aura® System Manager
61451V	Administering Avaya Aura® Communication Manager

Viewing Avaya Mentor videos

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

About this task

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

- To find videos on the Avaya Support website, go to <https://support.avaya.com/> and do one of the following:
 - In **Search**, type `Avaya Mentor Videos`, click **Clear All** and select **Video** in the **Select Content Type**.
 - In **Search**, type the product name. On the Search Results page, click **Clear All** and select **Video** in the **Select Content Type**.

The **Video** content type is displayed only when videos are available for that product.

In the right pane, the page displays a list of available videos.

- To find the Avaya Mentor videos on YouTube, go to www.youtube.com/AvayaMentor and do one of the following:
 - Enter a keyword or keywords in the **Search Channel** to search for a specific product or topic.

- Scroll down Playlists, and click a topic name to see the list of videos available. For example, Contact Centers.

 Note:

Videos are not available for all products.

Support

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

Appendix A: Traps and MIBs

Branch Gateway traps

Name	Parameters (MIB variables)	Class	Msg Facility	Severity	Trap Name / Mnemonic	Format	Description
coldStart		STD	Boot	Warning	coldStart	Agent Up with Possible Changes (coldStart Trap) enterprise:\$E (\$e) args(\$#):\$*	A coldStart trap indicates that the entity sending the protocol is reinitializing itself in such a way as to potentially cause the alteration of either the agent's configuration or the entity's 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 and the entity's implementation intact.
LinkUp	ifIndex, ifAdminStat us,	STD	System	Warning	LinkUp	Agent Interface Up (linkUp Trap)	A linkUp trap indicates that the entity

Table continues...

Name	Parameters (MIB variables)	Class	Msg Facility	Severity	Trap Name / Mnemonic	Format	Description
	ifOperStatus					enterprise:\$E (\$e) on interface \$1	sending the protocol recognizes that one of the communication links represented in the agent's configuration has come up. The data passed with the event is 1) The name and value of the ifIndex instance for the affected interface. The name of the interface can be retrieved via an snmpget of 1.3.6.1.2.1.2.2.1.2.INST, where INST is the instance returned with the trap.
linkDown	ifIndex, 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 the agent's configuration.

Table continues...

Name	Parameters (MIB variables)	Class	Msg Facility	Severity	Trap Name / Mnemonic	Format	Description
							The data passed with the event is 1) The name and value of the ifIndex instance for the affected interface. The name of the interface can be retrieved via an snmpget of 1.3.6.1.2.1.2.2.1.2.INST, where INST is the instance returned with the trap.
SNMP_Authen_Failure		P330	SECURITY	Notification	authentication Failure	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, alarmSample Type, alarmValue, alarmRising Threshold	RMON	THRESHOLD	Warning	rising Alarm	Rising Alarm: \$2 exceeded threshold \$5; value = \$4. (Sample type = \$3; alarm index = \$1)	The SNMP trap that is generated when an alarm entry crosses its rising threshold and generates an event that is configured for sending SNMP traps
fallingAlarm	alarmIndex, alarmVariable, alarmSample	RMON	THRESHOLD	Warning	falling Alarm	Falling Alarm: \$2 fell below threshold \$5; value = \$4.	The SNMP trap that is generated when an alarm

Table continues...

Name	Parameters (MIB variables)	Class	Msg Facility	Severity	Trap Name / Mnemonic	Format	Description
	e Type, alarmValue, alarmRising Threshold, alarmFalling Threshold					(Sample type = \$3; alarm index = \$1)	entry crosses its falling threshold and generates an event that is configured for sending SNMP traps
deleteSW Redundancy Trap	soft Redundancy Status	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.
createSW Redundancy Trap	soft Redundancy Status	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-mentioned variables. The trap is

Table continues...

Name	Parameters (MIB variables)	Class	Msg Facility	Severity	Trap Name / Mnemonic	Format	Description
							enabled/ disabled by chLntAgConfig ChangeTraps.
IselIntPort CAMLastC hange Trap	IselIntPortC AMLastCha nge	P330	SWITCH FABRIC	Info	IselIntPort 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	ipNetToMed iaPhysAddr ess, ipNetToMed iaNetAddre ss	P330	ROUTER	Warning	duplicateIPT rap	Duplicate IP address \$2 detected; MAC address \$1	This trap reports to the Management station on Duplicate IP identification. CRP identify the new IP on the network. If it similar to one of its IP interfaces, the CRP will issue a SNMP trap, containing the MAC of the intruder.
IntPolicy ChangeEv ent	ipPolicy Activation EntID, ipPolicy ActivationLi st, ipPolicy Activationif Index, ipPolicy ActivationS ub Context	P330	POLICY	Info	IntPolicyCha ngeEvent	Module \$1 - Active policy list changed to \$2	The trap reports a change in the active list specific for a policy-enabled box or module.
IntPolicy AccessCo ntrolViolati onFlt	ipPolicy AccessCont rol	P330	POLICY	Warning	IntPolicy Access Control ViolationFlt	IP PolicyAccess Control violation, if-	This trap reports to the Management station on IP

Table continues...

Name	Parameters (MIB variables)	Class	Msg Facility	Severity	Trap Name / Mnemonic	Format	Description
	ViolationEnt ID, ipPolicy AccessControlViolation Src Addr, ipPolicy AccessControl ViolationDst Addr, ipPolicy AccessControl Violation Protocol, ipPolicy AccessControl Violation L4SrcPort, ipPolicy AccessControl ViolationL4 DstPort, ipPolicy AccessControlViolation Established, ipPolicyRuleID, ipPolicyRule ListID, ipPolicy AccessControlViolationIf Index, ipPolicy AccessControl ViolationSub Ctxt, ipPolicy					index\$9 ip-protocol=\$4 src-ip=\$2 dst-ip=\$3 src-port=\$5 dst-port=\$6 rule-id=\$8 rule-list=\$\$9	PolicyAccess Control violation. The trap includes in its varbind information about the slot where the event occurred. The 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.

Table continues...

Name	Parameters (MIB variables)	Class	Msg Facility	Severity	Trap Name / Mnemonic	Format	Description
	AccessControl ViolationTime						
DormantPort Fault	genPortSWRdFault, genPortGroup Id, genPortId	P330	SWITCH FABRIC	Warning	DormantPortFault	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	DormantPortOk	Dormant Port Connection Returned to Normal on Module \$2 Port \$3;	This trap reports the return of connection on a dormant port.
InlinePwrFilt	genGroupFaultMask, genGroupId, genGroupBUPSAActivity Status	P330	POE	Error	InlinePwrFilt	Module \$2 Inline Power Supply failure	This trap reports the failure of an inline power supply.
InlinePwrFiltOK	genGroupFaultMask, genGroupId, genGroupBUPSAActivity Status	P330	POE	Notification	InlinePwrFiltOK	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, ifAlias, dsx1LineStatus	WAN	WAN	Critical	WanPhysicalAlarmOn	Cable Problem on port \$4	An E1/T1/serial cable was disconnected.
wanPhysical AlarmOff	ifIndex, ifAdminStatus, ifOperStatus, ifName, ifAlias, dsx1LineStatus	WAN	WAN	Notification	wanPhysicalAlarmOff	Cable Problem on port \$4 was cleared	An E1/T1/serial cable was reconnected.

Table continues...

Name	Parameters (MIB variables)	Class	Msg Facility	Severity	Trap Name / Mnemonic	Format	Description
wanLocal AlarmOn	ifIndex, ifAdminStatus, ifOperStatus, ifName, ifAlias, dsx1Line Status	WAN	WAN	Error	wanLocal AlarmOn	Local Alarm on interface \$4	Local alarms, such as LOS.
wanLocal AlarmOff	ifIndex, ifAdminStatus, ifOperStatus, ifName, ifAlias, dsx1Line Status	WAN	WAN	Notification	wanLocal AlarmOff	Local Alarm on interface \$4 was cleared	Local alarms, such as LOS, was cleared.
wanRemote AlarmOn	ifIndex, ifAdminStatus, ifOperStatus, ifName, ifAlias, dsx1Line Status	WAN	WAN	Error	wan Remote AlarmOn	Remote Alarm on interface \$4	Remote alarms, such as AIS.
wanRemote AlarmOff	ifIndex, ifAdminStatus, ifOperStatus, ifName, ifAlias, dsx1Line Status	WAN	WAN	Notification	wan Remote AlarmOff	Remote Alarm on interface \$4 was cleared	Remote alarms, such as AIS, was cleared.
wanMinor AlarmOn	ifIndex, ifAdminStatus, ifOperStatus, ifName, ifAlias, dsx1Line Status	WAN	WAN	Warning	wanMinor AlarmOn	Minor Alarm on interface \$4	Low BER.
wanMinor Alarm Off	ifIndex, ifAdminStatus, ifOperStatus	WAN	WAN	Notification	wanMinor AlarmOff	Minor Alarm on interface \$4 was cleared	Normal BER.

Table continues...

Name	Parameters (MIB variables)	Class	Msg Facility	Severity	Trap Name / Mnemonic	Format	Description
	s, ifName, ifAlias, dsx1Line Status						
AvEntFan Flt	entPhysical Index, entPhysical Descr, entPhySensorValue, avEntPhySensorLo Warning	AVAYA-ENTITY	TEMP		AvEntFan Flt	Fan \$2 is Faulty	This trap reports a faulty fan.
AvEntFan Ok	entPhysical Index, entPhysical Descr, entPhySensorValue, avEntPhySensorLo Warning	AVAYA-ENTITY	TEMP	Notification	AvEntFanOk	Fan \$2 is OK	This trap reports the return to function of a faulty fan.
avEnt48V Pwr Flt	entPhysical Index, entPhysical Descr, entPhySensorValue, avEntPhySensorHi Warning, avEntPhySensorLo WarningentPhysical ParentRelPos	AVAYA-ENTITY	SUPPLY		avEnt48v PwrFlt	48V power supply Fault	This trap reports a problem with a 48V power supply.
avEnt5vP wrFlt	entPhysical Index, entPhysical Descr, entPhySensorValue, avEntPhySensorHi	AVAYA-ENTITY	SUPPLY		avEnt5v PwrFlt	5V power supply Fault	This trap reports a problem with a 5V power supply.

Table continues...

Name	Parameters (MIB variables)	Class	Msg Facility	Severity	Trap Name / Mnemonic	Format	Description
	Warning, avEntPhy SensorLo Warningent Physical ParentRelP os						
avEnt3300 mv PwrFlt	entPhysical Index, entPhysical Descr, entPhySens or Value, avEntPhy SensorHi Warning, avEntPhy SensorLo Warningent Physical ParentRelP os	AVAYA -ENTIT Y	SUPPLY		avEnt3300m v PwrFlt	3.3V (3300mv) power supply Fault	This trap reports a problem with a 3.3V power supply.
avEnt2500 mv PwrFlt	entPhysical Index, entPhysical Descr, entPhySens or Value, avEntPhy SensorHi Warning, avEntPhy SensorLo Warningent Physical ParentRelP os	AVAYA -ENTIT Y	SUPPLY		avEnt2500m v PwrFlt	2.5V (2500mv) power supply Fault	This trap reports a problem with a 2.5V power supply.
avEnt1800 mv PwrFlt	entPhysical Index, entPhysical Descr, entPhySens or Value, avEntPhy SensorHi	AVAYA -ENTIT Y	SUPPLY		avEnt1800m v PwrFlt	1.8V (1800mv) power supply Fault	This trap reports a problem with a 1.8V power supply.

Table continues...

Name	Parameters (MIB variables)	Class	Msg Facility	Severity	Trap Name / Mnemonic	Format	Description
	Warning, avEntPhy SensorLo Warningent Physical ParentRelP os						
avEnt1600 mv PwrFlt	entPhysical Index, entPhysical Descr, entPhySens or Value, avEntPhy SensorHi Warning, avEntPhy SensorLo Warningent Physical ParentRelP os	AVAYA -ENTIT Y	SUPPLY		avEnt1600m v PwrFlt	1.6V (1600mv) power supply Fault	This trap reports a problem with a 1.6V power supply.
avEnt48vP wr FltOk	entPhysical Index, entPhysical Descr, entPhySens or Value, avEntPhy SensorHi Warning, avEntPhy SensorLo Warningent Physical ParentRelP os	AVAYA -ENTIT Y	SUPPLY	Notificati on	avEnt48v PwrFltOk	48V power supply Fault Cleared	This trap reports the correction of a problem with a 48V power supply.
avEnt5vP wr FltOk	entPhysical Index, entPhysical Descr, entPhySens or Value, avEntPhy SensorHi	AVAYA -ENTIT Y	SUPPLY	Notificati on	avEnt5v PwrFltOk	5V power supply Fault Cleared	This trap reports the correction of a problem with a 5V power supply.

Table continues...

Name	Parameters (MIB variables)	Class	Msg Facility	Severity	Trap Name / Mnemonic	Format	Description
	Warning, avEntPhy SensorLo Warningent Physical ParentRelP os						
avEnt3300 mv PwrFltOk	entPhysical Index, entPhysical Descr, entPhySens or Value, avEntPhy SensorHi Warning, avEntPhy SensorLo Warningent Physical ParentRelP os	AVAYA -ENTIT Y	SUPPLY	Notificati on	avEnt3300m vPwrFlt Ok	3.3V (3300mv) power supply Fault Cleared	This trap reports the correction of a problem with a 3.3V power supply.
avEnt2500 mv PwrFltOk	entPhysical Index, entPhysical Descr, entPhySens or Value, avEntPhy SensorHi Warning, avEntPhy SensorLo Warningent Physical ParentRelP os	AVAYA -ENTIT Y	SUPPLY	Notificati on	avEnt2500m vPwrFlt Ok	2.5V (2500mv) power supply Fault Cleared	This trap reports the correction of a problem with a 2.5V power supply.
avEnt1800 mv PwrFltOk	entPhysical Index, entPhysical Descr, entPhySens or Value, avEntPhy SensorHi	AVAYA -ENTIT Y	SUPPLY	Notificati on	avEnt1800m vPwrFlt Ok	1.8V (1800mv) power supply Fault Cleared	This trap reports the correction of a problem with a 1.8V power supply.

Table continues...

Name	Parameters (MIB variables)	Class	Msg Facility	Severity	Trap Name / Mnemonic	Format	Description
	Warning, avEntPhy SensorLo Warningent Physical ParentRelP os						
avEnt1600 mv PwrFltOk	entPhysical Index, entPhysical Descr, entPhySens or Value, avEntPhy SensorHi Warning, avEntPhy SensorLo Warningent Physical ParentRelP os	AVAYA -ENTIT Y	SUPPLY	Notificati on	avEnt1600m v PwrFlt Ok	1.6V (1600mv) power supply Fault Cleared	This trap reports the correction of a problem with a 1.6V power supply.
avEntAmbi ent TempFlt	entPhysical Index, entPhysical Descr, entPhySens or Value, avEntPhy SensorHi Warning, entPhysical ParentRelP os	AVAYA -ENTIT Y	TEMP		avEnt Ambient TempFlt	Ambient Temperature fault (\$3)	This trap reports that the ambient temperature in the device is not within the acceptable temperature range for the device.
avEntAmbi ent TempOk	entPhysical Index, entPhysical Descr, entPhySens or Value, avEntPhy SensorHi Warning, entPhysical ParentRelP os	AVAYA - ENTIT Y	TEMP	Notificati on	avEnt Ambient TempOk	Ambient Temperature fault (\$3) cleared	This trap reports that the ambient temperature in the device has returned to the acceptable range for the device.

Appendix B: ASG authentication

ASG authentication CLI commands

* Note:

ASG is no longer supported from Release 7.1.2 and has been replaced with EASG. ASG authentication file commands can be used if you downgrade to the release previous to Release 7.1.2.

The commands listed in the table manage ASG authentication. For more information about these commands, see *Avaya G450 Branch Gateway CLI Reference*.

Command	Description
<code>copy ftp auth-file</code>	Download an ASG authentication file from a remote FTP server
<code>copy scp auth-file</code>	Download an ASG authentication file from a remote SCP server
<code>copy tftp auth-file</code>	Download an ASG authentication file from a remote TFTP server
<code>copy usb auth-file</code>	Download an ASG authentication file from a USB mass storage device
<code>erase auth-file</code>	Erase the gateway's ASG authentication file
<code>no login authentication services-logins</code>	Deactivate all Avaya Services logins.
<code>show auth-file info</code>	Display ASG authentication file information
<code>show login authentication</code>	Display login authentication settings and information.
<code>show download auth-file status</code>	Display download status of ASG authentication file, after using <code>copy ftp scp tftp usb auth-file</code> to download an authentication file to the gateway

Related links

[Replacing the ASG authentication file](#) on page 574

Replacing the ASG authentication file

Before you begin

If you need to install an authentication file with a different ID, delete the current authentication file using the `erase auth-file` command. This command requires Supervisor level access and

can be used only when directly connecting to the Console or Services port. You can delete the authentication file and replace it with one that has a new ID. However, you must ensure that the authentication file label on the gateway chassis is replaced.

About this task

If there are any problems with the ASG authentication file, you can download a new authentication file from Authentication File System (AFS). You cannot install an authentication file with an authentication file ID different from the authentication file installed on Branch Gateway.

* Note:

ASG is no longer supported from Release 7.1.2 and has been replaced with EASG. ASG authentication file commands can be used if you downgrade to the release previous to Release 7.1.2.

Procedure

1. Use the **show auth-file info** command to view the current ASG authentication file.

For example:

```
Gxxx-001(super)# show auth-file info
Authentication File (AF) information:
AF-ID :7000012345
Date/time : 15:02:27 23-AUG-2015
Major release : 6.x
```

2. Use Windows File Explorer or another file management program to create a directory on an FTP, SCP or TFTP server for storing authentication files.

For example, C:\licenses.

3. Open Internet Explorer and go to rfa.avaya.com.
4. Log in using your SSO login and password.

The AFS and RFA information home page displays.

5. Start the AFS application from the RFA information page.

Follow the instructions outlined in *Authentication File System (AFS) Guide* to create and download the authentication file.

6. Download the authentication file on to Branch Gateway from an FTP, SCP or TFTP server, or a USB mass storage device.

filename contains the name of the authentication file and the path of the file. *ip* is the IP address of the host. **source-usb-device** is the source USB mass storage device and **source-filename** contains the name of the authentication file and the path of the file. Branch Gateway prompts you for a user name and password after you enter the command. To install the authentication file, use one of the following commands:

- **copy ftp auth-file filename ip**
- **copy scp auth-file filename ip**
- **copy tftp auth-file filename ip**

- **copy usb auth-file source-usb-device source-filename**

Auth-files are used in releases prior to Release 7.1.2.

7. After the authentication file is downloaded, you can view the download status using the **show download auth-file status** command.

Related links

[ASG authentication CLI commands](#) on page 574

Appendix C: Surv-MIB files

Avaya-SURV-MIB files

Object	OID
avSurvAdminState	1.3.6.1.4.1.6889.2.6.4.1.1
avSurvStatus	1.3.6.1.4.1.6889.2.6.4.1.2
avSurvMaxIPReg	1.3.6.1.4.1.6889.2.6.4.1.3
avSurvDateFormat	1.3.6.1.4.1.6889.2.6.4.1.4
avSurvEndDLTimeStamps	1.3.6.1.4.1.6889.2.6.4.1.5
avSurvNotificationSeverity	1.3.6.1.4.1.6889.2.6.4.1.6
avSurvConfigCommand	1.3.6.1.4.1.6889.2.6.4.1.7
avSurvGatewayNumber	1.3.6.1.4.1.6889.2.6.4.1.8
avSurvPimLockout	1.3.6.1.4.1.6889.2.6.4.1.9
avSurvAttendantAccessCode	1.3.6.1.4.1.6889.2.6.4.1.10
avSurvAttendantExtension	1.3.6.1.4.1.6889.2.6.4.1.11
avSurvStationTable	1.3.6.1.4.1.6889.2.6.4.2
avSurvStationEntry	1.3.6.1.4.1.6889.2.6.4.2.1
avSurvStationIndex	1.3.6.1.4.1.6889.2.6.4.2.1.1
avSurvStationExt	1.3.6.1.4.1.6889.2.6.4.2.1.2
avSurvStationType	1.3.6.1.4.1.6889.2.6.4.2.1.3
avSurvStationInterfaceIndex	1.3.6.1.4.1.6889.2.6.4.2.1.4
avSurvStationCOR	1.3.6.1.4.1.6889.2.6.4.2.1.5
avSurvStationTrunkDest	1.3.6.1.4.1.6889.2.6.4.2.1.6
avSurvStationRowStatus	1.3.6.1.4.1.6889.2.6.4.2.1.7
avSurvStationExpansionModule	1.3.6.1.4.1.6889.2.6.4.2.1.8
avSurvStationSlotPort	1.3.6.1.4.1.6889.2.6.4.2.1.9
avSurvStationSwitchHookFlash	1.3.6.1.4.1.6889.2.6.4.2.1.10
avSurvStationIpAddressRegistered	1.3.6.1.4.1.6889.2.6.4.2.1.11
avSurvStationName	1.3.6.1.4.1.6889.2.6.4.2.1.12
avSurvTrunkGroupTable	1.3.6.1.4.1.6889.2.6.4.3

Table continues...

Object	OID
avSurvTrunkGroupEntry	1.3.6.1.4.1.6889.2.6.4.3.1
avSurvTrunkGroupNum	1.3.6.1.4.1.6889.2.6.4.3.1.1
avSurvTrunkGroupType	1.3.6.1.4.1.6889.2.6.4.3.1.2
avSurvTrunkGroupTAC	1.3.6.1.4.1.6889.2.6.4.3.1.3
avSurvTrunkGroupDial	1.3.6.1.4.1.6889.2.6.4.3.1.4
avSurvTrunkGroupRowStatus	1.3.6.1.4.1.6889.2.6.4.3.1.5
avSurvTrunkGroupDidDigitTreatment	1.3.6.1.4.1.6889.2.6.4.3.1.6
avSurvTrunkGroupDidDigitsInsert	1.3.6.1.4.1.6889.2.6.4.3.1.7
avSurvTrunkGroupDidSupervision	1.3.6.1.4.1.6889.2.6.4.3.1.8
avSurvTrunkGroupName	1.3.6.1.4.1.6889.2.6.4.3.1.9
avSurvTrunkGroupCodesetDisplay	1.3.6.1.4.1.6889.2.6.4.3.1.10
avSurvTrunkGroupCodesetNational	1.3.6.1.4.1.6889.2.6.4.3.1.11
avSurvTrunkGroupChannelPreference	1.3.6.1.4.1.6889.2.6.4.3.1.12
avSurvTrunkGroupDigitHandling	1.3.6.1.4.1.6889.2.6.4.3.1.13
avSurvTrunkGroupJapanDisconnect	1.3.6.1.4.1.6889.2.6.4.3.1.14
avSurvTrunkGroupSendName	1.3.6.1.4.1.6889.2.6.4.3.1.15
avSurvTrunkGroupSendCallingNumber	1.3.6.1.4.1.6889.2.6.4.3.1.16
avSurvTrunkGroupNumberingFormat	1.3.6.1.4.1.6889.2.6.4.3.1.17
avSurvTrunkGroupIncomingDestination	1.3.6.1.4.1.6889.2.6.4.3.1.18
avSurvTrunkGroupIncomingDialTone	1.3.6.1.4.1.6889.2.6.4.3.1.19
avSurvTrunkGroupR2MFCSignaling	1.3.6.1.4.1.6889.2.6.4.3.1.20
avSurvTrunkGroupTrunkHunt	1.3.6.1.4.1.6889.2.6.4.3.1.21
avSurvTrunkGroupDs1Supervision	1.3.6.1.4.1.6889.2.6.4.3.1.22
avSurvTrunkGroupCbc	1.3.6.1.4.1.6889.2.6.4.3.1.23
avSurvTrunkGroupCbcServiceFeature	1.3.6.1.4.1.6889.2.6.4.3.1.24
avSurvTrunkGroupCbcParameter	1.3.6.1.4.1.6889.2.6.4.3.1.25
avSurvTrunkGroupBusyDisconnect	1.3.6.1.4.1.6889.2.6.4.3.1.26
avSurvTrunkTable	1.3.6.1.4.1.6889.2.6.4.4
avSurvTrunkEntry	1.3.6.1.4.1.6889.2.6.4.4.1
avSurvTrunkGroupRefNumber	1.3.6.1.4.1.6889.2.6.4.4.1.1
avSurvTrunkIndex	1.3.6.1.4.1.6889.2.6.4.4.1.2
avSurvTrunkInterfaceIndex	1.3.6.1.4.1.6889.2.6.4.4.1.3
avSurvTrunkRowStatus	1.3.6.1.4.1.6889.2.6.4.4.1.4
avSurvTrunkSlotPort	1.3.6.1.4.1.6889.2.6.4.4.1.5
avSurvTrunkSigGroupRefNumber	1.3.6.1.4.1.6889.2.6.4.4.1.6

Table continues...

Object	OID
avSurvArsTable	1.3.6.1.4.1.6889.2.6.4.5
avSurvArsEntry	1.3.6.1.4.1.6889.2.6.4.5.1
avSurvDialIndex	1.3.6.1.4.1.6889.2.6.4.5.1.1
avSurvDialString	1.3.6.1.4.1.6889.2.6.4.5.1.2
avSurvDialType	1.3.6.1.4.1.6889.2.6.4.5.1.3
avSurvDialMaximumLength	1.3.6.1.4.1.6889.2.6.4.5.1.4
avSurvDialGroupRefNumber	1.3.6.1.4.1.6889.2.6.4.5.1.5
avSurvDialAction	1.3.6.1.4.1.6889.2.6.4.5.1.6
avSurvDialRowStatus	1.3.6.1.4.1.6889.2.6.4.5.1.7
avSurvDialDeleteDigits	1.3.6.1.4.1.6889.2.6.4.5.1.8
avSurvDialInsertDigits	1.3.6.1.4.1.6889.2.6.4.5.1.9
avSurvDialMinimumLength	1.3.6.1.4.1.6889.2.6.4.5.1.10
avSurvFacTable	1.3.6.1.4.1.6889.2.6.4.6
avSurvFacEntry	1.3.6.1.4.1.6889.2.6.4.6.1
avSurvFacIndex	1.3.6.1.4.1.6889.2.6.4.6.1.1
avSurvFacId	1.3.6.1.4.1.6889.2.6.4.6.1.2
avSurvFacRowStatus	1.3.6.1.4.1.6889.2.6.4.6.1.3
avSurvFacType	1.3.6.1.4.1.6889.2.6.4.6.1.4
avSurvIpVoiceCodecSetTable	1.3.6.1.4.1.6889.2.6.4.7
avSurvIpVoiceCodecSetEntry	1.3.6.1.4.1.6889.2.6.4.7.1
avSurvIpVoiceCodecSetNum	1.3.6.1.4.1.6889.2.6.4.7.1.1
avSurvIpVoiceCodecSetIndex	1.3.6.1.4.1.6889.2.6.4.7.1.2
avSurvIpVoiceCodecSetPriority	1.3.6.1.4.1.6889.2.6.4.7.1.3
avSurvIpVoiceCodecSetType	1.3.6.1.4.1.6889.2.6.4.7.1.4
avSurvIpVoiceCodecSetSilence	1.3.6.1.4.1.6889.2.6.4.7.1.5
avSurvIpVoiceCodecSetFrames	1.3.6.1.4.1.6889.2.6.4.7.1.6
avSurvIpVoiceCodecSetRowStatus	1.3.6.1.4.1.6889.2.6.4.7.1.7
avSurvIpCodecSetFaxMode	1.3.6.1.4.1.6889.2.6.4.8.1
avSurvIpCodecSetFaxRedundancy	1.3.6.1.4.1.6889.2.6.4.8.2
avSurvIpCodecSetModemMode	1.3.6.1.4.1.6889.2.6.4.8.3
avSurvIpCodecSetModemRedundancy	1.3.6.1.4.1.6889.2.6.4.8.4
avSurvIpCodecSetTtyMode	1.3.6.1.4.1.6889.2.6.4.8.5
avSurvIpCodecSetTtyRedundancy	1.3.6.1.4.1.6889.2.6.4.8.6
avSurvIpCodecSetClearChanMode	1.3.6.1.4.1.6889.2.6.4.8.7
avSurvIpCodecSetClearChanRedundancy	1.3.6.1.4.1.6889.2.6.4.8.8

Table continues...

Object	OID
avSurvIpCodecSetEncryptPriority1	1.3.6.1.4.1.6889.2.6.4.8.9
avSurvIpCodecSetEncryptPriority2	1.3.6.1.4.1.6889.2.6.4.8.10
avSurvIpCodecSetEncryptPriority3	1.3.6.1.4.1.6889.2.6.4.8.11
avSurvSlotConfigTable	1.3.6.1.4.1.6889.2.6.4.9
avSurvSlotConfigEntry	1.3.6.1.4.1.6889.2.6.4.9.1
avSurvSlotConfigIndex	1.3.6.1.4.1.6889.2.6.4.9.1.1
avSurvSlotConfigNumberId	1.3.6.1.4.1.6889.2.6.4.9.1.2
avSurvSlotConfigBoardType	1.3.6.1.4.1.6889.2.6.4.9.1.3
avSurvSlotConfigRowStatus	1.3.6.1.4.1.6889.2.6.4.9.1.4
avSurvDs1Table	1.3.6.1.4.1.6889.2.6.4.10
avSurvDs1Entry	1.3.6.1.4.1.6889.2.6.4.10.1
avSurvDs1Index	1.3.6.1.4.1.6889.2.6.4.10.1.1
avSurvDs1Name	1.3.6.1.4.1.6889.2.6.4.10.1.2
avSurvDs1BitRate	1.3.6.1.4.1.6889.2.6.4.10.1.3
avSurvDs1SignalingMode	1.3.6.1.4.1.6889.2.6.4.10.1.4
avSurvDs1ChannelNumbering	1.3.6.1.4.1.6889.2.6.4.10.1.5
avSurvDs1Connect	1.3.6.1.4.1.6889.2.6.4.10.1.6
avSurvDs1Interface	1.3.6.1.4.1.6889.2.6.4.10.1.7
avSurvDs1Side	1.3.6.1.4.1.6889.2.6.4.10.1.8
avSurvDs1CountryProtocol	1.3.6.1.4.1.6889.2.6.4.10.1.9
avSurvDs1ProtocolVersion	1.3.6.1.4.1.6889.2.6.4.10.1.10
avSurvDs1BearerCapability	1.3.6.1.4.1.6889.2.6.4.10.1.11
avSurvDs1InterfaceCompanding	1.3.6.1.4.1.6889.2.6.4.10.1.12
avSurvDs1LongTimer	1.3.6.1.4.1.6889.2.6.4.10.1.13
avSurvDs1RowStatus	1.3.6.1.4.1.6889.2.6.4.10.1.14
avSurvDs1SlotNumberId	1.3.6.1.4.1.6889.2.6.4.10.1.15
avSurvSigGroupTable	1.3.6.1.4.1.6889.2.6.4.11
avSurvSigGroupEntry	1.3.6.1.4.1.6889.2.6.4.11.1
avSurvSigGroupIndex	1.3.6.1.4.1.6889.2.6.4.11.1.1
avSurvSigGroupChannelSelection	1.3.6.1.4.1.6889.2.6.4.11.1.2
avSurvSigGroupAssociatedSignaling	1.3.6.1.4.1.6889.2.6.4.11.1.3
avSurvSigGroupPrimaryDChannel	1.3.6.1.4.1.6889.2.6.4.11.1.4
avSurvSigGroupRowStatus	1.3.6.1.4.1.6889.2.6.4.11.1.5
avSurvBriTable	1.3.6.1.4.1.6889.2.6.4.12
avSurvBriEntry	1.3.6.1.4.1.6889.2.6.4.12.1

Table continues...

Object	OID
avSurvBriIndex	1.3.6.1.4.1.6889.2.6.4.12.1.1
avSurvBriName	1.3.6.1.4.1.6889.2.6.4.12.1.2
avSurvBriInterface	1.3.6.1.4.1.6889.2.6.4.12.1.3
avSurvBriSide	1.3.6.1.4.1.6889.2.6.4.12.1.4
avSurvBriCountryProtocol	1.3.6.1.4.1.6889.2.6.4.12.1.5
avSurvBriBearerCapability	1.3.6.1.4.1.6889.2.6.4.12.1.6
avSurvBriInterfaceCompanding	1.3.6.1.4.1.6889.2.6.4.12.1.7
avSurvBriTeiAssignment	1.3.6.1.4.1.6889.2.6.4.12.1.8
avSurvBriDirectoryNumberA	1.3.6.1.4.1.6889.2.6.4.12.1.9
avSurvBriDirectoryNumberB	1.3.6.1.4.1.6889.2.6.4.12.1.10
avSurvBriSpidA	1.3.6.1.4.1.6889.2.6.4.12.1.11
avSurvBriSpidB	1.3.6.1.4.1.6889.2.6.4.12.1.12
avSurvBriEndpointInit	1.3.6.1.4.1.6889.2.6.4.12.1.13
avSurvBriLayer1Stable	1.3.6.1.4.1.6889.2.6.4.12.1.14
avSurvBriRowStatus	1.3.6.1.4.1.6889.2.6.4.12.1.15
avSurvBriSlotPortNumberId	1.3.6.1.4.1.6889.2.6.4.12.1.16
avSurvIncomingRoutingTable	1.3.6.1.4.1.6889.2.6.4.13
avSurvIncomingRoutingEntry	1.3.6.1.4.1.6889.2.6.4.13.1
avSurvIncomingRoutingGroupRefNumber	1.3.6.1.4.1.6889.2.6.4.13.1.1
avSurvIncomingRoutingIndex	1.3.6.1.4.1.6889.2.6.4.13.1.2
avSurvIncomingRoutingMatchPattern	1.3.6.1.4.1.6889.2.6.4.13.1.3
avSurvIncomingRoutingLength	1.3.6.1.4.1.6889.2.6.4.13.1.4
avSurvIncomingRoutingDeleteDigits	1.3.6.1.4.1.6889.2.6.4.13.1.5
avSurvIncomingRoutingInsertDigits	1.3.6.1.4.1.6889.2.6.4.13.1.6
avSurvIncomingRoutingMode	1.3.6.1.4.1.6889.2.6.4.13.1.7
avSurvIncomingRoutingRowStatus	1.3.6.1.4.1.6889.2.6.4.13.1.8
avSurvNfasTable	1.3.6.1.4.1.6889.2.6.4.14
avSurvNfasEntry	1.3.6.1.4.1.6889.2.6.4.14.1
avSurvNfasSigGroupRefNumber	1.3.6.1.4.1.6889.2.6.4.14.1.1
avSurvNfasIndex	1.3.6.1.4.1.6889.2.6.4.14.1.2
avSurvNfasInterface	1.3.6.1.4.1.6889.2.6.4.14.1.3
avSurvNfasInterfaceId	1.3.6.1.4.1.6889.2.6.4.14.1.4
avSurvNfasRowStatus	1.3.6.1.4.1.6889.2.6.4.14.1.5

Index

A

Access Code 2	142
Access control list	
CLI commands	523
access control list rule specifications	504
access control lists, see policy	504
Access through Services port	31
access-control-list	250
Accessing	
Avaya Aura Communication Manager	33
MGC	33
via modem	31
Accessing Branch Gateway	29
accessing port matrix	557
Active PMI	65
add nfas-interface	165, 168
add port	158, 168
Address Resolution Protocol table	418
Administering Encrypted SRTCP	299
Administering Media encryption	296
administration	
fips	542
AES-256	296
analog telephones	106
analog-test	382, 384
Announcement files	
CLI commands	309
managing and transferring using SCP	303
area	427
arp	418–420
ARP table	418
changing an entry	420
CLI commands	420
description	418
dynamic entries	418
static entries	418
ARP table entries	419
arp timeout	420
ARS	142
ARS Dial Patterns	144
ARS dial patterns data	144
ARS FAC	142
ASG commands	574
Associated Signaling	138
async mode interactive	218
async mode terminal	218
async-limit-string	217
async-reset-modem	217
Authenticating	
Service logins	62
authentication	499
Auto Fallback in SLS	99
Auto Route Selection (ARS) Access Code 1	142
automatic failover and fallback	533
automatically activating ETR	284
autoneg	182
Autonomous System Boundary Router	427
Avaya Aura Communication Manager	
accessing	33
configuring for SLS	113
functions	33
Avaya Aura™ Communication Manager	
configuring for SLS	113
Avaya Services	
authenticating logins with EASG	62
Avaya Site Administration	33
Avaya support website	560
Avaya Voice Announcement Manager (VAM)	303

B

Backing up the Branch Gateway	
using the Branch Gateway USB port	89
Backup and Restore of Gateway Configuration	541
backup config usb	89, 94
backup control for data and VoIP	474
backup delay	240, 241
backup interface	241, 244, 247, 250, 257
Backup interfaces	239
CLI commands	241
dynamic bandwidth reporting	261
GRE tunnels as	398
limitations	240
modem dial backup, Modem dial backup	241
modem dial backup, see Modem dial backup	241
overview	182
backup mechanism configuration	272
backup peer mechanism	479
Backup service	283
bandwidth	227, 229, 426, 427
Bandwidth	
dynamic reporting	261
manual adjustment	426
reducing via header compression	206
used to calculate Cost	426
Basic	
LAN deployment	22
bc out	277
be out	277
Before Enabling or Disabling FIPS Approved Mode	541
Bit Rate	134
bootfile	415
BOOTP	
description	407
BOOTP relay	407

BOOTstrap Protocol		CIR	276
see BOOTP	407	cir out	277
BPDU	322	Class values in SLS station context	151
Branch Gateway		class-identifier	413, 415
documentation	556	clear arp-cache	420
Branch Gateway access	29	clear attendant	168
Branch Office 1 configuration	467	clear bri	156, 168
Branch Office 2 configuration	470	clear capture-buffer	370
bri	156, 168	clear crypto isakmp	455, 499
Bridge Protocol Data Units		clear crypto sa	499
see BPDU	322	clear crypto sa all	455
Bridges		clear crypto sa counters	454, 499
direct handshaking	322	clear dial-pattern	166, 168
loops	322	clear ds1	152, 168
Broadcast relay		clear dynamic-trap-manager	294
CLI commands	417	clear extension	168
description	417	clear fac	168
directed broadcast forwarding	417	clear fragment	434
NetBIOS rebroadcast	417	clear frame-relay counters	237
C		clear incoming-routing	168
cable length long	226	clear ip dhcp-client statistics	186
cable length short	226	clear ip dhcp-server binding	413, 415
cablelength long	223	clear ip dhcp-server statistics	415
cablelength short	223	clear ip domain statistics	78
CAC-BL	261	clear ip route	397
Call admission control		clear ip rtp header-compression	209, 211
Dynamic CAC	261	clear ip tcp header-compression	209, 211
Call admission control, see Dynamic CAC	261	clear logging file	196, 204
Call Type ARS only		clear logging server	194
AAR and ARS Digit Analysis Table	124	clear mgc list	71, 73
call types	167	clear port mirror	321
Called Len	145	clear port static-vlan	317
Called Number	145	clear profile	383, 384
cancel	383, 384	clear radius authentication server	47
capture buffer mode	370	clear rmon statistics	329
capture buffer-mode	376	clear sig-group	165, 168
capture buffer-size	376	clear slot-config	168
capture filter-group	369, 371	clear ssh-client known-hosts	46
capture interface	363, 370	clear station	168
capture max-frame-size	370	clear survivable-config	168
capture start	371	clear sync interface	532, 534
capture stop	372	clear tac	168
captured packets	372	clear tcp syn-cookies	50
CAS Remote Hold/Answer Hold-Unhold Access Code	142	clear tcp syn-cookies counters	50
CDR, SLS information	111	clear trunk-group	158, 168
certificate validation	537	clear vlan	312, 317
Challenge Handshake Authentication Protocol	216	CLI	
Changing crypto list parameters	451	accessing from local network	31
Channel Groups		accessing from remote location	31
creating	223	accessing with modem	31
illustration	220	commands	543
mapping	223	contexts	29
Channel Numbering	135	contexts example	30
channel-group	223, 226	FIPS	543
CHAP	216	listing files	97
		managing configuration files	95
		managing firmware banks	83

CLI (<i>continued</i>)		Commands (<i>continued</i>)	
online help	30	interface fastethernet, interface configuration	390
upgrading firmware using SCP/FTP/TFTP/HTTPS	83	interface loopback	390
using to configure the system	27	interface serial, interface configuration	390
viewing device status	79	interface tunnel	390
CLI access using a PC device	31	interface usb-modem	390
CLI output per RTP session	341	interface vlan	390
client identifier	410	ip address, console port	218
client identifiers	415	ip admin-state	390
clock source	223 , 226	ip broadcast-address	390
Codec	212	ip capture-list	376
Codecs in SLS	143	ip peer address	218
collection		ip rtp compression-connections	207
delete	557	ip rtp header-compression	207 , 210
edit	557	ip rtp max-period	207
generating PDF	557	ip rtp max-time	207
sharing content	557	ip rtp non-tcp-mode	207
command sequence	249	ip rtp port-range	207
Commands	217 , 427	ip tcp compression-connections	207 , 210
async modem-init-string	218	ip tcp header-compression	207 , 210
async reset-modem	218	ip-protocol, packet sniffing	376
bri	146	ip-rule, packet sniffing	376
capture filter-group	376	key config-key password-encryption	48
capture interface	376	login authentication local-craft-password	574
capture ipsec	376	login authentication lockout	574
capture max-frame-size	376	login authentication response-time	574
capture start	376	login authentication services-logins	574
capture stop	376	name, packet sniffing	376
capture-service	362 , 376	owner, packet sniffing	376
clear capture-buffer	376	ping	238
composite-operation, packet sniffing	376	ppp authentication, ASG authentication	574
cookie, capture list	376	ppp authentication, console port	218
copy auth-file ftp	574	ppp chap-secret	218
copy auth-file scp	574	ppp timeout authentication, console port	218
copy auth-file tftp	574	rtp-stat qos-trap-rate-limit	338
copy auth-file usb	574	set logging session, object tracking	269
copy capture-file ftp	373 , 376	set mgc list	71
copy capture-file scp	373 , 376	set sls	125
copy capture-file tftp	373 , 376	show auth-file info	574
copy capture-file usb	373 , 376	show auth-file status	574
copy ftp auth-file	574	show capture	372 , 376
copy running-config startup-config	48	show capture-buffer hex	372 , 376
copy scp auth-file	574	show controllers	238
copy tftp auth-file	574	show frame-relay fragment	238
copy usb auth-file	574	show frame-relay lmi	238
crypto ipsec df-bit	452	show frame-relay map	238
destination-ip, packet sniffing	376	show frame-relay pvc	238
dial-pattern	146	show frame-relay traffic	238
ds1	146	show interfaces, WAN configuration	238
dscp, packet sniffing	376	show ip capture-list	376
dscp, policy lists	517	show ip interface	238
erase auth-file	574	show ip interface brief	390
fragment, packet sniffing	368 , 376	show login authentication	574
icmp	376	show map-class frame-relay	238
incoming-routing	146	show ppp authentication	218
interface console	390	show rtp-stat config	334
interface dialer	390	show rtp-stat detailed	339

Commands (<i>continued</i>)		Configuration (<i>continued</i>)	
show rtp-stat sessions	339	using GUI applications	26
show running-config	238	using the CLI	27
show startup-config	238	WAN ethernet port	181
show traffic-shape	238	Configuration file	
show upload auth-file status	574	CLI commands	96
show upload status	376	Configured PMI	65
shutdown, console port	218	Connect	135
sig-group	146	Console device	
sls	146	configuring console port to detect	218
snmp-server view	289	console interface	25
source-ip, packet sniffing	376	Console messages	254
speed	218	Console port	
station	146	associating with Dialer interface	250
tcp destination-port	376	CLI commands	218
tcp source-port	376	configuring for modem use	33
timeout absolute	218	configuring to detect console device	218
trunk-group	146	configuring to detect modem	218
tunnel path-mtu-discovery	402	connecting modem	33
udp destination-port	376	description	218
udp source-port	376	entering interface context	218
Committed Burst size	276	contact closure	110
communication methods for agents and managers on		Contact closure	
SNMP	285	activating when access code dialed	301
composite operations	517	closure modes	301
Composite operations		configuring software	301
adding to IP rule	519	deactivating manually	301
configuring	519	displaying status	302
deleting from IP rule	519	overview	300
example	519	relay control methods	300
pre-configured for access control lists	517	setting manually	301
composite-operation		setting pulse duration	301
IP rule configuration	519	using in SLS mode	109
composite-operation, access control list	523	Contact Closure Close Code	142
composite-operation, DSCP table	520 , 525	Contact closure configuration	
composite-operation, MSS configuration	53	CLI commands	302
composite-operation, QoS list	519 , 525	Contact Closure Open Code	142
Computer, connecting to fixed router port	178	Contact Closure Pulse Code	142
conference call	358	content	
Configuration		publishing PDF output	557
defining an interface	63	searching	557
DHCP client	184	sharing	557
dynamic trap manager	293	sort by last updated	557
header compression	206	watching for updates	557
installation and setup	25	Contexts	29
LLDP	188	Contexts example	30
managing configuration files	95	Continuous channel in VPN	463
MGC list	68	continuous-channel	442 , 446 , 463 , 499
modem	216	controller	223 , 226
primary management interface	64	Controller	
RTCP	206	configuring mode	223
RTP	206	displaying configuration	223
running configuration	27	entering context	223
saving configuration changes	27	cookie, access control list	523
startup	238	cookie, capture list	363
startup configuration	27	cookie, policy list	508
switching	311	cookie, QoS list	525

copy announcement-file ftp	86 , 87 , 303 , 304 , 309
copy announcement-file https	305 , 306
copy announcement-file scp	86 , 87 , 303 , 309
copy announcement-file usb	86 , 87 , 304 , 305 , 309
copy auth-file ftp	86 , 87 , 574
copy auth-file scp	86 , 87 , 574
copy auth-file tftp	574
copy auth-file usb	86 , 87 , 574
copy capture-file ftp	86 , 87
copy capture-file scp	86 , 87
copy capture-file usb	86 , 87
copy cdr-file ftp	86 , 87
copy cdr-file scp	86 , 87
copy cdr-file usb	86 , 87
copy dhcp-binding ftp	86 , 87
copy dhcp-binding scp	86 , 87
copy dhcp-binding usb	86 , 87
copy file usb	86
copy ftp announcement-file	304 , 309
copy ftp auth-file	574
copy ftp module	83 , 87
copy ftp startup-config	96
copy ftp sw_imageA	91 , 94
copy ftp SW_imageA	84 , 87
copy ftp SW_imageB	87
copy https announcement-file	309
copy https startup-config	96
copy https SW_imageA	84
copy license-file usb	86 , 87
copy phone-script usb	86 , 87
copy running-config ftp	96
copy running-config https	96
copy running-config scp	96
copy running-config startup-config	50
copy running-config tftp	96
copy scp announcement-file	303 , 304 , 309
copy scp auth-file	574
copy scp startup-config	96
copy scp SW_imageA	84
copy startup-config ftp	96
copy startup-config https	96
copy startup-config scp	96
copy startup-config tftp	96
copy startup-config usb	86 , 87 , 96
copy syslog-file ftp	195 , 204
copy syslog-file https	195
copy syslog-file scp	195 , 204
copy syslog-file tftp	204
copy syslog-file usb	86 , 87 , 195 , 204
copy tftp auth-file	574
copy tftp module	87
copy tftp startup-config	96
copy tftp sw_imageA	91 , 94
copy tftp SW_imageA	84 , 87
copy tftp SW_imageB	87
copy usb	84
copy usb announcement-file	87 , 305 , 309
copy usb auth-file	87 , 574
copy usb modules	87
copy usb phone-image	87
copy usb phone-script	87
copy usb startup-config	87 , 96
copy usb SW_image	87
copyedge announcement-file scp	306
copyedge running-config scp	96
copyedge scp announcement-file	307 , 309
copyedge scp startup-config	96
copyedge startup-config scp	96
copyedge syslog-file https	195
copying and installing EASG site certificate using scp	
copying EASG site certificate	59
copying and installing EASG site certificate using usb	
device	
copying EASG site certificate using usb device	59
cos	519 , 525
Cost	426
Country Protocol	136
crypto ipsec df-bit	499
crypto ipsec minimal pmtu	452
crypto ipsec minimal-pmtu	499
crypto ipsec nat-transparency udp-encapsulation	452 , 499
crypto ipsec transform-set	441 , 485 , 491 , 499
crypto isakmp invalid-spi-recovery	451 , 499
crypto isakmp nat keepalive	452 , 499
crypto isakmp peer	442 , 485 , 491 , 499
crypto isakmp peer-group	445 , 491 , 499
crypto isakmp policy	485 , 491 , 499
crypto isakmp suggest-key	499
crypto ispec nat-transparency udp-encapsulation	499
crypto ispec transform-set	499
crypto key generate	41 , 45
crypto list	
overview	436
Crypto list	
configuring	448
deactivating	450
crypto list parameters	
changing	451
crypto map	446 , 485 , 491 , 499
Crypto map	
configuring	446
overview	436
crypto-group	452
cyrpto isakmp policy	440
D	
data and VoIP control backup	474
Data Link Connection Identifier	235
see DLCI	235
Date Format on Terminals	143
DCP stations data	128
DCP telephones	106
DCP/ANALOG Bearer Capability	137

decrypted IPSec VPN packets	372	DHCP client (<i>continued</i>)	
Default gateway		CLI logging, setting logging session conditions	186
defining	66	CLI logging, viewing	186
default sink severity levels	201	configuring	184
default-metric	424 , 427 , 430	determining DHCP option requests	184
default-router	412	displaying configuration	186
default-routers	415	displaying parameters	184
defining other interfaces	26	enabling	184
Del		interface fastethernet, DHCP client	184
AAR Digit Conversion Table	124	ip address dhcp	184
ARS Digit Conversion Table	124	ip dhcp client client-id	184
Incoming Call Handling Treatment	146	ip dhcp client hostname	184
Deleting EASG site certificate		ip dhcp client lease	184
deleting site certificate	60	ip dhcp client request	184
deleting site certificate	60	ip dhcp client route track	184
DeMilitarized Zone		lease, releasing	185
see DMZ	388	lease, renewing	185
Denial of Service reporting	51	maintaining	186
Deployments		overview	183
basic	22	setting the client identifier	184
introduction	22	setting the client lease	184
overview	22	setting the hostname	184
port redundancy	22 , 23	show ip dhcp-client	184
RSTP	23	DHCP Client configuration	462
RSTP and switch redundancy	24	DHCP options	412
switch redundancy	23	DHCP relay	407
description, crypto list rule	499	DHCP server	
description, crypto map	499	CLI commands	415
description, DNS servers list	78	configuration examples	413
description, ISAKMP peer	442 , 499	configuring DHCP options	412
description, ISAKMP peer-group	499	configuring vendor-specific options	413
description, ISAKMP policy	440 , 499	overview	409
description, object tracker	275	typical application	410
description, policy rule	513	Diagnosing	
destination-ip		and monitoring the network	328
packet sniffing	366	Dial On Demand Routing (DDR)	241
destination-ip, access control list	523	dial-pattern	166 , 168
destination-ip, crypto list rule	448 , 499	Dialed String	
destination-ip, MSS configuration	53	AAR and ARS Digit Analysis Table	124 , 145
destination-ip, policy list	514	AAR and ARS Digit Conversion Table	124 , 145
destination-ip, QoS list	525	dialer interface	252
determining	539	Dialer interface	
enabled or disabled	540	activating with object tracking	247
FIPS	540	as backup for Loopback interface	241
Determining Configuration is FIPS Compliant	540	as backup for WAN interface	241
Device status		assigning access control list to	250
CLI commands	80	assigning to Console port	250
viewing	79	authentication method	244
DHCP		CHAP authentication	244
BOOTP relay	407	CLI commands	257
description	407	configuring	244
DHCP and BOOTP relay		configuring as backup	244
CLI commands	408	configuring backup routing	244
DHCP client		dynamic IP	247
applications	183	dynamic routing	241
CLI commands	186	giving priority to VoIP	241
CLI logging, enabling	186	logging	252

Dialer interface (<i>continued</i>)		documentation (<i>continued</i>)	
setting IP address	244	Branch Gateway	556
static routing	241	documentation center	557
unnumbered IP	241 , 247 , 391	finding content	557
verifying connection	244	navigation	557
Dialer Messages	253	documentation portal	557
dialer modem-interface	250 , 257	domain-name	415
dialer order	244 , 257	lease	412
dialer persistent	244 , 257	DoS reporting	51
dialer persistent delay	244 , 250 , 257	dos-classification	53
dialer persistent initial delay	244 , 250 , 257	Downloading	
dialer persistent max-attempts	244 , 257	public key to branch gateway	44
dialer persistent re-enable	244 , 257	downloading announcement files	304
dialer string	244 , 250 , 257	ds-mode	223 , 226
Dialer strings	244	ds1	168
dialer wait-for-ipcp	244 , 257	dscp	
dir	87 , 94 , 97	packet sniffing	365
Directed broadcast forwarding	417	DSCP	
Directory Number	140	as access control list rule criteria	517
Disabling		as policy-based routing rule criteria	517
SSH public key authentication	42	as QoS list rule criteria	517
disabling EASG	57	in RTR probes	264
disabling EASG authentication		in VPN packets	446
disabling EASG	57	DSCP table	
disabling EASG authentication for a specified user		Policy	520
disabling EASG for user	58	DSCP table, see Policy	520
disabling EASG for specified user	58	dscp-table	520 , 525
disabling FIPS		dscp, access control list	523
administration	549	dscp, object tracking	264 , 275
Disabling FIPS Approved Mode	542	dscp, QoS list	519 , 525
Discard routes	397	duplex	182
disconnect ssh	41 , 45	Dynamic CAC	
displaying DHCP server information	414	and modem dial backup	241 , 247
Distribution access lists	423	CLI commands	262
distribution list	423	description	261
distribution-list	424	Dynamic CAC tasks	262
DLCI		Dynamic Host Configuration Protocol	
configuring for frame relay sub-interface	235	see DHCP	407
OSPF mapping	278	Dynamic IP	
Priority	235	configuring	461
Priority, see Priority DLCI	235	Dialer interface	247
DMZ	388	overview	460
DNS resolver		dynamic local peer IP	462
CLI commands	78	dynamic MTU discovery	402
configuration example	77	Dynamic routes	
features	74	redistributing	429
maintaining	78	Dynamic time slots allocation	
overview	74	CLI commands	310
typical application	75	overview	310
when not necessary	75	Dynamic trap manager	
DNS servers		CLI commands	294
requesting list of DNS servers during a PPP/IPCP		configuring	293
session	232	dynamic trap manager parameters	293
requesting list of DNS servers from a DHCP server	184	dynamic-cac	262
dns-server	412 , 415		
document changes	21		
documentation			

E

E1/T1 default settings	225
E1/T1 lines	
CLI commands	226
connecting to WAN media module	220
default settings	223
E1/T1 ports	223
EASG	
Enhanced Access Security Gateway	56
EASG authentication	39 , 62
EASG site certificate information	60
EASG Status enabled or disabled	61
EASG users list	58
Echo cancellation	
CLI commands	379
overview	379
ECMP	427
Emergency Transfer Relay	
see ETR	283
enable	
edge mode	69
Enabling	
SSH public key authentication	42
enabling EASG	56
enabling EASG authentication	
enabling EASG	56
enabling EASG authentication for a specified user	
enabling EASG for user	57
enabling EASG for specified user	57
enabling FIPS	
administration	544
Enabling FIPS Approved Mode	542
encapsulation	230 , 231 , 235 , 237
encapsulation pppoe	232 , 233
encrypted SRTCP	298
Encrypted SRTCP	298
Encrypting gateway secrets	48
encryption	440 , 499
end-ip-addr	410 , 415
Endpt Init	140
Enhanced Access Security Gateway	56
Enhanced Access Security Gateway (EASG)	
authentication	62
erase announcement-file	305 , 307 , 309
erase auth-file	574
error states 1	
FIPS	554
Ethernet ports	
CLI commands	179
configuring switch port	179
connecting devices to	178
list of	178
port redundancy	318
WAN Ethernet port	181
WAN Ethernet port, see WAN Ethernet port	181
Ethernet ports on the router	178

ETR

CLI commands	284
deactivating	284
description	283
LED	283
manual activation	283
setting state	283
trunk-to-port latching	283
ETR automatic activation	284
Excess Burst size	276
exit	64
Expansion Module	123

F

FAC data	141
fail-retries	264 , 275
failback	533
failover	533
Fair VoIP queue	213
fair-queue-limit	213
fair-voip-queue	213
Fast Ethernet interface	
configuring PPPoE	231
Fast Ethernet port	260
configuring interface	181
firewall connected	388
VPN connected	388
FastEthernet interface	
checking status	258
dynamic bandwidth reporting	261
ICMP keepalive	258
FastEthernet Interface	
described	388
fdl	226
File transfer	
SCP, FTP or TFTP	82
File transfer, see SCP, FTP or TFTP	82
finding content on documentation center	557
finding port matrix	557
FIPS	
next hops static routes	395
FIPS (Federal Information Processing Standards)	538
FIPS Approved Mode of Operation	539
FIPS Certified Firmware is Installed	539
FIPS error states	553
FIPS Security Level of the Cryptographic Module	538
Firewall	388
Firmware	
CLI commands	87
firmware bank defaults	83
firmware banks	28
load with ASB button	83
managing firmware banks	83
redundancy	83
upgrade overview	82
upgrading using SCP/FTP/TFTP/HTTPS	83

Firmware (<i>continued</i>)		
upgrading using USB mass storage device	84	
version control	28	
firmware versions in the banks displays	83	
Fixed analog trunk port	283	
fragment	277	
fragment chain	434	
fragment size	434	
fragment timeout	434	
fragment, access control list	516 , 523	
fragment, QoS list	525	
Fragmentation		
as map class parameter	276	
CLI commands	434	
description	433	
GRE tunneling	402	
Frame relay		
displaying configuration	238	
enabling traffic shaping	276	
Frame relay encapsulation		
CLI commands	237	
down status	240	
encapsulation types	235	
establishing Layer 3 interface	396	
IETF	235	
illustration	221	
non-IETF	235	
supported features	276	
supported on Serial interfaces	220 , 389	
Frame relay traffic shaping		
CLI commands	277	
configuring within map classes	276	
description	276	
displaying configuration	238	
enabling	276	
frame-relay class-dlci	237	
frame-relay counters	237	
frame-relay interface-dlci	235 , 237	
frame-relay lmi-n391dte	235 , 237	
frame-relay lmi-n392dte	235 , 237	
frame-relay lmi-n393dte	235 , 237	
frame-relay lmi-type	235 , 237	
frame-relay priority-dlci-group	235 , 237 , 278	
frame-relay traffic-shaping	235 , 237 , 276 , 277	
framing	223 , 226	
frequency	264 , 275	
FRF.12 fragmentation		
configuring within map classes	276	
description	276	
FTP	82	
G		
General context	29	
General context example	30	
Generating		
SSH Key Pair on Linux	43	
Generating (<i>continued</i>)		
SSH key pair on windows	43	
Generic Routing Encapsulation		
GRE tunneling	398	
Generic Routing Encapsulation, see GRE tunneling	398	
Gigabit Ethernet port		
port redundancy	318	
global parameters	451	
GRE	404	
GRE application example	404	
GRE tunnel	404	
GRE tunneling		
applications	398	
checking tunnel status	401 , 403	
CLI commands	405	
compared to VPN	398	
dynamic bandwidth reporting	261	
dynamic MTU discovery	402	
optional features	401	
overview	388 , 398	
preventing recursive routing	399	
routing packets to tunnel	399	
group	440 , 499	
GUI tools, configuring the system with	26	
H		
hash	440 , 499	
Header compression		
clearing rtp header compression statistics	211	
clearing tcp header compression statistics	211	
decompression	206	
IPCH method - RTP and TCP header compression,		
CLI commands	209	
IPCH method - RTP and TCP header compression,		
disabling	207	
IPCH method - RTP and TCP header compression,		
enabling	207	
IPCH method - RTP and TCP header compression,		
overview	207	
IPHC method - RTP and TCP header compression,		
configuring UDP ports range	207	
methods	207	
overview	206	
show ip rtp header-compression	211	
show ip tcp header-compression	211	
showing rtp header compression statistics	211	
showing tcp header compression statistics	211	
supported methods per interface type	207	
transmission rate	206	
Van Jacobson Method - TCP header compression,		
CLI commands	211	
Van Jacobson Method - TCP header compression,		
configuring	210	
Van Jacobson Method - TCP header compression,		
disabling	210	

Header compression (<i>continued</i>)		Integrated analog testing (<i>continued</i>)	
Van Jacobson Method - TCP header compression, enabling	210	healing trunks	384
Van Jacobson Method - TCP header compression, overview	207	overview	380
help	30	profiles, clearing	383
Help		profiles, configuring	382
CLI	30	profiles, displaying	383
commands	30	test cancelling	383
High Preference static routes	395	test launching	383
hostname	41 , 45	test lines	381
HTTPS	82	types of tests	381
hub-and-spoke with VPN	474	Inter-Gateway Alternate Routing	
I		IGAR	261
ICC configuration		Inter-Gateway Alternate Routing, see IGAR	261
server-blade-oob-vlan	316	Interactions for Encrypted SRTCP	299
show server-blade-vlan	316	interface	63 , 64 , 257
ICC Configuration		Interface	135 , 137
no servr-blade-oob-vlan	316	Interface configuration	
server-blade-vlan	315	CLI commands	390
ICC configuraion		interface console	218 , 250
show server-blade-oob-vlan	317	interface dialer	244 , 250 , 257
icc-vlan	313 , 317	interface fastethernet, DHCP and BOOTP relay	408
ICC-VLAN	313	interface fastethernet, DHCP client	186
configuring	313	interface fastethernet, PPPoE	232
Configuring	313	interface fastethernet, WAN Ethernet port	181 , 182
icc-vlan	313	interface Loopback	250
ICC-VLAN	313	interface serial	229
icmp	368 , 516 , 523 , 525	E1/T1 ports	226
ICMP errors	421	frame relay	237
CLI commands	421	frame relay traffic shaping	277
ICMP keepalive	258	interface Serial	223
and policy-based routing	529	interface serial, frame relay	235
CLI commands	260	interface serial, PPP	230 , 231
ICMP keepalive feature, enabling	259	interface serial, USP port	227
idle character	227	Interface status	
idle-character	229	CLI commands	378
IGAR	241 , 247 , 261	interface tunnel	403 , 405
ignore dcd	227 , 229	interface usb-modem	216 , 217
IKE		interface vlan	311 , 317
phase 1	435	Interfaces	
phase 2	435	adjusting bandwidth	426
incoming call handling data	145	assigning Cost	426
incoming-routing	167 , 168	assigning IP addresses	63
Ingress Access Control List	529	backup	182
Ingress QoS List	529	configuration	388
initiate mode	442 , 499	configuration examples	389
Insert		defining	63
Incoming Call Handling Treatment	146	disabling	394
installing EASG site certificate	59	displaying information	238
installing EASG site certificate using usb device	59	displaying status	378
Integrated analog testing		dynamic bandwidth reporting	261
CLI commands	384	fastethernet	388
displaying corrections	384	frame relay	235
displaying test results	384	GRE tunnel, GRE tunneling	388
		GRE tunnel, see GRE tunneling	388
		IP	389
		IP, see IP interfaces	389
		Layer 2	388 , 394

Interfaces (<i>continued</i>)		
Layer 3	396	
logical	389	
Loopback	388, 529	
physical	388	
Serial	220, 389	
Serial, see Serial interfaces	220	
setting load calculation intervals	63	
switching	388, 389	
testing configuration	238	
USP WAN	388	
virtual	220, 388	
WAN	388	
Internet Key Exchange (IKE)	435	
invalid SPI recovery	451	
invert txclock	227, 229	
ip access-group	510	
ip access-control-list	53, 451, 507, 523	
ip access-group	250, 462, 523	
ip address	229	
E1/T1 ports	226	
IP address		
assigning to USB port	26	
defining	389	
obtaining via DHCP	183	
obtaining via PPP/IPCP negotiation	232	
storing in ARP table	418	
ip address dhcp	75, 186	
ip address negotiated	232, 233, 244, 257, 461	
ip address, dialer interface	244, 257	
ip address, E1/T1 ports	223	
ip address, frame relay	235, 237	
ip address, interface configuration	63, 389	
ip address, PPP	230, 231	
ip address, PPPoE	232, 233	
ip address, USB port	217	
ip bootp-dhcp network	408	
ip bootp-dhcp relay	408	
ip bootp-dhcp server	408	
ip capture-list	363	
ip crypto list	448	
ip crypto-group	450, 463, 499	
ip crypto-list	499	
ip default-gateway	66, 257, 397	
ip default-gateway dialer	244	
ip dhcp activate pool	410, 415	
ip dhcp client client-id	186	
ip dhcp client hostname	186	
ip dhcp client lease	186	
ip dhcp client request	186, 485	
ip dhcp client route track	186	
ip dhcp ping packets	415	
ip dhcp ping timeout	415	
ip dhcp pool	410	
ip dhcp pools	415	
ip dhcp-server	410, 415	
ip directed-broadcast	417	
ip distribution access-default-action	423, 424	
ip distribution access-list	423, 424	
ip distribution access-list-cookie	424	
ip distribution access-list-copy	424	
ip distribution access-list-name	424	
ip distribution access-list-owner	424	
ip domain list	75, 78	
ip domain lookup	75, 78	
ip domain name-server-list	75, 78	
ip domain retry	75, 78	
ip domain timeout	75, 78	
ip icmp-errors	421	
IP interfaces	389	
ip max-arp-entries	420	
ip netbios-rebroadcast	417	
ip netmask-format	397	
ip ospf authentication	427	
ip ospf authentication-key	427	
ip ospf cost	426, 427	
ip ospf dead-interval	427	
ip ospf hello-interval	427	
ip ospf message-digest-key	427	
ip ospf network point-to-multipoint	222, 427	
ip ospf priority	427	
ip ospf router-id	427	
ip peer address	217	
ip policy-list-copy	450, 507, 523, 525	
ip proxy-arp	420	
ip qos-group	510, 525	
ip qos-list	507, 525	
ip redirects	397	
ip rip authentications key	424	
ip rip authentications mode	424	
ip rip default-route-mode	424	
ip rip poison-reverse	422, 424	
ip rip rip-version	424	
ip rip send-receive-mode	424	
ip rip split-horizon	422, 424	
ip route	395-397	
ip routing	387, 397	
ip rtp compression-connections	209	
ip rtp header-compression	209	
ip rtp max-period	209	
ip rtp max-time	209	
ip rtp non-tcp-mode	209	
ip rtp port-range	209	
ip rule	513	
IP Security		
VPN	435	
IP Security, see VPN	435	
ip show rule	513	
ip simulate	522, 523, 525	
ip ssh	41, 45	
IP stations data	129	
ip tcp compression-connections	209, 211	
ip tcp header-compression	211	
IP telephones	106	

ip telnet	47
ip telnet-client	47
ip telnet-services	47
ip unnumbered	244 , 250 , 392
IP unnumbered interface configuration	
CLI commands	393
ip vrrp	432
ip vrrp address	432
ip vrrp auth-key	432
ip vrrp override addr owner	432
ip vrrp preempt	432
ip vrrp primary	432
ip vrrp priority	432
ip vrrp timer	432
ip-fragments-in	512 , 523
ip-option-in	512 , 523
ip-protocol	
packet sniffing	365
ip-protocol, access control list	523
ip-protocol, MSS configuration	53
ip-protocol, policy list	513
ip-protocol, QoS list	525
ip-rule, access control list	523
ip-rule, crypto list	448
ip-rule, MSS configuration	53
ip-rule, packet sniffing	363 , 364
ip-rule, QoS list	525
ip-rule, VPN	499
IPSec VPN	435
IPSec VPN configuration display	454
IPSec VPN packets decryption	372
IPSec VPN, see VPN	435
ISAKMP	
peer-group configuration	445
policies	440
VPN peer configuration	442
isakmp policy	442
isakmp-policy	499
ITN-C7 Long Timers	138

K

keepalive	230–233 , 401 , 403 , 405 , 442 , 499
configuring on PPP WAN line	230
keepalive feature	401
keepalive ICMP	
ICMP keepalive	258
keepalive ICMP, see ICMP keepalive	258
keepalive-icmp	259 , 260
keepalive-icmp failure-retries	260
keepalive-icmp interval	260
keepalive-icmp source-address	260
keepalive-icmp success-retries	260
keepalive-icmp timeout	260
keepalive-track	182 , 232 , 233 , 442 , 499
configuring in VPN	442
configuring on PPPoE interface	232

Keepalive, GRE tunnel	401
key config-key password-encryption	94

L

LAN	388
launch	383 , 384
Layer 1 Stable	141
Layer 2 interfaces	394
Layer 2 logical interfaces	389
Layer 2 virtual interfaces	388
Layer 3 interfaces	396
lease	410 , 415
LEDs, ETR	283
legal notice	
lifetime	440 , 499
linecode	223 , 226
Link Layer Discovery Protocol	
LLDP	187
Link Layer Discovery Protocol, see LLDP	187
Link-state algorithm	426
list rule specification for access control	504
Listing files	97
LLDP	
802.1 TLVs (optional)	188
CLI commands	189
configuration	188
enabling	188
mandatory TLVs	188
optional TLVs	188
overview	187
setting additional TLVs	188
setting port status	188
supported ports	189
supported TLVs	188
verify advertisements	188
LMI parameters	235
Load balancing	
ECMP	427
VRRP	431
load sharing topologies	481
load-interval	63
local calls between IP and analog telephones	355
Local Management Interface	235
see LMI parameters	235
local-address	448 , 499
Log file	
see Logging	195
Log file generation	203
log file messages	196
Logging	
CLI commands	204
configuring and enabling the log file	195
configuring session log	198
configuring Syslog server	192
copying the Syslog file	195
default severity levels	200

Logging (<i>continued</i>)		
defining filters	200	
deleting log file	196	
deleting Syslog server	193	
Dialer interface	252	
disabling log file	196	
disabling session log	199	
disabling Syslog server	192	
displaying log file contents	196	
displaying Syslog server status	194	
enabling session log	198	
enabling Syslog server	192	
filtering by application	201	
introduction	191	
limiting Syslog access	192	
log file	191	
log file example	203	
log file filter contents	200	
log file message format	197	
modem dial backup	252	
object trackers	269	
object tracking	269	
overview	191	
RTR	269	
saving settings	191	
session log	191 , 199	
session log example	203	
session log message format	199	
setting filters	200	
sinks	191	
specifying Syslog output facility	192	
Syslog default settings	194	
Syslog server	191	
Syslog server example	202	
Syslog server message format	195	
VPN	455	
Logging session		
Logging	198	
Logging session, see Logging	198	
Logical interfaces	389	
login authentication	39	
login authentication inactivity-period	36 , 37	
login authentication lockout	36 , 37	
login authentication min-password-digit-chars	35 , 37	
login authentication min-password-length	35 , 37	
login authentication min-password-lower-chars	35 , 37	
login authentication min-password-special-chars	35 , 37	
login authentication min-password-upper-chars	35 , 37	
login authentication password-expire	36 , 37	
login authentication response-time	39	
loopback	226	
loopback activation on an E1/T1 line	226	
Loopback interface	241 , 388 , 529	
loopback remote	226	
Loops		
defined	322	
preventing in GRE tunneling	399	
Loops (<i>continued</i>)		
preventing in RIP	422	
Low preference static routes	395	
M		
MAC addresses, storing in ARP table	418	
Maintaining FIPS Approved Mode	542	
Managed Security Services		
MSS	51	
Managed Security Services, see MSS	51	
map classes	277	
configuring	277	
Map classes		
applying to all configured Permanent Virtual Channels	276	
default	276	
number that can be configured	276	
parameters	276	
map-class frame-relay	277	
Master Configuration Key		
CLI commands	50	
configuring	48	
Max		
AAR Digit Conversion Table	124 , 144	
ARS Digit Conversion Table	124 , 144	
MCG		
CLI commands	73	
MCK (Master Configuration Key)	48	
Media encryption	296	
media encryption using AES 256	297	
media gateway controller		
setting the list	68	
Media Gateway Controller (MGC)	26	
Media modules		
adding, using a USB mass-storage device	94	
MM340	222 , 223 , 388	
MM342	222 , 227 , 388	
upgrading, using a USB mass-storage device	94	
USP WAN, MM342 media module	227	
USP WAN, see MM342 media module	227	
WAN	222	
mesh VPN topology configuration	465	
Metrics	430	
MGC		
accessing	33	
accessing the registered MGC	72	
auto fallback to primary	67	
changing the list	71	
checking connectivity with	241	
clearing the list	71	
displaying the list	69	
monitoring the ICC	73	
monitoring the Survivable Remote Server	73	
reporting bandwidth to	261	
running Avaya Aura Communication Manager	33	
setting reset times	71	

MGC list	
SLS entry	103
MGC settings	69
Min	
AAR Digit Conversion Table	124 , 144
ARS Digit Conversion Table	124 , 144
MM340 media module	
configuring	223
E1/T1 WAN interface	388
MM342 media module	
configuring	227
USP WAN interface	388
mode	441 , 499
Modem	
configuring	216
configuring console port to detect	218
connecting to Console port	33
connecting to USB port	32
dial backup, Modem dial backup	241
dial backup, see Modem dial backup	241
serial	218
USB	216
Modem dial backup	
activating with object tracking	247
and dynamic CAC	241 , 247
as backup interface	241
authentication method	244
bandwidth available for	241
CHAP authentication	244
configuration example	248
configuring backup routing	244
entering dialer strings	244
feature interactions	247
logging	252
overview	241
policy lists and	241
prerequisites	244
RAS configuration	244
typical installations	243
using VPN	241
Weighted Fair Queuing and	241
Monitoring applications	
configuring	328
MSS	
CLI commands	55
configuring	51
example	54
Overview	51
predefined DoS classes	52
reporting mechanism	51
user-defined DoS classes	53
mtu	232 , 233
Multipoint topology support	222
mutual	537
mutual authentication	
authentication	537

N

Name	
DS1 Circuit Pack	134
ISDN BRI Trunk Circuit Pack	140
Station	123
name server	75
name-server	78
name, access control list	523
name, crypto list	448
name, DHCP option	412 , 415
name, DHCP server	410 , 415
name, DHCP vendor specific option	413 , 415
name, packet sniffing	363
name, policy list	508
name, QoS list	519 , 525
NAT Traversal	
configuring	452
overview	452
Nested tunneling	399
NetBIOS	417
network	427
Network monitoring	
applications	328
Next hops	395
next-hop	264 , 275
next-server	415
no oob-interface	81
no servr-blade-oob-vlan	316
non-compliant CLI commands	
FIPS	543
nrzi-encoding	227 , 229
nslookup	78
O	
object	267 , 275
object tracker	267
object tracking	
configuration workflow	267
Object tracking	
activating Dialer interface	247
applying to DHCP client	184
applying to static routes	394
backup for the FastEthernet interface	272
CLI commands	275
configuration	264
enabling logging	269
interface backup using policy-based routing	273
maintenance	268
object tracker configuration	267
overview	263
RTR configuration	264
verifying MGC connectivity	241
viewing log messages	269
VPN failover	271
oob-interface configuration	81

Open Shortest Path First protocol		Packet sniffing (<i>continued</i>)	
see OSPF	426	simulating packets	375
option	412 , 415	specifying and excluding ICMP type and code	368
OSPF		specifying bugger size	370
advertising static routes	394	specifying capture actions	363
CLI commands	427	specifying interfaces	363
compared to RIP	421 , 426	streams that always be captured	361
default metric	430	streams that can be captured	361
description	426	streams that can never be captured	362
DLCI mapping	278	uploading capture file	373
dynamic Cost	426	uploading capture files to remote servers or USB	
limitations	427	storage device	373
modem dial backup and	243	uploading capture files to the S8300	374
shortest-path-first algorithm	426	viewing the capture-list	369
using with RIP	429	viewing, captured packet hex dump	372
OSPF Autonomous System Boundary Router	427	with conditional capture requirements	362
overview		packets, simulating	
edge gateway	66	Policy	522
MGC	66	packets, simulating, see Policy	522
owner, access control list	523	passive-interfaces	427
owner, packet sniffing	363	password	37
owner, policy list	508	Password authentication process	40
owner, QoS list	525	Password Authentication Protocol	216
		password changes	36
P		Passwords	
Packet sniffing		creating by the admin	35
analyzing capture file	374	disabling	36
analyzing captured packets	372	displaying password information	36
applying a capture-list	369	managing	34
applying rules to an address range	366	managing contents	35
applying rules to packets with DSCP values	365	managing expiry	36
applying rules to packets with ip protocols	365	managing length	35
capture list examples	368	managing lockout	36
clearing the capture buffer	370	overview	34
CLI commands	376	PBR lists	
configuring	362	attaching to Loopback interface	529
creating capture-list	363	PC device for CLI access	31
defining rule criteria	364	Permanent routes	396
disabling	362	Permit / Deny	125
enabling	362	ping	239
enabling the service	371	Ping	238
excepting protocols from rules	365	pmi	64 , 65
identifying the interface	375	PMI	
information, viewing	372	CLI commands	65
overview	361	configuration	64
packets captured	361	entering the interface context	64
reducing the size of the capture file	370	explanation	64
rule criteria commands	364	resetting the interface	64
scp file upload limit	373	setting location information	64
service, starting	371	setting system contact information	64
service, stopping	372	setting the system name	64
setting buffers	370	showing the PMI	64
setting capture list context	363	PMI, active and configured	65
setting capture list parameters	363	pmi6	65
setting max frame size	370	Point to Multi-Point topology	222
settings	370	Point-to-Point frame relay	222
		Poison-reverse	422

policy		Policy (<i>continued</i>)	
access control lists	504	sequence of policy list application	509
network security with access control lists	505	simulated packet properties	523
simulated packet properties	522	source port range	515
simulating packets	522	specifying a destination ip address	514
Policy		specifying an ip protocol	513
attaching policy list to interface at IACL	510	specifying operations	517
attaching policy lists to an interface	509	TCP, establish bit	516
attaching QoS list to interface at ingress QoS list	510	testing policy lists	521
changing DSCP table entries	520	using ip wildcards	512
configuring composite operations	519	Policy-based routing	
copy list	507	object tracking and	273
create access control lost	507	overview	529
create QoS list	507	packets not considered router packets	529
creating policy lists	507	PBR lists, PBR lists	529
creating rules	513	PBR lists, see PBR lists	529
default actions	508	routing to GRE tunnel	399
defining global rules	512	Port	
defining list identification attributes	508	Station	121
defining policy lists	507	Port classification	
deleting a policy list	509	CLI commands	326
deleting a QoS list	509	Ports	326
destination port range	515	Port classification, see Ports	326
device wide policy lists	511	port matrix	557
displaying access control lists	512	Port mirroring	
displaying composite operation lists	512	CLI commands	321
displaying ip rules	513	description	321
displaying policy lists in DSCP table context	521	Port redundancy	
displaying policy lists in general context	521	CLI commands	320
displaying policy lists in QoS list context	521	configuration	319
displaying policy lists in QoS list rule context	521	description	318
DSCP as rule criteria	517	disabling	319
DSCP default value	520	displaying information	319
DSCP methods	520	enabling	319
DSCP table	520	LAN deployment	22, 23
edit access control list	507	secondary port activation	319
editing policy lists	507	setting redundancy-intervals	319
editing rules	513	switchback	319
example composite operation	519	port redundancy schemes	320
fragments	516	Ports	
ICMP code	516	alternate	322
ICMP type	516	analog line	283
managing policy lists	506	backup	322
mapping DSCP to a CoS	520	classification	326
modem dial backup and	241	configuring E1 port	223
overview	504	configuring T1 port	223
policy lists and loopback interfaces	511	Fast Ethernet, Fast Ethernet port	181
policy-based routing, Policy-based routing	506	Fast Ethernet, see Fast Ethernet port	181
policy-based routing, see Policy-based routing	506	FastEthernet	388
preconfigured composite operations	517	FastEthernet, see Fast Ethernet port	388
preconfigured for QoS lists	518	mirroring, see Port mirroring	321
QoS fields	505	opening traffic	322
QoS list	507	redundancy, Port redundancy	318
QoS list parts	505	redundancy, see Port redundancy	318
QoS lists	505	roles in RSTP	323
rule criteria	512	USP, see USP ports	227
sequence of device-wide policy list application	511	USP, USP ports	227

power-up		product-id	61
testing	553	profile	382, 384
PPP		protect crypto-map	448, 499
as default WAN protocol	222	Protocol Version	137
CLI commands	231	Proxy ARP	420
configuring on WAN line	230	CLI commands	420
connection	32, 33	PTMP, see Point to Multi-Point topology	222
establishing Layer 3 interface	396	Public Key Authentication process	41
supported on Serial interfaces	220, 389		
ppp authentication, USB port	216, 217	Q	
ppp chap hostname	232, 233, 244, 250	QoS	
ppp chap password	232, 233, 244	analyzing fault and clear trap output	349
ppp chap refuse	232, 233	CLI commands	212
ppp chap-secret	216, 217	configuration	212
PPP configuration	230	displaying parameters	212
ppp ipcp dns request	75, 78, 232, 233, 257, 485	fair packet scheduling	213
ppp pap refuse	232, 233	fault and clear traps	337
ppp pap sent username	233	metrics for RTP statistics application	332
ppp pap sent-username	244	policy, Policy	212
ppp pap-sent username	232	policy, see Policy	212
PPP protocol and USP ports	221	Priority DLCI, see Priority DLCI	278
ppp timeout authentication	216	Priority Queuing	214
ppp timeout authentication, USB port	217	queue sizes for VoIP traffic	212
ppp timeout ncp	230–233	resolving conflicts	212
ppp timeout retry	230–233	SNMP traps	336
PPP VoIP configuration	279	traps in messages file	346
PPP VoIP configuration example	280, 281	traps, viewing	345
PPP/PCP address negotiation	232	VoIP Queuing	214
PPPoE		Weighted Fair VoIP Queuing	213
authentication	232	QoS allowed values	506
CLI commands	233	QoS list	
description	231	CLI commands	525
shutting down client	232	queue-limit	214
pppoe-client persistent delay	232, 233	Queues	
pppoe-client persistent max-attempts	232, 233	fair packet scheduling	213
pppoe-client service-name	232, 233	Priority	214
pppoe-client wait-for-ipcp	232, 233	Priority Queuing	214
pre-classification	525	VoIP	214
pre-shared-key	442, 499	VoIP Queuing	214
preparing SLS data set	128	Weighted Fair VoIP Queuing	213
Prerequisites for entering FIPS Approved Mode	540		
Primary Management IP address (PMI)	26	R	
Priority DLCI		RADIUS authentication	34, 46
applying map classes	276	RAS	
CLI commands	279	dialer strings for modem dial backup	250
configuring	235, 278	modem dial backup and	241
description	278	modem dial backup configuration options	243
Priority queueing		modem dial backup prerequisites	244
CLI commands	214	serving multiple branch offices	243
Priority queuing		redistribute	424, 427, 429, 430
general	276	Registration Source Port	
Priority Queuing	214	H.248	73
Priority VoIP queuing	213	release dhcp	185, 186
priority-queue	213, 214	Remote Access Server	
Privilege levels		RAS	241
creating	35		
description	34		

Remote Access Server, see RAS	241	Router (<i>continued</i>)	
remote calls from analog to IP telephones	354	connecting to fixed router port	178
remote calls from IP telephone to IP telephone	356	determining shortest path	426
Remote services logins	62	disabling	387
remove nfas-interface	168	displaying interfaces	392
remove port	168	enabling	387
rename announcement-file	307 , 309	features	387
renew dhcp	185 , 186	fragmentation	433
Replacement String		fragmentation, see Fragmentation	433
AAR Digit Conversion Table	124	interfaces	388
ARS Digit Conversion Table	124	load balancing	431
reset	64	OSPF Autonomous System Boundary	427
reset and display controller counters	226	overview	387
reset and display frame-relay counters	237	redundancy	431
restore	91 , 94	RIP	421
restore usb	85 , 91 , 94	RIP, see RIP	421
restoring ETR to automatic activation	284	setting the borrowed ip interface	392
Restoring the Branch Gateway		unnumbered ip interfaces in table	392
using the Branch Gateway USB port	91	virtual	431
RIP		router ospf	250 , 257 , 427 , 430
advertising static routes	394	Router port, connecting to	178
CLI commands	424	router rip	424 , 430
compared to OSPF	426	router vrrp	432
default metric	430	Routes	
description	421	setting route preference	399
distribution access lists	423	Routing	
limitations	424	policy based, Policy	506
poison-reverse	422	policy based, see Policy	506
preventing loops	422	Routing Information Protocol	
RIPv1	422	see RIP	421
RIPv2	422	routing sources	393
split-horizon	422	Routing table	
using with OSPF	429	CLI commands	397
versions supported	421	deleting static routes	394
RIPv1 and RIPv2 differences	422	description	394
RMON		RSTP	
agent	328	designating ports as edge ports	323
CLI commands	329	displaying port point-to-point status	323
overview	328	displaying the port edge state	323
rmon alarm	329	fast network convergence	323
RMON configuration examples	328	features	322
rmon event	329	LAN deployment	23 , 24
rmon history	329	manually configure uplink and backbone ports	323
Route redistribution	421	role of ports	323
CLI commands	430	setting port-to-port admin status	323
configuration	429	RSVP	212
description	429	RTCP	206
metric translation	429	RTP	
metrics	430	configuring	206
Router		overview	330
backup	431	statistics application functionality	330
computing path	426	viewing configuration thresholds	332
configuration commands	45 , 47	RTP header compression	
configuring BOOTP	407	Header compression	206
configuring broadcast relay	417	RTP header compression, see Header compression	206
configuring DHCP	407	RTP session data	330
configuring unnumbered ip addresses	392	RTP statistics	

RTP statistics (<i>continued</i>)		
CLI commands	360	
RTP statistics application		
configuration and output examples	351	
configuring	331	
configuring additional trap destinations	336	
configuring fault and clear traps	337	
configuring QoS traps	336	
display session information	339	
displaying RTP session statistics	339	
displaying VoIP engine RTP statistics	338	
enabling	334	
enabling traps	336	
modifying the statistics window	336	
QoS metric thresholds	331	
QoS metrics	332	
resetting	334	
sample network	351	
setting QoS event thresholds	333	
setting QoS indicator thresholds	333	
setting the trap rate limiter	338	
statistics summary report output	338	
viewing configuration	334	
viewing QoS traps in messages file	346	
rtp-stat clear	334 , 360	
rtp-stat event-threshold	333 , 360	
rtp-stat fault	337 , 360	
rtp-stat min-stat-win	336 , 360	
rtp-stat qos-trap	336 , 360	
rtp-stat qos-trap-rate-limit	338 , 360	
rtp-stat service	360	
rtp-stat thresholds	333 , 360	
rtp-stat-service	334	
rtr	264 , 275	
RTR		
Object tracking	264	
rtr-schedule	264 , 275	
RTR, see Object tracking	264	
running-config startup-config	27 , 28	
S		
safe-removal usb	94	
SCP	46 , 82	
transferring announcement files using	303	
SCP/FTP/TFTP used for upgrades	84	
searching for content	557	
Secure Shell protocol		
SSH	40	
Security		
DoS attack detection	51	
overview	34	
special features	47	
VLANs	313	
Security Associations (SAs)	435	
Security Code	115	
self-identity	442 , 499	
Serial interfaces	389	
configuring encapsulation	223	
default encapsulation	223	
dynamic bandwidth reporting	261	
entering context	223 , 227	
serial modems	33	
server-blade-oob-vlan	316	
server-blade-vlan	315	
server-name	415	
Services port		
connecting console and PC devices	31	
session	72 , 73	
Session log		
Logging	198	
Session log, see Logging	198	
session mgc	374	
set associated-signaling	165 , 168	
set attendant	147 , 168	
set balance	384	
set bearer-capability (bri)	156 , 168	
set bearer-capability (ds1)	155 , 168	
set bit-rate	152 , 168	
set boot bank	83 , 87	
set busy-disconnect	168	
set cbc	168	
set cbc-parameter	168	
set cbc-service-feature	168	
set channel-numbering	168	
set channel-preferences	158 , 168	
set codeset-display	158 , 168	
set codeset-national	168	
set connect	152 , 168	
set contact-closure admin	301 , 302	
set contact-closure pulse-duration	301 , 302	
set cor	149 , 168	
set country-protocol (bri)	156 , 168	
set country-protocol (ds1)	152 , 154 , 168	
set crosstalk-destination	382 , 384	
set crosstalk-port	382 , 384	
set crosstalk-responder	382 , 384	
set date-format	147 , 168	
set delete-digits (dial-pattern)	166 , 168	
set delete-digits (incoming-routing)	167 , 168	
set deny	166 , 168	
set destination	382 , 384	
set dial	158 , 168	
set digit-handling	158 , 168	
set digit-treatment	158 , 168	
set digits	158 , 168	
set directory-number-a	156 , 168	
set directory-number-b	156 , 168	
set dscp	446 , 499	
set echo-cancellation analog	379	
set echo-cancellation config analog	379	
set echo-cancellation config voip	379	
set echo-cancellation voip	379	
set endpoint-init	156 , 168	

set etr	283	set numbering-format	158, 168
set etr 10 auto	284	set password	149, 168
set expansion-module	149, 168	set peer	445, 446, 499
set fac	168	set peer group	446
set fault-threshold timeslot	310	set peer-group	499
set icc-monitoring	73	set pfs	441, 499
set incoming-destination	158, 168	set pim-lockout	147, 168
set incoming-dialtone	158, 168	set port	149, 168, 382, 384
set insert-digits (dial-pattern)	166, 168	set port auto-negotiation-flowcontrol-advertisement	179
set insert-digits (incoming-routing)	167, 168	set port classification	326
set interface (bri)	156, 168	set port duplex	179
set interface (ds1)	152, 168	set port edge admin state	179, 323, 325
set interface-companding (bri)	156, 168	set port flowcontrol	179
set interface-companding (ds1)	152, 168	set port level	179
set ip-codec-set	147, 168	set port lldp	188, 189
set japan-disconnect	158, 168	set port lldp tlv	188, 189
set layer 1-stable	156, 168	set port mirror	321
set length	167, 168	set port name	179
set lldp re-init-delay	188, 189	set port negotiation	179
set lldp system-control	188, 189	set port point-to-point admin status	179, 323, 325
set lldp tx-delay	188, 189	set port redundancy	319, 320
set lldp tx-hold-multiplier	188, 189	set port redundancy enable disable	319, 320
set lldp tx-interval	188, 189	set port redundancy-intervals	319, 320
set logging file	200, 204	set port spantree	325
set logging file condition	200	set port spantree cost	325
set logging file disable	196	set port spantree force-protocol-migration	325
set logging file enable	195	set port spantree priority	325
set logging file retention	197	set port speed	179
set logging server	192, 204	set port static-vlan	317
set logging server access level	204	set port trap	291
set logging server access-level	192	set port vlan	317
set logging server condition	200, 204	set port vlan-binding-mode	317
set logging server disable	192	set primary-dchannel	165, 168
set logging server enable	192	set protocol-version	154, 168
set logging server facility	192, 204	set qos bearer	212
set logging session	204, 252	set qos control	212
set logging session condition	200	set qos rsvp	212
set logging session condition dhcp	186	set qos rtcp	212
set logging session disable	199	set qos signal	212
set logging session enable	186	set radius authentication	47
set logging session, dialer interface	257	set radius authentication retry-number	47
set logging session, DNS resolver	78	set radius authentication retry-time	47
set logging session, session log	198	set radius authentication secret	47
set logging session, VPN	455	set radius authentication server	47
set long-timer	152, 168	set radius authentication udp-port	47
set match-pattern	167, 168	set receive-gain	384
set max-ip-registrations	147, 168	set registration source-port-range	73
set max-length	166, 168	set reset-times	71, 73
set mediaserver	72, 73	set responder	382, 384
set mgc list	68, 73	set responder-type	382, 384
set min-length	166, 168	set security-association lifetime	499
set mss-notification rate	51	set security-association lifetime kilobytes	441
set name (bri)	156, 168	set security-association lifetime seconds	441
set name (ds1)	152, 168	set send-name	158, 168
set name (station)	149, 168	set send-number	158, 168
set name (trunk-group)	158, 168	set side (bri)	156, 168
set non-oob-interfaces	81	set side (ds1)	152, 168

set signaling-mode	152 , 168	show backup status	94
set slot-config	147 , 168	show boot bank	83 , 87
set sls	125 , 147 , 168	show bri	168
set snmp community	292	show cam vlan	317
set snmp retries	292	show capture-dummy-headers	375
set snmp timeout	292	show composite-operation, access control list	512 , 523
set snmp trap	291	show composite-operation, policy list	521
set spantree default-path-cost	325	show composite-operation, QoS list	525
set spantree enable/disable	325	show contact-closure	302
set spantree forward-delay	325	show controller	239
set spantree hello-time	325	show controllers	223
set spantree max-age	325	show controllers remote	226
set spantree priority	325	show correction	384
set spantree tx-hold-count	325	show crypto ipsec sa	452 , 499
set spantree version	325	show crypto ipsec transform-set	454 , 499
set spid-a	156 , 168	show crypto isakmp peer	454 , 499
set spid-b	156 , 168	show crypto isakmp peer-group	454 , 499
set supervision	158 , 168	show crypto isakmp policy	454 , 499
set swhook-flash	149 , 168	show crypto isakmp sa	454 , 499
set sync interface	531 , 534	show crypto ispsec sa	454
set sync source	531 , 532 , 534	show crypto map	454 , 499
set sync switching	532 , 534	show date-format	168
set system contact	64 , 65	show dial-pattern	168
set system location	64 , 65	show download announcement-file status	308 , 309
set system name	64 , 65	show download software status	84 , 87
set tac	158 , 168	show download status	96
set tei-assignment	156 , 168	show ds-mode	223
set tgnum	166 , 168	show ds1	168
set transform-set	446 , 499	show dscp-table	521 , 525
set transmit-gain	384	show dynamic-cac	262
set trunk	317	show echo-cancellation	379
set trunk-destination	149 , 168	show extension	168
set trunk-group-chan-select	165 , 168	show fac	168
set trunk-hunt	158 , 168	show fault-threshold timeslot	310
set type	382 , 384	show faults	80
set type (dial-pattern)	166 , 168	show fragment	434
set type (station)	149 , 168	show frame-relay fragment	239
set utilization cpu	80	show frame-relay lmi	239
set vlan	311 , 317	show frame-relay map	239
setting buffer-size	370	show frame-relay pvc	239
Setting synchronization		show frame-relay traffic	239
Synchronization	531	show icc-monitoring	73
Setting synchronization, see Synchronization	531	show icc-vlan	313 , 317
sharing content	557	show image version	80 , 87 , 91 , 94
show (bri)	156 , 168	show incoming-routing	168
show (dial-pattern)	166 , 168	show interface	217
show (ds1)	152 , 168	show interfaces	
show (incoming-routing)	167 , 168	frame relay	237
show (profile)	383 , 384	show interfaces, dialer interface	244 , 257
show (sig-group)	165 , 168	show interfaces, frame relay	235
show (station)	149 , 168	show interfaces, GRE tunnel	405
show (trunk-group)	158 , 168	show interfaces, interface status	378
show all logs	203	show interfaces, PPP	230 , 231
show announcement-file	309	show interfaces, unnumbered IP interface	392
show announcements-files	307 , 308	show interfaces, VLANs	317
show attendant	168	show interfaces, WAN configuration	239
show auth-file info	38 , 574	show ip access-control-list	521 , 523

show ip active-lists	454, 499	show mgc list	70, 73
show ip arp	420	show mm	79
show ip capture-list	369	show module	79, 80
show ip crypto-list	454	show oob-interface	81
show ip crypto-list list#	454	show pim-lockout	168
show ip crypto-lists	499	show pmi	64, 65
show ip dhcp-client	186	show point-to-point status	325
show ip dhcp-client statistics	186	show port auto-negotiation-flowcontrol-advertisement	179
show ip dhcp-pool	415	show port classification	326
show ip dhcp-server bindings	415	show port edge state	323, 325
show ip dhcp-server statistics	415	show port edge status	179
show ip distribution access-lists	424	show port flowcontrol	179
show ip domain	78	show port lldp config	189
show ip domain statistics	78	show port lldp vlan-name config	189
show ip icmp	421	show port mirror	321
show ip interfaces	239	show port point-to-point status	323
show ip ospf	427	show port redundancy	319, 320
show ip ospf database	427	show port trap	291
show ip ospf interface	427	show port vlan-binding-mode	317
show ip ospf neighbor	427	show ppp authentication	217
show ip ospf protocols	427	show profile	383, 384
show ip protocols	424	show protocol	47
show ip qos-list	521, 525	show protocols	78
show ip reverse-arp	420	show qos-rtcp	212
show ip route	397	show queue	213
show ip route best-match	397	show queueing	213, 214
show ip route static	397	show radius authentication	47
show ip route summary	397	show recovery	72, 73
show ip rtp header-compression	209	show restart-log	80
show ip rtp header-compression brief	209	show restore status	85, 91
show ip ssh	41, 45	show result	384
show ip tcp header-compression	209, 211	show result (profile)	384
show ip tcp header-compression brief	209, 211	show rmon alarm	329
show ip telnet	47	show rmon event	329
show ip track-table	397	show rmon history	329
show ip vrrp	432	show rmon statistics	329
show ip-codec-set	168	show rtp-stat config	360
show ip-qos-list	525	show rtp-stat detailed	360
show ip-rule, access control list	523	show rtp-stat sessions	360
show ip-rule, policy list	521	show rtp-stat summary	338, 360
show ip-rule, QoS list	525	show rtp-stat thresholds	332, 360
show keepalive-icmp	260	show rtp-stat traceroute	350, 360
show last-pim-update	168	show rtr configuration	268, 275
show list	508, 521, 523, 525	show rtr operational-state	268, 275
show lldp	188, 189	show server-blade-oob-vlan	317
show lldp config	189	show server-blade-vlan	316
show logging file condition	196, 204	show sig-group	168
show logging file content	196, 200, 204	show slot-config	168
show logging file retention	198	show sls	168
show logging server condition	194, 204	show snmp	51, 291, 292, 336
show logging session condition	199, 204	show snmp engineID	292
show login authentication	36-38	show snmp group	292
show map-class frame-relay	239	show snmp retries	292
show max-ip-registration	168	show snmp timeout	292
show mediaserver	73	show snmp user	292
show mg list_config	79, 80	show snmp usertogroup	292
show mgc	69, 73, 80	show snmp view	292

show spantree	325	SLS (<i>continued</i>)	
show station	168	introduction	98
show sync timing	533 , 534	IP Softphone administration in SLS mode	110
show system	67 , 80 , 89 , 94	logging	111
show tcp syn-cookies	50	manual CLI configuration, administering BRI parameters	156
show temp	80	manual CLI configuration, administering dial-pattern parameters	166
show timeout	80	manual CLI configuration, administering DS1 parameters	152
show track	268 , 275	manual CLI configuration, administering incoming- routing parameters	167
show traffic-shape	239	manual CLI configuration, administering signaling- group parameters	165
show trunk	317	manual CLI configuration, administering station parameters	149
show trunk-group	168	manual CLI configuration, administering trunk-group parameters	158
show upload announcement-file status	308 , 309	manual CLI configuration, command sub-contexts	146
show upload auth-file status	574	manual CLI configuration, commands hierarchy	168
show upload status	374	manual CLI configuration, instructions	147
show username	36–38	manual CLI configuration, introduction	126
show utilization	80	manual CLI configuration, preparing SLS data set	126
show vlan	312 , 317	manual CLI configuration, prerequisites	126
show voltages	80	preparing SLS data set	126 , 129 , 138 , 141 , 143–145
shutdown		preparing SLS data set, analog stations data	127
WAN port	182	preparing SLS data set, DS1 trunks data	133
shutdown, PPPoE	232 , 233	preparing SLS data set, ISDN-BRI trunks data	139
shutdown, USB port	217	provisioning data	102
Side		registered state process	104
DS1 Circuit Pack	136	states	103
sig-group	165 , 168	states, registered	104
signaling groups data	138	states, setup	104
Signaling Mode	134	states, teardown	104
sink severity levels defaults	201	states, unregistered	104
site certificates list	60	supported functionality	101
site-to-site IPsec VPN	496	SLS changes	126
SLA monitor		SLS codecs	143
overview	386	SLS feature interactions	110
sls	147 , 168	SLS station context class values	151
SLS	128	SNMP	
Avaya telephones supported in SLS	99	agent and manager communication methods	285
call processing not supported by SLS	102	changing user parameters	288
call processing supported by SLS	101	configuration examples	294
capabilities	98	configuring traps	290
capacities	127	creating OID lists	289
capacities by Branch Gateway model	127	creating user groups	289
CDR log	111	creating users	288
CLI command hierarchy	168	default security name, read	286
configuring	113	default security name, write	286
configuring Avaya Aura™ Communication Manager for SLS	113	DoS alerts	51
configuring Communication Manager for SLS	113	enabling traps and notifications	290
disabling	125	mapping user groups to views	288
enabling	125	MSS notifications	51
entry in MGC list	103	overview	285
features	99	potential agent residences	285
interaction with, call transfer	108	predefined user groups	288 , 289
interaction with, contact closure	109		
interaction with, Direct Inward Dialing	105		
interaction with, Hold feature	106		
interaction with, multiple call appearances	106		
interaction with, shared administrative identity with softphone	110		

SNMP (<i>continued</i>)	
QoS	336
required information for creating views	290
setting dynamic trap manager parameters	293
user groups	288
user-based security model (USM)	287
USM security levels	287
version 1	286
version 2	287
version 3	287
versions	286
views	289
SNMP access configuration	
CLI commands	292
SNMP trap configuration	
CLI commands	291
snmp trap link-status	291
snmp-server community	292
snmp-server dynamic-trap-manager	51 , 293 , 294 , 336
snmp-server enable notification	291
snmp-server enable notifications	290
snmp-server engineID	292
snmp-server group	51 , 292
snmp-server host	51 , 291 , 336
snmp-server informs	291
snmp-server remote-user	292
snmp-server user	51 , 288 , 292
snmp-server view	292
Software	
Firmware	28
Software, see Firmware	28
sort documents	557
source-address	264 , 275
source-ip	
packet sniffing	366
source-ip, access control list	523
source-ip, crypto list rule	448 , 499
source-ip, policy list	514
source-ip, QoS list	525
Spanning tree	
CLI commands	325
configuration	321
disabling	322
examples	324
protocol	322
speed	182
speed, USB port	217
SPI recovery	451
SPID	140
Split-horizon	422
SSH	
configuration	41
overview	40
Standard Local Survivability	
SLS	98
Standard Local Survivability, see SLS	98
start-ip-addr	410 , 415
static ARP table entries	419
Static routes	
advertising	394
applying object tracking	394 , 395
configuring next hops	395
deleting	394 , 396
description	394
discard route	397
dropping packets to	397
High Preference	395
inactive	394
IP addressed next hops	396
load-balancing	394
Low Preference	395
permanent	396
redistributing to RIP and OSPF	429
types	395
via interface	396
station	168
subnet-mask	410 , 412 , 415
success-retries	264 , 275
suggest-key	442 , 499
support	560
Surv_MIB files	577
Survivability	
auto fallback to primary MGC	67
configuring the MGC list	68
connection preserving migration	67
ELS	67
enhanced local survivability, ELS	67
enhanced local survivability, see ELS	67
MGC list	67
modem dial-backup	67
options	67
overview	67
setting reset times	71
SLS, see SLS	67
SLS, SLS	67
Survivable COR	122
Survivable GK Node Name	122
Survivable Trunk Dest	122
Switch	
connecting to fixed router port	178
displaying configuration	238
interface	388 , 389
Switch ports	
configuring	179
Switch redundancy	
LAN deployment	23 , 24
Switchback	319
Switchhook Flash	123
Switching	
configuring	311
interface	388 , 389
SYN attacks protection	
SYN cookies	49
SYN attacks protection, see SYN cookies	49

SYN cookies	50	track	267 , 275
attack notification	50	track list	267
configuring	50	track rtr	267
introduction	49	Traffic marking	276
overview	49	Traffic shaping	
strategies employed	49	activating on frame relay interface	235
SYN flood attack protection		displaying configuration	238
SYN cookies	49	DLCI	235
SYN flood attack protection, see SYN cookies	49	enabling on frame relay interface	276
Synchronization		per Virtual Channel	276
CLI commands	534	WAN Ethernet port	181
defining a stratum clock source	531	traffic-shape rate	181 , 182
disassociating specified primary or secondary clock source	532	training	559
displaying synchronization timing	533	Transform-sets	
LED status	533	overview	436
overview	531	VPN, defining	441
setting interface	531	transmitter-delay	227 , 229
setting the sync source	531 , 532	trap manager parameters	293
toggling sync source switching	532	traps	561
Syslog server		TRK port	
see Logging	192	see Fixed analog trunk port	283
system parameters data	143	Trunk Group	125
T			
tcp destination-port	367 , 515 , 523 , 525	trunk group data collection	130
tcp established	516 , 523	Trunk Group for Channel Selection	138
TCP header compression		trunk-group	168
Header compression	206	tunnel checksum	405
TCP header compression, see Header compression	206	tunnel destination	403 , 405
tcp source-port	367 , 515 , 523 , 525	tunnel dscp	405
tcp syn-cookies	50	tunnel key	405
TCP/IP connection	32 , 33	tunnel path-mtu-discovery	405
Telephones supported in SLS mode	99	tunnel source	403 , 405
telnet	47	tunnel ttl	405
Telnet		type	264 , 275
accessing gateway via	32 , 33	Type	
enabling and disabling access	47	Station	116
TFTP	82	U	
threshold count	267 , 275	UDP	
time constants, configuring	319	header compression	206
Time slots, mapping	223	udp destination-port	367 , 515 , 523 , 525
timeout absolute	217	udp source-port	367 , 515 , 523 , 525
timers basic	424	unencrypted communication	
timers spf	427	FIPS	544
TLS Certificate Stores	535	Unnumbered IP interface	
TLS certificates	535	configuring	392
TLVs		Dialer interface	241 , 247
802.1 (optional)	188	examples	392
mandatory	188	feature overview	391
optional	188	in routing table	392
supported	188	upgrade using SCP/FTP/TFTP	84
Tools		USB mass storage device	
for monitoring	328	overview	89
VMON	330	upgrading firmware	84
traceroute	397	USB mass-storage device	
		backing up the Branch Gateway	89
		CLI commands	94

USB mass-storage device (<i>continued</i>)		viewing valid EASG site certificate information	60
restoring the Branch Gateway	91	viewing valid EASG site certificates list	
upgrading media modules	94	viewing valid sites certificates list	60
USB port	89	Virtual Channels	
assigning IP address	26	applying map classes	276
CLI commands	217	assigning by QoS level	278
configuring for modem use	32	described	276
connecting modem	32	Virtual interface	388
default parameters	216	Virtual Private Network	
description	216	see VPN	388
enabling	216	VPN	435
resetting	216	Virtual Private Network, see VPN	435
setting authentication method	216	Virtual router	431
User accounts		Virtual Router Redundancy Protocol	
CLI commands	37	VRRP	431
managing	34	Virtual Router Redundancy Protocol, see VRRP	431
User authentication	34	Vlan 1	388
SSH	40	VLANs	
User names		binding modes	312
creating	35	clearing the VLAN table	312
user privilege changes	35	CLI commands	317
username	37	configuration examples	313
Usernames		description	389
managing	34	DHCP/BOOTP requests	407
overview	34	displaying the VLAN table	312
Using		dynamic bandwidth reporting	261
SSH client to Connect Public Key Authentication for		ICC-VLAN	313
Windows	45	ingress security	313
SSH to connect public key authentication for linux	45	multi VLAN binding	312
USP default settings	229	overview	311
USP port and PPP protocol	221	setting the VLAN	311
USP ports		setting vlan 2 example	313
CLI commands	229	switching interface	388, 389
configuring	227	table	312
illustration	222	tagging	311
USP WAN lines	220	VLMS	422
default settings	227	VMON, for troubleshooting QoS	330
USP WAN media module		VoIP	
MM342 media module	227	assigning to unique Virtual Channel	278
USP WAN media module, see MM342 media module	227	available transmission protocols	206
		enabling queuing	212
		fair packet scheduling	213
		overview	206
		PPP configuration example	279
		priority over Dialer interface	241
		queue delay	212
		queue size	212
		RSVP protocol	212
		VoIP queuing	214
		Weighted Fair VoIP Queuing	213
		VoIP Queuing	214
		voip-queue	213, 214
		voip-queue-delay	214
		VPN	388, 398
		activating	452
		assigning an access control list	451
		basic parameters	439
V			
validation	537		
value	412, 413, 415		
VAM	303		
vendor-specific-option	413, 415		
via interface static routes	396		
videos	559		
viewing available EASG users list			
EASG users list	58		
viewing EASG product certificate information			
EASG product certificate information	59		
viewing EASG status			
EASG status	61		
viewing product id			
product id	61		

VPN (<i>continued</i>)		
clearing VPN data	455	
CLI commands	499	
commands summary	437	
components and relationships	436	
components overview	436	
configuration, overview	439	
configuration, procedure	439	
continuous channel	463	
coordinating with the VPN peer	439	
crypto list, assigning to an interface	452	
crypto list, configuring	448	
crypto list, deactivating	450	
crypto list, overview	436	
crypto map, configuring	446	
crypto map, overview	436	
failover mechanisms	478	
introduction	435	
ISAKMP policies, configuring	440	
ISAKMP policies, overview	436	
logging	455	
maintenance	454	
modem dial backup and	241	
NAT Traversal	452	
object tracking for failover	271	
peer-group, configuring	445	
peer-group, overview	436	
peer, configuring	442	
peer, overview	436	
show status	454	
simple VPN topology	456	
site-to-site configuration	439	
transform-sets, configuring	441	
transform-sets, overview	436	
typical failover applications, failover using a peer-group	490	
typical failover applications, failover using DNS	485	
typical failover applications, failover using GRE	479	
typical failover applications, failover using object-tracking	490	
typical failover applications, overview	478	
typical installations, configuring dynamic IP	461	
typical installations, enabling continuous channel	463	
typical installations, full or partial mesh	464	
typical installations, full solution	473	
typical installations, hub and spokes installation	456	
VPN hub redundancy	481	
VPN hub-and-spoke	474	
VPN topology	457 , 465	
VRRP		
CLI commands	432	
configuration example	431	
description	431	
W		
wait-interval	264 , 275	
WAN		
checking interface status	258	
default encapsulation	230	
default protocol	222	
Dialer interface as backup	241	
dynamic bandwidth reporting	261	
features	220	
ICMP keepalive	258 , 529	
initial configuration	222	
interfaces	388	
overview	220	
PPP	222	
PPP configuration	230	
testing configuration	238	
testing configuration, CLI commands	239	
WAN endpoint device		
connecting to fixed router port	178	
WAN Ethernet port		
backup interfaces	182	
configuring	181	
traffic shaping	181	
WAN Ethernet port feature configuration	181	
WAN Ethernet ports		
CLI commands	182	
watchlist	557	
Weighted Fair VoIP Queuing	213 , 241	
WFVQ		
CLI commands	213	
Weighted Fair VoIP Queuing	213	
WFVQ, see Weighted Fair VoIP Queuing	213	
Z		
zeroization		
error state1	554	
status	554	